ANEXOS

Anexo 1 Políticas de Seguridad

DERECHOS DE AUTOR

CAPITULO 1 – Introducción

Las políticas de seguridad informática representan un tipo especial de reglas de negocios documentadas. Hace 25 años no existía tal necesidad de políticas, pero el cambio ha sido estimulado por la explosión de tecnologías de manejo de información, incluyendo a los teléfonos celulares, los buscapersonas y los computadores. Los que trabajan en el ambiente empresarial deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información generada en el complejo mundo de los negocios. Así como es inconcebible pensar que millones de conductores de automóviles puedan conducir sin leyes de tránsito, es también difícil pensar que millones de personas de negocios pudieran operar sistemas sin políticas de seguridad informática.

Existen muchas otras importantes razones para disponer de políticas de seguridad informática. Por ejemplo, las políticas son importantes documentos de referencia para auditorías internas y para la resolución de disputas legales acerca de la debida diligencia de la gerencia. Por otra parte, existen indicios de que los documentos de políticas pueden servir de demostración de la intención original de la gerencia y, por lo tanto, reducir su potencial responsabilidad legal, e inclusive pueden utilizarse como evidencia de las intenciones gerenciales de salvaguardar información intelectual. Este es un paso esencial pero desatendido en la protección de los secretos industriales. Igualmente, las políticas de seguridad informática pueden ser evidencia de los procesos de control de calidad, lo cual puede conferir a un socio la suficiente confianza como para suministrar material confidencial, así como asistir en un proceso de certificación de control de calidad ISO 9000.

CAPITULO 2 - **Consideraciones**

Políticas de Seguridad Informática Políticas Versus Lineamientos y Normas

Las políticas son instrucciones gerenciales que trazan una dirección predeterminada o describen la manera de manejar un problema o situación. Las políticas son planteamientos de alto nivel que transmiten a los trabajadores la orientación que necesitan para tomar decisiones presentes y futuras. Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro, y en algunos casos fuera, de la organización. Las políticas también pueden considerarse como reglas de negocio. Aunque los documentos de políticas de seguridad informática varían de una organización a otra,

un típico documento de este tipo incluye una exposición de motivos, la descripción de las personas a quienes van dirigidas las políticas, el historial de las modificaciones efectuadas, unas cuantas definiciones de términos especiales y las instrucciones gerenciales específicas sobre el tratamiento de las políticas. Las políticas son obligatorias y pueden considerarse el equivalente de una ley propia de la organización. Se requiere una autorización especial cuando un empleado desea irse por un camino que no está contemplado en la política. Debido a que el cumplimiento es obligatorio, las políticas utilizan palabras como "no se debe hacer" o "se tiene que hacer", ya que estas estructuras semánticas transmiten certeza e indispensabilidad. Por razones de simplicidad y uniformidad, se emplea el verbo "deber" en todo el manual, pero cualquier equivalente es aceptable.

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
3. POLITICAS DE SEGURIDAD				
3.01 Política de Seguridad Informática				
3.01.01 Documento de Políticas de Seguridad Informática				
1. Protección de la Información	La información debe ser protegida de acuerdo con su confidencialidad, valor y criticidad.	“Mecanismo Único de Acceso,’ “Normas de Implantación de Controles, “Comité de Gestión de Seguridad Informática,’ y “Dispersión de Sistemas Computacionales”	Personal técnico	Ambientes de Seguridad: Todos
2. Uso de la Información	La información de la Gobernación debe ser usada únicamente para los propósitos de negocios expresamente autorizados por la gerencia.	“Clasificación de Datos en Cuatro Categorías,’ “Uso Distinto al Empresarial de la Información de la Organización,’ y “Manejo de Información Sensible”	Todos	Ambientes de Seguridad: Todos
3. Manejo, Acceso y Uso de la Información	La información es un activo vital y todos los accesos, usos y manejos de la información de la Gobernación deben ser consistentes con sus políticas y normas.	“Uso Distinto al Empresarial de la Información de la Organización”	Todos	Ambientes de Seguridad: Todos
4. Excepciones de Responsabilidad por Daños a Datos y Programas	La Gobernación no se hace responsable por pérdidas o daños a datos o software, que provengan de su esfuerzo por proteger la confidencialidad, integridad y disponibilidad de la información manejada por los computadores y los sistemas de comunicación.	“Privilegios Especiales en Sistema” y “Sin Responsabilidad en Mensajes”	Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
5. Conflictos Legales	Las políticas de seguridad informática de la Gobernación han sido diseñadas de tal manera que cumplan o excedan las protecciones derivadas de las leyes y los reglamentos existentes y cualquier política de seguridad informática de la Gobernación que se suponga en conflicto con dichas leyes o regulaciones debe ser reportada inmediatamente a la gerencia de Seguridad Informática.	"Informes de Incidentes" y "Propiedad de Archivos y Mensajes"	Usuarios finales	Ambientes de Seguridad: Todos
6. Excepciones a las Políticas	Se dan excepciones a las políticas de seguridad informática en las raras ocasiones en que se ha producido una evaluación de riesgo de las implicaciones de no cumplir las políticas, preparándose entonces un formulario normalizado de aceptación de riesgo por parte del Propietario de los datos o la gerencia, siendo dicho formulario aprobado tanto por la gerencia de Seguridad Informática como por la de Auditoría Interna.	"Consecuencias de Incumplimiento,' "Renuncia a Derechos de Privacidad,' y "Cumplimiento Forzoso de los Controles de Seguridad"	Gerencia	Ambientes de Seguridad: Todos
7. Sin Obligación de Hacer Cumplir las Políticas	El hecho de que la gerencia no haga cumplir algún requerimiento de las políticas no significa que otorga su consentimiento.	"Revisión de los Controles de los Sistemas Informáticos — Interno" y "Mensaje de Inicio de Sesión en la Red"	Usuarios finales	Ambientes de Seguridad: Todos
8. Infracción de la Ley	La gerencia de la Gobernación debe considerar seriamente el enjuiciamiento de toda infracción conocida de las leyes.	"Informes de Incidentes"	Gerencia	Ambientes de Seguridad: Todos
9. Revocación de Privilegios de Acceso	La Gobernación se reserva el derecho de revocar los privilegios sobre tecnología informática al usuario en cualquier momento.	"Privilegios Predeterminados de Usuario" y "Reautorización de los Privilegios de Acceso de Usuario"	Usuarios finales	Ambientes de Seguridad: Todos
10. Normas de Seguridad Informática Específicas a Cada Industria	Los sistemas informáticos de la Gobernación deben regirse por normas de seguridad informática específicas a cada tipo de industria.	"Compra de Soluciones de Seguridad Informática,' "Normas de Implantación de Controles,' y "Controles Mínimos en Sistemas Informáticos"	Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
11. Uso de Políticas y Procedimientos de Seguridad Informática	Toda la documentación referente a la Seguridad Informática de la Gobernación, inclusive, sin limitación, de las políticas, normas y procedimientos, debe ser clasificada como "Sólo Para Uso Interno", a menos que haya sido expresamente creada para ser utilizada para procesos de negocios externos o por socios.	"Convenio de Trabajo" y "Clasificación de Datos en Cuatro Categorías"	Todos	Ambientes de Seguridad: Todos
3.01.02 Revisión y Evaluación				
1. Cumplimiento Forzoso de los Controles de Seguridad	Todos los sistemas de control de la seguridad informática deben ser susceptibles de cumplimiento forzoso antes de adoptarse como parte normal del proceso operativo.	"Revisión de los Controles de los Sistemas Informáticos — Interno" y "Convenios con Terceros"	Gerencia y personal técnico	Ambientes de Seguridad: Todos

Políticas de Seguridad Organizacional

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
4.01 Infraestructura de la Seguridad Informática				
4.01.01 Foro Gerencial Sobre Seguridad Informática				
1. Alteración No Detectada de la Información	Política: La gerencia debe establecer y mantener las medidas de seguridad, prevención y detección necesarias para garantizar que la información de la Gobernación está protegida del riesgo de alteraciones no detectadas.	Políticas Relacionadas: "Identificación de Requisitos de Seguridad"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Comité de Gestión de Seguridad Informática	Política: Un comité gerencial de seguridad informática, compuesto por la alta gerencia o sus delegados de cada división principal de la Gobernación, debe reunirse trimestralmente para revisar el nivel actual de seguridad informática, revisar los procesos de monitoreo de los incidentes de seguridad de la Empresa, aprobar y luego revisar los proyectos de seguridad informática, aprobar políticas nuevas o modificadas de seguridad informática y realizar otras actividades gerenciales de alto nivel necesarias para mantener la seguridad informática.	Políticas Relacionadas: "Seguridad Informática Centralizada" y "Revisión del Impacto Sobre la Privacidad"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
4.01.02 Coordinación de Seguridad Informática				
1. Riesgos Significativos para la Seguridad Informática	Política: Por cada riesgo importante para la seguridad de los sistemas informáticos, la gerencia debe tomar una decisión específica acerca del extremo al que está dispuesta a llegar la Gobernación para aplicar su propio seguro y aceptar el riesgo, buscar cobertura externa o ajustar los controles para reducir las pérdidas.	Políticas Relacionadas: "Normas de Implantación de Controles" y "Evaluación del Riesgo en los Sistemas de Producción"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Cobertura de Seguros	Política: Se debe obtener una cobertura de seguro adecuada y vigente para cada amenaza significativa a la confidencialidad, integridad y disponibilidad de la información manejada a través de los sistemas de computadores y de comunicaciones de la Gobernación.	Políticas Relacionadas: "Evaluación del Riesgo en los Sistemas de Producción,' "Directorio de Almacenamiento de Archivos,' y "Fianzas de Trabajadores"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
4.01.03 Asignación de Responsabilidades en Seguridad Informática				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Propiedad de la Información	Política: El jefe principal de la seguridad informática debe claramente especificar, por escrito, la asignación de las responsabilidades de la propiedad de la información para las bases de datos, los archivos maestros y otras recopilaciones de información compartidas y debe designar a las personas con derecho a acceder a dichas recopilaciones en nombre de los Propietarios.	Políticas Relacionadas: "Asignación de la Propiedad de la Información" y "Transferencia de Responsabilidad en Custodia"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
2. Cambios en Situación del Trabajador	Política: Toda modificación en la condición laboral de los trabajadores de la Gobernación, inclusive, sin limitantes, de los asesores, contratistas y temporales, debe ser reportada inmediatamente por la gerencia a Recursos Humanos, quienes a su vez deben notificar a los administradores de los sistemas informáticos correspondientes.	Políticas Relacionadas: "Informe de Cambios en Situación de Empleados" y "Reautorización de los Privilegios de Acceso de Usuario"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
3. Enfoque Gerencial de la Seguridad	Política: La gerencia debe garantizar que la seguridad informática dentro de cada departamento sea tratada como un problema empresarial normal a ser afrontado y resuelto, siendo la misma gerencia responsable de promover la seguridad como problema de todos.	Políticas Relacionadas: "Convenio de Trabajo" y "Planes de Recuperación Ante Desastre Computacional"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
4. Evaluaciones de Riesgos	Política: La evaluación de los riesgos en seguridad informática debe ser realizada por terceros no interesados.	Políticas Relacionadas: "Evaluaciones de Riesgo de los Sistemas" y "Evaluación de Nuevas Tecnologías"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
5. Productos y Servicios de Seguridad	Política: Toda función crítica de seguridad informática debe estar apoyada con lo mejor de lo mejor en productos y servicios comerciales disponibles en el mercado.	Políticas Relacionadas: "Madurez del Producto de Seguridad" y "Compra de Soluciones de Seguridad Informática"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Alto
6. Recursos para la Seguridad Informática	Política: La gerencia debe suministrar suficientes recursos y atención al personal para poder ocuparse adecuadamente de la seguridad de los sistemas informáticos.	Políticas Relacionadas: "Evaluación del Riesgo en los Sistemas de Producción" y "Controles Mínimos en Sistemas Informáticos"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
7. Partida Presupuestaria para la Seguridad Informática	Política: Los productos y servicios de seguridad informática deben cargarse a los presupuestos de gastos corporativos y no deben revertirse a cada filial.	Políticas Relacionadas: "Recursos para la Seguridad Informática" y "Facturas por Servicios Computacionales y Comunicacionales"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
8. Autorización para Cambios de los Sistemas Informáticos	Política: Los gerentes de departamento u otros integrantes del equipo gerencial no pueden firmar contratos, iniciar proyectos internos ni de otra manera comprometer a la Gobernación a efectuar modificaciones en sus sistemas de computación o de comunicación, a menos que tales modificaciones hayan sido autorizadas previamente tanto por el jefe principal de información como por la gerencia de Seguridad Informática.	Políticas Relacionadas: "Procura de Hardware y Software" y "Correo Electrónico del Departamento de Ventas"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
9. Seguridad Informática Centralizada	Política: La orientación, dirección y autoridad de las actividades de seguridad informática están centralizadas para toda la organización en la Gerencia de Seguridad Informática.	Políticas Relacionadas: "Comité de Gestión de Seguridad Informática,' "Convenciones en Desarrollo de Sistemas,' "Solicitudes de Información Organizacional,' "Cambios en la Línea de Comunicación, "Procura de Hardware y Software,' y "Punto Central de Falla de la Red"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
10. Responsabilidades del Departamento de Seguridad Informática	Política: El departamento de Seguridad informática es responsable de establecer y mantener las políticas, normas, lineamientos y procedimientos relativos a la seguridad informática de toda la organización.	Políticas Relacionadas: "Seguridad Informática Centralizada,' "Responsabilidad en la Seguridad Informática, "Misión del Departamento de Seguridad Informática,' y "Tareas del Departamento de Seguridad Informática"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
11. Tareas del Departamento de Seguridad Informática	Política: La gerencia de Seguridad Informática debe proporcionar dirección y pericia técnica para garantizar que la información de la Gobernación está protegida con procesos que mantienen la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas que la manejan.	Políticas Relacionadas: "Responsabilidades del Departamento de Seguridad Informática"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
12. Misión del Departamento de Seguridad Informática	Política: El departamento de Seguridad Informática es responsable de evitar perder o comprometer los recursos informáticos críticos, valiosos y sensibles de la Gobernación, a través de la coordinación y direccionamiento de acciones específicas que proporcionen un ambiente informático seguro y estable, consistente con las metas y objetivos de la Gobernación.	Políticas Relacionadas: "Responsabilidades del Departamento de Seguridad Informática"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
13. Normas y Procedimientos de Seguridad Informática	Política: El departamento de Seguridad Informática tiene la autoridad para crear y periódicamente modificar las normas técnicas y los procedimientos operativos que apoyan a estos datos documentales de la política de Seguridad Informática, los cuales, al ser aprobados por la gerencia correspondiente de la Gobernación, tendrán el mismo alcance y autoridad que tendrían si estuvieran incluidos en este documento.	Políticas Relacionadas: “Seguridad Informática Centralizada” y “Control de los Activos Informáticos”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
14. Planes de Seguridad Informática	Política: Conjuntamente con la gerencia correspondiente, el departamento de Seguridad Informática debe preparar planes anuales para el mejoramiento de la seguridad de todos los sistemas informáticos de la Gobernación.	Políticas Relacionadas: “Clasificación del Software y los Sistemas,’ “Planes de Recuperación Ante Desastre Computacional,’ “Planes de Respuesta Ante Emergencias Computacionales,’ “Planes Divisionales para el Cumplimiento de la Seguridad Informática,’ “Análisis de Violaciones y Problemas,’ y “Seguridad Informática Centralizada”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
15. Manual de Seguridad Informática	Política: El departamento de Seguridad Informática debe preparar, mantener y distribuir uno o más manuales de seguridad informática que describan con exactitud las políticas, las normas y los procedimientos de seguridad informática de la Gobernación.	Políticas Relacionadas: “Documentación de Adiestramiento y Operaciones,’ “Adiestramiento en Seguridad Informática,’ y “Tiempo de Adiestramiento”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
16. Enlaces de Seguridad Informática	Política: Cada gerente de departamento debe designar un enlace de seguridad informática y suministrarle suficiente adiestramiento, materiales de apoyo y otros recursos para realizar adecuadamente su trabajo.	Políticas Relacionadas: “Administrador de Seguridad Designado”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
17. Asignación de la Propiedad de la Información	Política: La gerencia ejecutiva debe asignar la responsabilidad de la propiedad a un único individuo interno que haga el mayor uso de la información.	Políticas Relacionadas: “Propiedad de la Información”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
18.Responsabilidad de la Propiedad en el Departamento de Sistemas Informáticos	Política: Con excepción de la información operacional relativa a los computadores y a la red, el departamento de Sistemas Informáticos no debe ser Propietario de ninguna información.	Políticas Relacionadas: “Propiedad de la Información”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
19. Propiedad Predeterminada de la Información	Política: Si la propiedad de un tipo específico de información residente en un computador multiusuario de producción no ha sido claramente asignada a un gerente específico, recaerá temporalmente en el gerente de Operaciones Computarizadas.	Políticas Relacionadas: " Responsabilidad de la Propiedad en el Departamento de Sistemas Informáticos" y "Custodio de la Información"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
20. Custodio de la Información	Política: Cada tipo importante de información debe tener un Custodio designado, quien ha de proteger apropiadamente la información de la Gobernación, en tanto cumpla las instrucciones emitidas por el Propietario designado en lo relativo al control de acceso, la confidencialidad y la criticidad de los datos.	Políticas Relacionadas: " Control de los Activos Informáticos,' "Partida Presupuestaria para la Seguridad Informática,' y "Inventario de Activos — Información"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
21. Responsabilidades del Custodio de la Información	Política: Los Custodios de la información son responsables de definir procedimientos de control específicos, administrar el control de acceso a la información, implementar y mantener medidas de bajo costo del control de acceso a la información, y suministrar capacidades de recuperación, en concordancia con las instrucciones de los Propietarios de la información.	Políticas Relacionadas: " Custodio de la Información"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
22. Responsabilidades del Usuario de la Información	Política: Todos los usuarios de la información de la Gobernación deben cumplir los requisitos de control especificados por el Propietario o Custodio de la información.	Políticas Relacionadas: "Propiedad de la Información" y "Resolución de Problemas de Seguridad Informática"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
23. Delegación de la Propiedad de la Información	Política: La responsabilidad de especificar controles de información apropiados por parte del Propietario de la información no debe ser delegada a proveedores de servicios fuera de la Gobernación.	Políticas Relacionadas: "Propiedad de la Información" y "Resolución de Problemas de Seguridad Informática"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
24. Políticas de Acceso a la Información	Política: Las políticas de acceso a la información deben ser desarrolladas de manera que especifiquen que los Propietarios de información designados, son responsables de establecer y poner al día políticas escritas pertinentes a las categorías de personas a quienes les será permitido acceder a la información por la cual serán responsables.	Políticas Relacionadas: "Propiedad de la Información" y "Otorgamiento de Privilegios del Sistema"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
4.01.04 Proceso de Autorización para el Procesamiento de la Información				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Control de Nuevas Tecnologías	Política: En cada instancia donde se utilice nueva tecnología en un sistema informático de producción en la Gobernación, las operaciones y controles de seguridad asociados a la nueva tecnología deben ser particularmente rigurosos hasta que se demuestre que la nueva tecnología es confiable, rápidamente controlable y que es un verdadero apoyo a las actividades del negocio.	Políticas Relacionadas: “Inhabilitación de Componentes Críticos de Seguridad” e “Identificación de Requisitos de Seguridad”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Inhabilitación de Componentes Críticos de Seguridad	Política: Los componentes críticos de la infraestructura de seguridad informática de la Gobernación, no deben ser inhabilitados, desviados, apagados o desconectados sin la previa autorización de la gerencia de Seguridad Informática.	Políticas Relacionadas: “Software Innecesario” e “Intentos de Introducir Contraseña”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4.01.05 Consejo Especializado en Seguridad Informática				
1. Evaluación del Riesgo en los Sistemas de Producción	Política: Todos los sistemas computarizados de producción deben ser evaluados periódicamente por la gerencia de Seguridad Informática para determinar el mínimo conjunto de controles requeridos para reducir y mantener el riesgo a un nivel aceptable.	Políticas Relacionadas: “Riesgos Significativos para la Seguridad Informática,’ “Tareas del Departamento de Seguridad Informática,’ “Planes de Seguridad Informática,’ y “Controles Mínimos en Sistemas Informáticos”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
4.01.06 Cooperación Entre Organizaciones				
1. Divulgación de Productos de Seguridad Informática	Política: No deben divulgarse en ningún momento el nombre de los productos, los proveedores involucrados y las configuraciones asociadas con los sistemas de seguridad informática instalados en la Gobernación, a menos que se obtenga el permiso previo de la gerencia de Seguridad Informática.	Políticas Relacionadas: “Notas de Prensa Sobre Información de Vulnerabilidad” y “Comunicaciones Públicas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
2. Divulgación Pública de Información Empresarial	Política: La Gobernación no debe divulgar públicamente ninguna información relacionada a acuerdos o transacciones empresariales de la que pueda razonablemente desprenderse un daño material para un cliente o un tercero.	Políticas Relacionadas: “Notas de Prensa Sobre Información de Vulnerabilidad” y “Representaciones en Internet Que Incluyan Afiliación”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
4.01.07 Revisión Independiente de la Seguridad Informática				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Uso de Investigadores	Política: La utilización de investigadores haciéndose pasar por otra persona para poner a prueba el servicio al cliente y las políticas de seguridad o investigar supuestas fechorías, debe ser autorizada por el gerente superior responsable de la seguridad física.	Políticas Relacionadas: “Información de Contacto del Remitente” y “Validación de la Identidad de Terceros”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
2. Revisión de los Controles de los Sistemas Informáticos — Independiente	Política: Periódicamente debe llevarse a cabo una revisión externa e independiente de los controles de los sistemas informáticos para determinar su calidad y cumplimiento.	Políticas Relacionadas: “Controles Mínimos en Sistemas Informáticos”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
4.02 Seguridad en el Acceso de Terceros				
4.02.01 Identificación de Riesgos Originados por Acceso de Terceros				
1. Identificadores de Usuario para Terceros	Política: No debe otorgarse identificador de usuario ni privilegios para utilizar los computadores o los sistemas de comunicación de la Gobernación a las personas que no sean empleados, a contratistas o consultores, a menos que se obtenga la autorización escrita del gerente del departamento.	Políticas Relacionadas: “Acceso a la Red,’ “Identificador Único de Usuario y Contraseña Obligatorios, “Formularios para Identificadores de Usuario,’ y “Reautorización de los Privilegios de Acceso de Usuario”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Privilegios de Trabajadores Temporales	Política: Los trabajadores temporales no deben recibir privilegios sobre los sistemas informáticos de la Gobernación, a menos que el Propietario de la información lo autorice por escrito.	Políticas Relacionadas: “Identificadores de Usuario para Terceros,’ “Revisión de Antecedentes de No Empleados,’ y “Acceso para Trabajadores Temporales y Consultores”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
3. Acceso Remoto de Terceros	Política: No debe concederse a proveedores externos la entrada a la red o a Internet vía telefónica, ni privilegios a las redes privadas virtuales, a menos que tengan una necesidad legítima de negocio para tal acceso y siempre que sean permitidos a personas específicas y sólo por el tiempo requerido para cumplir las tareas autorizadas.	Políticas Relacionadas: “Activación del Puente de Conferencias” y “Conexiones Discadas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Anotaciones de los Consultores	Política: Los consultores de la Gobernación no deben tomar notas acerca de las reuniones confidenciales con sus clientes.	Políticas Relacionadas: “Divulgación de la Información del Cliente” y “Enlaces con Información Privada”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
5. Acuerdo de Confidencialidad para el Personal de Reparación de Máquinas de Oficina	Política: Todo el personal externo de reparación de equipos de oficina debe firmar un acuerdo de confidencialidad con la Gobernación antes de comenzar su trabajo.	Políticas Relacionadas: "Acuerdos de Confidencialidad,' "Términos y Condiciones para el Acceso de Terceros,' y "Medios de Almacenamiento de Información Sensible"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
6. Diseminación de la Información	Política: El acceso de terceros a cualquier información interna de la Gobernación se concede sólo demostrando la necesidad de conocerla y cuando tal divulgación este expresamente autorizada por la gerencia de la Gobernación.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Mal Funcionamiento del Control de Acceso"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
7. Acuerdos de Confidencialidad — Terceros	Política: Antes de enviarse cualquier información secreta, confidencial o privada a un tercero para copiar, imprimir, formatear u otro tipo de manejo, dicho tercero debe firmar un acuerdo de confidencialidad con la Gobernación.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Acuerdos de Confidencialidad — Organización"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
8. Acuerdos de Confidencialidad	Política: Toda divulgación de información secreta, confidencial o privada de la Gobernación a terceros se hará a través de la firma de un acuerdo de confidencialidad que incluya restricciones a la subsiguiente diseminación y manejo de la información.	Políticas Relacionadas: "Diseminación Secundaria de la Información Secreta,' "Manejo de Información Sensible,' y "Convenio de Cumplimiento"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
9. Acceso para Trabajadores Temporales y Consultores	Política: Las actividades que requieren acceso a información sensible de la Gobernación deben ser realizadas únicamente por empleados permanentes a tiempo completo, a menos que no posean el conocimiento o las habilidades necesarias, o que una emergencia exija la presencia de trabajadores adicionales o se tenga la autorización del director de Recursos Humanos y la del Propietario de la información.	Políticas Relacionadas: "Acuerdos de Confidencialidad — Organización,' "Clasificación de Datos en Cuatro Categorías,' y "Restricción de Privilegios — Necesidad de Conocer"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
10. Guías Telefónicas Internas	Política: Las guías telefónicas internas no deben ser distribuidas a terceros distintos de contratistas, consultores, trabajadores temporales y otros terceros que trabajan para la Gobernación, sin la autorización específica de un gerente departamental.	Políticas Relacionadas: "Números de Acceso a Computadores"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
11. Acceso de Terceros a Sistemas Internos	Política: El coordinador de seguridad informática designado debe autorizar el acceso de terceros a los sistemas internos de la Gobernación distintos de aquéllos claramente públicos.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
12.Responsabilidades de Terceros en la Seguridad Informática	Política: Previo al contacto que los usuarios de un tercero hagan con los sistemas de la Gobernación a través de conexiones informáticas en tiempo real, se requiere autorización escrita dada por la gerencia de Seguridad Informática especificando las responsabilidades relacionadas a la seguridad de la Gobernación, las del proveedor de la conexión y las de todos los terceros involucrados.	Políticas Relacionadas: "Interconexión de Sistemas, "Cambios en la Línea de Comunicación,' y "Conexiones a Internet"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
13. Condición Financiera de Proveedores Importantes	Política: El jefe principal de informática, o su delegado, debe revisar anualmente las condiciones financieras de los proveedores que suministran o respaldan los sistemas informáticos de producción críticos para la Gobernación.	Políticas Relacionadas: "Instalación de Software de Sistemas Proporcionado por Proveedores" y "Enunciados de la Integridad del Software"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
4.02.02 Requisitos de Seguridad en Contratos con Terceros				
1. Términos y Condiciones para el Acceso de Terceros	Política: Antes de recibir acceso a los sistemas de la Gobernación, un gerente en representación de la organización del tercero debe firmar un contrato donde se definan los términos y condiciones del acceso, y éste debe ser autorizado por Seguridad Informática y por el vicepresidente del departamento Legal de la Gobernación.	Políticas Relacionadas: "Revocación de Privilegios de Acceso" y "Reautorización de los Privilegios de Acceso de Usuario"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Transferencia de Información a Terceros	Política: La documentación, el software o cualquier tipo de información interna de la Gobernación no deben ser vendidos o de manera alguna transferidos a algún grupo ajeno a la Gobernación para propósitos no autorizados por la gerencia.	Políticas Relacionadas: "Convenios de Intercambio de Software y Datos"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
3. Uso por Parte de Terceros del Nombre de la Organización	Política: Ninguna organización de terceros puede utilizar el nombre de la Gobernación en sus materiales de propaganda o mercadeo, a menos que reciba el permiso del consejero legal corporativo.	Políticas Relacionadas: "Propiedad Intelectual" y "Páginas Web No Oficiales"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
4. Manejo de la Información al Finalizar el Contrato	Política: Si la Gobernación finaliza su contrato con un tercero que maneja información privada de la Gobernación, dicho tercero debe destruir o devolver inmediatamente todos los datos privados de la Gobernación que estén en su posesión.	Políticas Relacionadas: "Compromiso en Acuerdos de Confidencialidad" y "Certificado de Destrucción de Medios de Almacenamiento"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
5. Prohibición de Invasión de Privacidad a Través de Terceros	Política: Si la Gobernación no puede realizar cierto acto o tomar determinado curso de acción en virtud de una política de privacidad que lo impide, la Gobernación no debe contratar a uno o más terceros para que realicen dicha acción.	Políticas Relacionadas: "Medidas de Seguridad en Organizaciones de Terceros" y "Transferencia de la Información sobre Clientes"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Compromiso en Acuerdos de Confidencialidad	Política: La información privada o confidencial bajo la custodia de la Gobernación no debe ser divulgada a terceros a menos que estos terceros firmen un acuerdo explícito de compromiso con la confidencialidad aprobado por la gerencia de Seguridad Informática.	Políticas Relacionadas: "Formularios para Identificadores de Usuario" y "Diseminación Secundaria de la Información Secreta"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
7. Divulgación de las Relaciones con Proveedores	Política: Al colocar pedidos de productos o servicios, o al establecer una relación de negocios nueva o modificada, el personal de la Gobernación debe informar a los proveedores que no deben hacer pública la naturaleza ni la existencia de su relación con la Gobernación, sin la autorización escrita de un gerente corporativo de la Gobernación.	Políticas Relacionadas: "Divulgación Pública de Información Empresarial" y "Representaciones en Internet Que Incluyan Afiliación"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
8. Recopilación de Información de Precios por Terceros	Política: Para evitar que los competidores obtengan información de propiedad interna, los terceros no deben reunir una cantidad significativa de precios de los productos o servicios de la Gobernación.	Políticas Relacionadas: "Restricciones a la Recopilación de la Información"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9. Manejo de Información Sensible	Política: Toda divulgación a terceros de información secreta, confidencial o privada perteneciente a la Gobernación, debe estar acompañada de una declaración explícita que describa exactamente cuál información está restringida y cómo puede o no ser utilizada.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Diseminación Secundaria de la Información Secreta"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
10. Recepción de Información de Terceros	Política: Si un agente, empleado, consultor o contratista debe recibir información secreta o confidencial de un tercero a nombre de la Gobernación, esta divulgación debe estar precedida por la firma del tercero de un documento donde libera dicha información, autorizado por el departamento legal de la Gobernación.	Políticas Relacionadas: "Entrega de Información Secreta"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
11. Sistemas de Terceros Conectados a la Red	Política: Para tener acceso a la red de computadores de la Gobernación, todo tercero debe asegurarse de que sus propios sistemas están conectados de manera consistente con los requisitos de la Gobernación, inclusive, sin limitantes, del derecho a auditar sin previo aviso las medidas de seguridad de aquellos sistemas conectados y el derecho a terminar de inmediato las conexiones de todos los sistemas de terceros.	Políticas Relacionadas: "Interconexión de Sistemas, "Conexiones a Redes de Terceros,' y "Conexiones en Red con Organizaciones Externas"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
12. Convenios con Terceros	Política: Todo convenio que se relacione con el manejo de información de la Gobernación por parte de terceros, debe incluir una cláusula que autorice a la Gobernación a auditar periódicamente los controles utilizados en las actividades en las cuales se maneja la información, y que especifique la manera en que se protege la información de la Gobernación.	Políticas Relacionadas: "Responsabilidades de Terceros en la Seguridad Informática,' "Aprobación de Contratos Externos,' y "Términos y Condiciones para el Acceso de Terceros"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
13. Medidas de Seguridad en Organizaciones de Terceros	Política: Antes de otorgarse un identificador de usuario a un tercero, éste debe presentar evidencia documentada de la existencia de un sistema o proceso de seguridad informática, la cual debe ser aprobada por la gerencia de Seguridad Informática de la Gobernación, y el tercero debe convenir por escrito en resguardar dicho sistema o proceso para evitar el uso no autorizado o inapropiado de los sistemas de la Gobernación.	Políticas Relacionadas: "Identificadores Personales de Usuario — Responsabilidad"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
14. Política de Seguridad del Tercero	Política: Antes de divulgarse cualquier información propia de la Gobernación a un tercero, éste debe firmar un acuerdo de confidencialidad con la Gobernación y someter una copia de su política de seguridad informática a la consideración de la gerencia de Seguridad Informática de la Gobernación.	Políticas Relacionadas: "Medidas de Seguridad en Organizaciones de Terceros"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
15. Información Recopilada Externamente	Política: Todo contrato con una organización externa, con un programador contratado o cualquier otra organización externa que maneje sistemas informáticos o los sistema de comunicación de la Gobernación, debe estipular que toda la información recopilada sobre la Gobernación será entregada al momento que ésta lo requiera, sin costo adicional.	Políticas Relacionadas: "Acceso del Cliente a Información Personal" y "Acceso a la Información Personal"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
16. Responsabilidades de Terceros en la Seguridad Informática	Política: Todo socio, distribuidor, cliente y asociado de la Gobernación debe estar consciente de sus responsabilidades en la seguridad informática a través de la inserción de lenguaje específico en los contratos que definan su relación con la empresa.	Políticas Relacionadas: "Convenios con Terceros, "Convenios de Software con Terceros,' "Cumplimiento de Seguridad Informática,' "Servicios de Protección de Mensajes en Red,' "Sistemas de Terceros Conectados a la Red,' y "Adiestramiento Multidisciplinario"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
17. Devolución de la Información por el	Política: Cuando un contrato termina o expira, todos los contratistas, consultores y temporales deben entregar a su gerente de proyecto todas las copias de la información perteneciente a la Gobernación recibida o creada durante la ejecución del contrato.	Políticas Relacionadas: “Derechos de Propiedad”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
18. Cumplimiento de Seguridad Informática	Política: Los consultores externos, los contratistas y los temporales externos deben estar supeditados a los mismos requisitos y tener las mismas responsabilidades en materia de seguridad informática que los empleados de la Gobernación.	Políticas Relacionadas: “Fianzas de Trabajadores” y “Responsabilidades de Terceros en la Seguridad Informática”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
4.03 Contratos Externos de Servicio				
4.03.01 Requerimientos de Seguridad en Contratos Externos de Servicio				
1. Reportes Independientes Sobre Controles	Política: Todo convenio hecho con organizaciones externas de sistemas informáticos debe estipular que la Gobernación recibirá anualmente un reporte que exprese una opinión independiente sobre la aceptabilidad de los controles en uso en la organización externa.	Políticas Relacionadas: “Situación Financiera de Contratista Externo” y “Aprobación de Contratos Externos”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
2. Software del Proveedor de Servicios de Aplicaciones.	Política: Todo proveedor de servicios de aplicaciones que maneje información de producción de la Gobernación debe licenciar el software a la Gobernación, depositar periódicamente en garantía la versión más reciente del código y suministrar documentación actualizada y detallada de los procedimientos.	Políticas Relacionadas: “Planes de Recuperación Ante Desastre Computacional”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
3. Proveedor Alternativo de Procesamiento	Política: En todos los casos donde una organización externa maneja información crítica sobre los sistemas informáticos de producción de la Gobernación, un proveedor alterno debe estar preparado para tomar el control de inmediato, en el caso que la organización externa no sea capaz o no desee cumplir con su contrato.	Políticas Relacionadas: “Planes de Respuesta Ante Emergencias Computacionales”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
4. Planes de Contingencia para Proveedores de Servicios	Política: Todos los contratos con organizaciones para hospedaje de páginas Web, proveedores de servicios de aplicaciones, proveedores de seguridad para sistemas y otras organizaciones externas de sistemas informáticos deben incluir tanto un plan documentado de respaldo como un cronograma de pruebas periódicas de terceros.	Políticas Relacionadas: “Compromiso en Acuerdos de Confidencialidad” y “Convenios con Terceros”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
5. Planes para el Retorno de Sistemas de Producción Manejados por Terceros	Política: Se debe preparar un plan de retorno eficaz, autorizado por la gerencia de Seguridad Informática y probarlo regularmente, que permita a la Gobernación realizar sus procesos internamente, antes que cualquier procesamiento de sistemas informáticos de producción se transfiera a una organización externa.	Políticas Relacionadas: “Planes de Contingencia en Conversión de Software” y “Reversión a Procedimientos Manuales”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
6. Cortafuegos y Servidores Compartidos Externamente	Política: La Gobernación no permite que su información interna esté contenida o sea procesada por un cortafuego, servidor u otro computador compartido con otra organización externa.	Políticas Relacionadas: “Consumo Excesivo de Recursos” y “Servidores para Aplicaciones Críticas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
7. Acceso a la Información Manejada por Contratista Externo	Política: IEn cada caso donde la Gobernación utilice una organización externa para procesar o manejar su información de producción, el contrato con dicha organización debe estipular claramente la entrega diaria a la Gobernación de una copia legible por computador de su información, o que la Gobernación tiene el derecho a obtener una copia legible por computador de su información, en cualquier momento y sin limitaciones.	Políticas Relacionadas: “Planes de Contingencia para Proveedores de Servicios”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
8. Decisiones Sobre Control de Acceso	Política: Las decisiones referentes a quiénes tendrán acceso a la información y los sistemas informáticos de la Gobernación deben ser tomadas únicamente por la gerencia de la Gobernación.	Políticas Relacionadas: “Propiedad de la Información” y “Delegación de la Propiedad de la Información”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
9. Aprobación de Contratos Externos	Política: Todos los contratos que estén relacionados con los sistemas informáticos deben ser revisados y autorizados por la gerencia de Seguridad Informática, que es responsable de garantizar que dichos contratos definan adecuadamente las responsabilidades de seguridad informática, cómo responder a una eventual variedad de problemas de seguridad y el derecho a terminar el contrato si se puede demostrar que la organización externa no cumple con los términos de seguridad informática establecidos en el contrato.	Políticas Relacionadas: “Delegación de la Propiedad de la Información,’ “Convenios con Terceros,’ y “Resolución de Problemas de Seguridad Informática”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
10. Situación Financiera de Contratista Externo	Política: Todas las organizaciones externas de sistemas informáticos que sean contratadas para encargarse de la información de producción de la Gobernación deben presentar declaraciones financieras trimestrales.	Políticas Relacionadas: “Condición Financiera de Proveedores Importantes” y “Planes de Recuperación Ante Desastre Computacional”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
11. Procesos de Producción Manejados por Compañías Extranjeras	Política: La gerencia de la Gobernación no debe entregar ningún aspecto del manejo de los sistemas informáticos de producción, inclusive sin limitantes, del diseño de sistemas, desarrollo, pruebas, operación y mantenimiento, a una organización externa que tenga su sede en un país extranjero o que pertenezca a una empresa extranjera.	Políticas Relacionadas: "Garantía Especial de Software" y "Compromiso en Acuerdos de Confidencialidad"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Políticas de Control de Activos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
5. CLASIFICACIÓN Y CONTROL DE ACTIVOS				
5.01 Responsabilidad por Activos				
5.01.01 Inventario de Activos				
1. Clasificación del Software y los Sistemas	Política: Seguridad Informática debe preparar anualmente una lista del software y de los sistemas desarrollados internamente, que puedan dar ventaja competitiva a la Gobernación.	Políticas Relacionadas: "Planes de Seguridad Informática"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Inventario de Activos — Tecnología	Política: La gerencia de Seguridad Informática debe preparar un inventario anual de los sistemas informáticos de producción detallando todo el hardware existente en producción, el software y los enlaces de comunicación.	Políticas Relacionadas: "Control de Inventario" y "Puestos Técnicos Esenciales"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
3. Control de Inventario	Política: Los Custodios de los equipos de la Gobernación deben mantener un control continuo de inventario, un registro del nuevo Custodio y la nueva ubicación de todo el equipo suministrado a otros, además de la seguridad física del equipo.	Políticas Relacionadas: "Responsabilidades del Custodio de la Información,' "Inventario de Activos — Información,' e "Inventario de Activos — Tecnología"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Diccionario de Datos	Política: Todo tipo de información nueva de la Gobernación, creada y utilizada en las operaciones de negocios del día a día, debe estar reflejada en el diccionario corporativo de datos.	Políticas Relacionadas: "Autorización de Recopilación de Información Privada" y "Sistemas Secretos"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
5. Procura de Hardware y Software	Política: Todo el hardware y software debe obtenerse a través del departamento de Compras de acuerdo con las normas de compatibilidad IT de la empresa.	Políticas Relacionadas: "Compra de Soluciones de Seguridad Informática,' "Seguridad Informática Centralizada,' "Sistemas de Computación Pertenecientes a Trabajadores,' y "Liberación de Componentes Usados"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
6. Propiedad de la Información	Política: Cuando una unidad organizacional en particular posea o utilice la información de producción, debe tener designada un Propietario responsable de determinar las clasificaciones correspondientes a la confidencialidad y la criticidad, tomar decisiones sobre quién tiene acceso a la información y garantizar que se utilizan los controles adecuados en el almacenamiento, manejo, distribución y uso regular de la información.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones, "Delegación de la Propiedad de la Información,' e "Inventario de Activos — Información"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
7. Control de los Activos Informáticos	Política: La Gerencia debe asignar específicamente las responsabilidades por las medidas de control que protejan todo activo informático importante.	Políticas Relacionadas: "Inventario de Activos — Información,' "Inventario de Activos — Tecnología, "Índices de Base de Datos Que Contienen Información Privada,' "Naturaleza y Ubicación de la Información de la Organización,' y "Custodio de la Información"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
8. Administrador de Seguridad Designado	Política: Todo sistema computarizado multiusuario de la Gobernación debe contar con un administrador de seguridad designado para definir los privilegios de los usuarios, monitorear los registros del control de acceso y realizar actividades similares.	Políticas Relacionadas: "Actualización de Información de Producción" y "Enlaces de Seguridad Informática"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
9. Administradores de Seguridad Suplentes	Política: Todo sistema multiusuario de la Gobernación con un sistema de control de acceso debe tener designado un empleado adiestrado como administrador de seguridad suplente, que lo pueda sustituir en caso de que el administrador principal no esté disponible.	Políticas Relacionadas: "Administrador de Seguridad Designado"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10. Inventario de Activos — Información	Política: La gerencia de Sistemas Informáticos debe recopilar y actualizar anualmente un diccionario corporativo de datos y otras descripciones de alto nivel de los activos informáticos más importantes de la Gobernación.	Políticas Relacionadas: "Control de los Activos Informáticos,' "Custodio de la Información, "Información Personal para el Funcionamiento del Negocio,' "Sistemas Secretos,' "Índices de Base de Datos Que Contienen Información Privada,' y "Naturaleza y Ubicación de la Información de la Organización"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
11. Seguimiento de Equipos	Política: Todos los computadores y equipos de comunicación de la Gobernación deben llevar un identificador único legible por el computador de manera que los inventarios físicos puedan hacerse de manera eficiente.	Políticas Relacionadas: "Procedimiento de Control de Cambios" y "Revisión de los Convenios de Licencia del Software"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
12. Códigos de Identificación de los Equipos	Política: Todos los computadores y equipos de comunicación de la Gobernación deben tener un número de identificación indeleble, grabado en el equipo para ayudar a la policía en sus intentos por devolver la propiedad robada.	Políticas Relacionadas: "Seguimiento de Equipos"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5.02 Clasificación de la Información				
5.02.01 Lineamientos para la Clasificación				
1. Propiedad de Archivos y Mensajes	Política: La Gobernación tiene la propiedad legal del contenido de todos los archivos y mensajes almacenados o transmitidos en sus computadores y sistemas de redes, y se reserva el derecho de acceder a esta información sin aviso previo cuando exista una necesidad genuina de negocios.	Políticas Relacionadas: "Uso Personal de los Sistemas de Computación y de Comunicaciones" y "Herramientas de Monitoreo de Sistemas"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Clasificación de Datos en Cuatro Categorías	Política: Todos los datos de la Gobernación deben ser divididos en las siguientes cuatro clasificaciones: SECRETA, CONFIDENCIAL, PRIVADA y NO CLASIFICADA. Deben establecerse procedimientos distintos para manejar, etiquetar y revisar cada clasificación	Políticas Relacionadas: "Fecha de Desclasificación, '"Revisión Anual de la Desclasificación,' "Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,' y "Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
3. Clasificación de Datos en Tres Categorías	Política: Toda la información de la Gobernación y toda la información confiada a ella por terceros corresponden a una de tres clasificaciones de sensibilidad.	Políticas Relacionadas: "Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones, '"Clasificación de Datos en Cuatro Categorías,' y "Propiedad de la Información"	Política Dirigida a:Todos	Ambientes de Seguridad: Bajos y medianos
4. Clasificación Cerrada de Datos en Dos Categorías	Política: Toda información de la Gobernación que no esté marcada específicamente como "autorizada para el conocimiento público" o que no es regular o repetidamente compartida con grupos externos, es confidencial y no debe ser compartida con grupos externos a menos que se obtenga la autorización del Propietario de la Información.	Políticas Relacionadas: "Clasificación Abierta de Datos en Dos Categorías,' "Mal Funcionamiento del Control de Acceso,' "Permisos Predeterminados de Archivo,' y "Restricción de Privilegios — Necesidad de Retener"	Política Dirigida a:Todos	Ambientes de Seguridad: Bajos y medianos
5. Clasificación Abierta de Datos en Dos Categorías	Política: Toda información de la Gobernación que no haya sido marcada específicamente como "confidencial" está autorizada para hacerse del conocimiento público y puede compartirse con grupos externos sin el permiso específico de la gerencia con la excepción de la información que está restringida por las leyes y los reglamentos.	Políticas Relacionadas: "Etiquetas Incorrectas de Clasificación de Datos,' "Uso de Derechos en Sistemas Informáticos,' y "Restricción de Privilegios — Necesidad de Conocer"	Política Dirigida a:Todos	Ambientes de Seguridad: Bajos
6. Prefijos de Categorías de Clasificación de Datos	Política: Deben utilizarse prefijos, tales como "médico" o "financiero", delante de las categorías autorizadas de clasificación de datos.	Políticas Relacionadas: "Etiquetado de Clasificación de Datos" y "Clasificaciones de Medios de Almacenamiento de Datos"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
7. Declaración de Secreto Industrial	Política: El consejero legal principal de la Gobernación es la única persona autorizada para designar cualquier información de la Gobernación como secreto industrial.	Políticas Relacionadas: "Divulgación de Secretos Industriales" y "Lógica Crítica de Negocios"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
8. Etiquetas Incorrectas de Clasificación de Datos	Política: Si el receptor de la información interna de la Gobernación piensa que es incorrecta la etiqueta de clasificación que tiene la información, debe proteger la información de la manera que corresponda con la más rigurosa de las dos formas posibles de etiquetas de clasificación y confirmar con el Propietario de la Información que la etiqueta ahora colocada a la información es la correcta.	Políticas Relacionadas: “Etiqueta de Sensibilidad Desconocida” y “Etiquetado de Clasificación Múltiple”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
9. Asignación de Etiquetas de Clasificación de Datos	Política: Para todos los tipos de información de producción existentes, el Propietario de la información es responsable de escoger una etiqueta de clasificación de datos apropiada a usar por los trabajadores que reproducen, compilan, alteran o procuran información de producción.	Políticas Relacionadas: “Restricciones a la Recopilación de la Información” y “Etiquetado Durante el Ciclo de Vida de la Información”	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
10. Etiquetado de Clasificación Múltiple	Política: Cuando información de distintas clasificaciones de sensibilidad se combinan, la información que resulta debe ser clasificada en el nivel más restringido de cualquiera de las fuentes.	Políticas Relacionadas: “Restricciones a la Recopilación de la Información” y “Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
11. Exposición de Medios a Datos Secretos	Política: Cualquier medio de almacenamiento que pueda ser modificado, como los discos flexibles, las cintas magnéticas o los CD-RW y que haya sido expuesto a datos o aplicaciones confidenciales, debe ser clasificado a ese nivel.	Políticas Relacionadas: “Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad” y “Etiquetado de Clasificación Múltiple”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos
12. Etiquetas de Clasificación Generadas por Usuarios	Política: Las etiquetas de clasificación asignadas por otra persona distinta al Propietario de la información designado, no restringe en forma alguna el derecho de la Gobernación a utilizar o acceder a esta información.	Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones” y “Propiedad de la Información”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
13. Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad	Política: Si un sistema de computación contiene información con diferentes clasificaciones de sensibilidad, los controles usados deben reflejar la información más sensible residente en el sistema.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Exposición de Medios a Datos Secretos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
14. Clasificaciones de Medios de Almacenamiento de Datos	Política: Si la información registrada en un medio de almacenamiento del computador con una clasificación de sensibilidad alta se pasa a otro medio con una clasificación de sensibilidad baja, entonces el medio con la clasificación de sensibilidad baja debe ser actualizado para que su clasificación refleje la clasificación de sensibilidad más alta.	Políticas Relacionadas: "Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad" y "Almacenamiento de Información de Clasificación Mixta"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
15. Fecha de Desclasificación	Política: Si se conoce, la fecha en que la información secreta, confidencial o privada dejará de ser sensible debe indicarse como parte de la información de la clasificación.	Políticas Relacionadas: "Retención de la Información Sensible" y "Clasificación de Datos en Cuatro Categorías"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
16. Desclasificación Acelerada de la Información	Política: El Propietario de la información puede desclasificar o degradar en cualquier momento la clasificación de sensibilidad que se aplica a la información, mediante el cambio de la etiqueta de clasificación que aparece en el documento original, notificando a todos los receptores conocidos y al Custodio de los archivos de la Gobernación.	Políticas Relacionadas: "Prórroga para la Desclasificación" y "Acceso de Escritura a Información Sensible"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
17. Prórroga para la Desclasificación	Política: El Propietario de la información designado puede en cualquier momento antes de fijar la desclasificación, prorrogar el período en el cual la información debe permanecer en determinado nivel de clasificación, cambiando la fecha de desclasificación o degradación que aparece en el documento original, notificando a todos los receptores, iniciando una búsqueda eficaz a nivel de costo de receptores adicionales y notificando al Custodio de los archivos de la Gobernación.	Políticas Relacionadas: "Desclasificación Acelerada de la Información" y "Acceso de Escritura a Información Sensible"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
18. Cronograma de Desclasificación	Política: La clasificación de sensibilidad de todos los documentos de la Gobernación debe ser rutinariamente degradada de acuerdo con la Tabla 3-3 excepto cuando un tipo de documento haya sido eximido o cuando el Propietario de la información haya suministrado instrucciones distintas para la desclasificación o degradación.	Políticas Relacionadas: "Fecha de Desclasificación" e "Información Liberada al Público — Autorización"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
19. Revisión Anual de la Desclasificación	Política: Al menos una vez al año los Propietarios deben revisar la clasificación de sensibilidad asignada a la información por la cual son responsables.	Políticas Relacionadas: "Fecha de Desclasificación" y "Clasificación de Datos en Cuatro Categorías"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
20. Desclasificación de la Información Sensible	Política: Desde el punto de vista de la sensibilidad, la información debe ser desclasificada o degradada tan pronto sea práctico.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,'y "Revisión Anual de la Desclasificación"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
21. Desclasificación de Archivos Secretos	Política: Los archivos secretos de la Gobernación deben ser hechos públicos cuando hayan transcurrido 30 años después de los eventos allí descritos.	Políticas Relacionadas: "Desclasificación Acelerada de la Información" y "Destrucción de Registros de Transacciones"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
22. Información y Software Esenciales	Política: La persona designada como Propietario de la información debe determinar si la información, y el software relacionado con ella que se encuentra bajo su control, es esencial en el sentido de que ambos son necesarios para representar el estatus exacto actual del negocio de la Gobernación, para completar una transacción de negocio o para satisfacer los requerimientos legales o regulatorios.	Políticas Relacionadas: "Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones, '"Respaldo de Datos,' y "Clasificación de Recursos Informáticos"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
23. Etiquetas de Entradas en Almacén de Datos	Política: Toda información incluida en el almacén de datos de la Gobernación, debe ir acompañada de información acerca de su origen, su clasificación de sensibilidad, su confiabilidad y la fecha de su más reciente revisión.	Políticas Relacionadas: "Avisos de Derechos de Autor en Software" y "Atribución de la Información"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5.02.02 Etiquetado y Manejo de la Información				
1. Retención de Datos en Grupos de Archivos	Política: Los usuarios deben guardar sus archivos en servidores compartidos en directorios que reflejen cuatro agrupaciones; financieros, recursos humanos, investigación y desarrollo, y otros, teniendo dichas agrupaciones sus requerimientos para el control de acceso y la retención de datos.	Políticas Relacionadas: "Retención de los Datos de Transacciones con Aplicaciones" y "Clasificación de Datos en Cuatro Categorías"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Low

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Convenciones en Nombres	Política: Para lograr un control de acceso consistente en todos los tipos de sistemas de computación, los códigos normales para identificadores de usuarios, nombres de programas de producción, nombres de archivos de producción, nombres de sistemas y otras convenciones en nombres deben ser soportadas adecuadamente.	Políticas Relacionadas: "Información de Contacto del Empleado" y "Convenciones en Nombres de Archivos"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
3. Nombres de los Sistemas de Computación	Política: La función que realiza el computador o el software que éste ejecuta no debe ser utilizada en ninguna parte del nombre del computador, si ese nombre es visible desde la red interna de la Gobernación u ocurre en cualquier archivo legible por computador.	Políticas Relacionadas: "Señalización de Centros de Computación y Comunicaciones" y "Convenciones en Nombres de Archivos"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
4. Convenciones en Nombres de Archivos	Política: Debe utilizarse una convención para nombrar los archivos de tal manera de distinguir entre aquellos archivos usados para la producción y aquellos archivos usados con fines de prueba y adiestramiento.	Políticas Relacionadas: "Convenciones en Nombres"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5. Transacciones Distintas a Producción	Política: Toda transacción utilizada para auditar, probar, adiestrar u otro fin que no sea de producción, deberá estar etiquetada o de alguna manera separada de las transacciones utilizadas para el procesamiento de producción.	Políticas Relacionadas: "Transacciones de Entrada en Producción,' y "Capacidad de Reconstrucción de Cambios en Producción"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
6. Divulgación de Secretos Industriales	Política: Los trabajadores deben proteger diligentemente toda la información de la Gobernación específicamente identificada como secreto industrial para que no sea divulgada sin autorización. Los secretos industriales deben ser identificados como tales antes de divulgarse a cualquier trabajador.	Políticas Relacionadas: "Divulgación de Secretos Industriales por Internet"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
7. Etiquetado de Clasificación de Datos	Política: Toda información secreta, confidencial y privada debe estar etiquetada de acuerdo con las normas emitidas por el departamento de Seguridad Informática, mientras que la información que no corresponda a ninguna de estas categorías no necesita etiquetarse.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Etiquetado Completo de la Clasificación"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
8. Etiqueta de Sensibilidad Desconocida	Política: Si no se puede determinar una etiqueta de sensibilidad para la información obtenida en instalaciones de la Gobernación que usualmente contienen información secreta, entonces dicha información debe ser tratada como secreta.	Políticas Relacionadas: "Etiquetado de Clasificación de Datos" y "Clasificación de Datos en Cuatro Categorías"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
9. Etiquetas de Clasificación por Departamento	Política: Las etiquetas de clasificación de datos específicas por departamento deben ser consistentes con el sistema de clasificación de datos de la Gobernación y complementarlo.	Políticas Relacionadas: "Identificación de Registros Vitales"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
10. Etiquetado de Información Externa	Política: Con excepción de la correspondencia general de negocios y el software con derechos de autor, toda información suministrada externamente y que no sea del dominio público, debe ser asignada una etiqueta con la clasificación de datos de la Gobernación por la persona que la recibe.	Políticas Relacionadas: "Asignación de Etiquetas de Clasificación de Datos"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos
11. Etiquetas de Clasificación Para Nueva Información	Política: Todo usuario que produzca archivos de computador o mensajes debe seleccionar una de las etiquetas de clasificación de datos autorizada al momento de guardar o enviar dichos archivos y mensajes.	Políticas Relacionadas: "Etiquetado Completo de la Clasificación" y "Etiqueta de Sensibilidad Desconocida"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
12. Etiquetado Completo de la Clasificación	Política: Todos los discos, cintas y otros medios de almacenamiento de computación que contengan información secreta, confidencial o privada deben ser etiquetados externamente con la clasificación de sensibilidad apropiada.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Etiquetado de Clasificación de Datos"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
13. Etiquetas de Sensibilidad en Papel	Política: Todas las manifestaciones legibles por humanos, impresas o escritas a mano de información secreta, confidencial o privada deben tener una etiqueta de sensibilidad apropiada en la esquina superior derecha de cada página.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos
14. Etiquetado de Material Impreso Encuadernado	Política: Si está encuadernada, toda información secreta, confidencial o privada impresa, escrita a mano y en cualquier otra manifestación tangible, debe tener la etiqueta de sensibilidad apropiada en la cubierta, en la página de título y en la cubierta posterior.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Etiquetado de Productos y Servicios Peligrosos"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
15. Presentación de la Información Sensible	Política: Si la información es secreta, confidencial o privada, todas las formas en las cuales se despliega en una pantalla o es presentada al usuario deben indicar la sensibilidad de la información.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Etiquetado Completo de la Clasificación,' "Cubrir Información Sensible,' "Visualización e Impresión de Contraseñas,' y "Avisos de Derechos de Autor en Software"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
16. Etiquetado Durante el Ciclo de Vida de la Información	Política: Desde el momento en que la información se crea hasta que se destruye, debe estar etiquetada en cuanto a su grado de sensibilidad, ya sea designada secreta, confidencial o privada.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Etiquetado Completo de la Clasificación"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
17. Mantenimiento de Etiquetas de Clasificación	Política: Los trabajadores que se encuentren en posesión de cualquier información que contenga etiquetas de sensibilidad de la clasificación de datos de la Gobernación, deben mantener, propagar y, de ser necesario, restablecer dicha etiqueta cada vez que la información cambie su forma, el formato o la tecnología con la que se maneja.	Políticas Relacionadas: "Etiquetado de Clasificación de Datos" y "Etiquetas de Clasificación Para Nueva Información"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
18. Copiado de Información Sensible	Política: No deben hacerse copias adicionales o imprimirse copias extras de información secreta, confidencial y privada, sin la autorización del Propietario de la Información.	Políticas Relacionadas: "Prevención del Copiado de Documentos Sensibles,' "Registro del Movimiento de Documentos Secretos,' "Clasificación de Datos en Cuatro Categorías,' y "Seguimiento de Información Sensible"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
19. Seguimiento de Información Sensible	Política: Cada vez que se obtengan copias adicionales de información sensible, se debe anotar en un registro el número de copias y los nombres de los receptores de dichas copias, y cada uno de los receptores debe ser informado que podrá distribuir o hacer copias adicionales sólo después de obtener el permiso del Propietario de la información.	Políticas Relacionadas: "Copiado de Información Sensible" y "Registro del Movimiento de Documentos Secretos"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
20. Productos Intermedios Con Información Sensible	Política: Si una máquina copiadora se tranca o funciona mal cuando los trabajadores están haciendo copias de información secreta, éstos no deben abandonar las máquinas hasta que todas las copias de la información sean removidas de la máquina o destruidas por completo.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Envío de Información Sensible Vía Fax — Notificación,' e "Impresión de Información Sensible"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
21. Copias Sobrantes de Información Sensible	Política: Todas las copias sobrantes de información secreta que se generen en el curso de copiado, impresión y cualquier otro manejo, deben ser destruidas de acuerdo con los procedimientos autorizados.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Envío de Información Sensible Vía Fax — Notificación,' e "Impresión de Información Sensible"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
22. Impresión de Información Sensible	Política: Las impresoras deben estar atendidas por personal autorizado para examinar la información que se está imprimiendo o que pronto se imprimirá en el caso de información sensible, a menos que se utilicen controles físicos de acceso para evitar que personas no autorizadas entren al área de la impresora y visualicen el material que se está imprimiendo.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Envío de Información Sensible Vía Fax — Notificación"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
23. Responsabilidad por la Información Sensible	Política: Toda información sensible de la Gobernación impresa en papel debe indicar tanto la página actual como la última en cada página del documento, tal como "Página X de Y".	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Seguimiento de Información Sensible"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
24. Prevención del Copiado de Documentos Sensibles	Política: Cuando se deba suministrar copias impresas de información privada, confidencial o secreta de la Gobernación a terceros, dichas copias deben ser distribuidas exclusivamente en un papel especial que no permita copias en una fotocopiadora regular.	Políticas Relacionadas: "Seguimiento de Información Sensible" y "Medios de Almacenamiento de Archivos"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
25. Impresión de Información Secreta	Política: La información secreta de la Gobernación puede ser impresa solamente en papel que muestre claramente que es un original o una copia mediante el uso de bordes coloreados, marcas de agua, u otra tecnología aprobada para su uso por el departamento de Seguridad Informática.	Políticas Relacionadas: "Registro del Movimiento de Documentos Secretos" y "Prevención del Copiado de Documentos Sensibles"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
26. Entrega de Salidas Computarizadas Confidenciales	Política: Todo trabajo producido por el computador, bien sea privado, confidencial o secreto debe ser entregado personalmente a los destinatarios designados y nunca debe ser dejado desatendido en un escritorio, o dejado al descubierto en una oficina vacía.	Políticas Relacionadas: "Etiquetado Durante el Ciclo de Vida de la Información" y "Clasificación de Datos en Cuatro Categorías"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
27. Uso de Mensajeros	Política: Toda información privada, confidencial o secreta impresa que se envíe a través de mensajeros comerciales debe recibir seguimiento a través de un número de guía y debe estar marcada con las instrucciones "se requiere la firma del destinatario".	Políticas Relacionadas: "Etiquetado Completo de la Clasificación"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
28. Entrega de Información Secreta	Política: Todas las entregas de información secreta deben ser conducidas de tal manera que el receptor acuse recibo formal de la información recibida.	Políticas Relacionadas: "Registro del Movimiento de Documentos Secretos,' "Clasificación de Datos en Cuatro Categorías,' "Recepción de Información Secreta,' y "Recepción de Información de Terceros"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
29. Recepción de Information Secreta	Política: Los receptores de información secreta de la Gobernación deben suministrar por escrito un acuse de recibo formal al momento de tomar posesión de la información.	Políticas Relacionadas: "Registro del Movimiento de Documentos Secretos,' "Clasificación de Datos en Cuatro Categorías,' y "Entrega de Información Secreta"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
30. Registro del Movimiento de Documentos Secretos	Política: Cuando se trate de información secreta, debe mantenerse un registro mientras dicha información retenga la clasificación de sensibilidad secreta, donde se refleje el número de copias hechas, la ubicación de las copias, los nombres de los receptores y cualquier persona que revise las copias.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Copiado de Información Sensible,' "Recepción de Información Secreta, "Entrega de Información Secreta,' "Números Secuenciales para Documentos Secretos,' y "Seguimiento de Información Sensible"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
31. Números Secuenciales para Documentos Secretos	Política: Todas las copias de documentos secretos deben ser numeradas de forma individual y secuencial para asegurar que las personas responsables de los documentos y la ubicación de los documentos puedan ser fácilmente encontrados.	Políticas Relacionadas: "Registro del Movimiento de Documentos Secretos"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
32. Aseguramiento de la Información Sensible	Política: Los trabajadores que tengan la custodia de información sensible, tal como la información confidencial o secreta de la Gobernación, deben tomar las medidas adecuadas para garantizar que este material no esté disponible para personas no autorizadas.	Políticas Relacionadas: "Responsabilidades del Custodio de la Información" y "Remoción de Información Sensible en Papel"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
33. Divulgación de Información Desclasificada	Política: La información sensible aparentemente desclasificada o degradada porque llegó su fecha de vencimiento, no debe divulgarse a otras personas hasta que su desclasificación o degradación se confirme con el Propietario designado de la información	Políticas Relacionadas: "Prórroga para la Desclasificación"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
34. Medios de Almacenamiento de Información Sensible	Política: Antes de que cualquier medio de almacenamiento se envíe al proveedor, bien sea como parte de pago, para servicio o para su disposición, toda información sensible de la Gobernación debe ser destruida u ocultada de acuerdo a los métodos autorizados por el departamento de Seguridad Informática.	Políticas Relacionadas: "Respaldo de Datos,' "Clasificación de Datos en Cuatro Categorías,' "Transferencia de Información Sensible,' y "Liberación de Componentes Usados"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
35. Etiqueado de Productos y Servicios Peligrosos	Política: Todos los productos y servicios de la Gobernación que representen un peligro para los consumidores, trabajadores o a personas involucradas, deben tener etiquetas identificando la naturaleza del peligro, formas de evitarlo y pasos a seguir en caso de que la situación cause pérdidas.	Políticas Relacionadas: "Mensaje de Advertencia en Inicio de Sesión"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
36. Etiquetado de Datos Usados Como Base de Decisión Gerencial	Política: Todos los datos utilizados para decisiones gerenciales que involucren cantidades por encima de los $100.000,00 deben estar etiquetados con su origen y fecha correspondiente.	Políticas Relacionadas: "Etiquetado de la Propiedad Intelectual"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
37. Información Incompleta u Obsoleta	Política: Toda información obsoleta o incompleta debe ser suprimida y no distribuida a los usuarios, a menos que esté acompañada de una explicación que describa el estatus de la información.	Políticas Relacionadas: "Atributos de la Integridad de la Información" y "Representaciones de la Organización"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
38. Documentos Oficiales Preparados a Mano	Política: Todos los documentos oficiales de la Gobernación preparados a mano, deben utilizar tinta imborrable y si alguna entrada requiere corrección, esa entrada debe ser tachada, firmada y fechada por el originador.	Políticas Relacionadas: "Prevención del Copiado de Documentos Sensibles" y "Retención del Documento Fuente"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
39. Fotografías Alteradas	Política: Toda fotografía que haya sido alterada debe estar etiquetada para indicar que se han efectuado modificaciones.	Políticas Relacionadas: "Divulgación de las Modificaciones a la Información" y "Capacidad de Reconstrucción de Cambios en Producción"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
40. Eliminación de la Información de Pago	Política: La eliminación de todos los documentos en papel que contengan información de pagos, tales como números de cuentas bancarias o de tarjetas de crédito, deben ser realizadas con máquinas trituradoras de papel o cualquier otro método autorizado de destrucción.	Políticas Relacionadas: "Copias Sobrantes de Información Sensible,' "Período de Retención del Documento Fuente,' y "Acceso a la Información Personal"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Políticas de Personal

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6 EL PERSONAL				
6.01 La Seguridad en Definiciones de Trabajo y Contratación				
6.01.01 Inclusión de la Seguridad en las Responsabilidades del Cargo				
1. Descripción del Cargo	Política: Deben incorporarse las responsabilidades específicas sobre la seguridad informática en todas las descripciones de cargo donde los trabajadores tengan acceso a información confidencial, valiosa o crítica.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Evaluaciones de Desempeño"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
2. Evaluaciones de Desempeño	Política: Se debe considerar el cumplimiento de las políticas y procedimientos de seguridad informática en todas las evaluaciones de desempeño de los empleados.	Políticas Relacionadas: "Responsabilidad en la Seguridad Informática"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
6.01.02 Selección de Personal y la Política				
1. Información de Empleado Potencial	Política: No se debe recopilar información personal sobre un empleado potencial, a menos que ésta sea necesaria para tomar decisiones pertinentes al cargo.	Políticas Relacionadas: "Notificación de Monitoreo Electrónico del Desempeño" y "Pruebas de Honestidad y Estabilidad Emocional"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
2. Verificaciones de Historia Crediticia de Empleados Potenciales	Política: Se debe notificar a todos los candidatos si sus referencias crediticias o sus antecedentes serán investigados como parte del proceso de reclutamiento y selección, y deben recibir la oportunidad de retirar su solicitud de empleo si no desean que la Gobernación conozca dicha información personal.	Políticas Relacionadas: "Distribución de los Registros del Personal" y "Huellas Digitales de Empleados"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
3. Información Sobre Estilo de Vida del Empleado Potencial	Política: Los candidatos a emplearse con la Gobernación no deben estar supeditados a exámenes que revelen su estilo de vida, su afiliación política o preferencias religiosas, a menos que esta información sea necesaria para determinar si el candidato es adecuado para el cargo.	Políticas Relacionadas: "Cargos de Confianza en el Área de Computación"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
4. Divulgación de Información a Solicitantes de Empleo	Política: Los detalles técnicos de sistemas informáticos tales como direcciones de redes, diagramas de redes y software de seguridad utilizado, no deben ser revelados a los aspirantes al empleo mientras no hayan firmado un acuerdo de confidencialidad y también hasta que hayan sido empleados o contratados.	Políticas Relacionadas: "Entrega de Documentación de Sistemas" y "Convenios de Intercambio de Software y Datos"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
5. Re-empleo de Empleados Despedidos	Política: No deben reengancharse o contratarse ex-empleados, ex-consultores y ex-contratistas despedidos, sin el consentimiento de un vicepresidente ejecutivo.	Políticas Relacionadas: “Período de Prueba Para Trabajadores Nuevos”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
6. Período de Prueba Para Trabajadores Nuevos	Política: Todos los nuevos trabajadores y aquéllos que hayan sido re-empleados o contratados después de una evaluación poco satisfactoria de su desempeño, deben ser colocados en un período de prueba de seis meses durante el cual la gerencia a quienes reportan debe seguir atentamente su desempeño y actitud, con el propósito de tomar la decisión de retenerlos o despedirlos.	Políticas Relacionadas: “Re-empleo de Empleados Despedidos”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
7. Fianzas de Trabajadores	Política: Todos los trabajadores con cargos de confianza particularmente en el área de computación deben contar con una fianza por un mínimo de $1.000.000.	Políticas Relacionadas: “Información Sensible en Pequeños Computadores,’ “Información Sobre Estilo de Vida del Empleado Potencial,’ “Revisión de Antecedentes,’ y “Cargos de Confianza en el Área de Computación”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
8. Trabajo en Proyectos Sensibles	Política: Sólo empleados con desempeño de bueno a excelente y con antigüedad de por lo menos dos años en la Gobernación, pueden trabajar en el desarrollo de nuevos productos y otros proyectos de alta sensibilidad.	Políticas Relacionadas: “Identificadores de Usuario para Terceros” y “Verificaciones de Historia Crediticia de Empleados Potenciales”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
9. Convictos Violentos	Política: No deben hacerse ofertas de trabajo a individuos que hayan sido condenados judicialmente por crímenes violentos que, de repetirse, representarían un daño físico para los empleados o la propiedad de la Gobernación.	Políticas Relacionadas: “Cargos de Confianza en el Area de Computación”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
10. Cargos de Confianza en el Area de Computación	Política: Las personas que hayan sido condenadas por delitos judiciales no deben ser empleados, contratados, promovidos o mantenidos en cargos de confianza en el área de computación.	Políticas Relacionadas: “Convictos Violentos, ’“Revisión de Antecedentes,’ “Fianzas de Trabajadores,’ e “Información Sobre Estilo de Vida del Empleado Potencial”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
11. Revisión de Antecedentes	Política: Todos los trabajadores en consideración para ser colocados en posiciones de confianza en el área de computación deben pasar la revisión de antecedentes, la cual incluye la verificación de prontuarios policiales, demandas, problemas crediticios, multas de tránsito y empleos anteriores.	Políticas Relacionadas: “Cargos de Confianza en el Área de Computación,’ “Informe de Cambios en Situación,’ y “Fianzas de Trabajadores”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
12. Pruebas con Polígrafos	Política: Todos los trabajadores de la Gobernación en consideración para ser colocados en posiciones de confianza en el área de computación, deben pasar la prueba del polígrafo antes de comenzar a trabajar en su nueva posición.	Políticas Relacionadas: “Fianzas de Trabajadores” y “Verificaciones de Historia Crediticia de Empleados Potenciales”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos
13. Acceso a Información Privada	Política: Los empleados deben pasar una investigación de antecedentes antes de recibir el acceso a información privada.	Políticas Relacionadas: “Revisión de Antecedentes” e “Integridad del Registro Personal”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
14. Información Sensible de Productos	Política: Todos los trabajadores que tendrán acceso a información sensible de productos, tales como planes de mercadeo, especificaciones de ingeniería o procedimientos de manufactura, deben pasar la investigación normal de antecedentes efectuada por el departamento de Recursos Humanos.	Políticas Relacionadas: “Acuerdos de Confidencialidad — Organización” e “Identificadores de Usuario para Terceros”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
15. Huellas Digitales de Empleados	Política: Antes de comenzar a trabajar, se deben tomar las huellas digitales de los empleados potenciales que tendrán acceso a información sensible, las cuales se utilizarán para determinar si el empleado potencial posee prontuario policial.	Políticas Relacionadas: “Fianzas de Trabajadores, ’“Verificaciones de Historia Crediticia de Empleados Potenciales,’ e “Iniciación de Transacciones en Computadores”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
16. Pruebas de Honestidad y Estabilidad Emocional	Política: Todos los trabajadores en consideración para ocupar posiciones de confianza en computación deben pasar las pruebas de honestidad y estabilidad emocional autorizadas por el departamento de Recursos Humanos.	Políticas Relacionadas: “Información de Empleado Potencial” y “Huellas Digitales de Empleados”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
17. Revisión de Antecedentes de No Empleados	Política: Los empleados temporales, los consultores, los contratistas y el personal de organizaciones externas no deben recibir acceso a información sensible o acceso a sistemas de información crítica, a menos que pasen por una verificación de antecedentes proporcional a las efectuadas a los empleados regulares.	Políticas Relacionadas: “Identificadores de Usuario para Terceros” y “Privilegios de Trabajadores Temporales”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
18. Extranjeros	Política: No deben trabajar extranjeros en los sistemas informáticos de la Gobernación .	Políticas Relacionadas: “Transporte Internacional de Información Secreta — Seguridad” y “Revisión de Antecedentes”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
19. Antiguos Hackers y Delincuentes Reformados	Política: La Gobernación no debe emplear antiguos hackers ni delincuentes reformados para trabajar en seguridad informática o realizar trabajos forenses.	Políticas Relacionadas: “Equipos de Investigación de Seguridad Informática” y “Conflictos de Intereses”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
20. Aumento Significativo de Riqueza	Política: En caso de que un trabajador de la Gobernación demuestre un inexplicable aumento de riqueza, la gerencia tiene el deber de investigar discretamente el origen de dicha nueva riqueza.	Políticas Relacionadas: “Trabajadores Como Clientes” e “Investigación de Delito Computarizado”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
6.01.03 Acuerdos de Confidencialidad				
1. Derechos de Propiedad	Política: Sin excepciones específicas escritas, todos los programas y la documentación generados o proporcionados por cualquier trabajador en beneficio de la Gobernación son propiedad de la Gobernación y todos los trabajadores que proporcionen tales programas o documentación deben firmar una declaración a tal efecto, previa a la entrega de dichos materiales.	Políticas Relacionadas: “Convenios de No Competencia,’ “Derechos de Propiedad Intelectual, ’“Confidencialidad de la Documentación,’ y “Recuperación de la Propiedad de la Organización”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Acuerdos de Confidencialidad — Organización	Política: Todos los empleados deben personalmente firmar un acuerdo de confidencialidad con la Gobernación antes de comenzar a trabajar, o si un trabajador ha estado trabajando sin dicho acuerdo, debe firmarlo como condición de empleo.	Políticas Relacionadas: “Revisión de Antecedentes, ’“Convenio de Cumplimiento,’ “Acuerdos de Confidencialidad,’ y “Acuerdos de Confidencialidad — Terceros”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
3. Cambios en el Empleo	Política: Cuando haya cambios en la situación laboral o cambios en la condición de trabajo de un trabajador externo, como un contratista, consultor o temporal, el contenido del acuerdo de confidencialidad de la Gobernación debe ser revisado con el gerente de la persona correspondiente.	Políticas Relacionadas: “Acuerdos de Confidencialidad — Organización”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
4. Acuerdos de Confidencialidad con Antiguos Patronos	Política: Los empleados que hayan trabajado en organizaciones de la competencia deben ser alentados a respetar los acuerdos de confidencialidad que firmaron con dichas organizaciones y ningún trabajador debe presionar a estos empleados en el sentido de divulgar información que pueda ser beneficiosa para la Gobernación.	Políticas Relacionadas: “Conflictos de Intereses” y “Solicitudes de Información Organizacional”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
5. Convenios de No Competencia	Política: Al momento de emplearse en la Gobernación, todos los empleados deben firmar un convenio de no competir con la Gobernación durante un período de seis meses después de su separación de ella.	Políticas Relacionadas: “Derechos de Propiedad Intelectual”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
6.01.04 Términos y Condiciones de Empleo				
1. Derechos de Propiedad Intelectual	Política: Mientras sean empleados de la Gobernación, todo el personal debe otorgar a la Gobernación derechos exclusivos sobre las patentes, los derechos de autor, los inventos u otra propiedad intelectual que originen o desarrollen.	Políticas Relacionadas: “Convenios de No Competencia,’ “Propiedad Intelectual Desarrollada Fuera de Sede,’ “Derechos de Propiedad,’ y “Comunicaciones Públicas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
2. Recuperación de la Propiedad de la Organización	Política: Los empleados, los temporales, los contratistas y los consultores no deben recibir su pago final hasta que no hayan devuelto todo el hardware, software, materiales de trabajo, información confidencial y cualquier otra propiedad de la Gobernación.	Políticas Relacionadas: “Derechos de Propiedad, ’“Derechos de Propiedad Intelectual,’ y “Remoción de Información Sensible”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
3. Empleados Que Viajan Conjuntamente	Política: Los empleados no deben abordar el mismo avión si ello implica que tres o más directivos, cinco o más empleados, o dos o más ingenieros del mismo departamento estarían en el mismo vuelo.	Políticas Relacionadas: “Adiestramiento Multidisciplinario” e “Información de Contacto”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
4. Informantes Internos	Política: De vez en cuando la Gobernación utiliza informantes, quienes pueden ser ubicados en diversas posiciones internas y que aparentan ser como cualquier otro trabajador, pero sin notificarles a otros trabajadores su presencia o la naturaleza del trabajo que efectúan tales informantes.	Políticas Relacionadas: “Uso de Investigadores”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
5. Inteligencia Competitiva	Política: Cuando se recopile información sobre la competencia, el personal de la Gobernación, o cualquier persona designada para recoger dicha información en representación del personal de la Gobernación, no debe mentir nunca o falsificar su identidad.	Políticas Relacionadas: “Recopilación de Información de Precios por Terceros” e “Identidades Falsas”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Medianos y altos
6. Distribución de los Registros del Personal	Política: Con el fin de permitir a cada empleado familiarizarse con la información y garantizar que no contenga errores, cada empleado debe recibir una copia de su archivo personal una vez al año.	Políticas Relacionadas: “Acceso a la Información Personal” y “Verificaciones de Historia Crediticia de Empleados Potenciales”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
7. Información Sobre Salud y Seguridad	Política: La gerencia debe dar a conocer plenamente a los trabajadores correspondientes, los resultados de las pruebas de sustancias tóxicas y cualquier otra información relacionada con la salud y seguridad de los trabajadores.	Políticas Relacionadas: “Peligros Laborales”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
8. Peligros Laborales	Política: La gerencia debe informar a los trabajadores sobre la existencia de peligros en el sitio de trabajo, suministrar medidas de seguridad para minimizar el riesgo a los trabajadores y adiestrar a los trabajadores en el uso apropiado de las medidas de seguridad.	Políticas Relacionadas: “Información Sobre Salud y Seguridad” y “Solicitudes Externas de Información”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
9. Transacciones Bursátiles de Empleados	Política: Los empleados no deben comprar o vender acciones o bonos de la Gobernación entre el fin del trimestre fiscal y el momento cuando se anuncien públicamente los resultados financieros finales.	Políticas Relacionadas: “Conflictos de Intereses”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
10. Acoso Sexual, Étnico y Racial	Política: Los trabajadores no deben acosar a otros por cuestiones de sexo, etnia o raza.	Políticas Relacionadas: “Conducta de los Empleados Fuera de la Oficina” y “Registros de Telemercadeo”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
11. Propiedad Intelectual Desarrollada Fuera de Sede	Política: La propiedad intelectual, incluyendo sin limitantes, patentes, derechos de autor, marcas registradas y todos los otros derechos de propiedad intelectual tal como se manifiestan en memorandos, planes, estrategias, productos, programas de computación, documentación y demás material desarrollado o concebido mientras el empleado esté trabajando en sitios alternativos de trabajo, es exclusiva propiedad de la Gobernación.	Políticas Relacionadas: “Derechos de Propiedad Intelectual” y “Derechos de Propiedad”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
12. Código de Conducta Corporativo	Política: Todos los trabajadores deben leer, entender y comportarse de acuerdo con el código de conducta corporativo.	Políticas Relacionadas: “Entendimiento del Código de Conducta”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
13. Entendimiento del Código de Conducta	Política: Todos los trabajadores deben indicar que entienden el código de conducta, firmando anualmente un formulario donde reconocen estar de acuerdo con suscribir el código.	Políticas Relacionadas: “Código de Conducta Corporativo”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
14. Conflictos de Intereses	Política: Todos los trabajadores deben evitar los conflictos de intereses, tanto los verdaderos como los aparentes, en sus tratos de negocios con la Gobernación.	Políticas Relacionadas: “Transacciones Bursátiles de Empleados”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
15. Relaciones Personales con la Competencia	Política: Los trabajadores de la Gobernación no deben tener compañeros románticos o familiares cercanos trabajando en organizaciones de la competencia.	Políticas Relacionadas: “Compartir Información de Mercadeo” y “Acuerdos de Confidencialidad con Antiguos Patronos”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
16. Renuncia de Empleados por la Competencia	Política: Todos los trabajadores que tengan la intención de trabajar para un competidor deben notificar inmediatamente a la gerencia de la Gobernación y, al momento de aceptar la oferta del competidor, el trabajador recogerá sus pertenencias personales en presencia de un escolta quien lo acompañará hasta la puerta, revocándose entonces todos sus derechos, privilegios y accesos a la Gobernación.	Políticas Relacionadas: “Transferencia de Responsabilidad en Custodia” y “Eliminación de Archivos de Trabajador Cesado”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
17. Notificación de Cese de Empleo	Política: Todos los empleados deben ser informados tan pronto se produzca el cese de un empleado, y el departamento de Recursos Humanos debe frecuentemente recordar a los empleados que los ex-trabajadores no deben entrar a las instalaciones de la Gobernación, usar los recursos de la Gobernación o estar afiliados de ninguna forma a la Gobernación.	Políticas Relacionadas: “Escolta para Trabajadores Despedidos” e “Informe de Cambios en Situación de Empleados”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
18. Notificación a Terceros de Cese de Trabajador	Política: Si un trabajador despedido tiene la autoridad de dirigir contratistas, consultores o temporales, o si este mismo trabajador tiene la autoridad para comprometer a la Gobernación en una compra u otra transacción, entonces el departamento de Recursos Humanos debe notificar inmediatamente a todos los terceros pertinentes que el trabajador despedido ya no es empleado de la Gobernación.	Políticas Relacionadas: “Acceso Físico de Trabajadores Cesados” y “Responsabilidad por Cese de Trabajador”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
19. Manejo de Despidos	Política: En todos los casos cuando trabajadores de apoyo técnico de tecnología informática sean despedidos, inmediatamente deben ser relevados de sus cargos, exigirles la devolución de todo el equipo e información de la Gobernación y escoltarlos mientras empacan sus pertenencias y salen de las instalaciones de la Gobernación.	Políticas Relacionadas: “Despidos Inmediatos”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
20. Escolta para Trabajadores Despedidos	Política: En todos los casos cuando los trabajadores sean despedidos por la Gobernación, la finalización del servicio debe ser efectuada en presencia de un guardia de seguridad, y seguidamente el despedido debe empacar sus pertenencias también en presencia del guardia de seguridad, ser escoltado a la puerta y ser informado que no puede volver a entrar a las instalaciones a menos que sea invitado por la gerencia.	Políticas Relacionadas: “Despidos Inmediatos” y “Responsabilidad por Cese de Trabajador”	Política Dirigida a:Gerencia	
21. Retención de Información al Terminar Empleo	Política: Toda la información de la Gobernación en custodia del trabajador saliente, debe ser entregada a su supervisor inmediato al momento de su salida, con la excepción de copias personales de información diseminadas al público y copias personales de correspondencia directamente relacionadas a los términos y condiciones del empleo.	Políticas Relacionadas: “Transferencia de Responsabilidad en Custodia”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
22. Devolución de Propiedad al Cesar Empleo	Política: En el momento que cualquier empleado, consultor o contratista termine su relación con la Gobernación, toda propiedad de la Gobernación debe ser devuelta, incluyendo, sin limitantes, computadores portátiles, libros de la biblioteca, documentación, llaves del edificio, tarjetas magnéticas de acceso, tarjetas de crédito y préstamos pendientes.	Políticas Relacionadas: “Responsabilidad por Cese de Trabajador” y “Acceso Físico de Trabajadores Cesados”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
23. Días Consecutivos de Vacaciones	Política: La gerencia debe garantizar que los trabajadores saldrán de vacaciones por lo menos cinco días consecutivos una vez al año.	Políticas Relacionadas: “Adiestramiento Multidisciplinario”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
24. Segundos Trabajos	Política: Los trabajadores no deben tener un segundo trabajo si el mismo perjudica o compromete de alguna manera la objetividad del trabajador en su cargo con la Gobernación, o si el otro patrono está de alguna manera en competencia con la Gobernación.	Políticas Relacionadas: “Divulgación de Segundos Trabajos,’ “Conflictos de Intereses,’ y “Días Consecutivos de Vacaciones”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
25. Divulgación de Segundos Trabajos	Política: Los trabajadores deben informar a su gerente inmediato que tienen un segundo o más trabajos en el momento en que son entrevistados para optar por una posición en la Gobernación o, si ya están empleados en la Gobernación, al momento de tomar estos otros trabajos.	Políticas Relacionadas: “Segundos Trabajos, ’“Renuncia de Empleados por la Competencia,’ y “Días Consecutivos de Vacaciones”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
26. Trabajadores Como Clientes	Política: Los trabajadores de confianza actualmente en posiciones relacionadas con computación en la Gobernación no deben ser al propio tiempo clientes de la Gobernación.	Políticas Relacionadas: “Fianzas de Trabajadores” y “Trabajo en Proyectos Sensibles”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Altos
27. Informe de Cambios en Situación	Política: Los empleados deben reportar a su gerente inmediato todos los cambios en su situación personal que pudiesen afectar su elegibilidad para mantener su cargo actual o, de lo contrario, estarán sujetos a acciones disciplinarias que podrían incluir la finalización de la relación de trabajo.	Políticas Relacionadas: “Revisión de Antecedentes”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
28. Transferencias de Trabajadores	Política: Los trabajadores que hayan declarado su intención de abandonar el empleo en la Gobernación y aquéllos que estén en conocimiento de su inminente despido y cualquier empleado descontento, deben ser transferidos a posiciones donde sólo puedan hacer mínimo daño a los activos de la Gobernación.	Políticas Relacionadas: “Acceso Físico de Trabajadores Cesados” y “Confidencialidad de la Información de las Investigaciones Internas”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
29. Resolución de Quejas	Política: La gerencia debe establecer y suministrar personal adecuado para realizar los procedimientos que agilicen todas y cada una de las quejas del trabajador.	Políticas Relacionadas: “Negativa a Proporcionar Información Innecessaria”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
30. Orientación Confidencial	Política: Todo trabajador con serios problemas personales deben recibir asesoramiento confidencial y gratuito.	Políticas Relacionadas: “Drogas y Alcohol” y “Resolución de Quejas”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
31. Drogas y Alcohol	Política: Con excepción de las medicinas recetadas por un profesional médico, los trabajadores no deben usar o estar bajo la influencia de drogas o de alcohol en el sitio de trabajo.	Políticas Relacionadas: “Orientación Confidencial”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
32. Remoción de Distintivos de Identificación	Política: Inmediatamente después de salir del área de la Gobernación, los trabajadores deben quitarse el distintivo de identificación y guardarlo en un lugar seguro y conveniente fuera de la vista pública.	Políticas Relacionadas: “Acceso Físico para Terceros” y “Escolta para Trabajadores Despedidos”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos
33. Aseguramiento de los Distintivos	Política: Al estar fuera del área de la Gobernación, los trabajadores deben proteger su distintivo de identificación de la misma manera que protegen sus carteras o tarjetas de crédito.	Políticas Relacionadas: “Personas Sin Distintivos de Identificación” y “Acceso Físico para Terceros”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
6.02 Adiestramiento de Usuarios				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6.02.01 Educación y Adiestramiento en Seguridad Informática				
1. Exámenes Sobre las Políticas	Política: Los usuarios no deben tener acceso a los sistemas informáticos de la Gobernación, a menos que hayan leído la Política de Seguridad Informática y tomado un pequeño examen que demuestre claramente que entienden el material descrito en dicha política.	Políticas Relacionadas: “Formularios para Identificadores de Usuario”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Políticas y Procedimientos Relativos a la Privacidad	Política: Con excepción de los relativos al manejo de datos privados de las personas, las políticas y procedimientos de seguridad informática deben ser revelados sólo a los trabajadores de la Gobernación y a terceros seleccionados, tales como los auditores, quienes tienen una necesidad legítima de negocio sobre esta información.	Políticas Relacionadas: “Anonimato del Cliente” y “Reportes Externos de Violaciones”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
3. Adiestramiento para Acceso Remoto	Política: Los trabajadores de la Gobernación deben completar y aprobar un curso de adiestramiento de acceso remoto a los sistemas, antes de recibir el privilegio de acceso a una red conmutada, a los protocolos que permiten la conexión e introducción de comandos en un computador remoto conectado a Internet, o cualquier otro acceso remoto al sistema de comunicación de datos.	Políticas Relacionadas: “Requisitos de Seguridad para Teletrabajo” y “Procedimientos de Seguridad Informática en Teletrabajo”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
4. Adiestramiento en Internet	Política: Los trabajadores pueden acceder a Internet a través de los servicios de la Gobernación sólo si han sido autorizados por la gerencia del departamento y han completado un curso de adiestramiento en políticas y prácticas de Internet.	Políticas Relacionadas: “Adiestramiento en Seguridad Informática” y “Tiempo de Adiestramiento”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos
5. Panfleto sobre Políticas de Seguridad Informática	Política: Antes o en su primer día de trabajo, todos los nuevos trabajadores de la Gobernación deben recibir una copia del folleto informativo de la política de seguridad informática y hacerles saber que deben satisfacer los requisitos descritos en el folleto.	Políticas Relacionadas: “Entendimiento del Código de Conducta” y “Adiestramiento en Seguridad Informática”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
6. Adiestramiento en Seguridad Informática	Política: Todos los trabajadores deben ser provistos con suficiente adiestramiento y material de referencia de soporte para permitirles proteger adecuadamente los recursos informáticos de la Gobernación.	Políticas Relacionadas: “Tiempo de Adiestramiento, ’“Manual de Seguridad Informática,’ “Responsabilidades del Usuario de la Información,’ y “Adiestramiento Técnico y Educación Continua”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
7. Adiestramiento Básico	Política: Los trabajadores deben haber terminado satisfactoriamente todos los otros adiestramientos básicos necesarios para efectuar su nuevo trabajo antes de recibir el adiestramiento de seguridad informática.	Políticas Relacionadas: “Adiestramiento para Acceso Remoto” y “Comandos y Capacidades del Sistema”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Medianos y altos
8. Cambios en Políticas de Seguridad Informática	Política: Todos los trabajadores de la Gobernación deben recibir notificación pronta de los cambios realizados a la política de seguridad informática de la empresa, incluyendo la manera en que estos cambios pueden afectarlos y cómo obtener información adicional.	Políticas Relacionadas: “Aviso de Cambio en Política de Privacidad” y “Entendimiento del Código de Conducta”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
9. Responsabilidad en Adiestramiento	Política: El departamento de Seguridad Informática debe proporcionar cursos de actualización y otros materiales, para recordar regularmente a los trabajadores sus obligaciones con respecto a la seguridad informática.	Políticas Relacionadas: “Tiempo de Adiestramiento” y “Tareas del Departamento de Seguridad Informática”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
10. Tiempo de Adiestramiento	Política: La gerencia debe asignar tiempo hábil para que los trabajadores se familiaricen con las políticas de seguridad, procedimientos y otras formas de llevar los negocios en la Gobernación.	Políticas Relacionadas: “Adiestramiento en Sistemas de Producción” y “Responsabilidad en Adiestramiento”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
11. Convenio de Trabajo	Política: Todo trabajador debe entender las políticas y procedimientos de la Gobernación referentes a seguridad informática y debe estar de acuerdo, por escrito, en ejecutar su trabajo de conformidad con dichas políticas y procedimientos.	Políticas Relacionadas: “Exámenes Sobre las Políticas” y “Clases Sobre Seguridad Informática”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
12. Clases Sobre Seguridad Informática	Política: Dentro de los tres meses siguientes a la fecha en que fue empleado en la Gobernación, cada trabajador debe asistir a una clase de toma de conciencia respecto de la seguridad informática y firmar una declaración de asistencia confirmando que ha asistido a las clases, entendido el material y que tuvo la oportunidad de hacer preguntas.	Políticas Relacionadas: “Convenio de Trabajo”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
13. Adiestramiento para Acceso al Sistema	Política: Todos los trabajadores de la Gobernación deben completar y aprobar una clase de adiestramiento en seguridad informática antes de recibir el acceso a cualquier sistema de computación de la Gobernación.	Políticas Relacionadas: “Acceso para Trabajadores Temporales y Consultores” y “Adiestramiento en Seguridad Informática”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
14. Adiestramiento en Sistemas de Producción	Política: Los trabajadores de la Gobernación no deben utilizar software para los procesos de producción del negocio, a menos que hayan completado y aprobado el adiestramiento autorizado para dicho software.	Políticas Relacionadas: "Tiempo de Adiestramiento"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
15. Convenio de Cumplimiento	Política: Como condición para la continuación del empleo, los empleados, consultores y contratistas deben firmar anualmente un convenio de cumplimiento de seguridad informática.	Políticas Relacionadas: "Acuerdos de Confidencialidad — Organización" y "Acuerdos de Confidencialidad"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
16. Adiestramiento Técnico y Educación	Política: Todo el personal técnico de los sistemas informáticos debe tener suficiente adiestramiento inicial y educación continua en todos los aspectos críticos de su trabajo, incluyendo seguridad, aseguramiento de la calidad y relaciones con el cliente.	Políticas Relacionadas: "Alertas Sobre Vulnerabilidades" y "Adiestramiento en Seguridad Informática"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
17. Responsabilidad en la Seguridad Informática	Política: La responsabilidad de la seguridad informática del día a día debe ser tarea de cada trabajador y no sólo del departamento de Seguridad de Informática.	Políticas Relacionadas: "Evaluaciones de Desempeño" y "Tareas del Departamento de Seguridad Informática"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
6.03 Respuesta a Incidentes y Anomalías de Seguridad				
6.03.01 Reporte de Incidentes de Seguridad				
1. Pérdida o Divulgación de Información Sensible	Política: Si la información sensible se pierde o se divulga a personas no autorizadas, o existe una sospecha de haberse perdido o divulgado a terceros no autorizados, tanto su Propietario como el personal apropiado de Seguridad Informática deben ser notificados inmediatamente.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Propiedad de la Información,' y "Notificación de Falla en los Controles de la Integridad"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
2. Divulgación de las Vulnerabilidades del Sistema Informático	Política: La información específica sobre las vulnerabilidades del sistema informático, tales como los detalles de una reciente intromisión en el sistema, no deben ser distribuidas a personas que no tienen una necesidad demostrada de conocerla.	Políticas Relacionadas: "Código Fuente del Software de Penetración de Sistemas" y "Presentación de la Imagen Pública"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
3. Notas de Prensa Sobre Información de Vulnerabilidad	Política: Las notas de prensa u otras declaraciones públicas dadas por la Gobernación que contengan información sobre la vulnerabilidad informática, no deben contener detalles específicos.	Políticas Relacionadas: "Presentación de la Imagen Pública" y "Código Fuente del Software de Penetración de Sistemas"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
4. Explotación de la Vulnerabilidad del Sistema y Datos de la Víctima	Política: El personal de la Gobernación no debe divulgar información acerca de individuos, organizaciones, métodos específicos utilizados para sacar provecho, o sistemas específicos que han sido dañados por delitos y abusos en computación.	Políticas Relacionadas: “Solicitudes Externas de Información” y “Divulgación de las Vulnerabilidades del Sistema Informático”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
5. Problemas en el Sistema de Producción	Política: Todos los errores importantes, los procesamientos incompletos y los procesamientos impropios de las aplicaciones de producción, deben ser inmediatamente reportados al Centro de Atención al Usuario.	Políticas Relacionadas: “Condiciones de Interrupción” y “Daño y Pérdida de Sistemas Fuera de Sede”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
6. Bromas en Seguridad Informática	Política: Los trabajadores no deben jugar o hacer travesuras, o de alguna otra manera humorística hacer ver que está ocurriendo un incidente de seguridad, o va a ocurrir, u ocurrió, cuando tal cosa no es cierta.	Políticas Relacionadas: “Páginas Web No Oficiales” y “Recopilación de Datos Personales Bajo Pretextos”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
7. Mensajes Ofensivos de Correo Electrónico	Política: Todos los trabajadores deben responder directamente a la fuente de mensajes electrónicos, llamadas telefónicas y otras comunicaciones ofensivas y, de no cesar los mensajes ofensivos, los trabajadores deben reportar las comunicaciones a su gerente y al departamento de Recursos Humanos.	Políticas Relacionadas: “Remoción de Material Ofensivo” y “Acoso Sexual, Étnico y Racial”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
8. Daño y Pérdida de Sistemas Fuera de Sede	Política: Los trabajadores deben reportar prontamente a sus gerentes en la Gobernación cualquier daño o pérdida de hardware, software o información confiada a ellos.	Políticas Relacionadas: “Informes de Incidentes” e “Informes de Violaciones y Problemas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
9. Informes de Incidentes	Política: Todas las sospechas de incidentes de seguridad informática deben ser reportadas tan pronto sea posible, a través de los canales internos autorizados de la Gobernación.	Políticas Relacionadas: “Daño y Pérdida de Sistemas Fuera de Sede,’ “Informes de Violaciones y Problemas, ’“Sistema de Alerta de Seguridad Informática,’ “Investigaciones Prolongadas,’ e “Infracción de la Ley”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
10. Severidad de los Incidentes Reportados	Política: A menos que razonablemente se suponga que la pérdida puede continuar, un incidente de seguridad informática con daños inferiores a $100 y que haya sido resuelto por las personas involucradas, no tiene que ser reportado al departamento de Seguridad Informática.	Políticas Relacionadas: “Informes de Incidentes” e “Informes de Violaciones y Problemas”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
11. Informes de Violaciones y Problemas	Política: Los trabajadores de la Gobernación tienen la obligación de reportar todas las infracciones y problemas de seguridad informática al departamento de Seguridad de Informática oportunamente, para que se tomen las acciones correctivas correspondientes.	Políticas Relacionadas: "Reportes Externos de Violaciones,' "Equipo de Respuesta Ante Emergencias Computacionales,' e "Informe de Sospecha de Virus"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
12. Alternativas para el Reporte de Violaciones y Problemas	Política: Los trabajadores de la Gobernación deben reportar inmediatamente todas las sospechas de problemas, vulnerabilidades e incidentes de seguridad informática a su gerente inmediato o a la gerencia de Seguridad Informática.	Políticas Relacionadas: "Informes de Incidentes" y "Cambios en Situación de Usuarios"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
13. Interferencia con Reportes de Violaciones y Problemas	Política: Los trabajadores nunca deben intentar interferir, impedir, obstruir o disuadir a un integrante del personal en su esfuerzo por reportar la sospecha de algún problema o infracción en la seguridad informática, o tomar represalias en contra de un individuo que reporte o investigue infracciones o problemas en seguridad informática.	Políticas Relacionadas: "Informes de Problemas"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
14. Protección para Reportes de Violaciones y Problemas	Política: La Gobernación debe proteger los trabajadores que en buena fe reporten lo que consideren una violación de las leyes o reglamentos o condiciones que puedan poner en peligro la salud o seguridad de otros trabajadores.	Políticas Relacionadas: "Reportes Externos de Violaciones"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
15. Identidad del Informante de Violaciones y Problemas	Política: Los trabajadores que reporten al departamento de Seguridad un problema de seguridad, vulnerabilidad, o una condición no ética dentro de la Gobernación pueden, a su discreción, mantener su identidad en estricta reserva.	Políticas Relacionadas: "Protección para Reportes de Violaciones y Problemas" y "Reportes Centralizados de Problemas"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
16. Reportes Externos de Violaciones	Política: A menos que la ley o los reglamentos exijan reportar las infracciones de seguridad informática a las autoridades externas, la gerencia, conjuntamente con representantes del departamento Legal, del departamento de Seguridad Informática, del departamento de Seguridad Física y del departamento de Auditoría Interna, deben sopesar las ventajas y desventajas de una divulgación externa antes de reportar las infracciones.	Políticas Relacionadas: "Retención de la Información Sobre Violaciones y Problemas de Seguridad, '"Informes de Violaciones y Problemas,' e "Informes de Problemas"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
17. Reporte de Violaciones y Problemas a las Autoridades	Política: Cualquier evento potencialmente material debe ser reportado por la gerencia de Seguridad Informática al vicepresidente del departamento Legal y al vicepresidente del departamento de Finanzas, quienes deben decidir si la divulgación pública es necesaria y apropiada.	Políticas Relacionadas: “Reportes Externos de Violaciones”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
18. Divulgación de Ataques a Sistemas de Computación	Política: A menos que esté obligada por ley a publicar ataques contra sus sistemas o redes de computación, la Gobernación no debe reportar estos incidentes al público o a agencias gubernamentales.	Políticas Relacionadas: “Reportes Externos de Violaciones”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
19. Reportes de Brechas de Seguridad a Terceros	Política: Cualquier brecha en la seguridad de un computador de la Gobernación que exponga información privada o propiedad de terceros, debe ser comunicada inmediatamente a la parte afectada.	Políticas Relacionadas: “Reporte de Violaciones y Problemas a las Autoridades” y “Reportes Externos de Violaciones”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
20. Informes de Actividad No Autorizada	Política: Los usuarios de los sistemas informáticos de la Gobernación deben inmediatamente reportar a la gerencia de Seguridad Informática cualquier actividad no autorizada incluyendo, sin limitantes, la pérdida o cambios en los datos computarizados de producción y el uso cuestionable de archivos, bases de datos, o redes de comunicación.	Políticas Relacionadas: “Informe de Funcionamiento Incorrecto de Software,’ “Informes de Violaciones y Problemas,’ y “Reportes Centralizados de Problemas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
21. Reporte de Eventos Cuestionables	Política: Los usuarios de los sistemas informáticos de la Gobernación deben reportar inmediatamente al departamento de Seguridad Informática cualquier evento inusual o información sospechosa relativa a la seguridad informática incluyendo, sin limitantes, solicitudes inusuales de información de la Gobernación efectuadas por personas externas y la conducta atípica del sistema.	Políticas Relacionadas: “Investigaciones Policiacas o Legales” y “Solicitudes de Información Organizacional”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
22. Reporte de Problemas en Diseño	Política: Todos los problemas potencialmente serios asociados con sistemas informáticos en diseño o desarrollo, que no se han abordado adecuadamente por los proyectos existentes o planificados, deben ser reportados inmediatamente a la gerencia de Seguridad Informática.	Políticas Relacionadas: “Diseño de Controles de Seguridad Informática” y “Excepciones a las Políticas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
23. Contacto con las Autoridades Policiales	Política: Toda decisión sobre incidentes o problemas de seguridad informática que involucre o amerite contacto con las autoridades policíacas, debe ser tomada por un representante corporativo de la Gobernación.	Políticas Relacionadas: “Informes de Problemas” y “Responsabilidad en la Seguridad Informática”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
24. Investigación de Delito Computarizado	Política: Cada vez que se evidencie claramente que la Gobernación ha sido víctima de un delito de computación o de comunicación, se debe efectuar una investigación profunda que contenga suficiente información, de manera que la gerencia pueda tomar acciones para asegurarse que tales incidentes no vuelvan a ocurrir, y que se han restablecido medidas efectivas de seguridad.	Políticas Relacionadas: “Confidencialidad de la Información de las Investigaciones Internas”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
25. Investigaciones Prolongadas	Política: Las investigaciones prolongadas de brechas de seguridad se deben efectuar mientras el trabajador sospechoso esté suspendido sin paga, y la razón de la suspensión sin paga no debe ser divulgada a los compañeros de trabajo sin el expreso permiso del director de Seguridad.	Políticas Relacionadas: “Responsabilidades en el Manejo de Incidentes” e “Informes de Incidentes”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
26. Distintivos de Acceso Extraviados	Política: Todo dispositivo de acceso faltante incluyendo, sin limitantes, distintivos de identificación, tarjetas de acceso físico, tarjetas inteligentes con contraseñas dinámicas y tarjetas telefónicas, que esté extraviado o no sea localizable, se debe reportar inmediatamente al departamento de Seguridad Física.	Políticas Relacionadas: “Uso de Tarjetas de Crédito” y “Credenciales Portátiles de Identificación”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
6.03.02 Reporte de Debilidades en la Seguridad				
1. Informe de Vulnerabilidades del Sistema	Política: Los usuarios deben reportar con prontitud todos los alertas de seguridad informática, las advertencias y sospechas de vulnerabilidades al Centro de Atención al Usuario de Sistemas Informáticos, y no deben compartir dicha información con personas internas o externas.	Políticas Relacionadas: “Equipo de Respuesta Ante Emergencias Computacionales”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
2. Condiciones de Interrupción	Política: Los trabajadores deben notificar a la gerencia con prontitud de todas las condiciones que pudieran llevar a una interrupción de las actividades del negocio.	Políticas Relacionadas: “Expectativas sobre el Empleado Durante la Restauración de las Actividades del Negocio” y “Sistema de Alerta de Seguridad Informática”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
3. Reportes Centralizados de Problemas	Política: Todas las vulnerabilidades conocidas e infracciones sospechadas o conocidas deben ser comunicadas de manera expedita y confidencial al departamento de Seguridad Informática, y las divulgaciones no autorizadas de información de la Gobernación deben adicionalmente ser reportadas al Propietario correspondiente de la información.	Políticas Relacionadas: “Daño y Pérdida de Sistemas Fuera de Sede” y “Conflictos Legales”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
4. Discusiones Sobre Debilidades y Vulnerabilidades en la Seguridad	Política: Los trabajadores que descubran debilidades o vulnerabilidades en las medidas de seguridad utilizadas por la Gobernación, no deben discutirlas con personas ajenas a la gerencia de Seguridad Informática, la gerencia de Auditoría Interna o los investigadores designados por uno de estos dos gerentes.	Políticas Relacionadas: “Reportes de Brechas de Seguridad a Terceros”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
5. Reporte de Vulnerabilidades en la Seguridad	Política: Cuando se descubra una vulnerabilidad nueva y seria en la seguridad de los sistemas informáticos, asociada con el hardware o software de un proveedor en particular, la vulnerabilidad debe ser inmediatamente reportada al foro público apropiado para lograr su diseminación pública.	Políticas Relacionadas: “Divulgación de Vulnerabilidades” y “Reportes Externos de Violaciones”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
6.03.03 Reporte de Fallas en el Software				
1. Notificación de Falla en los Controles de la Integridad	Política: Si fallan los controles que aseguran la integridad de la información, si se sospecha de fallas en estos controles o si los controles no están disponibles, la gerencia debe ser notificada de estos hechos cada vez que se obtenga la información correspondiente.	Políticas Relacionadas: “Responsabilidad en la Seguridad Informática”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Divulgación de Vulnerabilidades	Política: Los trabajadores deben otorgar al proveedor un tiempo razonable para arreglar cualquier problema serio de vulnerabilidad en el sistema descubierto en la Gobernación, antes de hacer pública cualquier información sobre dicho problema.	Políticas Relacionadas: “Reportes Centralizados de Problemas” y “Discusiones Sobre Debilidades y Vulnerabilidades en la Seguridad”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
3. Informe de Sospecha de Virus	Política: Los trabajadores que sospechen de la existencia de un virus en el computador y lo reporten al departamento de Seguridad Informática inmediatamente después de descubierto, no deben ser castigados a menos que el trabajador conscientemente haya causado la introducción del virus en los sistemas de la Gobernación.	Políticas Relacionadas: "Exploración del Software, '"Informes de Violaciones y Problemas,' y "Erradicación de Virus de Computadores"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
4. Informe de Funcionamiento Incorrecto de Software	Política: Todo funcionamiento aparentemente incorrecto del software debe ser inmediatamente reportado a la gerencia de línea o al proveedor de servicios de sistemas informáticos.	Políticas Relacionadas: "Informe de Sospecha de Virus"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
6.03.04 Aprendizaje de Incidentes				
1. Análisis de Violaciones y Problemas	Política: El departamento de Seguridad Informática debe preparar un análisis anual de los problemas y violaciones reportados en seguridad informática.	Políticas Relacionadas: "Investigación de Delito Computarizado" y "Retención de la Información Sobre Violaciones y Problemas de Seguridad"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
6.03.05 Proceso Disciplinario				
1. Consecuencias de Incumplimiento	Política: El incumplimiento de las políticas, normas o procedimientos de seguridad informática es causa de acciones disciplinarias que pueden llegar hasta el despido.	Políticas Relacionadas: "Consecuencias de las Violaciones"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
2. Consecuencias de las Violaciones	Política: Suponiendo que las acciones son incidentales o accidentales, la primera infracción de seguridad informática debe generar una advertencia, la segunda vez por el mismo motivo debe generar una carta para incluirla en el archivo personal del trabajador correspondiente; la tercera infracción por el mismo asunto implica suspensión por cinco días sin paga; la cuarta vez por el mismo motivo deben ser despedidos y las infracciones premeditadas o intencionales, independientemente de la cantidad, deben generar una acción disciplinaria que puede incluir el despido inmediato.	Políticas Relacionadas: "Consecuencias de Incumplimiento"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
3. Pérdida de Opciones en Valores	Política: Si el receptor de opciones en valores divulga información interna de la Gobernación a personas no autorizadas, dichas opciones deben ser revocadas.	Políticas Relacionadas: "Consecuencias de Incumplimiento" y "Despidos Inmediatos"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
4. Despidos Inmediatos	Política: A menos que se obtenga un permiso especial de un vicepresidente ejecutivo, todos los trabajadores que hayan robado propiedad de la Gobernación, o que actúen con insubordinación, o que hayan sido convictos de un delito, deben ser despedidos inmediatamente, acompañados mientras recogen sus pertenencias personales y escoltados fuera de las instalaciones de la Gobernación.	Políticas Relacionadas: “Consecuencias de las Violaciones”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
5. Despidos Bajo Coacción	Política: Los computadores personales utilizados por el trabajador despedido bajo coacción deben ser inmediatamente aislados tanto de Internet como de la red interna de la Gobernación, se deben reformatear sus discos duros y se debe reinstalar el sistema correspondiente de software.	Políticas Relacionadas: “Base de Datos Centralizada de Controles de Acceso” y “Manejo de Despidos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Políticas de Seguridad Física

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
7 SEGURIDAD FÍSICA Y AMBIENTAL				
7.01 Áreas Seguras				
7.01.01 Perímetro de Seguridad Física				
1. Acceso Físico para Terceros	Política: El acceso de visitantes o terceros a las oficinas de la Gobernación, o salones de computación y otras áreas de trabajo que contengan información confidencial, debe ser controlado por guardias, recepcionistas u otro personal.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones, ' y "Control de Acceso Físico a la Información Sensible"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
2. Plan de Seguridad Física	Política: Todo centro de datos de la Gobernación debe tener un plan de seguridad física que debe ser revisado y actualizado anualmente por el gerente a cargo de las instalaciones.	Políticas Relacionadas: "Lógica Crítica de Negocios" y "Planes de Respuesta Ante Emergencias Computacionales"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
3. Ubicación del Centro de Computación y Comunicaciones	Política: Los computadores multiusuario y las instalaciones de comunicaciones deben estar ubicados más arriba de un primer piso, alejados de cocinas y en una ubicación separada de las paredes exteriores del edificio mediante una pared interna, en un salón sin ventanas.	Políticas Relacionadas: "Posiciones de las Pantallas de los Computadores" y "Ubicaciones de Centros de Computación"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
4. Resistencia al Fuego de Centros de Computación	Política: Debe haber paredes cortafuego alrededor de los centros de computación, las cuales deben ser resistentes al fuego por lo menos durante una hora y todas las salidas de dichas paredes, tales como las puertas y los ductos de ventilación, deben cerrarse automáticamente y ser resistentes al fuego por lo menos durante una hora.	Políticas Relacionadas: "Fumar, Comer y Beber"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
5. Solidez de las Puertas de Centros de Computación	Política: Los salones de los centros de computación deben estar equipados con puertas antimotines, puertas resistentes al fuego y cualquier otra puerta resistente a entradas forzadas.	Políticas Relacionadas: "Resistencia al Fuego de Centros de Computación" y "Cierre de Puertas en Centros de Computación"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Cierre de Puertas en Centros de Computación	Política: Los salones de las instalaciones de computación deben estar equipados con puertas que se cierren inmediatamente después de ser abiertas, y con una alarma sonora que se dispare cuando han estado abiertas más allá de un cierto tiempo.	Políticas Relacionadas: "Resistencia al Fuego de Centros de Computación" y "Solidez de las Puertas de Centros de Computación"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
7. Puertas Adicionales de Acceso al Centro de Computación	Política: Todas las puertas adicionales de un centro de computación deben estar equipadas con barras de choque que activen una alarma al abrirse.	Políticas Relacionadas: "Control de Acceso Físico a la Información Sensible" y "Áreas Desatendidas"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
7.01.02 Controles Físicos de las Entradas				
1. Control de Acceso Físico a la Información Sensible	Política: El acceso a toda oficina, sala de computación y área de trabajo que contenga información sensible debe ser físicamente restringido para limitar el acceso a aquéllos que necesitan la información.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,' y "Acceso Físico de Trabajadores Cesados"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
2. Cierre de Oficinas Personales	Política: Todos los trabajadores con oficinas propias separadas deben cerrar sus puertas con llave cuando las oficinas no estén en uso.	Políticas Relacionadas: "Control de Acceso Físico a la Información Sensible"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
3. Distintivos de Identificación	Política: Mientras se encuentren dentro de las instalaciones o edificios seguros de la Gobernación, las personas deben portar sus dispositivos de identificación de tal manera que la foto y la información sean claramente visibles.	Políticas Relacionadas: "Personas Sin Distintivos de Identificación"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
4. Distintivos Temporales	Política: Los trabajadores que hayan olvidado traer sus distintivos de identificación deben obtener un distintivo temporal válido por un día, a cambio de su licencia de conducir o cualquier otra identificación con foto.	Políticas Relacionadas: "Iniciación de Transacciones en Computadores" y "Reportes de Distintivos de Identificación"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
5. Acceso Controlado con Distintivos	Política: Toda persona debe presentar su distintivo al lector de distintivos antes de entrar por cualquier puerta controlada, dentro de las instalaciones de la Gobernación.	Políticas Relacionadas: "Distintivos de Acceso Compartidos"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Distintivos de Acceso Compartidos	Política: Los trabajadores no deben permitir a personas desconocidas o no autorizadas pasar por puertas, rejas u otras entradas a áreas restringidas al mismo tiempo que las personas autorizadas.	Políticas Relacionadas: “Personas Sin Distintivos de Identificación” y “Acceso Controlado con Distintivos”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
7. Entradas Individuales	Política: Todas las entradas de tráfico peatonal a todos los centros de datos de la Gobernación deben tener mecanismos de trampas humanas.	Políticas Relacionadas: “Acceso Físico para Terceros” y “Etiquetas Anti-Robo”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
8. Intentos No Autorizados de Acceso Físico	Política: Los trabajadores no deben intentar entrar en áreas restringidas de la Gobernación para las que no han sido autorizados.	Políticas Relacionadas: “Prueba de los Controles del Sistema Informático”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
9. Inspección de Bolsos	Política: Todos los maletines, maletas, carteras y demás equipajes deben ser abiertos para que los guardias de la Gobernación los revisen al momento de salir las personas de las instalaciones.	Políticas Relacionadas: “Pases de Propiedad” e “Información Secreta Fuera de Oficinas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos
10. Registros del Sistema de Control de Acceso	Política: El departamento de Seguridad debe mantener registros de las personas que están y han estado dentro de los edificios de la Gobernación, y guardar esta información en sitio seguro por lo menos durante tres meses.	Políticas Relacionadas: “Período de Retención de Registros” y “Reportes de Distintivos de Identificación”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
11. Acceso Físico de Trabajadores Cesados	Política: Cuando el trabajador finaliza su relación de trabajo con la Gobernación, todos los códigos de seguridad para el acceso físico conocidos o disponibles al trabajador, deben ser desactivados o cambiados.	Políticas Relacionadas: “Separación de Actividades y Datos,’ “Devolución de Propiedad al Cesar Empleo, ’“Transferencias de Trabajadores,’ e “Informe de Cambios en Situación de Empleados”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
12. Acceso de Trabajadores Cesados a Areas Restringidas	Política: Cuando un trabajador termina su relación de trabajo con la Gobernación, todos los derechos de acceso a las áreas restringidas de la Gobernación deben ser revocados inmediatamente.	Políticas Relacionadas: “Acceso Físico de Trabajadores Cesados” y “Restricción de Privilegios — Necesidad de Conocer”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
13. Lista de Otorgantes de Acceso Físico	Política: La lista de gerentes autorizados para otorgar permiso de acceso a las instalaciones de la Gobernación se debe mantener al día y debe ser revisada periódicamente por los gerentes superiores que hayan delegado esa autoridad al gerente correspondiente.	Políticas Relacionadas: "Otorgamiento de Privilegios del Sistema,' "Autorización para Transacciones de Producción,' y "Reportes de Distintivos de Identificación"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
14. Reportes de Distintivos de Identificación	Política: Una lista mensual de todas las personas de cada departamento que actualmente tienen distintivos de identificación autorizados, debe ser enviada a los jefes de departamento para su revisión y el inicio de alguna acción correctiva.	Políticas Relacionadas: "Lista de Otorgantes de Acceso Físico,' "Reautorización de los Privilegios de Acceso de Usuario,' y "Acceso a la Información Secreta"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
15. Identificación de Visitantes	Política: Todos los visitantes de la Gobernación deben mostrar una identificación con foto y firmar un registro antes de entrar.	Políticas Relacionadas: "Escolta de Visitantes, '"Distintivos de Acceso Compartidos,' e "Identificación Positiva para Uso del Sistema"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
16. Escolta de Visitantes	Política: Los visitantes a las oficinas de la Gobernación incluyendo, sin limitantes, clientes, ex-empleados, familiares de trabajadores, contratistas de reparación de equipos, personal de correo de la compañía y policías, deben permanecer escoltados todo el tiempo por un trabajador autorizado.	Políticas Relacionadas: "Distintivos de Acceso Compartidos,' "Supervisión de Terceros,' e "Identificación de Visitantes"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Medianos y altos
17. Escoltas Obligatorios para Todos los Visitantes en Horas No Hábiles	Política: Los visitantes deben ser escoltados por un empleado autorizado por un gerente departamental, cuando se encuentren en las oficinas o instalaciones de la Gobernación fuera del horario normal del negocio.	Políticas Relacionadas: "Despidos Inmediatos" y "Visitantes sin Escolta"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
18. Supervisión de Terceros	Política: Los individuos que no sean empleados, contratistas o consultores autorizados deben estar bajo supervisión mientras estén dentro de áreas que contengan información sensible de la Gobernación.	Políticas Relacionadas: "Escolta de Visitantes" y "Personas Sin Distintivos de Identificación"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
19. Personas Sin Distintivos de Identificación	Política: Los individuos que no porten distintivo de identificación de la Gobernación en sitio visible deben ser interrogados sobre el mismo, y si no pueden producirlo inmediatamente deben ser escoltados hasta la recepción.	Políticas Relacionadas: "Visitantes sin Escolta" y "Distintivos Temporales"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
20. Visitantes sin Escolta	Política: Cuando un trabajador se percate de la presencia de un visitante sin escolta dentro de las área restringidas de la Gobernación, debe interrogarlo acerca de su visita a dicha área, y luego escoltarlo hasta la recepción, hasta un guardia de seguridad o hasta la persona a quien viene a visitar.	Políticas Relacionadas: "Distintivos de Acceso Compartidos,' "Escolta de Visitantes,' y "Distintivos de Identificación"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Medianos y altos
21. Visitantes al Centro de Datos y al Departamento de Sistemas Informáticos	Política: Los visitantes que no tengan que efectuar reparaciones a equipos de la Gobernación, o que no necesiten estar dentro del Centro de Datos o el departamento de Sistemas Informáticos, no deben entrar en dichas áreas.	Políticas Relacionadas: "Visitantes sin Escolta" y "Escoltas Obligatorios para Todos los Visitantes en Horas No Hábiles"	Política Dirigida a:Todos	Ambientes de Seguridad: Altos
22. Acceso a Sistemas de Computación y Comunicación	Política: Los edificios que contengan sistemas de computadores o de comunicaciones de la Gobernación, deben estar protegidos con medidas de seguridad física que impidan el acceso a personas no autorizadas.	Políticas Relacionadas: "Acceso Físico para Terceros" y "Seguridad de la Información Sensible"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
23. Aseguramiento de Actividades de Manejo de Información Sensible o Crítica	Política: Todas las actividades de manejo de información crítica o sensible de la Gobernación, se deben efectuar en áreas físicamente seguras y protegidas contra accesos no autorizados, interferencias y daños.	Políticas Relacionadas: "Acceso a Sistemas de Computación y Comunicación" e "Información Secreta Fuera de Oficinas"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
24. Acceso al Centro de Computación	Política: Los programadores, los usuarios y otros que no tengan necesidades de negocio para tal acceso, no deben entrar a los centros de computación.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer,' "Separación de Tareas, '"Cambios en Producción,' y "Acceso a Librerías de Medios"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
25. Acceso del Personal al Centro de Computación	Política: El gerente de Operaciones Computarizadas debe mantener una lista revisada y actualizada por lo menos cada tres meses, del personal con acceso al centro de computación.	Políticas Relacionadas: “Acceso al Centro de Computación” y “Acceso a Sistemas de Computación y Comunicación”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
26. Acceso a Librerías de Medios	Política: Las bibliotecas de cintas magnéticas, discos y documentación deben estar restringidas a los trabajadores cuya responsabilidad exige su presencia en dichas áreas.	Políticas Relacionadas: “Separación de Tareas” y “Acceso al Centro de Computación”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
27. Visitas a las Instalaciones de Computación	Política: No deben hacerse visitas públicas de las instalaciones de los principales centros de computación y comunicaciones.	Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer,’ “Señalización de Centros de Computación y Comunicaciones” y “Distintivos de Identificación”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
7.01.03 Aseguramiento de Oficinas, Salones e Instalaciones				
1. Limpieza Periódica para Evitar Equipos de Espionaje	Política: El gerente del departamento de Telecomunicaciones debe iniciar y supervisar barridos periódicos para detectar micrófonos ocultos no autorizados, intercepciones y equipos de grabación en las oficinas y las instalaciones de la Gobernación, donde se discute, se almacena o se maneja información secreta.	Políticas Relacionadas: “Conversaciones Telefónicas Sobre Información Sensible” y “Cifrado de Contraseñas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
2. Aseguramiento de los Sistemas de Computación o Comunicación	Política: Todos los equipos multiusuario de computación y de comunicaciones deben estar ubicados en salones cerrados con llave.	Políticas Relacionadas: “Gabinetes Metálicos con Cerradura” y “Aislamiento de Equipos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Aseguramiento de Puertas Abiertas de Par en Par en Centros de Computación	Política: Cada vez que sea necesario mantener abiertas de par en par las puertas del centro de computación, la entrada debe estar continuamente monitoreada por un empleado o un guardia del departamento de Seguridad Física.	Políticas Relacionadas: “Pases de Propiedad” y “Acceso al Centro de Computación”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
4. Equipos en Áreas de Información Secreta	Política: Los equipos de impresión, de copiado y de fax no deben estar ubicados en las zonas físicamente aisladas dentro de las oficinas de la Gobernación que contengan información secreta.	Políticas Relacionadas: “Estaciones de Trabajo Sin Discos” y “Operadores de Entrada de Datos”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Altos
5. Señalización de Centros de Computación y Comunicaciones	Política: No debe haber señalización que indique la ubicación de los centros de computación o de comunicaciones.	Políticas Relacionadas: “Visitas a las Instalaciones de Computación”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
7.01.04 Trabajo en Áreas Seguras				
1. Presencia del Personal del Centro de Computación	Política: El centro principal de computación debe tener personal técnico competente asignado todo el tiempo, las 24 horas del día, los siete días de la semana y los 365 días del año.	Políticas Relacionadas: “Problemas por Accesos No Autorizados”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
2. Uso de Teléfonos Celulares	Política: No deben utilizarse teléfonos celulares dentro de las salas de computación de la Gobernación.	Políticas Relacionadas: “Teléfonos Celulares o Inalámbricos” y “Pases de Propiedad”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
3. Trabajo en Areas Restringidas	Política: Los trabajadores nunca deben trabajar solos en áreas restringidas que contengan información sensible.	Políticas Relacionadas: “Separación de Tareas” y “Horario de Áreas Restringidas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
4. Horario de Areas Restringidas	Política: Los trabajadores autorizados no deben entrar a las instalaciones de la Gobernación donde se maneje información sensible, crítica o valiosa, fuera de las horas de acceso autorizadas.	Políticas Relacionadas: “Separación de Tareas” y “Trabajo en Areas Restringidas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos
5. Areas de Equipos Vacías	Política: Todas las áreas desocupadas que contengan equipos de sistemas informáticos, deben permanecer cerradas con llave e inspeccionarse periódicamente a través de un sistema de monitor remoto o por un guardia de seguridad.	Políticas Relacionadas: “Acceso al Centro de Computación”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Areas de Equipos de Comunicaciones	Política: Las casetas telefónicas, las salas de enrutadores y concentradores de red, los espacios para el sistema de correo de voz y áreas similares que contengan equipos de comunicaciones deben mantenerse siempre cerrados con llave, y los visitantes no deben entrar sin la escolta proporcionada por el personal técnico autorizado para monitorear todo el trabajo que se esté efectuando.	Políticas Relacionadas: “Puertos de Red en Oficinas Vacías” y “Entregas al Centro de Computación”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Altos
7. Equipos de Grabación de Audio o Video	Política: Las cámaras y los equipos de grabación de audio o de video propios, no deben usarse o estar disponibles dentro de los perímetros controlados de las oficinas de la Gobernación.	Políticas Relacionadas: “Prevención del Copiado de Documentos Sensibles” y “Posiciones de las Pantallas de los Computadores”	Política Dirigida a:Todos	Ambientes de Seguridad: Altos
7.01.05 Areas Aisladas de Carga y Descarga				
1. Entregas al Centro de Computación	Política: Se debe utilizar un área intermedia segura de almacenamiento para guardar los suministros de materiales de computación, equipos y otros materiales entregados.	Políticas Relacionadas: “Mal Funcionamiento del Control de Acceso”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
7.02 Seguridad de los Equipos				
7.02.01 Ubicación y Protección de los Equipos				
1. Fumar, Comer y Beber	Política: Los trabajadores y visitantes deben abstenerse de fumar, comer o beber en el área de sobrepiso del salón de computación.	Políticas Relacionadas: “Control de Acceso Físico a la Información Sensible” y “Resistencia al Fuego de Centros de Computación”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
2. Ubicación de Sistemas de Computación de Producción	Política: Todos los sistemas computarizados de producción incluyendo, sin limitantes, servidores, cortafuegos, concentradores, enrutadores y sistemas de correo de voz deben estar ubicados físicamente dentro de un centro de datos seguro.	Políticas Relacionadas: “Aseguramiento de Actividades de Manejo de Información Sensible o Crítica” y “Ubicaciones de Centros de Computación”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
3. Dirección de los Centros de Computación	Política: La dirección física de todos los centros de computación de la Gobernación es confidencial y no debe ser divulgada a aquéllos que no tengan la necesidad demostrable de conocerla.	Políticas Relacionadas: “Naturaleza y Ubicación de la Información de la Organización”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
4. Controles Ambientales del Centro de Computación	Política: La gerencia local debe suministrar y mantener adecuadamente los sistemas de prevención y supresión de incendios, aire acondicionado, control de humedad y otros sistemas de protección de ambientes computarizados, en todos los centros de computación de la Gobernación.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Equipo de Protección Eléctrica"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
5. Protección Contra Electricidad Estática	Política: Si las condiciones del tiempo y del edificio presentan riesgo de descarga de electricidad estática, todos los computadores personales y estaciones de trabajo deben ser provistos de equipos con protección antiestática aprobados por el departamento de Sistemas Informáticos.	Políticas Relacionadas: "Equipo de Protección Eléctrica"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
6. Dispersión de Sistemas Computacionales	Política: Los sistemas de computación y de comunicaciones deben estar geográficamente dispersos siempre que sea posible, si esto no perturba indebidamente el funcionamiento operacional, ni pone en peligro la seguridad ni aumenta los costos.	Políticas Relacionadas: "Protección de la Información" y "Requerimientos para el Soporte de Emergencias y Desastres"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
7. Infraestructura de Respaldo para Centro de Datos	Política: La Gobernación debe dividir sus centros de procesamiento de datos en tres instalaciones distintas y físicamente aisladas, cada una capaz de manejar todos los servicios de los sistemas críticos de información de producción, y no deben compartir la misma subestación eléctrica de la compañía local, ni la misma central de la compañía telefónica.	Políticas Relacionadas: "Múltiples Operadoras Telefónicas" y "Punto Central de Falla de la Red"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
8. Sistemas de Computación Pertenecientes a Trabajadores	Política: Los trabajadores no deben traer a las instalaciones de la Gobernación sus propios computadores, periféricos o software, sin la debida autorización de sus jefes de departamento.	Políticas Relacionadas: "Pases de Propiedad" y "Procura de Hardware y Software"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
9. Llaves de las Estaciones de Trabajo	Política: Todas las estaciones de trabajo de escritorio de la Gobernación deben utilizar cierre con llave metálica para controlar el acceso de personas no autorizadas, reteniendo el gerente del departamento una copia de la llave.	Políticas Relacionadas: "Gabinetes de Archivo con Llave" y "Protección de la Reinicialización Basada en Contraseña"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
10. Puertas de Gabinetes de Equipos	Política: Todas las puertas de los estantes y gabinetes de equipos de computación y comunicaciones ubicados en el centro de computación deben permanecer cerradas con llave, a menos que un técnico autorizado esté efectuando reparaciones, mantenimiento o alguna actividad de reconfiguración.	Políticas Relacionadas: “Gabinetes de Archivo con Llave” y “Requisitos de Seguridad para Teletrabajo”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
11. Sistemas Comerciales y Financieros en Internet	Política: Todos los servidores y equipos de comercio de Internet, así como los sistemas que procesen o faciliten el proceso de transferencias y otras actividades financieras, deben estar físicamente aislados y asegurados.	Políticas Relacionadas: “Aislamiento de Equipos” y “Aseguramiento de Actividades de Manejo de Información Sensible o Crítica”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
12. Aislamiento de Equipos	Política: Los equipos de computación y comunicaciones manejados por personal de la Gobernación, deben estar físicamente aislados de los equipos manejados por terceros.	Políticas Relacionadas: “Acceso a Sistemas de Computación y Comunicación,’ “Distintas Zonas de Riesgo de Incendio,’ y “Aseguramiento de los Sistemas de Computación o Comunicación”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
13. Ubicaciones de Centros de Computación	Política: Todos los centros nuevos de computación o de comunicación de la Gobernación, deben estar ubicados en un área donde exista baja probabilidad de desastres naturales, accidentes serios causados por el hombre, motines y otros problemas relacionados.	Políticas Relacionadas: “Proveedores Redundantes de Suministros Básicos” y “Ubicación del Centro de Computación y Comunicaciones”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
14. Construcción del Centro de Computación	Política: Los centros de computación y comunicación de la Gobernación, tanto nuevos como remodelados, se deben construir de manera tal que estén protegidos contra incendios, daños causados por agua, vandalismo y otras amenazas conocidas o que puedan ocurrir en las instalaciones correspondientes.	Políticas Relacionadas: “Normas de Implantación de Controles” y “Ubicaciones de Centros de Computación”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
15. Precauciones ante Daños por Agua	Política: Todos los locales de la Gobernación que albergan equipos de computación y comunicación deben cumplir los requerimientos mínimos de prevención contra daños por agua y las precauciones mínimas de alarma establecidas por el departamento de Seguridad Informática, ubicándolos por encima de la planta baja y del nivel de inundaciones de desagües y ríos cercanos, con un sistema de drenaje adecuado y no ubicados debajo de tanques de agua o tuberías de agua.	Políticas Relacionadas: "Presencia del Personal del Centro de Computación" y "Alarmas del Centro de Computación"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
16. Alarmas del Centro de Computación	Política: Todos los centros de computación de la Gobernación deben estar equipados con sistemas de alarma contra incendios, agua e intrusión física que automáticamente alerten a aquéllos en capacidad de tomar medidas inmediatas.	Políticas Relacionadas: "Pases de Propiedad" y "Sistemas de Detección de Intrusos"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
7.02.02 Suministro Eléctrico				
1. Equipo de Protección Eléctrica	Política: Todos los computadores personales y estaciones de trabajo deben estar equipados con sistemas que suplan corriente eléctrica sin interrupciones, filtros de potencia eléctrica o supresores de alzas de voltaje aprobados por el departamento de Sistemas Informáticos.	Políticas Relacionadas: "Protección Contra Electricidad Estática"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
2. Proveedores Redundantes de Suministros Básicos	Política: Todos los nuevos centros de computación y de comunicaciones de la Gobernación deben estar ubicados de tal forma que tengan acceso a dos compañías suplidoras de energía eléctrica y dos compañías de teléfonos.	Políticas Relacionadas: "Ubicaciones de Centros de Computación"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
7.02.03 Seguridad en el Tendido de Cables				
1. Cables Eléctricos y de Telecomunicaciones	Política: La instalación y el mantenimiento de los cables de electricidad y de telecomunicaciones deben ser efectuados por un diseñador certificado de distribución de comunicaciones, que cumpla las normas establecidas de seguridad de la industria.	Políticas Relacionadas: "Cambios en la Línea de Comunicación" y "Registro de Línea de Modem"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
7.02.04 Mantenimiento de Equipos				
1. Productos de Sistemas Informáticos	Política: Todos los productos de hardware y software se deben registrar con su proveedor correspondiente inmediatamente después de que el personal de la Gobernación reciba los productos nuevos o actualizados del sistema informático, o tan pronto se determine que los productos no se han registrado todavía.	Políticas Relacionadas: “Duplicación de Software” y “Copias de Software”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
2. Mantenimiento Preventivo	Política: Debe ejecutarse regularmente el mantenimiento preventivo de todos los sistemas de computación y comunicación.	Políticas Relacionadas: “Niveles de Soporte de Interrupción del Negocio” y “Mantenimiento de Equipos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Mantenimiento de Equipos	Política: Todos los equipos de los sistemas informáticos utilizados en el proceso de producción, deben conservarse de acuerdo a las especificaciones e intervalos de servicio recomendadas por el proveedor, con reparaciones y servicios ejecutados solamente por personal de mantenimiento calificado y autorizado.	Políticas Relacionadas: “Mantenimiento Preventivo”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
4. Retención de Hardware y Software	Política: El hardware y software requeridos para leer los medios de almacenamiento de datos en los archivos de la Gobernación deben estar a la mano, correctamente configurados y mantenidos en condiciones operativas.	Políticas Relacionadas: “Pruebas de Medios de Almacenamiento de Archivos” y “Versiones de Software para Firmas Digitales y Cifrado de Archivos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5. Modificaciones a Computadores	Política: Los equipos de computación suministrados por la Gobernación no deben alterarse de ninguna manera ni añadírseles nada, sin el conocimiento y autorización de la gerencia del departamento.	Políticas Relacionadas: “Equipo de Teletrabajo” y “Computadores Portátiles con Información Sensible”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
7.02.05 Seguridad de Equipos Fuera de las Oficinas				
1. Autorización de Uso de Equipo Fuera de Sede	Política: La gerencia debe autorizar el uso de equipos de la Gobernación fuera del área de la empresa.	Políticas Relacionadas: “Remoción de Información Sensible” y “Requisitos de Seguridad para Teletrabajo”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
7.02.06 Disposición Segura o Re-Utilización de Equipos				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Liberación de Componentes Usados	Política: Seguridad Informática debe certificar que toda la información sensible ha sido removida de cualquier componente del sistema informático utilizado para los negocios de la Gobernación, antes de entregar los componentes a terceros.	Políticas Relacionadas: "Procura de Hardware y Software" y "Transferencia de Información Sensible"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
2. Disposición de Información y Equipos	Política: Los gerentes departamentales son responsables de la disposición de la propiedad sobrante que ya no se necesite para las actividades del negocio, en concordancia con los procedimientos establecidos por el departamento de Seguridad de Informática, incluyendo la remoción irreversible de información y software.	Políticas Relacionadas: "Transferencia de Información Sensible" y "Procedimientos para la Destrucción de la Información Sensible"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
7.03 Controles Generales				
7.03.01 Política sobre Pantallas y Escritorios Limpios				
1. Escritorios Limpios — Horas No Hábiles	Política: Fuera del horario normal de trabajo, todos los trabajadores deben despejar sus escritorios y áreas de trabajo, de tal manera que todos los datos valiosos o sensibles estén resguardados adecuadamente.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Escritorios Limpios — Uso Activo"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
2. Escritorios Limpios — Uso Activo	Política: A menos que la información esté siendo utilizada por personal autorizado, los escritorios deben mantenerse limpios y libres fuera del horario normal de trabajo, con toda la información bajo llave.	Políticas Relacionadas: "Escritorios Limpios — Horas No Hábiles"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
3. Manejo de Información en Otros Turnos	Política: La información sensible debe estar siempre bajo llave en contenedores cerrados autorizados para información sensible, y no debe ser desatendida en ninguna ubicación insegura durante el segundo o tercer turno.	Políticas Relacionadas: "Escritorios Limpios — Horas No Hábiles"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
4. Areas Desatendidas	Política: Cuando no esté en uso, la información sensible que se deje en un salón no vigilado, debe mantenerse bajo llave en contenedores apropiados.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Cubrir Información Sensible"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
5. Almacenamiento de Información Sensible	Política: Todas las copias impresas y todos los medios de computación que contengan información sensible que no esté siendo utilizada por trabajadores autorizados, o cuando no sea claramente visible en un área donde están trabajando personas autorizadas, deben guardarse bajo llave en archivadores, escritorios, caja fuerte u otro tipo de mobiliario.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" e "Información Sensible en Computadores Personales"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
6. Apagado de Computadores	Política: Con excepción de los computadores independientes colocados en áreas con controles estrictos de acceso físico, deben apagarse al final del día, a la hora de almuerzo, y al terminar una sesión, todos los computadores que hayan estado usándose para procesar información secreta.	Políticas Relacionadas: "Clasificaciones de Medios de Almacenamiento de Datos" y "Clasificación de Datos en Cuatro Categorías"	Política Dirigida a:Todos	Ambientes de Seguridad: Altos
7. Cubrir Información Sensible	Política: Todos los trabajadores que manejen información secreta, confidencial o privada de la Gobernación, deben ocultar esta información de personas no autorizadas que estén en los alrededores.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Areas Desatendidas,' "Comunicaciones Potencialmente Ofensivas,' y "Sesiones Activas Desatendidas"	Política Dirigida a:Todos	Ambientes de Seguridad: Altos
8. Gabinetes de Archivo con Llave	Política: Todos los trabajadores de oficina deben recibir archivadores con llave, donde todo el material sensible se debe guardar al retirarse los trabajadores de su escritorio, y una copia de la llave del gabinete debe ser entregada al gerente del departamento.	Políticas Relacionadas: "Llaves de las Estaciones de Trabajo,' "Escritorios Limpios — Uso Activo,' y "Requisitos de Seguridad para Teletrabajo"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
7.03.02 Remoción de Propiedades				
1. Pases de Propiedad	Política: A menos que tengan un pase autorizado, las máquinas de escribir, los teléfonos celulares, los computadores portátiles, el equipo de modem y todo lo relacionado con sistemas informáticos, no deben salir de las instalaciones de la Gobernación.	Políticas Relacionadas: "Acceso Físico para Terceros" y "Traslado de Equipos de Computación de Oficinas"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
2. Etiquetas Anti-Robo	Política: La información sensible de la Gobernación no se debe almacenar o cargar en ningún aparato de computación portátil, a menos que los aparatos porten una etiqueta electrónica de seguridad autorizada.	Políticas Relacionadas: "Viajes con Información Secreta" y "Remoción de Información Sensible en Papel"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
3. Traslado de Medios	Política: Todo medio de almacenamiento de computación que salga de la Gobernación debe estar acompañado de un pase autorizado, el cual debe registrarse en la recepción del edificio.	Políticas Relacionadas: “Pases de Propiedad” e “Inspección de Bolsos”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos

Políticas de Operaciones

Políticas de Control de Acceso

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
9 CONTROL DE ACCESO				
9.01 Requisitos para el Control de Acceso				
9.01.01 Política de Control de Acceso				
1. Actividades del Hacker	Política: Los trabajadores no deben utilizar los sistemas informáticos de la Gobernación para dedicarse a actividades de "hacking" incluyendo, sin limitantes, el acceder en forma no autorizada a cualesquiera otros sistemas informáticos, para dañar, alterar o irrumpir las operaciones de otros sistemas informáticos y capturar o de algún modo obtener las contraseñas, las claves de cifrado u otro mecanismo de control de acceso que permitan un acceso no autorizado.	Políticas Relacionadas: “Prueba de los Controles del Sistema Informático” y “Evidencia de Delito o Abuso Informático”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
2. Regulación del Software	Política: Todo el software instalado en los sistemas multiusuarios de la Gobernación, debe estar regulado por un sistema aprobado de control de acceso que controle la sesión de un usuario antes de entregar el control a otro software de aplicación.	Políticas Relacionadas: “Mal Funcionamiento del Control de Acceso” y “Autentificación del Usuario por el Sistema Operativo”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Control de Acceso Basado en Contraseña	Política: Cualquier sistema pequeño que maneje información bien sea crítica o sensible, debe utilizar una versión mantenida adecuadamente de un sistema de control de acceso basado en contraseñas.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,’ “Control de Acceso a Computadores de Red,’ y “Control de Acceso Físico a la Información Sensible”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
4. Acceso de Lectura a Información Sensible	Política: Los trabajadores que han sido autorizados para ver la información clasificada con un cierto nivel de sensibilidad, pueden acceder sólo a la información de ese nivel o a la de menor nivel de sensibilidad.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías”	Política Dirigida a:Todos	Ambientes de Seguridad: Altos
5. Acceso de Escritura a Información sensible	Política: Los trabajadores no deben trasladar la información clasificada con un cierto nivel de sensibilidad a un nivel de menor sensibilidad, a menos que esta acción forme parte de un proceso de degradación autorizado.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías”	Política Dirigida a:Todos	Ambientes de Seguridad: Altos
6. Permisos Predeterminados de Archivo	Política: Los permisos para el control de acceso de los archivos para todos los sistemas en red de la Gobernación, se deben establecer de forma predeterminada para que bloquee el acceso a los usuarios no autorizados.	Políticas Relacionadas: “Privilegios Predeterminados de Usuario,’ “Mal Funcionamiento del Control de Acceso,’ y “Restricción de Privilegios — Necesidad de Conocer”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
7. Mal Funcionamiento del Control de acceso	Política: Si un sistema de control de acceso de una computador o red no está funcionando de manera adecuada, debe negar de manera predeterminada los privilegios a los usuarios finales.	Políticas Relacionadas: “Capacidad de Acceso de Usuarios” y “Restricción de Privilegios — Necesidad de Conocer”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
8. Base de Datos Centralizada de Controles acceso	Política: Los registros no ambiguos, organizados y actualizados de todos los privilegios de acceso al sistema informático de producción, se deben mantener en una base de datos centralizada que esté en manos de la Administración de Seguridad Informática.	Políticas Relacionadas: “Cambios en Situación del Trabajador”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9. Software Intérprete de Líneas de Comando	Política: Se debe eliminar todo software de interpretación de líneas de comandos de aquellos computadores que no lo requieran, a fin de que realicen el procesamiento normal.	Políticas Relacionadas: “Software Innecesario” y “Computadores para Cortafuegos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
10. Burlado de los Controles de Acceso	Política: Los programadores y demás personal técnico deben abstenerse de instalar cualquier código que bloquee los mecanismos autorizados de control de acceso que se encuentran en los sistemas operativos o en los paquetes de control de acceso.	Políticas Relacionadas: “Autentificación del Usuario por el Sistema Operativo” y “Vías de Acceso en Software de Producción”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
11. Comprometer Mecanismos de Seguridad para los clientes	Política: No deben aceptarse las solicitudes de clientes que comprometan los mecanismos de seguridad de la Gobernación, salvo que el vicepresidente ejecutivo lo apruebe por escrito o la Gobernación se vea obligada a hacerlo por requisito de ley.	Políticas Relacionadas: “Código Fuente del Software de Penetración de Sistemas,’ “Vías de Acceso en Software de Producción,’ “Enunciados de la Integridad del Software,’ y “Prueba de los Controles del Sistema Informático”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
12. Restricciones a la Recopilación de la información	Política: Si la información sensible de la Gobernación se encuentra en un sistema de computación y si se permite a los usuarios solicitar esta información en parte o en su totalidad a través de instalaciones en línea, se deben establecer controles de acceso especiales para proteger la información, de modo que la serie de solicitudes de información permisibles no revelen de manera colectiva alguna información que esté restringida.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,’ “Información Estadística de los Registros de los Clientes,’ “Asignación de Etiquetas de Clasificación de Datos,’ y “Etiquetado de Clasificación Múltiple”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
13. Divulgación de la Información de terceros	Política: Los trabajadores de la Gobernación no deben divulgar ninguna información sensible que le haya sido confiada a través de terceros a otras terceras personas, salvo que la persona que originó la información haya dado su aprobación con antelación en lo referente a su divulgación, y que la parte que reciba dicha información haya firmado un acuerdo de confidencialidad.	Políticas Relacionadas: “Divulgación de Información Privada a Terceros,’ “Acuerdos de Confidencialidad,’ y “Solicitudes Externas de Información”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
14. Solicitudes de Información organizacional	Política: Todas las solicitudes de información sobre la Gobernación y sus actividades de negocios, incluyendo, sin limitantes, cuestionarios, sondeos y entrevistas periodísticas, deben ser referidas al departamento de Relaciones Públicas, a menos que la alta gerencia lo autorice.	Políticas Relacionadas: “Liberación de Información de la Organización,’ “Seguridad Informática Centralizada,’ y “Presentación de la Imagen Pública”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
15. Divulgación de Información de Negocios del Cliente	Política: Los trabajadores de la Gobernación no deben divulgar a ninguna persona ajena a la Gobernación la naturaleza de los proyectos del cliente, sus estrategias empresariales o sus relaciones comerciales.	Políticas Relacionadas: “Compartir Información de Mercadeo” y “Comunicaciones Públicas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
16. Compartir Información de Mercadeo	Política: No se debe divulgar jamás a la competencia información de mercadeo, incluyendo, sin limitaciones, precios, políticas de ventas, estrategias, planes, segmentos de mercado y otra información sobre el área de mercadeo.	Políticas Relacionadas: “Acuerdos de Confidencialidad con Antiguos Patronos” y “Renuncia de Empleados por la Competencia”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
17. Información Liberada al Público — Nombre del Contacto	Política: La información generada por la Gobernación y dada a la luz pública debe estar acompañada del nombre del integrante del personal designado para actuar como única fuente oficial reconocida y único contacto.	Políticas Relacionadas: “Aprobación de las Representaciones Públicas” y “Solicitudes Externas de Información”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
18. Información de Asuntos Legales	Política: No debe satisfacerse ninguna solicitud de información por parte de terceros relacionada con un caso legal actual, a menos que la solicitud sea efectuada por un organismo gubernamental autorizado.	Políticas Relacionadas: “Información Liberada al Público — Nombre del Contacto,’ “Uso del Nombre de la Organización,’ y “Solicitudes de Información Organizacional”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
19. Liberación de Información de la Organización	Política: Se debe obtener permiso previo de la gerencia principal de la Gobernación para divulgar cualquier información interna de la misma a los medios noticiosos o a otros terceros.	Políticas Relacionadas: “Solicitudes de Información Organizacional,’ “Presentación de la Imagen Pública,’ y “Entrega de Documentación de Sistemas”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
20. Ganancias o Productos Futuros	Política: Los empleados no deben hacer ningún tipo de representación pública sobre las ganancias a futuro de la Gobernación o las posibilidades que existan de nuevos productos.	Políticas Relacionadas: “Solicitudes de Información Organizacional” y “Comunicaciones Públicas”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
21. Solicitudes Externas de Información	Política: Todas las solicitudes de información interna provenientes de terceros que no tenga como origen el departamento de ventas, mercadeo o relaciones públicas, deben ser aprobadas por el Propietario de la información y el asesor legal corporativo, quienes contarán con un plazo de cinco días hábiles para evaluar los méritos de la solicitud.	Políticas Relacionadas: “Solicitudes de Información Organizacional”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
22. Información Sensible Controversial	Política: La información sensible y controversial de la Gobernación debe salir a la luz pública por entregas.	Políticas Relacionadas: “Presentación de la Imagen Pública” y “Solicitudes de Información Organizacional”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
23. Avisos Solicitando Empleados	Política: La gerencia de Recursos Humanos debe aprobar con antelación todos los avisos o anuncios públicos en los que se soliciten ayudantes, antes de su publicación.	Políticas Relacionadas: “Comunicaciones Públicas” y “Solicitudes Externas de Información”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
24. Información Liberada al Público — Autorización	Política: La gerencia debe revisar toda información a publicarse, de acuerdo con un proceso establecido y documentado.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Liberación de Información de la Organización”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
25. Comunicaciones Públicas	Política: Todo discurso, presentación, documento técnico, libro o comunicación a distribuirse al público debe contar con la autorización de publicación correspondiente emitida por el jefe inmediato del empleado involucrado.	Políticas Relacionadas: “Aprobación de las Representaciones Públicas” y “Liberación de Información de la Organización”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
26. Autorización de Divulgación de información	Política: La divulgación de cualquier archivo almacenado y todo mensaje enviado a través de la red de la Gobernación a terceros debe estar precedida de una revisión y una autorización por parte del director del departamento legal.	Políticas Relacionadas: “Información Liberada al Público — Autorización” y “Acuerdos de Confidencialidad — Organización”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
27. Naturaleza y Ubicación de la Información de la Organización	Política: La información relativa al origen y ubicación de la información sobre la Gobernación, por ejemplo la que se encuentra en un diccionario de datos, es confidencial y debe divulgarse únicamente a aquellas personas que tengan una necesidad demostrable de conocerla.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer,' "Atributos de la Integridad de la Información,' e "Inventario de Activos — Información"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
28. Exploración de Sistemas	Política: Los empleados no deben explorar los sistemas informáticos o redes de la Gobernación.	Políticas Relacionadas: "Errores y Manipulación de Registros"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
29. Madurez del Producto de Seguridad	Política: Los productos de seguridad con menos de un año en el mercado no deben emplearse como componentes integrales de cualquier sistema informático de producción crítico para la Gobernación.	Políticas Relacionadas: "Versiones de Sistemas Operativos,' "Herramientas y Técnicas de Desarrollo Maduras,' y "Arreglos de Seguridad"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
30. Creación de Herramientas de Seguridad	Política: Los desarrolladores y diseñadores de los sistemas internos de la Gobernación no deben crear nuevos protocolos de seguridad, componer nuevos esquemas de seguridad, desarrollar nuevos algoritmos de cifrado o, de modo alguno, volverse creativos en lo relativo a la seguridad informática.	Políticas Relacionadas: "Algoritmos de Cifrado Evaluados Públicamente" y "Algoritmo de Cifrado Normal e Implantación"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
31. Facilidad de Uso de los Controles de seguridad	Política: Todas las medidas de seguridad aplicadas a equipos de computación y de comunicaciones deben ser simples y de fácil uso, administración y auditoría.	Políticas Relacionadas: "Controles Mínimos en Sistemas Informáticos" y "Aceptación del Usuario de las Medidas de Seguridad Informática"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
32. Uso de Derechos en Sistemas Informáticos	Política: No deben utilizarse los derechos en sistemas informáticos para cualquier propósito empresarial de la Gobernación hasta obtener la autorización escrita del gerente de Seguridad Informática.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer" y "Dependencia de Mecanismos Comunes para los Controles"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
33. Sistemas de Seguridad Independientes	Política: La seguridad de un sistema de computadores jamás debe depender totalmente de la seguridad de otro sistema de computadores.	Políticas Relacionadas: "Pericia en Sistemas, '"Autentificación del Usuario por el Sistema Operativo,'y "Dependencia de Mecanismos Comunes para los Controles"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
34. Otorgamiento de Acceso a la Información de la Organización	Política: El acceso a la información de la Gobernación siempre debe estar autorizado por el Propietario designado de dicha información, y debe limitarse a aquellas personas que lo necesiten.	Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer,’ “Control de Acceso a Computadores de Red,’ y “Mal Funcionamiento del Control de Acceso”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
9.02 Administración del Acceso de Usuario				
9.02.01 Registro de Usuarios				
1. Identificadores de Usuarios Anónimos	Política: Los identificadores de usuario deben ser asignados en secuencia numérica, de modo que no exista una correlación evidente entre el identificador de usuario y su nombre.	Políticas Relacionadas: “Longitud Mínima de Contraseñas” y “Norma de Creación para Identificadores de Usuario”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Altos
2. Identificador de Usuario No Anónimo	Política: Todos los identificadores de usuario de los computadores y redes de la Gobernación deben construirse de conformidad con la norma de construcción de identificadores de usuario de la Gobernación, deben indicar claramente el nombre de la persona encargada y, en ninguna circunstancia, deben tales identificadores de usuario permitirse ser genéricos, descriptivos de un puesto o papel organizacional, descriptivos de un proyecto o anónimos.	Políticas Relacionadas: “Identidad del Recolector de Información Privada” e “Identidad en Internet”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Identificador Único de Usuario y Contraseña Obligatorios	Política: Todo usuario debe tener un identificador único y una contraseña personal secreta para acceder a los computadores multiusuario y las redes de la Gobernación.	Políticas Relacionadas: “Acceso a la Información Secreta,’ “Identificadores de Usuarios Anónimos, ’“Identificadores de Usuarios Únicos,’ “Contraseñas de Control de Acceso al Sistema,’ y “Contraseñas en Distintos Sistemas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Vencimiento de los Identificadores de Usuario para No Empleados	Política: Todo identificador de usuario establecido para un no empleado debe tener una fecha de vencimiento especificada, con vencimiento predeterminado de 30 días cuando no se conozca su vencimiento.	Políticas Relacionadas: “Privilegios de Identificadores de Usuarios Inactivos” y “Manejo de Despidos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5. Finiquito de los Privilegios de Acceso	Política: Todos los privilegios informáticos proporcionados por la Gobernación deben terminar cuando el trabajador cesa sus servicios a la misma.	Políticas Relacionadas: “Informe de Cambios en Situación de Empleados”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Vencimiento de los Identificadores de usuario	Política: Deben establecerse fechas de vencimiento para todos los identificadores de usuario almacenados en los sistemas multiusuario de la Gobernación, después de las cuales dichos identificadores quedarán inhabilitados. Los archivos correspondientes quedarán retenidos durante las siguientes dos semanas.	Políticas Relacionadas: "Vencimiento de Identificador de Usuario" y "Reautorización de los Privilegios de Acceso de Usuario"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
7. Identificadores de Usuarios Únicos	Política: Todo identificador de usuario en un computador y sistema de comunicación debe identificar de un modo particular a un solo usuario y no deben crearse o utilizarse identificadores de usuario grupales.	Políticas Relacionadas: "Identificador Único de Usuario y Contraseña Obligatorios" y "Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
8. Identificadores de Usuario Genéricos	Política: Los identificadores de usuario deben identificar de manera única a individuos específicos y no deben crearse o utilizarse identificadores genéricos basados en cargos o tareas.	Políticas Relacionadas: "Identificador Único de Usuario y Contraseña Obligatorios" y "Contraseñas de Control de Acceso al Sistema"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
9. Re-Utilización de Identificadores de usuario	Política: Todo identificador de usuario dentro del sistema de computadores y de comunicaciones de la Gobernación debe ser único, debe estar relacionado solamente con el usuario al cual se asignó y no debe ser reasignado luego de terminar la relación del empleado o cliente con la Gobernación.	Políticas Relacionadas: "Privilegios de Identificadores de Usuarios Inactivos" e "Identificadores de Usuarios Anónimos"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10. Norma de Creación para Identificadores de usuario	Política: Los identificadores de usuario de un trabajador de la Gobernación deben ser iguales en cada sistema de computación y deben cumplir las normas para el nombramiento de identificadores de usuario establecidas por el departamento de Tecnología Informática.	Políticas Relacionadas: "Mecanismo Único de Acceso,' "Identificador Único de Usuario y Contraseña Obligatorios,' "Base de Datos Maestra de Identificadores de Usuario,' e "Identificadores de Usuarios Anónimos"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
11. Múltiples Identificadores de Usuario	Política: Todos los empleados de la Gobernación deben utilizar por lo menos dos conjuntos distintos de identificadores de usuarios para dos tipos distintos de computadores, aquéllos conectados a Internet y aquéllos conectados a una red interna.	Políticas Relacionadas: "Norma de Creación para Identificadores de Usuario" e "Identificador Único de Usuario y Contraseña Obligatorios"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
12. Autorización de Solicitud de Acceso al sistema	Política: Todas las solicitudes de privilegios adicionales en los sistemas multiusuario o redes de la Gobernación deben ser presentadas mediante una planilla de solicitud de acceso al sistema debidamente llenada y autorizada por el jefe inmediato del usuario.	Políticas Relacionadas: "Formularios para Identificadores de Usuario" y "Otorgamiento de Acceso a la Información de la Organización"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
13. Privilegios de Identificadores de Usuarios Inactivos	Política: Después de 30 días de inactividad, deben revocarse automáticamente todos los privilegios de los identificadores de usuario.	Políticas Relacionadas: “Ultima Hora y Fecha de Inicio de Sesión”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
14. Formularios para Identificadores de usuario	Política: Los usuarios deben firmar tanto un acuerdo de confidencialidad como un convenio de seguridad del sistema informático antes de emitírseles el identificador de usuario que les permita acceder a los sistemas de la Gobernación.	Políticas Relacionadas: “Convenio de Cumplimiento”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
15. Informe de Cambios en Situación de Empleados	Política: La gerencia debe informar con prontitud todos los cambios significativos ocurridos en las tareas y condiciones laborales de los usuarios finales a los administradores de seguridad que manejen sus identificadores de usuario.	Políticas Relacionadas: “Acceso Físico de Trabajadores Cesados” y “Transferencia de Responsabilidad en Custodia”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
16. Cambios en Situación de Usuarios	Política: Todo usuario debe notificar a la Unidad de Administración de Sistemas de los cambios en su relación con la Gobernación.	Políticas Relacionadas: “Cambios en Situación del Trabajador” e “Informe de Cambios en Situación de Empleados”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
17. Transferencia de Responsabilidad en Custodia	Política: En el momento en que un trabajador deja su cargo en la Gobernación, su jefe inmediato debe revisar con prontitud los archivos y documentos guardados en el computador, con el fin de reasignar las tareas y delegar específicamente la responsabilidad de estos archivos que anteriormente estaban en manos del ex-trabajador.	Políticas Relacionadas: “Acceso Físico de Trabajadores Cesados” y “Propiedad de la Información”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
18. Eliminación de Archivos de Trabajador Cesado	Política: Salvo que el departamento de Operaciones Computarizadas haya recibido instrucciones al contrario, se deben depurar todos los archivos residentes en los directorios del usuario, cuatro semanas después de la salida permanente del empleado de la Gobernación.	Políticas Relacionadas: “Base de Datos Maestra de Identificadores de Usuario” y “Transferencia de Responsabilidad en Custodia”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
19. Vencimiento de Identificador de Usuario	Política: Se debe fijar a seis meses el vencimiento de los identificadores de usuario residentes en los computadores accesibles desde internet, contados a partir del momento de su establecimiento, con renovación cada seis meses.	Políticas Relacionadas: “Contraseñas Iniciales” y “Vencimiento de los Identificadores de Usuario”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
20. Autentificación para Cuentas Nuevas	Política: Cada vez que la Gobernación abra una nueva cuenta con un cliente, debe autentificar la identidad del cliente de manera definitiva.	Políticas Relacionadas: "Acceso a la Información Personal" y "Validación de la Identidad de Terceros"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
9.02.02 Administración de Privilegios				
1. Restricción de Privilegios — Necesidad de conocer	Política: Los privilegios en sistemas de computación y de comunicaciones de todos los usuarios, sistemas y programas deben restringirse de acuerdo con la necesidad de conocer.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Privilegios Especiales en Sistema,' "Otorgamiento de Acceso a la Información de la Organización,' "Naturaleza y Ubicación de la Información de la Organización,' "Restricción de Privilegios — Necesidad de Retener,' y "Acceso a Información Sensible o Valiosa"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Restricción de Privilegios — Necesidad de retener	Política: El acceso a los sistemas de computación y de comunicaciones de la Gobernación debe ser otorgado a todos los empleados, a menos que la gerencia a cargo de un sistema específico haya definido reglas específicas de control de acceso.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer,' "Naturaleza y Ubicación de la Información de la Organización,' y "Acceso a Información Sensible o Valiosa"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
3. Usuarios Especiales Privilegiados	Política: Todos los sistemas de redes y de computadores multiusuario deben soportar un tipo especial de identificador de usuario que cuente con privilegios ampliamente definidos que habiliten a personas autorizadas para modificar la condición de seguridad del sistema.	Políticas Relacionadas: "Privilegios Predeterminados de Usuario"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
4. Privilegios Especiales en Sistema	Política: Los privilegios especiales en sistemas, tales como la capacidad para examinar los archivos de otros usuarios, deben limitarse a aquellos que están encargados directamente de la administración o seguridad de los sistemas, y sólo deben otorgarse a aquéllos que hayan asistido a una sesión autorizada de adiestramiento como administrador de sistemas.	Políticas Relacionadas: "Cantidad de Identificadores de Usuarios Privilegiados" y "Restricción de Privilegios — Necesidad de Conocer"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
5. Cantidad de Identificadores de Usuarios Privilegiados	Política: La cantidad de identificadores de usuarios privilegiados debe limitarse estrictamente a aquellas personas que necesariamente deban contar con dichos privilegios por razones autorizadas de negocios.	Políticas Relacionadas: "Privilegios Especiales en Sistema" y "Acceso a Comandos del Sistema Operativo"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Identificador de Usuario Administrador	Política: Los administradores de sistemas que manejan sistemas de computación con más de un usuario deben tener por lo menos dos identificadores de usuario, uno que le proporcione acceso privilegiado al sistema con su respectivo registro, y otro que le proporcione privilegios de un usuario normal, para efectuar su trabajo diario.	Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
7. Autorización de Identificador de Usuario y Privilegio	Política: Los identificadores de usuario, los privilegios de sistemas de aplicaciones de negocios y los privilegios de sistemas que superen las capacidades rutinariamente otorgadas a los usuarios, deben ser autorizados con antelación por, respectivamente, el supervisor inmediato del usuario, el Propietario de la información y el gerente del departamento de Soporte Técnico.	Políticas Relacionadas: “Propiedad de la Información” y “Privilegios Predeterminados de Usuario”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
8. Acceso a Comandos del Sistema Operativo	Política: No se debe permitir que los usuarios finales utilicen comandos a nivel de sistema operativo, mediante su limitación a los menús que muestran sólo aquellas funciones para las cuales han sido autorizados.	Políticas Relacionadas: “Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema” y “Cantidad de Identificadores de Usuarios Privilegiados”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
9. Actualización de Información de Producción	Política: Los privilegios en sistemas deben definirse de modo tal que el personal no relacionado con el área de producción, incluyendo entre otros a auditores internos, administradores de seguridad informática, programadores y operadores de computadores, no pueda actualizar la información de producción.	Políticas Relacionadas: “Autorización para Transacciones de Producción,’ “Administrador de Seguridad Designado,’ y “Modificación de Información por Internet”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
10. Base de Datos Maestra de Identificadores de Usuario	Política: Deben mantenerse registros actualizados que incluyan a todos los sistemas de computación donde los usuarios tengan identificadores de usuario.	Políticas Relacionadas: “Transferencia de Responsabilidad en Custodia” y “Norma de Creación para Identificadores de Usuario”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
11. Otorgamiento de Privilegios del Sistema	Política: Los privilegios del sistema de computación y del sistema de comunicaciones deben ser otorgados únicamente por una cadena definida de delegación de la autoridad.	Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer,’ “Acceso a Información Sensible o Valiosa,’ “Reportes de Distintivos de Identificación,’ y “Lista de Otorgantes de Acceso Físico”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
9.02.03 Gestión de Contraseñas de Usuario				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Contraseñas Iniciales	Política: Las contraseñas emitidas por el administrador de seguridad deben estar vencidas, obligando así al usuario a seleccionar otra contraseña antes de completar el procedimiento de inicio de sesión.	Políticas Relacionadas: “Estructura de las Contraseñas,’ “Contraseñas Proporcionadas por Proveedores,’ “Cambios Obligatorios de Contraseña,’ y “Códigos de Identificación para Soporte Técnico”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Transmisión de Contraseña Inicial	Política: La contraseña inicial de un nuevo usuario remoto debe enviarse a través de un canal de comunicaciones distinto al canal utilizado para tener acceso a los sistemas de la Gobernación, incluyendo, sin limitantes, el servicio de mensajería que requiera de firma y presentación en persona ante una oficina de un intermediario confiable, conjuntamente con identificación con fotografía.	Políticas Relacionadas: “Transmisión de Datos y Claves de Cifrado” y “Envío de Información Sensible”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Confirmación de Cambio de Contraseña Fija	Política: Todos las reinicializaciones o cambios de contraseñas fijas deben confirmarse con prontitud a través de correo regular, de modo que el usuario autorizado pueda rápidamente detectar y reportar cualquier conducta fraudulenta o abusiva.	Políticas Relacionadas: “Contraseñas Iniciales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Bajos y medianos
4. Envío de Contraseñas por Correo	Política: En caso de que sean enviadas por correo regular o por sistemas físicos de distribución similares, las contraseñas se deben enviar separadas de los identificadores de usuario, no deben tener marcas que indiquen el origen del envío y deben estar ocultas dentro de un sobre opaco que fácilmente revele si ha sido alterado.	Políticas Relacionadas: “Sistemas de Gestión de Claves de Cifrado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5. Contraseñas Fijas Olvidadas	Política: Todo usuario que olvide o pierda su contraseña debe registrarse nuevamente y recibir nuevo identificador de usuario y nueva contraseña.	Políticas Relacionadas: “Confirmación de Cambio de Contraseña Fija” y “Intentos de Introducir Contraseña”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Bajos y medianos
6. Reinicialización de la Contraseña Posterior a la Desactivación	Política: Todos los sistemas de computación de la Gobernación con contraseñas fijas deben estar configurados para permitir sólo tres intentos para introducir la contraseña correcta, luego de lo cual el identificador de usuario debe quedar desactivado, pudiendo reiniciarse solamente a través del personal del Centro de Atención al Usuario cuando el identificador de usuario haya sido autentificado.	Políticas Relacionadas: “Transmisión de Contraseña Inicial” y “Confirmación de Cambio de Contraseña Fija”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
7. Contraseñas en Software	Política: Las contraseñas nunca deben incorporarse al software desarrollado o modificado por los empleados de la Gobernación.	Políticas Relacionadas: “Sospecha de Divulgación de Contraseña”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
8. Cambios de Contraseña Luego de Estar Comprometido el Sistema	Política: Si un sistema multiusuario emplea contraseñas fijas como mecanismo primario de control de acceso, todas las contraseñas de dicho sistema deben ser cambiadas de inmediato al comprobarse que el sistema está comprometido, y todos los usuarios deben cambiar sus contraseñas fijas en los demás computadores, si usan esas mismas contraseñas.	Políticas Relacionadas: “Sospecha de Intrusión en los Sistemas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9. Cambio de Contraseña de Usuario Privilegiado Comprometida	Política: Si un intruso u otro usuario no autorizado ha comprometido una cuenta privilegiada, todas las contraseñas de ese sistema deben ser cambiadas de inmediato.	Políticas Relacionadas: “Cambios de Contraseña Luego de Estar Comprometido el Sistema” y “Cambios de Seguridad Después de Estar Comprometido el Sistema”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10. Autentificación de Contraseña en Persona	Política: El usuario debe ser autentificado en persona a fin de obtener una contraseña nueva o modificada.	Políticas Relacionadas: “Envío de Contraseñas por Correo,’ “Contraseñas Compartidas,’ “Contraseñas Iniciales,’ y “Códigos de Identificación para Soporte Técnico”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
11. Divulgación de Contraseñas	Política: Los administradores de seguridad deben divulgar las contraseñas a un usuario que suministre dos pruebas definitivas que comprueben su identidad, sólo si se le asigna un nuevo identificador de usuario, si el usuario involucrado ha olvidado o colocado erróneamente la contraseña, o si la desactivó sin querer.	Políticas Relacionadas: “Sospecha de Divulgación de Contraseña” y “Contraseñas Compartidas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
12. Identificación Positiva para Uso del sistema	Política: Todos los usuarios deben quedar identificados positivamente, antes de que puedan utilizar cualquier recurso de sistemas de computación multiusuario o de comunicaciones.	Políticas Relacionadas: “Mecanismo Único de Acceso”e “Identificación de Visitantes”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
9.02.04 Revisión de Derechos de Acceso del Usuario				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Reautorización de los Privilegios de Acceso de Usuario	Política: Los privilegios del sistema que otorga el jefe inmediato del usuario deben ser nuevamente evaluados cada tres meses, para determinar si necesitan los privilegios de sistema habilitados actualmente para realizar las tareas propias del trabajo que realiza el usuario.	Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer,’ “Vencimiento de los Identificadores de Usuario,’ y “Reportes de Distintivos de Identificación”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
9.03 Responsabilidades del Usuario				
9.03.01 Utilización de Contraseñas				
1. Estructura de las Contraseñas	Política: Los empleados no deben utilizar ninguna estructura o característica de contraseña que podría dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical.	Políticas Relacionadas: “Caracteres de las Contraseñas,’ “Contraseñas Cíclicas,’ “Configuración de Modem para Llamadas Discadas Entrantes,’ y “Sospecha de Divulgación de Contraseña”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
2. Contraseñas Cíclicas	Política: Los usuarios no deben crear contraseñas fijas que combinen un conjunto de caracteres no cambiantes con un conjunto de caracteres que cambien de manera predecible.	Políticas Relacionadas: “Histórico de Contraseñas, ’“Reutilización de Contraseñas,’ y “Estructura de las Contraseñas”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
3. Almacenamiento de Contraseñas Legibles	Política: No se deben almacenar contraseñas fijas legibles dentro de archivos agrupados en lotes, comandos de inicio de sesión, macros de software y claves de funcionamiento de terminales en computadores que no tengan control de acceso, o en otras ubicaciones en las que las personas no autorizadas las pudieran descubrir o utilizar.	Políticas Relacionadas: “Divulgación Pública de Contraseñas,’ “Escritura de Contraseñas,’ y “Contraseñas Legibles”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
4. Contraseñas en Distintos Sistemas	Política: Los usuarios de computadores deben emplear distintas contraseñas en cada uno de los sistemas para los que se les ha otorgado el acceso.	Políticas Relacionadas: “Mecanismo Único de Acceso,’ “Divulgación Pública de Contraseñas,’ y “Contraseñas en Distintos Sistemas — Permiso”	Política Dirigida a:Todos	Ambientes de Seguridad: Altos
5. Contraseñas en Distintos Sistemas — Permiso	Política: Los usuarios no deben utilizar la misma contraseña en múltiples sistemas de computadores, a menos que el departamento de Seguridad Informática les haya informado que el hacerlo no comprometerá de manera indebida la seguridad del sistema.	Políticas Relacionadas: “Contraseñas en Distintos Sistemas” y “Mecanismo Único de Acceso”	Política Dirigida a:Todos	Ambientes de Seguridad: Altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Sospecha de Divulgación de Contraseña	Política: Todo usuario debe cambiar su contraseña de inmediato si sospecha la divulgación de ésta o si sabe que ha sido divulgada a una persona no autorizada.	Políticas Relacionadas: "Contraseñas Iniciales, '"Cambios de Seguridad Después de Estar Comprometido el Sistema,' "Cambios Obligatorios de Contraseña,' y "Sincronización de los Intervalos de Cambios de Contraseñas"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
7. Divulgación Pública de Contraseñas	Política: No se deben escribir las contraseñas ni abandonarlas en sitios donde personas no autorizadas pudieran descubrirlas.	Políticas Relacionadas: "Contraseñas Generadas por el Sistema,' "Escritura de Contraseñas,' y "Contraseñas en Distintos Sistemas"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
8. Proximidad de Contraseñas a Dispositivos de Acceso	Política: Los usuarios no deben nunca escribir o de otro modo registrar una contraseña legible y almacenarla cerca de los dispositivos de acceso a los que pertenece.	Políticas Relacionadas: "Credenciales Portátiles de Identificación" y "Escritura de Contraseñas"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
9. Contraseñas en Software de Comunicaciones	Política: Los usuarios no deben guardar en ningún momento contraseñas fijas en programas de comunicaciones con sistema de discado, exploradores de Internet o software relacionado con comunicaciones de datos.	Políticas Relacionadas: "Almacenamiento de Contraseñas Legibles" y "Recuperación de Contraseñas"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
10. Cookies para Inicios Automáticos de Sesión	Política: Los usuarios de computadores de la Gobernación deben negar todas las ofertas hechas por el software para colocar cookies en su computador, de modo que puedan ingresar al sistema de manera automática, la próxima vez que visiten un sitio específico en Internet.	Políticas Relacionadas: "Información Personal Incluida" y "Contraseñas en Software de Comunicaciones"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
11. Tarjetas de Contraseñas Dinámicas	Política: Las tarjetas portátiles con contraseñas dinámicas no deben guardarse en el mismo maletin de los computadores portátiles que se utilizan para obtener acceso remoto a las redes de la Gobernación.	Políticas Relacionadas: "Distintivos de Acceso Extraviados" e "Identificación Positiva para Uso del Sistema"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
12. Números de Identificación Personal	Política: Todos los números de identificación se deben construir con las mismas reglas aplicables a las contraseñas fijas.	Políticas Relacionadas: "Autentificación de Usuario Que Accede Vía Telefónica" e "Intentos de Contraseñas por Discado"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
13. Escritura de Contraseñas	Política: Los usuarios no deben escribir sus contraseñas, a menos que hayan ocultado las mismas de manera efectiva en caracteres no relacionados similares o que hayan utilizado un sistema de códigos para ocultar la contraseña.	Políticas Relacionadas: “Divulgación Pública de Contraseñas” y “Contraseñas Legibles”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
14. Contraseñas Compartidas	Política: Nunca se deben distribuir ni revelar las contraseñas a ninguna persona distinta al usuario autorizado.	Políticas Relacionadas: “Autentificación de Contraseña en Persona,’ “Límite al Acceso Diario,’ y “Contraseñas de Control de Acceso al Sistema”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
15. Uso de Contraseñas por Terceros	Política: Los usuarios no deben suministrar sus identificadores de usuario ni sus contraseñas a ningún tercero, incluyendo entre otros, agregadores de datos y servicios de resumen/formateo de datos.	Políticas Relacionadas: “Prohibición de Invasión de Privacidad a Través de Terceros” y “Números de Cuenta Bancaria”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
16. Identificadores Personales de Usuario — Responsabilidad	Política: Los usuarios deben responsabilizarse de toda la actividad realizada con sus identificadores personales de usuario y no deben permitir que otras personas realicen cualquier actividad con éstos o que realicen actividad alguna con identificadores que pertenezcan a otros usuarios.	Políticas Relacionadas: “Cuentas Unicas de Correo Electrónico”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
17. Compartir Códigos de Acceso	Política: Las cuentas de computación, los identificadores de usuario, las contraseñas de red, los números de identificación personal en la casilla de correos de voz, los números de tarjetas de crédito y otros códigos de la Gobernación, no debe utilizarlos ninguna otra persona distinta a aquélla para quien fueron emitidas originalmente.	Políticas Relacionadas: “Identificadores Personales de Usuario — Responsabilidad” y “Cuentas Unicas de Correo Electrónico”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
18. Prueba de los Controles del Sistema Informático	Política: Los empleados no deben probar o tratar de comprometer los controles internos, a menos que la gerencia de Seguridad Informática lo apruebe específicamente con antelación y por escrito.	Políticas Relacionadas: “Comprometer Mecanismos de Seguridad para los Clientes,’ “Intentos No Autorizados de Acceso Físico,’ “Actividades del Hacker,’ y “Evidencia de Delito o Abuso Informático”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
19. Explotación de las Vulnerabilidades de la Seguridad del Sistema	Política: Los usuarios no deben explotar los puntos vulnerables o las deficiencias en la seguridad de los sistemas informáticos, para dañar estos sistemas o la información, obtener recursos más allá de aquellos autorizados, quitar los recursos a otros usuarios u obtener acceso a otros sistemas para los que no han recibido la autorización adecuada.	Políticas Relacionadas: “Informes de Incidentes” y “Hardware y Software de Diagnóstico”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
20. Construcción de Contraseñas de Correo voz	Política: Las contraseñas para correo de voz no deben ser obligadas a cumplir las normas de construcción de contraseñas establecidas por la Gobernación, pero los usuarios deben seleccionar una contraseña que sea distinta a su extensión telefónica, su número de oficina, su número de empleado y cualquier otro número que pudiera deducirse con facilidad.	Políticas Relacionadas: “Excepciones a las Políticas, ’“Estructura de las Contraseñas,’ e “Información Sensible en Máquinas Contestadoras”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
21. Cuentas Unicas de Correo Electrónico	Política: Los empleados no deben utilizar una cuenta de correo electrónico que haya sido asignada a otra persona, ya sea para enviar o recibir mensajes.	Políticas Relacionadas: “Identificador Único de Usuario y Contraseña Obligatorios,’ “Información Secreta en Correo Electrónico,’ “Monitoreo de Mensajes de Correo Electrónico,’ “Revisión de Mensajes de Correo Electrónico de Terceros,’ y “Contraseñas de Control de Acceso al Sistema”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
9.03.02 Equipos de Usuario Desatendidos				
1. Sesiones Activas Desatendidas	Política: Si el sistema de computación al cual están conectados o el cual están utilizando contiene información sensible, los usuarios no deben dejar desatendidos sus computadores personales, estaciones de trabajo o terminales sin salir del sistema o invocar un protector de pantalla.	Políticas Relacionadas: “Cierre de Sesión Automático” y “Sistemas de Redes Desatendidos”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
2. Sistemas de Redes Desatendidos	Política: En caso de que los computadores personales se encuentren conectados a una red, siempre deben estar fuera de sistema si se encuentran desatendidos.	Políticas Relacionadas: “Sesiones Activas Desatendidas,’ “Modem de Estaciones de Trabajo,’ “Control de Acceso a Computadores de Red,’ y “Cierre de Sesión Automático”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
9.04 Control de Acceso a la Red				
9.04.01 Política para el Uso de los Servicios de Red				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Descontinuación del Servicio	Política: La Gobernación debe reservarse el derecho a bloquear, ocultar, negar o descontinuar su servicio en cualquier momento y sin previo aviso.	Políticas Relacionadas: “Confirmación de Información de Pago” y “Esconder Transmisión de la Información”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Altos
2. Control de Acceso a Computadores de Red	Política: Si los empleados dejan encendidos sus computadores durante horas no laborables, y si están conectados a una red, los computadores deben estar protegidos por un sistema de control de acceso que cuente con la aprobación de la gerencia de Seguridad Informática.	Políticas Relacionadas: “Modem de Estaciones de Trabajo” y “Respaldos Automáticos”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
3. Autorización para Conexiones a Internet	Política: Los empleados no deben establecer ninguna conexión externa que pudiera permitir a los usuarios ajenos a la Gobernación obtener acceso a los sistemas informáticos de la misma, a menos que se obtenga una aprobación previa de la gerencia de Sistemas Informáticos.	Políticas Relacionadas: “Interconexión de Sistemas, “Responsabilidades de Terceros en la Seguridad Informática,’ “Conexiones a Internet,’ y “Conexiones en Red con Organizaciones Externas”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
4. Normas de Telefónicas Comunes	Política: Los servicios de conexión en la red suministrados por la Gobernación deben prestarse con base en un contrato como operadora y no como operadora común.	Políticas Relacionadas: “Servicios de Protección de Mensajes en Red” y “Sin Responsabilidad en Mensajes”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
5. Acceso a la Red Interna	Política: Sólo los computadores suministrados por la Gobernación deben tener capacidad para acceder a la red interna de la Gobernación.	Políticas Relacionadas: “Discos Flexibles” y “Equipo de Teletrabajo”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
6. Derechos de Acceso a Internet	Política: Todos los tipos de acceso a Internet, con la excepción del correo electrónico, deben contar con autorización anticipada por escrito del gerente del departamento correspondiente que asegure que el usuario tiene una necesidad demostrable de dicho acceso.	Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
7. Restricción de Acceso a Internet	Política: El acceso a Internet debe otorgarse solamente a los empleados de la Gobernación que realicen investigaciones como parte regular de su trabajo.	Políticas Relacionadas: “Derechos de Acceso a Internet” y “Fuentes de Noticias en Internet”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
8. Sitios Web No Relacionados con Negocio	Política: Los sistemas informáticos de la Gobernación deben evitar rutinariamente que los usuarios se conecten a determinadas páginas web no comerciales.	Políticas Relacionadas: "Uso Personal de los Sistemas de Computación y de Comunicaciones,' "Restricciones en Contenido de Mensajes,' y "Fuentes de Noticias en Internet"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
9. Bloqueo de Acceso a Sitios Ajenos al Negocio	Política: La Gobernación debe utilizar, como rutina, software que evite que los usuarios visiten cualquier página web en Internet que la administración considere censurable o claramente personal por su naturaleza.	Políticas Relacionadas: "Control de Tráfico en Internet" y "Acceso de Usuarios a Internet"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
10. Descargas Grandes desde Internet	Política: Los usuarios de Internet no deben emplear facilidades de flujo de videos, de flujo de audio o descargar grandes archivos gráficos, a menos que el jefe inmediato del usuario lo apruebe con antelación.	Políticas Relacionadas: "Uso Personal del Teléfono" y "Registros de Uso de Internet"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
11. Identidad en Internet	Política: Los empleados no deben ocultar o falsificar su identidad al utilizar los sistemas informáticos o al llevar a cabo actividades comerciales de la Gobernación.	Políticas Relacionadas: "Acceso Entrante a Internet"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
12. Propiedad Intelectual	Política: Al acceder a Internet utilizando los sistemas de la Gobernación, los empleados deben republicar o reproducir material sólo después de obtener el permiso de la fuente, citar material de otras fuentes sólo si proceden a identifican las mismas o revelar información interna de la Gobernación en Internet sólo si se ha aprobado la información de manera oficial para su emisión al público.	Políticas Relacionadas: "Validación de Información en Intranet" y "Derechos de Propiedad Intelectual"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
9.04.02 Vía Exigida				
1. Control de Acceso a los Computadores Conectados a la Red	Política: Todos los computadores de la Gobernación que lleguen a las redes de terceros deben estar protegidos mediante un sistema de control de acceso de privilegios autorizado por la gerencia de Seguridad Informática.	Políticas Relacionadas: "Interconexión de Sistemas" y "Control de Acceso a Computadores de Red"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Conexiones a Redes de Terceros	Política: Los computadores o redes de la Gobernación deben conectarse sólo a computadores o redes de terceros después de que la gerencia de Seguridad Informática determine que el sistema combinado satisface los requerimientos de seguridad de la Gobernación.	Políticas Relacionadas: “Sistemas de Terceros Conectados a la Red” e “Interconexión de Sistemas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Modem de Estaciones de Trabajo	Política: Los trabajadores no deben conectar modem de discado a las estaciones de trabajo, computadores personales o a los clientes de red de área local que estén conectados simultáneamente a otra red de área local o a otra red de comunicación interna.	Políticas Relacionadas: “Autentificación de Usuario Que Accede Vía Telefónica,’ “Conexiones Discadas, “Cambios en la Línea de Comunicación,’ y “Sistemas de Redes Desatendidos”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
4. Conexiones de Discado Directo	Política: Todas las conexiones de discado con sistemas y redes de la Gobernación deben enrutarse a través de un grupo de modem que incluya un sistema de seguridad aprobado de autentificación extendida de usuario.	Políticas Relacionadas: “Modem de Estaciones de Trabajo” y “Conexiones Discadas”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos
5. Registro de Línea de Modem	Política: Los empleados no deben instalar o contratar la instalación de líneas de modem que se conecten a computadores o redes de la Gobernación, a menos que ue estas líneas hayan sido autorizadas por la gerencia del departamento de Telecomunicaciones e ingresadas al registro de líneas de modem de toda la organización.	Políticas Relacionadas: “Conexiones de Discado Directo” y “Sistemas Que Aceptan Llamadas Discadas Entrantes”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
6. Modem en Auto-Respuesta	Política: Los usuarios no deben dejar conectados los modem a los computadores personales en función de respuesta automática, de modo que puedan recibir llamadas discadas entrantes.	Políticas Relacionadas: “Conexiones Discadas” y “Autentificación de Usuario Que Accede Vía Telefónica”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Bajos y medianos
9.04.03 Autentificación del Usuario para Conexiones Externas				
1. Contraseñas de Acceso Remoto	Política: No debe permitirse que identificadores de usuario que presenten contraseñas en blanco o nulas, obtengan acceso remoto a cualquier computador o red de la Gobernación.	Políticas Relacionadas: “Estructura de las Contraseñas” y “Longitud Mínima de Contraseñas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Autentificación de Usuario Mediante Dos Factores	Política: Todos los accesos entrantes que se realicen a través de una red pública hasta todos los computadores de la Gobernación deben emplear una autentificación del usuario mediante dos factores, sin someter a repetición al menos a uno de los factores.	Políticas Relacionadas: “Contraseñas Legibles” y “Acceso Entrante a Internet”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
3. Controles de Acceso para Sistemas Remotos	Política: Todos los computadores que tengan diálogos remotos en tiempo real con los sistemas de producción de la Gobernación, deben ejecutar un paquete de control de acceso aprobado por la gerencia de Seguridad Informática.	Políticas Relacionadas: “Controles de Acceso al Sistema de Computación” y “Procedimientos de Seguridad Informática en Teletrabajo”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
4. Acceso a la Red	Política: Todos los usuarios deben verificar su identidad a través de un identificador de usuario y una contraseña secreta o por otro medio que proporcione una seguridad igual o mayor, antes de permitirse su utilización de los computadores de la Gobernación conectados a una red.	Políticas Relacionadas: “Códigos de Identificación para Soporte Técnico” e “Identificadores de Usuario para Terceros”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5. Administración Remota	Política: La gestión remota de computadores conectados a Internet debe emplear contraseñas que se utilicen una sola vez sobre enlaces cifrados.	Políticas Relacionadas: “Conexiones a Redes Externas en Tiempo Real,’ “Autentificación del Usuario por el Sistema Operativo,’ y “Contraseñas para los Dispositivos Internos de la Red”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
6. Comandos Inter-Procesador	Política: No se deben satisfacer los comandos iniciados por usuarios provenientes de zonas externas, a menos que el usuario inicie su sesión.	Políticas Relacionadas: “Información en Mensaje de Inicio de Sesión,’ “Autentificación de Usuario Que Accede Vía Teléfonica,’ y “Autentificación del Usuario por el Sistema Operativo”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
7. Autentificación de Usuario Que Accede Vía Teléfonica	Política: Todas las conexiones discadas entrantes con la red de datos de computación de la Gobernación deben utilizar autentificación extendida de usuario.	Políticas Relacionadas: “Modem de Estaciones de Trabajo,’ “Cambios en la Sensibilidad, Criticidad y Valor de la Información,’ “Validación de la Identidad de Terceros,’ “Acceso Entrante a Internet,’ y “Autentificación del Usuario por el Sistema Operativo”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
8. Intentos de Contraseñas por Discado	Política: Todas las líneas de discado deben configurarse de manera de concluir la conexión con el usuario que no haya proporcionado una contraseña correcta luego de tres intentos consecutivos.	Políticas Relacionadas: “Configuración de Modem para Llamadas Discadas Entrantes” e “Intentos de Introducir Contraseña”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9. Acceso Entrante a Internet	Política: Todos los usuarios que establezcan una conexión con los computadores de la Gobernación en su red interna a través de Internet deben autentificarse en un cortafuego que emplee un proceso extendido de autentificación de usuario aprobado por la gerencia de Sistemas Informáticos.	Políticas Relacionadas: “Conexiones a Internet, “Contraseñas Legibles,’ y “Autentificación de Usuario Que Accede Vía Telefónica”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9.04.04 Autentificación de Nodos				
1. Sistemas Que Aceptan Llamadas Discadas Entrantes	Política: Los empleados de la Gobernación no deben establecer ningún sistema de comunicación que acepte llamadas entrantes discadas, a menos que la gerencia de Seguridad Informática lo haya aprobado.	Políticas Relacionadas: “Conexiones Discadas” y “Cambios en la Línea de Comunicación”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
9.04.05 Protección del Puerto Remoto de Diagnóstico				
1. Acceso al Puerto de Diagnóstico	Política: El acceso a los puertos de diagnóstico debe controlarse de manera segura con el uso de un bloqueador de teclados y de procedimientos eficaces.	Políticas Relacionadas: “Hardware y Software de Diagnóstico”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
9.04.06 Segregación en las Redes				
1. Conexiones Personales a la Red	Política: Todo acceso personal que permita a los visitantes conectarse con sus propias redes, debe emplear una subred separada que no tenga conexión con la red interna de la Gobernación.	Políticas Relacionadas: “Interconexión de Sistemas” y “Servidores Públicos en Internet”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
2. Computadores y Redes de Alta Seguridad y Alta Confiabilidad	Política: Todo sistema de alta seguridad y de alta confiabilidad manejado o propiedad de la Gobernación debe tener sus propios computadores y redes dedicados, a menos que estén aprobados con antelación por la gerencia de Seguridad Informática.	Políticas Relacionadas: “Sistemas Comerciales y Financieros en Internet” y “Aislamiento de Sistemas con Información Secreta”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
9.04.07 Control de las Conexiones de la Red				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Contraseñas para los Dispositivos Internos de la Red	Política: Todas las redes internas de la Gobernación, incluyendo entre otros, enrutadores, cortafuegos y servidores de control de acceso, deben tener contraseñas únicas u otros mecanismos de control de acceso.	Políticas Relacionadas: “Identificador Único de Usuario y Contraseña Obligatorios” y “Contraseñas Iniciales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Acceso a Internet Sin Cortafuegos	Política: Todo acceso a Internet sin el uso de un cortafuego debe lograrse a partir de un computador independiente que no esté conectado a ninguna red interna de la Gobernación.	Políticas Relacionadas: “Conexiones a Redes Externas en Tiempo Real” y “Conexiones a Internet”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
3. Acceso Público a Puertos Activos de la red	Política: Los puertos activos de red desatendidos que estén conectados a la red de computadores internos de la Gobernación no deben estar ubicados en áreas públicas que incluyan, entre otros, entradas de edificios, cafetines de la empresa y salas de conferencia.	Políticas Relacionadas: “Conexiones Personales a la Red” y “Configuración de Conexiones a la Red”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
4. Puertos de Red en Oficinas Vacías	Política: Todos los puertos de red que se encuentren en oficinas desocupadas y otras áreas normalmente no utilizadas, deben desconectarse rápidamente en el cajetín de instalación o desde otra zona centralizada.	Políticas Relacionadas: “Conexiones Personales a la Red” y “Modem de Estaciones de Trabajo”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
5. Inhabilitación de Java	Política: Todos los usuarios de Internet deben inhabilitar los programas Java, modificando la configuración predeterminada de su explorador de Internet.	Políticas Relacionadas: “Descarga de Software”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
9.04.08 Control de Ruta de la Red				
1. Zonas de Seguridad de la Red	Política: Todas las redes internas de datos de la Gobernación deben estar divididas en zonas de seguridad.	Políticas Relacionadas: “Aislamiento de Equipos” y “Distintas Zonas de Riesgo de Incendio”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
9.04.09 Seguridad de los Servicios de la Red				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Cortafuegos de Servidores Web	Política: Todos los servidores web accesibles desde Internet deben estar protegidos por un enrutador o cortafuego autorizado por el departamento de Seguridad Informática.	Políticas Relacionadas: “Contraseñas para los Dispositivos Internos de la Red” y “Acceso a Internet Sin Cortafuegos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9.05 Control de Acceso al Sistema Operativo				
9.05.01 Identificación Automática del Terminal				
1. Seguridad Física del Terminal	Política: El acceso físico al terminal debe estar restringido a aquellos empleados que necesitan conocer la información, cuando se utilice la identificación del terminal para autentificar la conexión de un terminal a un área específica.	Políticas Relacionadas: “Cierre de Sesión Automático”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
9.05.02 Procedimientos para Inicio de Sesión en Terminales				
1. Intentos de Introducir Contraseña	Política: Luego de tres intentos infructuosos por introducir su contraseña, la identidad del usuario correspondiente debe quedar suspendida hasta que un administrador de sistemas la reinicialice, desactivada momentáneamente por lo menos durante tres minutos, o desconectada si se utilizan conexiones discadas o externas.	Políticas Relacionadas: “Sospecha de Divulgación de Contraseña,’ “Contraseñas Iniciales,’ “Estructura de las Contraseñas,’ e “Intentos de Contraseñas por Discado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Protección de la Re inicialización Basada en Contraseña	Política: Todos las estaciones de trabajo, incluyendo entre otros los computadores personales, computadores portátiles, computadores transportables y computadores	Políticas Relacionadas: “Sistemas de Cifrado de Propósito General” y “Sesiones Activas Desatendidas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
3. Información de Inicio de Sesión	Política: Si alguna parte de la secuencia de inicio de sesión es incorrecta al momento de ingresar al sistema de computación o comunicaciones de datos de la Gobernación, el usuario debe únicamente recibir información de que todo el proceso de inicio de sesión fue incorrecto.	Políticas Relacionadas: “Respuesta por Inicio Incorrecto de Sesión”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Respuesta por Inicio Incorrecto de Sesión	Política: Si alguna parte de la secuencia de inicio de sesión resulta incorrecta al momento de entrar al sistema de computación o de comunicaciones de datos de la Gobernación, el sistema debe dar por terminada la sesión o esperar hasta recibir la información correcta de inicio de sesión.	Políticas Relacionadas: “Información de Inicio de Sesión” e “Información en Mensaje de Inicio de Sesión”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Alto

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
5. Mensaje de Advertencia en Inicio de Sesión	Política: Toda pantalla de ingreso de los computadores multiusuario debe incluir un aviso especial que indique que sólo los usuarios autorizados pueden acceder al sistema, lo cual significa que los usuarios que ingresan al sistema están autorizados para hacerlo, y que el uso	Políticas Relacionadas: “Información en Mensaje de Inicio de Sesión”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
6. Información en Mensaje de Inicio de sesión	Política: Todos los mensajes de bienvenida de los sistemas de computador de la Gobernación que estén conectados a una red deben guiar al usuario para iniciar su sesión en el sistema y no deben suministrar ninguna información que identifique a la empresa, el sistema operativo, la configuración del sistema u otros asuntos internos hasta que se autentifique exitosamente la identidad del usuario.	Políticas Relacionadas: “Estructura de las Contraseñas,’ “Comandos Inter-Procesador,’ y “Respuesta por Inicio Incorrecto de Sesión”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
7. Mensaje de Inicio de Sesión en la Red	Política: Se debe utilizar el mensaje normal de advertencia desarrollado por la gerencia de Tecnología Informática y aprobado por el departamento Legal, cuando los usuarios se conecten a los computadores internos de la Gobernación.	Políticas Relacionadas: “Mensaje de Advertencia en Inicio de Sesión,’ “Información en Mensaje de Inicio de Sesión,’ “Herramientas de Monitoreo de Sistemas,’ y “Conexiones Discadas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
8. Ultima Hora y Fecha de Inicio de Sesión	Política: Al momento de iniciar su sesión, todo usuario debe recibir información que refleje la hora y fecha del último ingreso al sistema.	Políticas Relacionadas: “Informes de Incidentes” y “Privilegios de Identificadores de Usuarios Inactivos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
9. Límite al Acceso Diario	Política: No se debe permitir a los usuarios ingresar al sistema más de diez veces al día.	Políticas Relacionadas: “Contraseñas Compartidas, “Ultima Hora y Fecha de Inicio de Sesión,’ y “Sesiones Múltiples Simultáneas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Bajos y medianos
9.05.03 Identificación y Autentificación del Usuario				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Mecanismo Único de Acceso	Política: Se debe exigir a los usuarios una sola combinación de identificador de usuario y contraseña, para el momento en que lleguen a la red o al sistema de computadores de destino, luego de lo cual se debe pasar la información relacionada con la identidad del usuario a otros computadores, cortafuegos, sistema de administración de base de datos, sistemas de aplicaciones y demás componente del sistema informático.	Políticas Relacionadas: “Protección de la Información” y “Conexiones Discadas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Credenciales Portátiles de Identificación	Política: Las credenciales portátiles de identificación que incluyan o funcionen con computadores, entre ellas las tarjetas inteligentes, las tarjetas portátiles de identidad y los distintivos con foto y barras magnéticas, deben requerir el suministro de una contraseña para funcionar cada vez que se empleen, quedando inhabilitadas de manera automática si los usuarios experimentan tres intentos incorrectos consecutivos para introducir la misma contraseña.	Políticas Relacionadas: “Proximidad de Contraseñas a Dispositivos de Acceso” y “Distintivos de Acceso Extraviados”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Alto
3. Autentificación del Usuario por el Sistema operativo	Política: Los desarrolladores de sistemas de aplicación para la Gobernación deben depender consistentemente de los controles de acceso que proporcionan los sistemas operativos, los sistemas de control de acceso disponibles a nivel comercial que mejoran los sistemas operativos, las puertas de enlace o cortafuegos, y no deben crear otros mecanismos para recopilar información, o crear o instalar otros mecanismos de control de acceso que acrediten o autentifiquen la identidad de los usuarios sin el permiso previo de la gerencia de Seguridad Informática.	Políticas Relacionadas: “Mecanismo Único de Acceso,’ “Regulación del Software,’ y “Burlado de los Controles de Acceso”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Sesiones Múltiples Simultáneas	Política: Los sistemas de computación no deben permitir que ningún usuario realice sesiones múltiples simultáneas en línea, a menos que la gerencia de Sistemas Informáticos otorgue un permiso especial.	Políticas Relacionadas: “Privilegios Especiales en Sistema”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5. Iniciación de Transacciones en Computadores	Política: La capacidad para ejecutar las transacciones a nombre de la Gobernación debe restringirse mediante los identificadores de usuario individuales y la identificación positiva de las personas involucradas que utilicen dichos identificadores de usuario.	Políticas Relacionadas: “Separación de Tareas”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Códigos de Identificación para Soporte Técnico	Política: La identidad de las personas que realicen llamadas telefónicas para solicitar soporte computarizado deben quedar autentificadas a través de un código especial de identificación, distinto al de la contraseña de computador y divulgado únicamente al personal interno autorizado, a menos que se reconozca de manera definitiva la voz de la persona que está realizando la llamada.	Políticas Relacionadas: "Contraseñas de Control de Acceso al Sistema" y "Ordenes para Cambiar Registros"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
9.05.04 Sistema de Manejo de Contraseñas				
1. Longitud Mínima de Contraseñas	Política: Todas las contraseñas deben tener por lo menos 10 caracteres y esta longitud debe revisarse siempre de manera automática al momento en que los usuarios crean y seleccionan sus contraseñas.	Políticas Relacionadas: "Identificadores de Usuarios Anónimos,' "Intentos de Introducir Contraseña, "Intentos de Contraseñas por Discado,' "Información en Mensaje de Inicio de Sesión,' y "Contraseñas en Distintos Sistemas"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Restricción a la Longitud Mínima de las Contraseñas	Política: Las contraseñas fijas seleccionadas por el usuario deben tener una longitud de por lo menos 10 caracteres o la extensión máxima que permita el sistema.	Políticas Relacionadas: "Longitud Mínima de Contraseñas" y "Acceso Entrante a Internet"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Contraseñas para Computadores Conectados a la Red	Política: Todos los computadores conectados a la red de la Gobernación deben emplear contraseñas fijas que contengan al menos 10 caracteres y todos los computadores que no estén conectados a la red deben emplear contraseñas fijas que contengan al menos 6 caracteres.	Políticas Relacionadas: "Información en Mensaje de Inicio de Sesión" y "Múltiples Identificadores de Usuario"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Longitud de Contraseña de Acuerdo con la Función	Política: Se debe establecer la longitud mínima de contraseñas fijas a seis caracteres para las casillas del correo de voz y computadores inalámbricos, ocho para todos los computadores conectados a una red y diez para administradores y otros identificadores de usuarios privilegiados.	Políticas Relacionadas: "Credenciales Portátiles de Identificación" y "Contraseñas Generadas por el Sistema"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
5. Reutilización de Contraseñas	Política: Los usuarios no deben crear contraseñas que sean idénticas o sustancialmente parecidas a las contraseñas que habían empleado anteriormente.	Políticas Relacionadas: "Contraseñas Cíclicas" e "Histórico de Contraseñas"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Caracteres de las Contraseñas	Política: Todas las contraseñas seleccionadas por el usuario deben contener por lo menos un carácter alfabético y otro no alfabético.	Políticas Relacionadas: “Estructura de las Contraseñas” y “Mayúsculas y Minúsculas en Contraseñas”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
7. Mayúsculas y Minúsculas en Contraseñas	Política: Todas las contraseñas seleccionadas por el usuario deben contener por lo menos un carácter alfabético en minúscula y uno en mayúscula.	Políticas Relacionadas: “Estructura de las Contraseñas” y “Caracteres de las Contraseñas”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
8. Histórico de Contraseñas	Política: Se deben utilizar un software del sistema y un software desarrollado a nivel local para mantener un histórico cifrado de contraseñas fijas anteriores, que contenga las 13 contraseñas anteriores de cada identificador de usuario.	Políticas Relacionadas: “Cambios Obligatorios de Contraseña” y “Contraseñas Cíclicas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9. Semilla para Contraseñas Generadas por el Sistema	Política: Si se utilizan contraseñas generadas por el sistema, éstas deben generarse utilizando bits del reloj del sistema de orden inferior u otras fuentes no predecibles que puedan cambiar con frecuencia.	Políticas Relacionadas: “Generación de Claves de Cifrado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
10. Contraseñas Generadas por el Sistema	Política: Todas las contraseñas generadas por el sistema destinadas a los usuarios finales deben ser pronunciables.	Políticas Relacionadas: “Generación de Claves de Cifrado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
11. Emisión y Almacenamiento de Contraseñas Generadas por el Sistema	Política: Si las contraseñas o los números de identificación personal son generados mediante un sistema de computación, éstos deben siempre emitirse inmediatamente después de que sean generados y nunca se deben almacenar en los sistemas de computación involucrados.	Políticas Relacionadas: “Recuperación de Contraseñas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
12. Materiales para la Generación de Contraseñas	Política: Todos los medios de almacenamiento computarizado o áreas de la memoria de un computador que sean utilizados en la creación, asignación, distribución o cifrado de contraseñas o de números de identificación personal, deben reescribirse reiteradamente con una serie de unos y ceros, inmediatamente después de utilizados.	Políticas Relacionadas: “Algoritmos Generadores de Contraseñas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
13. Algoritmos Generadores de Contraseñas	Política: Se deben controlar el software y todos los archivos que contengan fórmulas, algoritmos y otros puntos específicos del proceso utilizado para generar las contraseñas o números de identificación personal, con las medidas de seguridad más estrictas que soporte el sistema de computación correspondiente.	Políticas Relacionadas: “Materiales para la Generación de Contraseñas,’ “Cifrado de Contraseñas,’ y “Sistemas de Gestión de Claves de Cifrado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
14. Visualización e Impresión de Contraseñas	Política: Se debe disfrazar, suprimir, o de algún modo ocultar la visualización e impresión de las contraseñas, de manera tal que las personas no autorizadas no puedan observarlas o recuperarlas posteriormente.	Políticas Relacionadas: “Materiales para la Generación de Contraseñas,’ “Posiciones de las Pantallas de los Computadores,’ y “Contraseñas Iniciales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
15. Máscaras para Cambios de Contraseña	Política: Cada vez que se especifiquen las contraseñas seleccionadas por los usuarios o las claves de cifrado, éstas deben introducirse dos veces y enmascararse.	Políticas Relacionadas: “Almacenamiento de Contraseñas Legibles” y “Ocultar Números de Cuenta de Clientes”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
16. Cambios Obligatorios de Contraseña	Política: Todos los usuarios deben ser obligados automáticamente a cambiar sus contraseñas al menos una vez cada 90 días.	Políticas Relacionadas: “Sospecha de Divulgación de Contraseña,’ “Estructura de las Contraseñas, “Sincronización de los Intervalos de Cambios de Contraseñas,’ y “Cambio de Números Discados”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
17. Sincronización de los Intervalos de Cambios de Contraseñas	Política: El intervalo de cambio de las contraseñas fijas debe estar sincronizado a lo largo y ancho de todas las plataformas de computación y redes de la Gobernación.	Políticas Relacionadas: “Cambios Obligatorios de Contraseña” y “Cambios de Seguridad Después de Estar Comprometido el Sistema”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
18. Contraseñas Legibles	Política: Las contraseñas fijas nunca deben encontrarse en forma legible fuera del computador personal o de la estación de trabajo.	Políticas Relacionadas: “Almacenamiento de Contraseñas Legibles” y “Acceso a la Red”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
19. Información de Control de Acceso en Cookies	Política: Los sistemas informáticos de la Gobernación nunca deben almacenar ninguna información de control de acceso en "cookies" depositados o almacenados en computadores de los usuarios finales.	Políticas Relacionadas: “Cookies para Inicios Automáticos de Sesión” y “Cookies”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
20. Cifrado de Contraseñas	Política: Las contraseñas siempre deben cifrarse cuando se almacenen por un lapso significativo de tiempo o cuando se transmitan a través de las redes.	Políticas Relacionadas: “Materiales para la Generación de Contraseñas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
21. Recuperación de Contraseñas	Política: Los sistemas de computación y comunicación deben ser diseñados, probados y controlados para prevenir tanto la recuperación como el uso no autorizado de las contraseñas almacenadas, se encuentren éstas en forma cifrada o descifrada.	Políticas Relacionadas: “Emisión y Almacenamiento de Contraseñas Generadas por el Sistema”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
22. Contraseñas de Control de Acceso al Sistema	Política: El control de acceso a computadores y sistemas de comunicación debe llevarse a cabo a través de contraseñas únicas para cada usuario individual.	Políticas Relacionadas: “Contraseñas Compartidas, “Identificador Único de Usuario y Contraseña Obligatorios,’ e “Identificadores de Usuarios Únicos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
23. Contraseñas Proporcionadas por Proveedores	Política: Todas las contraseñas predeterminadas suplidas por el proveedor deben ser cambiadas antes de que algún computador o sistema de comunicaciones sea utilizado para el negocio de la Gobernación.	Políticas Relacionadas: “Contraseñas Iniciales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
24. Cambios de Seguridad Después de Estar Comprometido el Sistema	Política: Cada vez que un sistema esté comprometido o se sospeche que se ha comprometido por un tercero no autorizado, los gerentes del sistema deben recargar inmediatamente una versión confiable del sistema operativo y de todo el software relacionado con la seguridad, y todos los cambios recientes de privilegios de usuarios y del sistema deben ser revisados para verificar los cambios no autorizados.	Políticas Relacionadas: “Sospecha de Divulgación de Contraseña”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9.05.05 Uso de las Utilidades del Sistema				
1. Selección de Herramientas de Seguridad	Política: Antes de distribuir software para identificación de vulnerabilidad u otras herramientas que puedan ser utilizadas para comprometer la seguridad de los sistemas informáticos, el personal de la Gobernación debe investigar y validar la necesidad del receptor de estas herramientas.	Políticas Relacionadas: “Prueba de los Controles del Sistema Informático,’ “Herramientas de Estado de Seguridad del Sistema,’ “Poderosas Herramientas de Sistemas Informáticos,’ y “Evidencia de Delito o Abuso Informático”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Software de Identificación de Vulnerabilidades	Política: Cuando el software de identificación de vulnerabilidades no se está utilizando activamente, debe ser removido del sistema en el que se estaba ejecutando.	Políticas Relacionadas: "Identificación de Vulnerabilidades" y "Evidencia de Delito o Abuso Informático"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Poderosas Herramientas de Sistemas Informáticos	Política: Todas las herramientas poderosas de los sistemas informáticos construidas o distribuidas por la Gobernación que puedan ser empleadas para provocar un	Políticas Relacionadas: "Prueba de los Controles del Sistema Informático,' "Herramientas de Estado de Seguridad del Sistema,' "Poderosas Herramientas de Sistemas Informáticos,' y "Evidencia de Delito o Abuso Informático"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
4. Herramientas de Estado de Seguridad del Sistema	Política: Todo sistema multiusuario debe poseer las suficientes herramientas automatizadas para asistir al administrador de seguridad en la verificación del estado de seguridad del computador y debe poseer mecanismos para la corrección de problemas de seguridad.	Políticas Relacionadas: "Evidencia de Delito o Abuso Informático"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
5. Hardware y Software de Diagnóstico	Política: El acceso a hardware y software para pruebas de diagnóstico debe ser estrictamente controlado y debe utilizarse únicamente por personal autorizado con propósitos de prueba, resolución de problemas y desarrollo.	Políticas Relacionadas: "Mal Funcionamiento del Control de Acceso"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
6. Almacenamiento de Utilidades del Sistema	Política: Los discos y demás facilidades de almacenamiento en línea utilizados en los sistemas de producción no deben contener compiladores, ensambladores, editores de texto, procesadores de palabras u	Políticas Relacionadas: "Uso de las Utilidades del Software del Sistema" y "Remoción de Software"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
7. Uso de las Utilidades del Software del Sistema	Política: El acceso a los programas utilitarios del sistema debe estar restringido a un número pequeño de usuarios confiables y autorizados y cada vez que dichos programas sean ejecutados, la actividad resultante debe ser registrada en forma segura y revisada por el gerente de Operaciones de Computación.	Políticas Relacionadas: "Almacenamiento de Utilidades del Sistema,' "Cambios del Sistema Operativo de Producción,' y "Registro de Eventos Importantes de Seguridad"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
8. Facilidades para Inhabilitar Controles	Política: La gerencia debe establecer y restringir el uso de las facilidades de inhabilitación que deban utilizarse en circunstancias excepcionales en las que los controles deben ser comprometidos para poder mantener las operaciones actuales del negocio.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer,' "Uso de la Inhabilitación de los Controles,' y "Registro de Inhabilitaciones"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
9. Uso de la Inhabilitación de los Controles	Política: La gerencia debe definir claramente las circunstancias específicas y los procedimientos de autorización que deben seguirse cuando se deban inhabilitar los controles del sistema.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer,' "Facilidades para Inhabilitar Controles,' y "Registro de Inhabilitaciones"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
10. Control de Acceso para Restaurar Archivos	Política: Si los usuarios finales reciben la capacidad para restaurar sus propios archivos, no debe otorgárseles privilegios para restaurar los archivos de otros usuarios o para ver cuáles archivos de otros usuarios han sido respaldados.	Políticas Relacionadas: "Mal Funcionamiento del Control de Acceso,' "Cifrado en Medios de Respaldo, y "Almacenamiento de Medios de Respaldo"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9.05.06 Alarmas Coercitivas para Salvaguardar a los Usuarios				
1. Contraseñas de Presión	Política: Cada vez que se otorgue a un usuario el acceso a datos particularmente valiosos y sensibles, deben emplearse contraseñas coercitivas o de presión para señalar en forma encubierta al sistema que dicho usuario está siendo presionado para conectarse.	Políticas Relacionadas: "Interrupción del Sistema por Seguridad" y "Proyectos que Involucran Seguridad Humana"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Alto
9.05.07 Desconexión por Tiempo				
1. Cierre de Sesión Automático	Política: Si no ha habido actividad en un terminal, estación de trabajo o computador personal por 10 minutos, el sistema debe automáticamente poner en blanco la pantalla, suspender la sesión y solicitar una contraseña para restablecer la sesión.	Políticas Relacionadas: "Sesiones Activas Desatendidas"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9.05.08 Limitación del Tiempo de Conexión				
1. Control de Acceso Crono-Dependiente	Política: Todos los sistemas de computación multiusuario deben emplear sistemas de identificación positiva de los usuarios para controlar el acceso tanto a la información como a los programas que se encuentran restringidos por la hora del día y el día de la semana.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
9.06 Control de Acceso a las Aplicaciones				
9.06.01 Restricción del Acceso a la Información				
1. Contraseñas de Servicio al Cliente	Política: Las contraseñas fijas utilizadas para verificar la identidad de un cliente a través del teléfono nunca deben ser mostradas por los sistemas informáticos de la Gobernación.	Políticas Relacionadas: "Ocultar Números de Cuenta de Clientes" y "Comprometer Mecanismos de Seguridad para los Clientes"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Identificadores de Usuario o Contraseñas Secretas	Política: Los desarrolladores no deben construir o desplegar identificadores de usuarios secretos o contraseñas que tengan privilegios especiales y que no se encuentren claramente descritos en la documentación generalmente disponible del sistema.	Políticas Relacionadas: "Burlado de los Controles de Acceso,' "Vías de Acceso en Software de Producción, y "Acceso Físico de Trabajadores Cesados"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Controles de Acceso al Sistema de Computación	Política: Toda información sensible, crítica o valiosa residente en el computador debe tener controles de acceso en el sistema para garantizar que no sea divulgada en forma inapropiada, modificada o convertida en no disponible.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Funcionalidad de la Seguridad en las Aplicaciones del Negocio,' y "Arquitectura de Sistemas para Registro de Actividades"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Acceso a Material Adulto	Política: Antes de permitir el acceso a cualquier material que el público general considera inapropiado para los niños, todos los sistemas de la Gobernación deben emplear un sistema de control de acceso mediante verificación de la edad, aprobado por la gerencia de Seguridad Informática.	Políticas Relacionadas: "Recopilación de Información Personal de Menores" y "Almacenamiento de Información de Clasificación Mixta"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5. Separación de Actividades y Datos	Política: La gerencia debe definir los privilegios de los usuarios de forma tal que los usuarios ordinarios no puedan tener acceso o interferir en las actividades individuales o los datos privados de otros usuarios.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer" y "Separación de Tareas"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
6. Capacidad de Acceso de Usuarios	Política: Los usuarios no deben leer, modificar, borrar o copiar un archivo que pertenezca a otro usuario sin obtener permiso del Propietario del mismo.	Políticas Relacionadas: "Mal Funcionamiento del Control de Acceso"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
7. Privilegios Predeterminados de Usuario	Política: Sin la autorización específica por escrito de la gerencia, los administradores no deben conceder ningún privilegio a ningún usuario más allá del correo electrónico y de los procesadores de palabras.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
8. Comandos y Capacidades del Sistema	Política: Se debe presentar a los usuarios finales únicamente las capacidades y comandos del sistema para los cuales tienen privilegios.	Políticas Relacionadas: "Privilegios Especiales en Sistema,' "Mecanismo Único de Acceso,' y "Restricción de Privilegios — Necesidad de Conocer"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
9. Privilegios Sobre la Información de Producción	Política: Los privilegios del sistema que permiten la modificación de la información de producción de la Gobernación deben estar restringidos a las aplicaciones de producción.	Políticas Relacionadas: “Acceso a Comandos del Sistema Operativo” y “Modificación de la Información de Negocio de Producción”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
10. Actualizaciones de la Base de Datos	Política: Las actualizaciones a las bases de datos de producción sólo podrán efectuarse a través de los canales establecidos que hayan sido autorizados por la gerencia.	Políticas Relacionadas: “Modificación de la Información de Negocio de Producción” y “Actualizaciones Automáticas de Software”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
11. Aplicaciones de Producción Multiusuario	Política: Todas las aplicaciones de negocios de producción que respaldan a múltiples usuarios deben ser protegidas por un sistema de control de acceso autorizado por la gerencia de Seguridad Informática.	Políticas Relacionadas: “Actualización de Información de Producción”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
12. Divulgación de Registro del Sistema y Seguimientos de Auditorías	Política: Los registros del sistema o rastros de auditoría de aplicaciones no deben ser divulgados a personas fuera del equipo de individuos que ordinariamente ven tal información para ejecutar su trabajo o investigar incidentes de seguridad informática.	Políticas Relacionadas: “Acceso a Registros” e “Investigaciones de Seguridad Informática”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
13. Acceso a la Información de las Aplicaciones de Producción	Política: El personal que desarrolla el software de aplicación del negocio no debe tener acceso a la información de producción, con la excepción de la información que sea importante para el software de la aplicación en la cual estén trabajando.	Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer,’ “Separación de Tareas,’ y “Acceso del Desarrollador a la Información de Producción”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
14. Información Confidencial de Terceros	Política: Toda la información confidencial o de propiedad confiada a la Gobernación por un tercero, debe ser protegida como si fuese información confidencial de la Gobernación, a menos que en un contrato se especifique lo contrario.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
15. Acceso a la Información Personal	Política: Toda la información de clientes que identifique números de tarjetas de crédito, referencias de crédito o cédulas de identidad, debe ser sólo accesible al personal de la Gobernación que necesita ese acceso para hacer su trabajo.	Políticas Relacionadas: “Eliminación de la Información de Pago”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
16. Acceso al Almacén de Datos	Política: El acceso al almacén de datos debe ser restringido a la gerencia media y alta de la Gobernación.	Políticas Relacionadas: “Restricciones a la Recopilación de la Información” y “Etiquetado de Clasificación Múltiple”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
17. Diseminación Secundaria de la Información Secreta	Política: La información secreta debe ser divulgada sólo cuando se haya obtenido la autorización explícita del Propietario, y ninguna persona a quien se haya otorgado el acceso a información secreta no debe divulgarla a ninguna otra persona.	Políticas Relacionadas: “Propiedad de la Información, “Clasificación de Datos en Cuatro Categorías, “Acuerdos de Confidencialidad,’ y “Manejo de Información Sensible”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
18. Acceso a Información Sensible o Valiosa	Política: El acceso a la información sensible o valiosa de la Gobernación debe ser otorgado sólo después de obtenerse la autorización expresa de la gerencia.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Restricción de Privilegios — Necesidad de Conocer”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
19. Acceso a la Información Secreta	Política: El acceso a la información secreta se debe otorgar solamente a personas específicas, no a grupos de personas.	Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer,’ “Identificador Único de Usuario y Contraseña Obligatorios,’ “Clasificación de Datos en Cuatro Categorías,’ y “Acceso a Información Sensible o Valiosa”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
9.06.02 Aislamiento de Sistemas Sensibles				
1. Servidores para Aplicaciones Críticas	Política: A menos que las consideraciones técnicas indiquen que sería excesivamente costoso, los servidores de producción críticos deben ser máquinas dedicadas a un propósito, ejecutando sólo una aplicación.	Políticas Relacionadas: “Dispersión de Sistemas Computacionales” y “Computadores para Cortafuegos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
2. Aislamiento de Sistemas con Información Secreta	Política: Los sistemas de computación de la Gobernación que contienen información secreta no deben estar conectados con ninguna red u otro computador.	Políticas Relacionadas: “Interconexión de Sistemas” e “Información Secreta en la Web”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Altos
9.07 Monitoreo del Acceso y Uso del Sistema				
9.07.01 Registro de Eventos				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Registros en Sistemas y Aplicaciones Sensibles	Política: Todos los sistemas de aplicaciones que manejen información sensible de la Gobernación deben generar registros que capten toda adición, cambio y eliminación de dicha información.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Contenido de Registros en Aplicaciones de Producción	Política: Todos los sistemas de computación que manejen sistemas de aplicaciones de producción de la Gobernación deben incluir un registro que contenga, como mínimo, actividades de sesiones de usuarios incluyendo su identificador de usuario, fecha y hora de inicio y cierre de la sesión, aplicaciones utilizadas, cambios a los archivos críticos de los sistemas de aplicaciones, adiciones y cambios a los privilegios de los usuarios e inicios y cierres de sistemas.	Políticas Relacionadas: "Registro de Eventos Importantes de Seguridad" y "Registros en Sistemas y Aplicaciones Sensibles"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Registro de Eventos Importantes de Seguridad	Política: Los sistemas de computación que manejen información sensible, valiosa o crítica, deben registrar de forma segura todos los eventos importantes relativos a la seguridad incluyendo, sin limitantes, los intentos de deducir la contraseña, utilizar privilegios no autorizados, y cambios al software de aplicación de producción y al software del sistema.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Registro de Intentos de Acceso	Política: Deben registrarse todos los intentos de los usuarios por iniciar la sesión y conectarse con los sistemas informáticos de producción de la Gobernación, sin importar si fueron exitosos o no.	Políticas Relacionadas: "Contenido de Registros en Aplicaciones de Producción" y "Sincronización del Reloj"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5. Registros de Eventos de Seguridad Iniciados Por Usuarios	Política: Se debe llevar uno o más registros que rastreen las actividades importantes de seguridad de un usuario específico por un período de tiempo razonable.	Políticas Relacionadas: "Consentimiento para Acciones Cuestionables en los Sistemas"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
6. Registros de Acceso a Información Privada	Política: Se debe registrar la identidad de cada usuario que acceda a la información privada contenida en los sistemas informáticos de la Gobernación.	Políticas Relacionadas: "Manejo del Registro Personal" y "Registros en Sistemas y Aplicaciones Sensibles"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
7. Período de Retención de Registros	Política: Los registros computarizados que contengan eventos importantes de seguridad se deben retener como mínimo tres meses, y dentro de ese tiempo se deben proteger para que no puedan modificarse y que sólo puedan leerlos las personas autorizadas.	Políticas Relacionadas: “Registros del Sistema de Control de Acceso” y “Retención de Registros de Privilegios de Control de Acceso”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
8. Remoción de Registros de Computadores Accesibles desde Internet	Política: Los registros de sistemas y aplicaciones contenidos en computadores accesibles por Internet deben ser movidos por lo menos diariamente a otras máquinas que no sean directamente accesibles desde Internet.	Políticas Relacionadas: “Información de Registro del Cliente,’ “Desactivación, Cambio o Eliminación de Registros,’ y “Retención de Registros de Privilegios de Control de Acceso”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9. Retención de Registros de Privilegios de Control de Acceso	Política: Los registros computarizados que reflejen los privilegios de acceso de cada usuario en los sistemas multiusuario y redes de la Gobernación se deben conservar de manera segura por un período razonable de tiempo.	Políticas Relacionadas: “Otorgamiento de Privilegios del Sistema”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10. Arquitectura de Sistemas para Registro de Actividades	Política: El software de sistemas de aplicaciones o base de datos de la gerencia debe conservar registros de las actividades de los usuarios y estadísticas relacionadas a esas actividades que permitan identificarlas y emitir alarmas que reflejen algún acontecimiento sospechoso del negocio.	Políticas Relacionadas: “Controles de Acceso al Sistema de Computación”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
11. Registros de Auditoría en los Sistemas	Política: Los registros de los eventos importantes de seguridad en computación deben proporcionar datos suficientes como para apoyar auditorías amplias de la eficacia y cumplimiento de las medidas de seguridad.	Políticas Relacionadas: “Revisión de los Controles de los Sistemas Informáticos — Interno”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
12. Notificación y Registro de Monitoreo de Usuarios	Política: Cuando una cuenta computarizada o de red de un usuario está siendo monitoreada con propósitos investigativos o disciplinarios, se debe informar inmediatamente de esta actividad al gerente del usuario involucrado, y todo el monitoreo debe ser registrado.	Políticas Relacionadas: “Notificación de Monitoreo Electrónico del Desempeño” y “Herramientas de Monitoreo de Sistemas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
15. Registros de Uso de Internet	Política: Los gerentes de departamento deben recibir, revisar y aprobar los reportes de las páginas web visitadas, los archivos descargados y otros intercambios de información en Internet para las actividades de negocio del departamento.	Políticas Relacionadas: “Notificación y Registro de Monitoreo de Usuarios” y “Uso Personal de Internet”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
16. Monitoreo de Mensajes de Correo Electrónico	Política: Los mensajes enviados por el sistema interno de correo electrónico de la Gobernación pueden ser leídos por la gerencia y administradores de sistemas de la Gobernación.	Políticas Relacionadas: “Uso Distinto al Empresarial de la Información de la Organización,’ “Examen de los Datos Almacenados en los Sistemas,’ “Monitoreo de Mensajes de Correo Electrónico,’ y “Privacidad en Correo Electrónico”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
9.08 Computación Móvil				
9.08.01 Computación Móvil				
1. Uso de Pequeños Computadores Portátiles	Política: Los asistentes digitales personales, los computadores portátiles y los teléfonos inteligentes no se deben utilizar para información de negocios de la Gobernación, a menos que hayan sido configurados con los controles necesarios y autorizados para dicho uso por la gerencia de Seguridad Informática.	Políticas Relacionadas: “Teléfonos Celulares o Inalámbricos”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
2. Información Sensible en Pequeños Computadores	Política: Los mecanismos de seguridad disponibles en los asistentes digitales personales, computadores portátiles, teléfonos inteligentes y similares, no deben ser utilizados con información sensible de la Gobernación.	Políticas Relacionadas: “Protección de la Re inicialización Basada en Contraseña,’ “Información Secreta en Computadores Portátiles,’ y “Préstamo de Computadores Que Contienen Información Sensible”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
3. Información Secreta en Computadores Portátiles	Política: Los empleados que posean dispositivos portátiles, un laptop, un libro de anotaciones, agenda u otro dispositivo similar que contenga información confidencial de la Gobernación, no deben dejarlos desatendidos a menos que la información esté cifrada.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,’ “Remoción de Información Sensible en Papel,’ “Computadores Portátiles en Aviones,’ y “Cifrado en Medios de Respaldo”	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
4. Uso de Computadores Portátiles	Política: Hasta tanto se emitan los requerimientos para la operación segura de computadores portátiles, los trabajadores no deben utilizar estos sistemas para procesar información de la Gobernación clasificada como confidencial o secreta.	Políticas Relacionadas: “Información Sensible en Pequeños Computadores” y “Uso de Pequeños Computadores Portátiles”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
5. Computadores Portátiles con Información Sensible	Política: Todos los computadores portátiles, laptops, libretas y otros computadores transportables que contengan información sensible de la Gobernación, deben emplear consistentemente el cifrado en el disco duro para todos los archivos y protección de arranque en el funcionamiento del computador.	Políticas Relacionadas: “Información Secreta en Computadores Portátiles”	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Información Sensible en Computadores Personales	Política: Si se almacena información sensible en el disco duro o en otros componentes internos de un computador personal, la información se debe proteger mediante una contraseña de control de acceso o cifrándola.	Políticas Relacionadas: "Etiquetado Durante el Ciclo de Vida de la Información,' "Etiquetado Completo de la Clasificación,' y "Almacenamiento de Información Sensible"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
7. Préstamo de Computadores Que Contienen Información Sensible	Política: No se debe prestar a nadie un computador personal, un computador manual, un computador transportable, un asistente personal digital, un teléfono inteligente o cualquier otro computador utilizado para actividades de negocios que contenga información sensible.	Políticas Relacionadas: "Identificador Único de Usuario y Contraseña Obligatorios" y "Contraseñas Compartidas"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
8. Propiedad de la Organización en Sitios Alternativos de Trabajo	Política: Deben tomarse precauciones razonables en los sitios alternativos de trabajo, para proteger el hardware, el software y la información de la Gobernación de robo, daño y abuso.	Políticas Relacionadas: "Protección de la Información,' "Remoción de Información Sensible,' y "Descarga de Información Sensible"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
9. Información Almacenada en Computadores Portátiles Propiedad de la Organización	Política: La información almacenada en computadores portátiles de la Gobernación es propiedad de ella y la Gobernación la puede inspeccionar o utilizar de cualquier manera y a cualquier hora y, al igual que el equipo, debe ser devuelta a la Gobernación al momento en que el empleado cese su relación laboral con la Gobernación.	Políticas Relacionadas: "Información Sensible en Computadores Personales" y "Retención de Información al Terminar Empleo"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
10. Posesión de los Computadores Portátiles	Política: Los empleados deben mantener los computadores portátiles de la Gobernación en su poder todo el tiempo, a menos que los hayan depositado en un lugar seguro, como por ejemplo en un armario cerrado con llave o en la caja fuerte de un hotel.	Políticas Relacionadas: "Computadores Portátiles con Información Sensible,' "Información Secreta en Computadores Portátiles,' y "Tarjetas de Contraseñas Dinámicas"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
11. Alternativas para Computadores Móviles	Política: Cuando estén fuera de las oficinas de la Gobernación, los usuarios de computadores móviles deben utilizar un software de cifrado para proteger la	Políticas Relacionadas: "Equipo de Teletrabajo, "Viajes con Información Secreta,' y "Exposición Pública de Información Sensible"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
9.08.02 Teletrabajo				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Operadores de Entrada de Datos	Política: Todos los operadores de la Gobernación que realicen el trabajo de introducción de datos deben emplear clientes simples, tal como los configure la gerencia de Sistemas Informáticos y descargar el software para su trabajo al comienzo de cada día de trabajo.	Políticas Relacionadas: “Estaciones de Trabajo Sin Discos,’ “Descarga de Software,’ y “Descarga de Información Sensible”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
2. Equipo de Teletrabajo	Política: Los empleados de la Gobernación que trabajen en sitios alternativos deben utilizar computadores y equipos de redes proporcionados por la Gobernación, a menos que el Centro de Atención al Usuario autorice el uso de otro equipo compatible con los sistemas y controles informáticos de la Gobernación.	Políticas Relacionadas: “Requisitos de Seguridad para Teletrabajo,’ “Computadores Portátiles con Información Sensible,’ y “Gabinetes Metálicos con Cerradura”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
3. Ambientes de Teletrabajo	Política: Para retener el privilegio de trabajar externamente, todos los teletrabajadores deben estructurar su ambiente de trabajo remoto para que esté de acuerdo con las políticas y normas de la Gobernación.	Políticas Relacionadas: “Reautorización de los Privilegios de Acceso de Usuario” e “Información Secreta en Computadores Portátiles”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
4. Requisitos de Seguridad para Teletrabajo	Política: Antes de que pueda comenzar un convenio de teletrabajo, el gerente del trabajador debe estar satisfecho de que el sitio alternativo de trabajo es apropiado para que el trabajador ejecute trabajos para la Gobernación.	Políticas Relacionadas: “Pases de Propiedad, ’“Software Antivirus Actual,’ y “Gabinetes Metálicos con Cerradura”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
5. Procedimientos de Seguridad Informática en Teletrabajo	Política: Los teletrabajadores deben cumplir todas las políticas de seguridad de los sistemas remotos incluyendo, sin limitantes, el cumplimiento de los convenios de licencia del software, ejecución de respaldos regulares y el uso de máquinas trituradoras de papel para disponer de la información sensible impresa.	Políticas Relacionadas: “Convenios con Terceros” y “Convenio de Cumplimiento”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
6. Inspección de Ambientes de Teletrabajo	Política: La Gobernación debe mantener el derecho a conducir inspecciones de las oficinas de los teletrabajadores con previo aviso de sólo uno o más días.	Políticas Relacionadas: “Revisión de los Controles de los Sistemas Informáticos — Interno”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
7. Gabinetes Metálicos con Cerradura	Política: Todos los trabajadores que deban mantener información confidencial de la Gobernación para realizar su trabajo en sus casas, deben recibir mobiliario de metal con cerradura para el almacenamiento adecuado de esta información.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,’ “Equipo de Teletrabajo, “Seguridad de la Información Sensible,’ “Requisitos de Seguridad para Teletrabajo,’ y “Remoción de Información Sensible”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos

Políticas de Software

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
10 DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
10.01 Requerimientos de Seguridad de los Sistemas				
10.01.01 Análisis y Especificaciones de los Requerimientos de Seguridad				
1. Identificación de Requisitos de Seguridad	Política: Antes de desarrollar o adquirir un nuevo sistema, la gerencia del departamento usuario debe haber especificado claramente los requisitos relevantes de seguridad.	Políticas Relacionadas: “Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas” y “Especificaciones para Software Desarrollado Internamente”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
2. Propuestas para Desarrollar Sistemas Internos	Política: Toda propuesta de proyecto de desarrollo interno de sistemas informáticos con un presupuesto propuesto por encima de $ 100.000 debe ser copiada a la gerencia de Seguridad Informática al mismo tiempo que se distribuya a la alta gerencia para su revisión y aprobación.	Políticas Relacionadas: “Evaluación de Nuevas Tecnologías” y “Enunciados Sobre el Impacto de la Seguridad”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Inclusión de Seguridad en Sistemas	Política: Los desarrolladores de sistemas internos deben incrustar la seguridad dentro de los sistemas que construyan o mejorar todas las instancias en las que haya una solución disponible comercialmente, a costo razonable y generalmente aceptada.	Políticas Relacionadas: “Facilidad de Uso de los Controles de Seguridad” e “Identificación de Requisitos de Seguridad”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Especificaciones para Software Desarrollado Internamente	Política: Todo software desarrollado por personal interno que se utilice para procesar información sensible, valiosa o crítica debe poseer una especificación formal por escrito que forme parte de un acuerdo entre el Propietario de la información y el desarrollador del sistema, redactada y elaborada antes de que comiencen los esfuerzos de programación.	Políticas Relacionadas: “Análisis del Impacto sobre la Seguridad Informática”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
5. Principios de Codificación de Aplicación	Política: Deben utilizarse principios y prácticas seguras de codificación, especificados y actualizados por la gerencia de Seguridad Informática para todo el software desarrollado o mantenido internamente.	Políticas Relacionadas: “Especificaciones para Software Desarrollado Internamente” e “Identificación de Requisitos de Seguridad”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
6. Herramientas y Técnicas de Desarrollo Maduras	Política: Todos los proyectos de desarrollo interno de software deben utilizar herramientas y técnicas de desarrollo maduras.	Políticas Relacionadas: “Versiones de Sistemas Operativos” e “Interfaces a Redes Externas”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
7. Lenguajes de Programación de Alto Nivel	Política: Todos los proyectos de desarrollo interno de sistemas que involucren un esfuerzo de más de $100.000 deben ser programados en un lenguaje aprobado de más alto nivel, a menos que se obtenga permiso de la gerencia de Sistemas Informáticos.	Políticas Relacionadas: “Programas de Aplicación de Usuarios Finales”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
8. Re-Usabilidad del Software	Política: Todos los proyectos de desarrollo interno con presupuesto por encima de $ 100.000, deben tener como meta secundaria el desarrollo de software modular confiable que pueda ser introducido en un repositorio de software compartido.	Políticas Relacionadas: “Migración de Software”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9. Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas	Política: Para todos los sistemas de aplicaciones de negocios, los diseñadores y desarrolladores de sistemas deben considerar la seguridad desde el principio del proceso de diseño de los sistemas, hasta su conversión en sistemas de producción.	Políticas Relacionadas: “Especificaciones para Software Desarrollado Internamente,’ “Proceso de Control de Cambios para Aplicaciones de Negocios,’ y “Convenciones en Desarrollo de Sistemas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10. Dependencia de Mecanismos Comunes para los Controles	Política: Deben seleccionarse y diseñarse controles de seguridad informática de costo justificado, de forma tal que se minimice la dependencia de un mecanismo común.	Políticas Relacionadas: “Sistemas de Seguridad Independientes,’ “Normas de Implantación de Controles,’ e “Intervención Humana en Procesos Asistidos por el Computador”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
11. Funcionalidad de la Seguridad en las Aplicaciones del Negocio	Política: Siempre que sea factible y eficaz en función de costos, los desarrolladores de sistemas deben confiar en los servicios del sistema para la funcionalidad de la seguridad en lugar de incorporar dicha funcionalidad en las aplicaciones.	Políticas Relacionadas: “Controles de Acceso al Sistema de Computación” y “Proceso de Control de Cambios para Aplicaciones de Negocios”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
12. Compra de Soluciones de Seguridad Informática	Política: La Gobernación debe adquirir soluciones de seguridad informática disponibles comercialmente en lugar de construirlas internamente, a menos que la efectividad en función de los costos de la solución interna sea claramente analizada, documentada y aprobada por la gerencia de Seguridad Informática.	Políticas Relacionadas: “Normas de Seguridad Informática Específicas a Cada Industria,’ “Procura de Hardware y Software,’ y “Requerimientos para el Soporte de Emergencias y Desastres”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
13. Controles Mínimos en Sistemas Informáticos	Política: Como mínimo, todos los sistemas informáticos de la Gobernación deben incluir los controles normales que se encuentran en otras organizaciones que enfrentan circunstancias similares.	Políticas Relacionadas: “Evaluación del Riesgo en los Sistemas de Producción,’ “Normas de Implantación de Controles,’ y “Revisión de los Controles de los Sistemas Informáticos — Independiente”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
14. Uso de Productos Evaluados	Política: Debe utilizarse un producto de seguridad de sistemas informáticos evaluado oficialmente en lugar de un producto que no haya sido evaluado.	Políticas Relacionadas: “Normas de Seguridad Informática Específicas a Cada Industria”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
10.02 Seguridad en Sistemas de Aplicaciones				
10.02.01 Validación de los Datos de Entrada				
1. Transacciones de Entrada en Producción	Política: Cada transacción de entrada presentada a un sistema de producción debe tener asignada un número secuencial o identificador único.	Políticas Relacionadas: “Retención del Documento Fuente,’ “Acceso Físico de Trabajadores Cesados,’ y “Transacciones Distintas a Producción”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Validación de Datos de Entrada y Manejo de Ítem Rechazado	Política: Todas las transacciones que deban ingresarse en un sistema multiusuario de producción deben estar sujetas a verificaciones razonables, verificaciones de edición o verificaciones de validación, y las transacciones que no aprueben esta clase de verificaciones deben ser rechazadas con una notificación del rechazo enviada al emisor, corregidas y reenviadas o suspendidas hasta que se haga una posterior investigación.	Políticas Relacionadas: “Transacciones de Entrada Rechazadas” y “Cronograma de Resolución de Archivos en Suspenso”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Entrada con Doble Tecla de Transacciones	Política: Todos los procesos de entrada de producción basados en el teclado que involucren cantidades por encima de $ 1.000 y que inicien una transacción deben incluir la entrada doble de la cantidad.	Políticas Relacionadas: “Investigación de Errores” y “Errores y Manipulación de Registros”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Originador de Transacciones	Política: Las transacciones que afecten información sensible, crítica o valiosa deben ser iniciadas únicamente por documentos fuente o mensajes computarizados en los que el individuo que las origina o el sistema estén claramente identificados.	Políticas Relacionadas: “Autorización para Transacciones en Sistema de Producción,’ “Clasificación de Datos en Cuatro Categorías,’ “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,’ y “Firmas en Correo Electrónico”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10.02.02 Control de Procesamiento Interno				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Modificación de la Información de Negocio de Producción	Política: Deben establecerse los privilegios de manera que los usuarios de los sistemas no puedan cambiar los datos de producción de manera irrestricta.	Políticas Relacionadas: “Privilegios Sobre la Información de Producción” y “Separación de Tareas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Falla de Operación del Software	Política: Cada vez que el software desarrollado internamente falle y no produzca los resultados esperados, siempre debe proporcionar un mensaje de error o alguna otra indicación de falla como respuesta al operador.	Políticas Relacionadas: “Retroalimentación del Software al Usuario” y “Mantenimiento Preventivo”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Retroalimentación del Software al Usuario	Política: Cada vez que el software desarrollado internamente reciba una entrada del usuario, debe dar respuesta indicando si se llevó a cabo la solicitud.	Políticas Relacionadas: “Falla de Operación del Software”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
4. Interrupción del Sistema por Seguridad	Política: Los robots y otras máquinas computarizadas deben ser programados de manera que la actividad actual se detenga inmediatamente si está dañando o es factible que dañe a una persona.	Políticas Relacionadas: “Contraseñas de Presión” e “Intervención Humana en Procesos Asistidos por el Computador”	Política Dirigida a:Gerencia y personal técnico	
5. Seguimiento de Errores y Problemas de Seguridad por Desarrolladores	Política: Todas las quejas sobre errores en el software, omisiones y problemas de seguridad que puedan ser atribuibles al software desarrollado internamente deben poder ser rastreadas hasta los diseñadores, programadores y demás personal involucrado en su desarrollo.	Políticas Relacionadas: “Proyectos que Involucran Seguridad Humana” y “Originador de Transacciones”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
6. Cambios en la Sensibilidad, Criticidad y Valor de la Información	Política: Las transacciones que afecten información sensible, crítica y valiosa deben ser procesadas únicamente si el iniciador o el sistema está autorizado para procesar dichas transacciones.	Políticas Relacionadas: “Autentificación de Usuario Que Accede Vía Telefónica,’ “Clasificación de Datos en Cuatro Categorías,’ “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones ‘y “Autentificación del Usuario por el Sistema Operativo”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
7. Validación de los Controles	Política: Antes de utilizar todos los datos financieros que sean críticos para la toma de decisiones que involucren más de $ 100.000, los datos deben ser verificados en forma cruzada mediante controles totales, registros de cuentas o controles similares.	Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones, “Validación Cruzada de la Información,’ y “Revisión de Análisis Computarizados”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
8. Transacciones de Entrada Rechazadas	Política: Todas las transacciones de entrada rechazadas deben ser colocadas en un archivo en suspenso e incluidas en reportes de excepción hasta que hayan sido reenviadas exitosamente para su procesamiento o resueltas de otra manera.	Políticas Relacionadas: “Cronograma de Resolución de Archivos en Suspenso” y “Validación de Entrada Rechazada o Suspendida”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9. Cronograma de Resolución de Archivos en Suspenso	Política: Todas las transacciones de entrada que se mantienen en estatus de suspenso en espera de una investigación deben ser o reenviadas o manejadas dentro de un plazo de 10 días hábiles a partir de su ingreso original.	Políticas Relacionadas: “Transacciones de Entrada Rechazadas” y “Validación de Entrada Rechazada o Suspendida”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10. Ocultar Números de Cuenta de Clientes	Política: Los números de cuenta que aparecen en los recibos generados por computador que se entregan a los clientes deben ser parcialmente ocultados o truncados.	Políticas Relacionadas: “Divulgación del Registro de las Actividades del Cliente,’ “Diseminación Secundaria de la Información Secreta,’ y “Entrega de Información Secreta”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
11. Entrega de Recibo de Compra	Política: Un aviso que indique que "los clientes que no reciban su comprobante no pagarán por su compra" debe ser colocado de manera destacada en todas las cajas registradoras.	Políticas Relacionadas: “Separación de Tareas” y “Ocultar Números de Cuenta de Clientes”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
12. Uso de Números de Tarjeta de Crédito	Política: Los números de las tarjetas de crédito no deben ser utilizados para la identificación de los clientes ni para ningún otro propósito excepto el de procesar pagos de bienes o servicios.	Políticas Relacionadas: “Cifrado de Datos de Pago” y “Números de Cuenta Bancaria”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
13. Diseño de Controles de Seguridad Informática	Política: Cuando se diseñen controles de seguridad informática, los empleados deben emplear grandes márgenes de error y grandes cantidades de tiempo.	Políticas Relacionadas: “Errores y Manipulación de Registros” y “Dependencia de Mecanismos Comunes para los Controles”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
14. Intervención Humana en Procesos Asistidos por el Computador	Política: Todos los procesos asistidos por computador deben involucrar la intervención humana antes de iniciar cualquier acción que pueda resultar en una amenaza a la vida o a la seguridad humana.	Políticas Relacionadas: “Dependencia de Mecanismos Comunes para los Controles” e “Interrupción del Sistema por Seguridad”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
15. Errores y Manipulación de Registros	Política: Los sistemas de computación de la Gobernación deben ser construidos de manera que ninguna persona pueda cometer un error o manipular los registros sin que esos eventos sean detectados por otra persona durante la ejecución rutinaria de sus responsabilidades.	Políticas Relacionadas: “Separación de Tareas, ’“Entrada con Doble Tecla de Transacciones Mayores,’ e “Investigación de Errores”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
16. Archivos y Almacenamiento Temporales	Política: Los archivos temporales y las ubicaciones de almacenamiento temporales dentro de la memoria de los computadores de propósito general, deben ser sobrescritos cuando el proceso programado que los creó haya completado su trabajo.	Políticas Relacionadas: “Apagado de Computadores, “Certificado de Destrucción de Medios de Almacenamiento,’ y “Materiales para la Generación de Contraseñas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Altos
10.02.03 Autentificación de Mensajes				
1. Autorización para Transacciones en Sistema de Producción	Política: Deben existir métodos que aseguren que todas las entradas a los sistemas de producción que han sido enviadas para su procesamiento hayan sido autorizadas adecuadamente.	Políticas Relacionadas: “Autorización para Transacciones de Producción,’ “Cambios en Producción” y “Originador de Transacciones”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Validación de Entrada Rechazada o Suspendida	Política: Las transacciones de entrada corregidas y reenviadas, o aquellas suspendidas y posteriormente aprobadas para ser reenviadas, deben estar sujetas a los mismos procedimientos de validación que las transacciones de entrada originales.	Políticas Relacionadas: “Prueba del Software” y “Transacciones de Entrada Rechazadas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10.02.04 Validación de Datos de Salida				
1. Controles de Datos de Salida	Política: Deben establecerse controles y procedimientos para validar toda la información sensible o crítica procesada por los sistemas de aplicaciones de la Gobernación.	Políticas Relacionadas: “Validación de Datos de Entrada y Manejo de Ítem Rechazado” y “Validación de Entrada Rechazada o Suspendida”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
2. Revisión de Cambios a Registros Internos	Política: La gerencia debe revisar o establecer mecanismos para que personas responsables y adecuadamente calificadas revisen la racionalidad y exactitud de todos los cambios en los registros internos.	Políticas Relacionadas: “Revisión de Registros del Sistema”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
10.03 Controles Criptográficos				
10.03.01 Política Sobre el Uso de los Controles Criptográficos				
1. Versiones de Software para Firmas Digitales y Cifrado de Archivos	Política: Los usuarios deben retener copias de respaldo de todas las versiones del software utilizado para producir firmas digitales y para cifrar archivos.	Políticas Relacionadas: “Ciclo de Vida de las Claves Privadas de Firmas Digitales” y “Controles para Modificaciones de los Registros del Sistema”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos
10.03.02 Cifrado				
1. Autorización del Proceso de Cifrado —Sistemas	Política: Los procesos de cifrado no deben ser utilizados para la información de la Gobernación, a menos que los procesos sean aprobados por la gerencia de Seguridad Informática.	Políticas Relacionadas: “Armamentos en Comercio Internacional”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
2. Autorización de Proceso de Cifrado —Usuarios	Política: Los usuarios no deben emplear el cifrado, las firmas digitales o los certificados digitales en ninguna de las actividades de negocios o información de negocios de la Gobernación sin la autorización escrita del jefe de su departamento, sin la finalización de un adecuado adiestramiento y sin que personal autorizado haya configurado sus sistemas.	Políticas Relacionadas: “Autorización del Proceso de Cifrado — Sistemas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
3. Contraseñas y Claves en Utilidades de Cifrado	Política: Los empleados nunca deben emplear programas utilitarios de cifrado que soliciten que el usuario ingrese una contraseña o clave de cifrado.	Políticas Relacionadas: “Autorización del Proceso de Cifrado — Sistemas”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Low
4. Algoritmo de Cifrado Normal e Implantación	Política: Si se utiliza el cifrado, deben emplearse algoritmos normales aprobados por el gobierno y las implantaciones normalizadas.	Políticas Relacionadas: “Procura de Hardware y Software”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
5. Algortimos de Cifrado Evaluados Públicamente	Política: Todo algoritmo de cifrado de propósito general utilizado para proteger la información de producción de la Gobernación y sus sistemas informáticos debe ser divulgado públicamente y debe haber sido evaluado por expertos criptográficos.	Políticas Relacionadas: “Algoritmo de Cifrado Normal e Implantación”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Inicialización del Sistema de Cifrado	Política: Siempre que se inicialice, instale, active o reinicialice un sistema de cifrado que se utilizará en los sistemas informáticos de producción de la Gobernación, debe estar presente un especialista auditor de computación.	Políticas Relacionadas: “Implantación de Sistemas Multiusuario” y “Revisión de los Controles de los Sistemas Informáticos — Interno”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
7. Eliminación de Datos Fuente Después de Cifrar	Política: Cada vez que se utilice el cifrado, los empleados no deben borrar la única versión legible de los datos, a menos que hayan demostrado que el proceso de cifrado puede restablecer una versión legible de los datos.	Políticas Relacionadas: “Sistemas de Cifrado de Propósito General”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos
8. Compresión y Cifrado de Datos Secretos	Política: Si la información secreta debe almacenarse en un sistema de computación multiusuario, debe ser comprimida y posteriormente cifrada utilizando un algoritmo de cifrado aprobado.	Políticas Relacionadas: “Autorización del Proceso de Cifrado — Sistemas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
9. Módulos de Hardware para el Proceso de Cifrado	Política: Todos los procesos relacionados con el cifrado deben ser realizados en módulos de hardware no modificables.	Políticas Relacionadas: “Divulgación de Claves de Cifrado — Controles,’ “Protección Contra la Radiación Electromagnética,’ y “Divulgación de Claves de Cifrado — Autorización”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
10. Protección de Mensajes Cifrados	Política: Todo contenido enviado a través de la red de datos interna de la Gobernación debe estar cifrado, acompañado de mensajes para desviar la atención y relleno de información ajena para ocultar la longitud de los mensajes enviados.	Políticas Relacionadas: “Esconder Transmisión de la Información” y “Privacidad de Información de Contacto de Remitentes”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Altos
11. Información en Servidores FTP Anónimos	Política: Todos los archivos proporcionados por los usuarios que no hayan sido aprobados explícitamente para su divulgación pública por la gerencia de Mercadeo y que se encuentren residentes en el servidor FTP anónimo de la Gobernación, deben cifrarse utilizando software normal de la Gobernación.	Políticas Relacionadas: “Transmisión de Datos Secretos”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
10.03.03 Firmas Digitales				
1. Ejecución de Programa Java	Política: Los empleados no deben ejecutar aplicaciones Java descargadas de Internet a menos que la aplicación provenga de una fuente conocida y confiable, que se haya verificado la firma digital y que no se haya descubierto ningún problema.	Políticas Relacionadas: “Inhabilitación de Java”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Sitios Web y Comerciales en Internet	Política: Se requiere un certificado digital actualizado para todo servidor de Internet que maneje los negocios de la Gobernación y al que puedan conectarse clientes, prospectos y demás personas.	Políticas Relacionadas: "Autorización de Proceso de Cifrado — Usuarios,' "Identificación Positiva para Uso del Sistema,' e "Identificadores Personales en Ubicaciones Públicas"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
10.03.04 Servicios de No Repudiación				
1. Sistemas de Cifrado de Propósito General	Política: Todos los procesos de cifrado de propósito general que se ejecuten en los sistemas informáticos de la Gobernación deben incluir funciones de custodia de claves.	Políticas Relacionadas: "Gestión Automática de Claves de Cifrado" y "Eliminación de Datos Fuente Después de Cifrar"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10.03.05 Manejo de Claves				
1. Divulgación de Claves de Cifrado —Autorización	Política: Las claves de cifrado no deben revelarse a consultores, contratistas, o terceros, a menos que se haya obtenido autorización del vicepresidente ejecutivo.	Políticas Relacionadas: "Sistemas de Gestión de Claves de Cifrado" y "Sospecha de Divulgación de Contraseña"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
2. Sistemas de Gestión de Claves de Cifrado	Política: El sistema de cifrado de la Gobernación, debe diseñarse de manera tal que no sea una sola persona la que tenga el conocimiento completo de la clave de cifrado.	Políticas Relacionadas: "Separación de Tareas" y "Algoritmos Generadores de Contraseñas"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
3. Delegación de la Responsabilidad en la Gestión	Política: La responsabilidad de la gestión de las claves debe delegarse solamente a personas que hayan pasado por una verificación de antecedentes, una auditoría de seguridad operacional, así como firmado un acuerdo de confidencialidad.	Políticas Relacionadas: "Otorgamiento de Privilegios del Sistema" y "Delegación de la Propiedad de la Información"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
4. Vigencia de los Certificados Digitales	Política: El período de validez para certificados digitales emitidos por la Gobernación no debe ser superior a un año.	Políticas Relacionadas: "Secreto de la Clave de Cifrado" y "Ciclo de Vida de Claves de Cifrado"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
5. Protección de Claves Raíces de Certificados Digitales	Política: La clave raíz para la jerarquía del certificado digital debe protegerse bajo seguridad física rigurosa, control dual, separación de componentes de clave y separación de tareas.	Políticas Relacionadas: "Delegación de la Responsabilidad en la Gestión" y "Sitios Web y Comerciales en Internet"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
6. Transmisión de Datos y Claves de Cifrado	Política: Si se utilizan los cifrados y si las claves se transmiten en forma legible a otra persona, la información protegida con cifrado debe transmitirse a través de un canal de comunicación diferente al de las claves utilizadas para manejar el proceso de cifrado.	Políticas Relacionadas: “Separación de Tareas, “Medios de Almacenamiento de Claves de Cifrado,’ y “Sistemas de Gestión de Claves de Cifrado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Altos
7. Gestión Automática de Claves de Cifrado	Política: Si están disponibles comercialmente, la Gobernación debe emplear procesos automatizados de gestión de claves.	Políticas Relacionadas: “Responsabilidad de la Gestión de Claves” y “Sistemas de Gestión de Claves de Cifrado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
8. Ciclo de Vida de Claves de Cifrado	Política: Las claves utilizadas para el cifrado de datos de la Gobernación deben cambiarse por lo menos cada noventa (90) días.	Políticas Relacionadas: “Vencimiento de Claves de Cifrado” y “Cambios Obligatorios de Contraseña”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
9. Vencimiento de Claves de Cifrado	Política: Todas las claves de cifrado deben tener un tiempo de vida establecido y deben cambiarse durante o antes de la fecha de vencimiento.	Políticas Relacionadas: “Ciclo de Vida de Claves de Cifrado” y “Etiquetado Durante el Ciclo de Vida de la Información”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
10. Generación de Claves de Cifrado	Política: Cuando se utilice el cifrado, las claves deben ser generadas a través de medios poco discernibles para el adversario, y que originen claves difíciles de adivinar.	Políticas Relacionadas: “Gestión Automática de Claves de Cifrado,’ “Longitud de Claves de Cifrado Seleccionadas por Usuarios,’ y “Semilla para Contraseñas Generadas por el Sistema”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
11. Longitud de Claves de Cifrado Seleccionadas por Usuarios	Política: Cuando el usuario elige las claves de cifrado, el sistema de cifrado debe impedir al usuario crear claves con menos de diez (10) caracteres.	Políticas Relacionadas: “Generación de Claves de Cifrado” y “Longitud Mínima de Contraseñas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
12. Materiales para la Generación de Claves	Política: Cuando se utilice el cifrado, los materiales para desarrollar las claves de cifrado y las copias impresas de versiones de claves deben mantenerse todas en un lugar seguro y bajo llave.	Políticas Relacionadas: “Destrucción de Materiales para Generación de Claves” y “Gestión Automática de Claves de Cifrado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
13. Claves Maestras de Cifrado en Texto	Política: Las claves maestras en texto deben manejarse manualmente a través de un control dual con conocimiento separado o almacenarse en módulos a prueba de todo.	Políticas Relacionadas: “Materiales para la Generación de Claves” y “Sistemas de Gestión de Claves de Cifrado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
14. Destrucción de Materiales para Generación de Claves	Política: Todos los materiales utilizados para generar, distribuir y almacenar claves deben protegerse y no divulgarse a personas no autorizadas. Cuando estos suministros ya no sean necesarios, deben destruirse mediante el uso de máquinas trituradoras de papeles, incineradores u otros métodos autorizados.	Políticas Relacionadas: "Materiales para la Generación de Claves,' "Disposición de Información en Papel,' y "Materiales Usados con Información Sensible"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
15. Destrucción de Material de Intercambio de Claves	Política: Los custodios del material de intercambio de claves deben destruir este material de acuerdo con los procedimientos autorizados, dentro de un período razonable que no exceda los diez (10) días hábiles siguientes a la verificación comprobada del proceso de intercambio de claves.	Políticas Relacionadas: "Productos Intermedios Con Información Sensible" y "Materiales Usados con Información Sensible"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
16. Secreto de la Clave de Cifrado	Política: La privacidad de cualquier clave de cifrado que se utilice por confidencialidad debe mantenerse intacta mientras toda la información protegida se considere confidencial.	Políticas Relacionadas: "Ciclo de Vida de Claves de Cifrado" y "Vencimiento de Claves de Cifrado"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Medianos y altos
17. Ciclo de Vida de las Claves Privadas de Firmas Digitales	Política: Las claves privadas de las firmas digitales deben mantenerse confidenciales al menos por el número de años que puedan utilizarse en materia legal.	Políticas Relacionadas: "Claves de Firmas Digitales y de Autentificación de Usuarios" y "Ejecución de Programa Java"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
18. Respaldos de Claves Privadas	Política: Los usuarios no deben permitir que los sistemas automáticos de respaldo hagan copias de la versión legible de su clave privada utilizada para firmas digitales y certificados digitales.	Políticas Relacionadas: "Claves de Firmas Digitales y de Autentificación de Usuarios" y "Protección de Claves Raíces de Certificados Digitales"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
19. Duplicación de Claves de Cifrado	Política: Las claves de cifrado utilizadas para ocultar datos respaldados también deben respaldarse y almacenarse bajo medidas de seguridad tan rigurosas o más que las aplicadas al respaldo de los datos pertinentes.	Políticas Relacionadas: "Claves de Firmas Digitales y de Autentificación de Usuarios" y "Medios de Almacenamiento de Claves de Cifrado"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
20. Divulgación de Claves de Cifrado — Controles	Política: Las claves de cifrado deben protegerse de la divulgación no autorizada a través de controles técnicos, tales como cifrados en claves separadas y la utilización de un hardware resistente a modificaciones.	Políticas Relacionadas: "Gestión Automática de Claves de Cifrado" y "Módulos de Hardware para el Proceso de Cifrado"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
21. Seguridad de Clave Privada para Certificados Digitales	Política: La clave privada asociada a cada trabajador en la Gobernación debe protegerse para que no sea divulgada sin autorización cuando no esté en uso, aplicando técnicas más avanzadas en lugar de una simple medida física de seguridad.	Políticas Relacionadas: "Ciclo de Vida de las Claves Privadas de Firmas Digitales"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
22. Almacenamiento de Claves de Cifrado y Firmas Digitales	Política: Las claves empleadas por los usuarios finales para cifrar y para las firmas digitales deben ser almacenadas en dispositivos con hardware resistente a modificaciones.	Políticas Relacionadas: "Módulos de Hardware para el Proceso de Cifrado" e "Información Sensible en Computadores Personales"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
23. Transmisión de Claves de Cifrado Privadas	Política: Si las claves de cifrado privadas se transmiten a través de líneas de comunicación, deben estar cifradas con un algoritmo más poderoso que el utilizado para cifrar otros datos secretos protegidos por dicho cifrado.	Políticas Relacionadas: "Transmisión de Datos y Claves de Cifrado"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
24. Cambios en Claves Públicas	Política: Si una clave de cifrado pública ha sido publicada en un servidor web o en otro sitio de acceso público, se debe notificar a todos los corresponsales regulares cada vez que haya cambios en dicha clave pública.	Políticas Relacionadas: "Transmisión de Claves de Cifrado Privadas"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
25. Claves Comprometidas	Política: Las claves de cifrado que se han comprometido, o revelado a terceras personas de conformidad con un acuerdo de custodia de clave, deben revocarse inmediatamente, en forma retroactiva al último momento conocido en que las claves estaban a salvo.	Políticas Relacionadas: "Sistemas de Cifrado de Propósito General" y "Contraseñas y Claves en Utilidades de Cifrado"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
26. Medios de Almacenamiento de Claves de Cifrado	Política: Si se utiliza el cifrado para proteger datos sensibles residentes en los medios de almacenamiento de un computador, la clave de cifrado y los materiales de cifrado de claves correspondientes utilizados en el proceso de cifrado, no deben guardarse en ninguno de los medios de almacenamiento mencionados sin su correspondiente cifrado.	Políticas Relacionadas: "Transmisión de Datos y Claves de Cifrado"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
27. Controles en la Operación de Recuperación de Claves	Política: Cada vez que se recuperen claves del archivo de claves de cifrado deben estar presentes dos funcionarios autorizados del personal de la Gobernación, y todas estas operaciones deben ser registradas de manera segura.	Políticas Relacionadas: "Contraseñas y Claves en Utilidades de Cifrado" y "Sistemas de Cifrado de Propósito General"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
28. Claves de Cifrado de Respaldo	Política: Si el trabajador de la Gobernación va a emplear cifrado en las actividades de procesamiento de la información del negocio de producción, este trabajador debe entregar de manera segura copias de respaldo de todas las claves a la gerencia del departamento de Seguridad Informática.	Políticas Relacionadas: "Llaves de las Estaciones de Trabajo" y "Contraseñas y Claves en Utilidades de Cifrado"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
29. Claves de Firmas Digitales y de Autentificación de Usuarios	Política: Las claves que se utilicen para firmas digitales, certificados digitales, y autentificación de usuarios nunca deben incluirse en un acuerdo de custodia garantizada de claves.	Políticas Relacionadas: "Sistemas de Cifrado de Propósito General"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
30. Separación de Claves de Cifrado y de Firmas Digitales	Política: Si se utilizan tanto la firma digital como el cifrado, deben utilizarse claves separadas en cada una de estas dos medidas de control.	Políticas Relacionadas: "Medios de Almacenamiento de Claves de Cifrado" y "Transmisión de Datos y Claves de Cifrado"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
31. Responsabilidad de la Gestión de Claves	Política: Cuando se utilice el cifrado para proteger datos sensibles, el Propietario respectivo de los datos debe asignar explícitamente la responsabilidad del manejo de la clave de cifrado.	Políticas Relacionadas: "Propiedad de la Información" y "Gestión Automática de Claves de Cifrado"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
10.04 Seguridad de los Archivos del Sistema				
10.04.01 Control del Software de Operaciones				
1. Prueba del Sistema de Aplicaciones de Negocios	Política: Todos los sistemas de aplicación desarrollados internamente deben pasar por tres ciclos de pruebas donde se descubran y corrijan todos los errores antes de poner los sistemas de aplicación en operación de producción.	Políticas Relacionadas: "Acceso del Desarrollador a la Información de Producción" y "Convenciones en Desarrollo de Sistemas"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
2. Migración de Software	Política: El personal de desarrollo de sistemas y aplicaciones no debe tener facultad para trasladar ningún software al ambiente de producción.	Políticas Relacionadas: "Separación de Tareas"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10.04.02 Protección de los Datos de Prueba del Sistema				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Información Usada en Pruebas de Software	Política: A menos que se obtenga un permiso por escrito de la gerencia de Seguridad Informática, toda prueba de software de sistemas diseñada para manejar información privada debe llevarse a cabo con información de producción que no contenga detalles específicos que puedan ser valiosos, críticos, confidenciales ni privados.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Divulgación de Información Privada a Terceros,' y "Acceso del Desarrollador a la Información de Producción"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
2. Acceso del Desarrollador a la Información de Producción	Política: Cuando se requiera el acceso a la información de negocios de producción para desarrollar o probar sistemas de aplicaciones nuevas o modificadas, sólo debe concederse acceso a la "lectura" o "copia" de datos en las máquinas de producción mientras duren las pruebas y trabajos del desarrollo pertinente, y deben desautorizarse tan pronto haya finalizado con éxito el trabajo.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer,' "Acceso a la Información de las Aplicaciones de Producción,' e "Información Usada en Pruebas de Software"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10.04.03 Control de Acceso a la Biblioteca Fuente de Programas				
1. Privilegios del Personal Técnico	Política: El personal de operaciones de computación no debe tener acceso a los datos de producción, programas de producción o sistemas operativos más allá de lo necesario para desempeñar su trabajo.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer" y "Separación de Tareas"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Acceso a Programas e Información de Producción	Política: Los controles de acceso se deben configurar de tal manera que no se concedan al personal de soporte técnico de software de sistemas informáticos y programas de producción, derechos de acceso sino para resolver problemas, que no se le concedan derechos para actualizar los sistemas de software al personal de desarrollo de aplicaciones, como tampoco el acceso a la copia maestra de la información de producción excepto para resolver problemas, y que prohíban que el personal de operaciones de computación modifique el software de sistemas, el software de las aplicaciones y la información de producción.	Políticas Relacionadas: "Acceso a Comandos del Sistema Operativo" y "Privilegios Sobre la Información de Producción"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
10.05 Seguridad en los Procesos de Desarrollo y Soporte				
10.05.01 Procedimientos para el Control de Cambios				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Prueba e Información del Software	Política: Antes de distribuir cualquier software o información en forma computarizada a terceras personas, los trabajadores de la Gobernación deben someter el software o la información a una prueba de seguridad, incluyendo una revisión exhaustiva para identificar la presencia de virus en el computador.	Políticas Relacionadas: "Prueba del Software"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Consumo de Recursos por Programas	Política: Los usuarios de computadores no deben ejecutar o escribir ningún programa de computación o proceso que pueda consumir recursos importantes del sistema o que pueda interferir con las actividades de negocios de la Gobernación.	Políticas Relacionadas: "Consumo Excesivo de Recursos,' "Procesos, Sesiones y Archivos de Usuarios,' y "Envíos de Correos Electrónicos No Solicitados"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
3. Convenciones en Desarrollo de Sistemas	Política: La gerencia debe garantizar que todas las actividades de desarrollo y mantenimiento de software ejecutadas por personal propio suscriban las políticas, las normas, los procedimientos y otras convenciones de desarrollo de sistemas de la Gobernación.	Políticas Relacionadas: "Programas de Aplicación de Usuarios Finales,' "Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas,' y "Seguridad Informática Centralizada"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
4. Vías de Acceso en Software de Production	Política: Antes de trasladar un software desarrollado internamente al modo de producción, los programadores y demás personal técnico deben eliminar todas las vías de acceso y los privilegios especiales en sistemas.	Políticas Relacionadas: "Comprometer Mecanismos de Seguridad para los Clientes" y "Burlado de los Controles de Acceso"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
5. Funcionalidad de los Sistemas	Política: Con la excepción de las reparaciones de emergencia, sólo aquellas funciones descritas en un documento autorizado de diseño de sistemas deben ser incluidas en sistemas de producción computarizada o comunicaciones desarrollados internamente.	Políticas Relacionadas: "Vías de Acceso en Software de Producción"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
6. Proyectos que Involucran Seguridad Humana	Política: Todos los proyectos internos que involucren riesgos de seguridad humana deben tener la firma de un gerente de proyecto de desarrollo computarizado en los formatos de autorización de la prueba, antes de ser utilizados con propósitos de negocios de producción.	Políticas Relacionadas: "Controles de Sistemas de Producción,' "Interrupción del Sistema por Seguridad, 'y "Contraseñas de Presión"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
7. Notificación de Problemas en los Sistemas	Política: Los diseñadores y desarrolladores de sistemas son individualmente responsables de notificar a la gerencia del proyecto sobre cualquier problema que pudiese ser causado por las aplicaciones que estén construyendo o modificando.	Políticas Relacionadas: "Información de Contacto en Seguridad" e "Informe de Vulnerabilidades del Sistema"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
8. Procedimiento de Control de Cambios	Política: Todos los sistemas de computación y comunicaciones utilizados para procesos de producción en la Gobernación deben emplear un procedimiento formal de control de cambios para autorizar todos los cambios significativos al software, hardware, redes de comunicación y procedimientos relacionados.	Políticas Relacionadas: “Cambios en Producción” y “Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
9. Consideraciones de Seguridad en Cambios en los Sistemas de Producción	Política: Todo cambio a sistemas de producción que no sea de emergencia debe ser consistente con la arquitectura de seguridad informática y estar autorizado por la gerencia como parte del proceso formal de control de cambios.	Políticas Relacionadas: “Carga de Programas Externos” y “Acuerdos de Negocios por Internet”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
10. Controles de Acceso a las Operaciones de Producción	Política: Todos los controles de acceso a nivel de usuario y administrativo requeridos por las políticas de seguridad informática de la Gobernación se deben establecer y habilitar antes de poner en operación los sistemas informáticos de producción.	Políticas Relacionadas: “Controles de Acceso para Sistemas Remotos” y “Controles de Acceso al Sistema de Computación”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
11. Software Innecesario	Política: Las características de software que pudiesen ser utilizadas para comprometer la seguridad y que son claramente innecesarias en el ambiente computarizado de la Gobernación, deben ser inhabilitadas en el momento de ser instalado el software en sistemas multiusuario.	Políticas Relacionadas: “Inhabilitación de Java,’ “Vías de Acceso en Software de Production,’ y “Restricción de Privilegios — Necesidad de Conocer”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
12. Documentación de Cambios en Sistemas de Producción	Política: La documentación que refleje la naturaleza, autorización y desenvolvimiento de todos los cambios significativos a sistemas de producción computarizada y comunicaciones de la Gobernación, debe ser preparada en el lapso de una semana después de efectuado el cambio.	Políticas Relacionadas: “Documentación de Adiestramiento y Operaciones” y “Cambios del Sistema Operativo de Producción”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
13. Documentación de Adiestramiento y Operaciones	Política: Los sistemas de aplicación de negocios en desarrollo o que estén sufriendo modificaciones importantes no deben ser movidos a un ambiente de procesos de producción sin tener materiales adecuados de adiestramiento y documentación de operaciones.	Políticas Relacionadas: “Responsabilidades del Usuario de la Información,’ “Documentación de Cambios en Sistemas de Producción,’ y “Documentación para Sistemas de Producción”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
14. Prueba de Software Externo	Política: Los programas ejecutables que se obtengan de entidades externas deben ser autorizados de acuerdo con las normas de la Gobernación y estar correctamente documentados antes de instalarse en cualquier sistema de producción de la Gobernación.	Políticas Relacionadas: “Prueba del Software” y “Exploración del Software”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
15. Revisión y Recompilación de Software	Política: Los módulos de software probados en su totalidad, deben ser revisados de manera independiente y recompilados antes de trasladarlos a las bibliotecas de producción.	Políticas Relacionadas: “Separación de Tareas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
16. Proceso de Control de Cambios para Aplicaciones de Negocios	Política: Se debe utilizar un proceso formal de control de cambios para garantizar que todo el software de aplicaciones de negocio que sea migrado a producción está autorizado por la gerencia de Sistemas Informáticos y la gerencia de la organización usuaria.	Políticas Relacionadas: “Migración de Software” y “Desarrollo de Sistemas por Usuarios Finales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
17. Autorización para Cambiar Paquete de Software de Producción	Política: Los cambios al software de aplicaciones suministrados por los vendedores deben efectuarse sólo después de conseguir permiso por escrito de la gerencia de Sistemas Informáticos, siguiendo los procedimientos de control de cambios utilizados para el software de aplicación desarrollado internamente.	Políticas Relacionadas: “Proceso de Control de Cambios para Aplicaciones de Negocios” y “Servicio Nuevo o Mejorado”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
18. Mantenimiento de Software	Política: Todos los cambios permanentes al software de producción deben ser efectuados utilizando el código fuente.	Políticas Relacionadas: “Garantía Especial de Software”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
19. Documentación de los Controles de Cambios	Política: La documentación de control de cambios en aplicaciones de producción se debe mantener para que indique qué cambio y cómo, quién hizo los cambios, quién probó los cambios, quién los autorizó, quién los migró a producción y permitió que cualquiera o toda versión anterior de aplicaciones de producción pueda ser fácilmente re-creada.	Políticas Relacionadas: “Garantía Especial de Software” y “Documentación de Cambios en Sistemas de Producción”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
20. Implantación de Cambios en Sistemas Informáticos de Producción	Política: Todos los cambios deben ser comunicados a las personas afectadas por lo menos con dos semanas de anticipación al cambio, y la implantación de todos los cambios que no sean de emergencia deben efectuarse en el primer fin de semana de cada mes.	Políticas Relacionadas: “Proceso de Control de Cambios para Aplicaciones de Negocios” y “Arreglos de Seguridad”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Altos
21. Documentación de Características y Funciones del Software	Política: Todas las características y funciones de software dadas a conocer al público deben estar contenidas en la documentación que se entregue a los usuarios.	Políticas Relacionadas: “Vías de Acceso en Software de Production” y “Burlado de los Controles de Acceso”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10.05.02 Revisión Técnica de los Cambios en Sistemas Operativos				
1. Configuración del Sistema Operativo	Política: El personal técnico de la Gobernación debe configurar los servidores de producción con aquellos sistemas operativos que permitan que la función innecesaria o no requerida se elimine completamente.	Políticas Relacionadas: “Inhabilitación de Componentes Críticos de Seguridad” y “Configuración de Cortafuegos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
2. Parches de Software, Arreglos y Actualizaciones	Política: Todos los sistemas de producción en la red de la Gobernación deben tener un proceso debidamente integrado del personal para, de manera expedita y regular, revisar e instalar todos los nuevos parches, arreglos de errores y actualizaciones de software de sistemas.	Políticas Relacionadas: “Actualizaciones de Software de Computadores Personales,’ “Versiones de Software,’y “Sistemas en Interface con Redes Externas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10.05.03 Restricciones en Cambios a Paquetes de Software				
1. Instalación de Software de Sistemas Proporcionado por Proveedores	Política: Las nuevas versiones de los sistemas operativos y software de sistemas de producción para computadores multiusuario deben pasar por el proceso de control de cambios establecido antes de ser instalados.	Políticas Relacionadas: “Proceso de Control de Cambios para Aplicaciones de Negocios” y “Cambios en Producción”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Acceso de Proveedor Tercero a Software	Política: Los paquetes de software de terceros que la Gobernación utilice en los sistemas informáticos de producción, deben estar libres de mecanismos de desactivación que pudiesen ser disparados por el proveedor sin el consentimiento de la Gobernación.	Políticas Relacionadas: “Software Innecesario” y “Procedimientos de Retorno”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
10.05.04 Canales Secretos y Código Troyano				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Uso de Herramientas y Lenguajes de Software	Política: Los diseñadores y desarrolladores de sistemas de la Gobernación no deben utilizar herramientas y lenguajes de software que no posean atributos comprobados de seguridad cuando construyan páginas web, extranets o cualquier otro sistema que tenga interface con terceros, a menos que se obtenga una aprobación previa de la gerencia de Seguridad Informática.	Políticas Relacionadas: “Herramientas y Técnicas de Desarrollo Maduras” e “Interfaces a Redes Externas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Enunciados de la Integridad del Software	Política: Si se está considerando la compra de un software a terceros, la gerencia debe obtener una declaración escrita de integridad por parte del proveedor involucrado, la cual debe garantizar que el software no contiene características que no se han documentado, que no contiene mecanismos ocultos que puedan ser utilizados para comprometer la seguridad del software, y que no requerirá ni el cambio ni el abandono de los controles presentes en el sistema operativo afectado.	Políticas Relacionadas: “Comprometer Mecanismos de Seguridad para los Clientes”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
10.05.05 Desarrollo de Software con Terceros				
1. Desarrollo de Software por Terceros	Política: Los terceros que desarrollen software para la Gobernación quedan obligados por un contrato que incluye, sin limitantes, definiciones claras y precisas de arreglos de licencia, expectativas de precisión y calidad, acuerdos de garantías, procedimientos de auditoría y requerimientos de pruebas.	Políticas Relacionadas: “Aprobación de Contratos Externos,’ “Transferencia de Información a Terceros, ’“Sistemas de Producción y Herramientas de Software,’y “Enunciados de la Integridad del Software”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Políticas de Continuidad

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
11 GESTIÓN DE CONTINUIDAD DE NEGOCIO				
11.01 Aspectos de Gestión de Continuidad de Negocio				
11.01.01 Proceso de la Gestión de Continuidad de Negocio				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Requerimientos para el Soporte de Emergencias y Desastres	Política: Todas las subsidiarias, divisiones, departamentos y otras unidades organizativas que requieran soporte del departamento de Sistemas Informáticos con prioridad en caso de una emergencia o desastre, deben implementar hardware, software, políticas y procedimientos relacionados que sean consistentes con las normas de la Gobernación.	Políticas Relacionadas: “Dispersión de Sistemas Computacionales” y “Seguridad Informática Centralizada”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Accesibilidad del Plan de Contingencia	Política: Los planes de contingencia de los sistemas informáticos deben estar accesibles de manera continua en Internet, por lo menos en dos sitios diferentes, apoyados por proveedores diferentes de servicios en Internet.	Políticas Relacionadas: “Equipo de Respuesta Ante Emergencias Computacionales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
11.01.02 Análisis de Contingencias del Negocio y su Impacto				
1. Clasificación de la Criticidad de las Aplicaciones Multiusuario	Política: Conjuntamente con los Propietarios de la Información, la gerencia del Sistemas Informáticos debe preparar o revisar periódicamente una evaluación del nivel de criticidad de todas las aplicaciones de producción en computadores multiusuario.	Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones, ’“Planes de Seguridad Informática,’ y “Clasificación de Recursos Informáticos”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones	Política: Todas las aplicaciones de producción en computadores deben ser ubicadas en una de las cinco clasificaciones de criticidad, cada una con requisitos de manejo diferente: altamente crítico, crítico, prioridad, requerido y diferible.	Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,’ “Clasificación de la Criticidad de las Aplicaciones Multiusuario,’ e “Información y Software Esenciales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Análisis del Impacto sobre el Negocio	Política: Concluida la evaluación de riesgo a lo largo de la organización, la gerencia de Seguridad Informática, o a quien se delegue, debe hacer un análisis del impacto sobre el negocio que precise la duración del tiempo máximo que la Gobernación puede tolerar la ausencia de los servicios informáticos críticos, el plazo en el cual la gerencia ha de decidir el sitio alternativo de procesamiento, y sobre la configuración de los sistemas mínimos aceptables para la recuperación de los sistemas informáticos de producción.	Políticas Relacionadas: “Evaluación de Nuevas Tecnologías” y “Evaluación del Riesgo en los Sistemas de Producción”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
11.01.03 Redacción e Implantación de Planes de Contingencia				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Clasificación de Recursos Informáticos	Política: La Gerencia de Operaciones de Computación conjuntamente con los Propietarios de la Información, deben establecer y utilizar un marco de referencia para clasificar todos los recursos de información, mediante el establecimiento de prioridades de recuperación que permitan que los recursos más críticos sean los primeros en ser recuperados.	Políticas Relacionadas: "Clasificación de la Criticidad de las Aplicaciones Multiusuario"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Preparación y Mantenimiento de Planes de Contingencia Empresarial	Política: La Gerencia debe preparar y periódicamente actualizar y con regularidad poner a prueba, una política de recuperación de negocios que especifique el uso de instalaciones alternativas para que los empleados puedan continuar las operaciones en caso de interrupción del negocio.	Políticas Relacionadas: "Planes de Recuperación Ante Desastre Computacional"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
11.01.04 Marco para la Planificación de la Continuidad del Negocio				
1. Plan de Continuidad de Negocios y Computación	Política: La gerencia de Sistemas Informáticos debe documentar y mantener un proceso normalizado para toda la organización para el desarrollo y mantenimiento tanto de las políticas de contingencia del negocio como los planes de contingencia para computación.	Políticas Relacionadas: "Clasificación de Recursos Informáticos" y "Excepciones a las Políticas"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Expectativas sobre el Empleado Durante la Restauración de las Actividades del Negocio	Política: Se espera la presencia de los empleados y su mejor ayuda en la retauración de la actividad normal de las operaciones del negocio de la Gobernación, después de que éstas hayan sido interrumpidas por una emergencia o desastre.	Políticas Relacionadas: "Equipo de Respuesta Ante Emergencias Computacionales"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
11.01.05 Pruebas, Mantenimiento y Re-Evaluación de los Planes de Continuidad del Negocio				
1. Reversión a Procedimientos Manuales	Política: Si las actividades cruciales del negocio de la Gobernación pudieran ser razonablemente realizadas con procedimientos manuales, en lugar de computadores, un plan de contingencia de computación manual tendrá que ser desarrollado, probado, periódicamente actualizado, e integrado con los planes de contingencia del sistema de computación y de comunicaciones.	Políticas Relacionadas: "Planes de Recuperación Ante Desastre Computacional"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Rotación del Personal Fuera de Sede	Política: Los empleados que participen en operaciones de recuperación fuera de sede con sistemas informáticos de la Gobernación, deben ser rotados regularmente para permitir que por lo menos dos personas tengan los conocimientos técnicos necesarios para realizar cada una de las tareas esenciales de recuperación.	Políticas Relacionadas: "Puestos Técnicos Esenciales" y "Rotación de Trabajo"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
3. Niveles de Soporte de Interrupción del Negocio	Política: Anualmente, las gerencias de los departamentos usuarios y de Tecnología Informática han de convenir y documentar los niveles de apoyo que serán suministrados en caso de desastre o emergencia.	Políticas Relacionadas: “Requerimientos para el Soporte de Emergencias y Desastres,’ “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,’ y “Mantenimiento Preventivo”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
4. Prueba del Plan de Contingencia	Política: Los planes de contingencia para los sistemas de computación y comunicación deben ser probados rutinariamente, y seguidos de un breve informe para la alta gerencia con los detalles de los resultados.	Políticas Relacionadas: “Planes de Recuperación Ante Desastre Computacional”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
5. Prueba de Números Telefónicos	Política: Cada trimestre, el equipo de Seguridad Informática deberá probar y revisar un árbol de llamadas, en el cual se indiquen todos los números de teléfonos disponibles para cada uno de los empleados involucrados en la planificación de contingencias relacionadas con los sistemas informáticos, y respuesta ante desastres y emergencias.	Políticas Relacionadas: “Información de Contacto” y “Números de Acceso a Computadores”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
6. Roles en la Planificación de Contingencias y Recuperación de Sistemas	Política: Las funciones y responsabilidades para tanto los sistemas de planificación de contingencias como de recuperación de sistemas, deben ser revisadas y actualizadas anualmente por la gerencia de Seguridad Informática.	Políticas Relacionadas: “Comité de Gestión de Seguridad Informática” y “Administradores de Seguridad Suplentes”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Políticas de Cumplimiento

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
12 CUMPLIMIENTO				
12.01 Cumplimiento de Requisitos Legales				
12.01.01 Identificación de la Legislación Pertinente				
1. Reglamentos y Requisitos	Política: Todos los requisitos estatutarios, regulatorios y contractuales, tienen que ser definidos y documentados para cada sistema informático de la Gobernación.	Políticas Relacionadas: “Avisos de Derechos de Autor en Software”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
12.01.02 Derechos de Propiedad Intelectual				
1. Fuente de Desarrollo de Software	Política: El software que soporte las aplicaciones de negocios de producción debe ser desarrollado internamente o adquirido de algún proveedor tercero reconocido y confiable.	Políticas Relacionadas: “Prueba de Software Externo”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
2. Sistemas de Producción y Herramientas de Software	Política: Los sistemas informáticos de producción de la Gobernación, sólo debe hacer uso de aquellas herramientas que hayan sido legítimamente desarrolladas por proveedores fiables, asociaciones profesionales, agrupaciones gremiales o agencias gubernamentales.	Políticas Relacionadas: “Prueba de Software Externo” y “Fuente de Desarrollo de Software”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Garantía Especial de Software	Política: Si se ha de usar software de terceros para una actividad crítica de negocios, el proveedor debe otorgar licencia de código de fuente a la Gobernación o debe conceder acceso al código fuente por medio de un convenio de plica (o de custodia en garantía) con dicho tercero.	Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones, ’“Software Distribuido a Terceros,’ y “Mantenimiento de Software”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
4. Verificación de Software En Garantía Especial	Política: Para cada puesta en circulación importante de software crítico para los negocios de la Gobernación y que un tercero la tenga en plica, un tercero independiente debe verificar que el agente de plica (o custodio garante) haya recibido todo el software necesario y su documentación.	Políticas Relacionadas: “Garantía Especial de Software”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
5. Atribución de la Información	Política: Los trabajadores de la Gobernación siempre deben acreditar de manera apropiada a la fuente de información utilizada para propósitos de la Gobernación.	Políticas Relacionadas: "Etiquetado de la Propiedad Intelectual" e "Identidades Falsas"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
6. Etiquetado de la Propiedad Intelectual	Política: Todos los usuarios que presenten información para la cual no poseen el derecho de autor o de cualquier otro derecho en el área pública del sitio web de la Gobernación, o en el sistema de foros electrónicos, deben identificar claramente la fuente de la información.	Políticas Relacionadas: "Atribución de la Información" y "Etiquetado de Datos Usados Como Base de Decisión Gerencial"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
7. Avisos de Derechos de Autor en Software	Política: Todos los programas de computación y documentación de programación que sean propiedad de la Gobernación deben ser incluidos en los avisos de derechos de autor correspondientes.	Políticas Relacionadas: "Derechos de Propiedad Intelectual"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
8. Copias Múltiples de la Información	Política: Los trabajadores no pueden hacer copias múltiples del material extraído de alguna publicación, excepto cuando se haya obtenido el permiso del Propietario de los derechos de autor o sólo cuando esto sea razonable y acostumbrado.	Políticas Relacionadas: "Derechos de Propiedad Intelectual"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
9. Revisión de los Convenios de Licencia del Software	Política: El convenio de licencia de todos los programas de computador debe ser revisado periódicamente.	Políticas Relacionadas: "Copias Autorizadas de Software"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
10. Evidencia de Licencia de Software	Política: Cuando se adquieran sistemas en paquete, la fuente debe entregar evidencia escrita del software que se traspasa.	Políticas Relacionadas: "Avisos de Derechos de Autor en Software" y "Revisión de los Convenios de Licencia del Software"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
11. Copias Autorizadas de Software	Política: La gerencia debe hacer los arreglos apropiados con todos los proveedores de software para obtener copias licenciadas, cada vez que se requieran copias adicionales para las actividades del negocio.	Políticas Relacionadas: "Revisión de los Convenios de Licencia del Software"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
12. Copias de Software	Política: El software de terceros en posesión de la Gobernación no deben ser copiado hasta que no se haga en conformidad con los convenios de licencia pertinentes de traspaso, y cuando la gerencia haya autorizado tal copiado con propósitos de planificación de contingencias.	Políticas Relacionadas: “Copias Maestras del Software”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
13. Información y Software No Autorizados	Política: Los administradores del sistema deben retirar la información de terceros que no haya sido autorizada para su uso, en concordancia con los derechos de autor o el software para el cual La Gobernación no tiene autorización específica para almacenar o usar, salvo que los usuarios involucrados puedan demostrar autorización de los propietarios de los derechos de autor.	Políticas Relacionadas: “Avisos Públicos Inadecuados” y “Remoción de Material Ofensivo”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
14. Protección Aplicable del Derecho de Autor	Política: Los trabajadores deben investigar la propiedad intelectual de todo el material que visualicen en Internet, antes de usarlo para cualquier propósito.	Políticas Relacionadas: “Información y Software No Autorizados” y “Copias No Autorizadas de Software y Datos”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
15. Duplicación de Software	Política: Los usuarios no deben copiar en medios de almacenamiento, el software suministrado por la Gobernación, transferir tal software a otro computador o divulgar dicho software a terceras personas sin permiso escrito de la gerencia de Tecnología Informática.	Políticas Relacionadas: “Avisos de Derechos de Autor en Software” y “Archivos Críticos de Respaldo”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
16. Copias No Autorizadas de Software y Datos	Política: Todos los usuarios de sistemas de la Gobernación o de internet deben abstenerse de hacer copias no autorizadas de software o de cualquier material con derechos de autor que no sea considerado de uso personal, sin el permiso del autor o de la editorial.	Políticas Relacionadas: “Copias Maestras del Software” y “Revisión de los Convenios de Licencia del Software”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
17. Material Con Derechos de Autor No Autorizado	Política: Los trabajadores no deben participar de ninguna manera ni en ninguna oportunidad en la distribución, transferencia o intercambio de copias ilegales de ningún material con derechos de autor.	Políticas Relacionadas: “Duplicación de Software” y “Directorios Modificables por el Público”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
18. Libros Electrónicos con Derecho de Autor	Política: Todos los libros electrónicos u otras obras con derechos de autor con base en textos publicados por la Gobernación en Internet o en cualquier otra red de acceso público, deben estar en mapas de bits.	Políticas Relacionadas: “Monitoreo en Internet del Uso de la Información” y “Material Con Derechos de Autor No Autorizado”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
19. Monitoreo en Internet del Uso de la Información	Política: El departamento Legal debe monitorear Internet por lo menos una vez al mes para detectar el uso no autorizado de las marcas registradas de la Gobernación, marcas de servicio, nombres de marca, o materiales registrados propiedad de la Gobernación.	Políticas Relacionadas: “Monitoreo de Mensajes de Correo Electrónico” y “Responsabilidad de Monitorear Contenido”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
20. Uso de Marcas Registradas de Terceros	Política: La página web y los sitios comerciales de la Gobernación no deben utilizar marcas registradas de otras organizaciones o marcas de servicio, excepto cuando el uso refleja los atributos verdaderos de los productos o servicios de la Gobernación, y cuando se haya obtenido permiso del asesor legal de la empresa.	Políticas Relacionadas: “Propiedad Intelectual” y “Páginas Web No Oficiales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
21. Acuerdos de Confidencialidad de Terceros	Política: Los trabadores no deben firmar acuerdos de confidencialidad suministrados por terceras personas sin la previa autorización del asesor legal de la Gobernación, designado para manejar asuntos de propiedad intelectual.	Políticas Relacionadas: “Acuerdos de Confidencialidad — Terceros”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
22. Revisión de Secretos Empresariales y Derechos de Autor	Política: El departamento Legal, en conjunción con la gerencia de Seguridad de Información, debe preparar una revisión anual de las leyes que protegen la propiedad intelectual y la información, que incluya el desarrollo de un inventario de los asuntos legales relativos a la información de la Gobernación, una evaluación de la eficiencia y efectividad de los controles	Políticas Relacionadas: “Evaluación de Riesgo de Seguridad Informática en Toda la Organización” y “Declaración de Secreto Industrial”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
12.01.03 Protección de los Registros Organizacionales				
1. Información de Registro del Cliente	Política: Las personas que mantienen los registros que reflejan las actividades de un usuario o de las personas asistidas por computadores, deben eliminar la información que identifica a los usuarios o personas asistidas tan pronto termine la relación de la Gobernación con dichas personas.	Políticas Relacionadas: “Divulgación del Registro de las Actividades del Cliente”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Retención de la Información Personal	Política: La información personal retenida en los sistemas informáticos de la Gobernación debe ser eliminada cuando la información ya no se necesite para la conducción del negocio y cuando ya no se necesite para el cumplimiento de requisitos legales o regulatorios.	Políticas Relacionadas: "Información de Registro del Cliente" y "Período de Retención de la Información"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
3. Destrucción de Registros de Transacciones	Política: La Gobernación debe destruir el registro de la transacción después de completar la transacción y después del plazo durante el cual se pueda aceptar una devolución.	Políticas Relacionadas: "Destrucción de Mensajes de Correo Electrónico" y "Enlaces Entre la Información Privada y la Identificadora"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
4. Retención de la Información Sensible	Política: Se debe establecer un período de retención para toda la información sensible.	Políticas Relacionadas: "Disposición de Información en Papel,' "Clasificación de Datos en Cuatro Categorías,' "Período de Retención de la Información,'y "Cronograma de Retención de los Archivos Almacenados"	Política Dirigida a:Todos	Ambientes de Seguridad: Medianos y altos
5. Identificación de Registros Vitales	Política: Los gerentes departamentales deben identificar y mantener una lista actualizada de los registros vitales que requieren sus departamentos para restaurar operaciones después de un desastre.	Políticas Relacionadas: "Copias de Información Sensible, Crítica o Valiosa" y "Retención del Documento Fuente"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
6. Almacenamiento de Registros Vitales	Política: Los registros de negocios vitales se deben mantener en cajas fuertes anti-incendios y cerradas cuando no estén en uso para propósitos del negocio.	Políticas Relacionadas: "Identificación de Registros Vitales" y "Destrucción de Información"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Medianos y altos
7. Período de Retención de la Información	Política: La información que no se encuentre específicamente en el Programa de Retención de Información, se debe retener sólo mientras sea necesaria.	Políticas Relacionadas: "Cronograma de Retención de los Archivos Almacenados" y "Retención de la Información Sensible"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
8. Cronograma de Retención de los Archivos Almacenados	Política: Todos los registros de contabilidad financiera, contabilidad de impuestos y documentos legales, deben ser retenidos durante un mínimo de siete años y el resto de los registros deben ser retenidos por un mínimo de cinco años.	Políticas Relacionadas: "Período de Retención de la Información,' "Cronograma de Retención de Datos, '"Disposición de Información en Papel,' y "Manejo de Mensajes de Correo Electrónico"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
9. Cronograma de Retención de Datos	Política: Toda la información de la Gobernación debe ser resguardada de manera segura, de conformidad con el programa publicado por el departamento Legal.	Políticas Relacionadas: "Cronograma de Retención de los Archivos Almacenados" y "Período de Retención de la Información"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
10. Retención del Documento Fuente	Política: Los documentos fuente del negocio y los archivos electrónicos originales de entradas se deben retener hasta que las transacciones relacionadas se hayan completado, hasta que se haya realizado una revisión gerencial de los documentos que integran estas transacciones, y durante un período de tiempo superior al que necesitarían tales transacciones para superar etapas contenciosas.	Políticas Relacionadas: "Período de Retención de la Información,' "Período de Retención del Documento Fuente,' y "Cronograma de Retención de los Archivos Almacenados"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
11. Período de Retención del Documento Fuente	Política: Los documentos fuente de negocios contentivos de datos de entrada se deben retener por un mínimo de 90 días, a partir de la fecha cuando la información fue ingresada en el sistema informático de la Gobernación.	Políticas Relacionadas: "Retención del Documento Fuente" y "Cronograma de Retención de los Archivos Almacenados"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
12. Retención de los Datos de Transacciones con Aplicaciones	Política: Todos los datos de transacción de las aplicaciones deben ser mantenidas bajo protección hasta tanto se consolide el respaldo total de los archivos maestros de producción.	Políticas Relacionadas: "Período de Retención del Documento Fuente" y "Respaldo Antes del Procesamiento"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
13. Destrucción de Información	Política: Toda la información de la Gobernación debe ser destruida o descartada cuando ya no se necesite.	Políticas Relacionadas: "Información Personal para el Funcionamiento del Negocio,' "Cronograma de Retención de los Archivos Almacenados,' "Directorio de Almacenamiento de Archivos,' "Información Sensible al Tiempo,' y "Disposición de Información en Papel"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
14. Destrucción de Registros	Política: Los trabajadores no deben destruir o descartar registros o la información de la Gobernación que sean potencialmente importantes, sin la previa autorización específica de la gerencia.	Políticas Relacionadas: “Personal para Destrucción de Información”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
15. Cronograma de Destrucción de Registros	Política: Los trabajadores no deben destruir los registros de la Gobernación, a menos que éstos aparezcan en una lista de registros autorizados para la destrucción, o que puedan ser destruidos según las instrucciones que aparezcan en el Programa de Retención y Descarte de Registros.	Políticas Relacionadas: “Procedimientos para la Destrucción de la Información Sensible”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
16. Moratoria en Destrucción de Datos	Política: Al recibir la Gobernación una solicitud de descubrimiento electrónico, todas las actividades periódicas y organizadas para la destrucción de datos electrónicos deben detenerse inmediatamente hasta que el departamento Legal determine si las actividades de destrucción hacen peligrar tales datos buscados.	Políticas Relacionadas: “Retención de la Información Personal” y “Destrucción de Mensajes de Correo Electrónico”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
17. Retención de Información Sensible para su Destrucción	Política: Los trabajadores no deben descartar información sensible en contenedores de basura de acceso público y deben retener la información sensible hasta que pueda ser programada su destrucción por métodos autorizados.	Políticas Relacionadas: “Requisitos de Seguridad para Teletrabajo” y “Disposición de Información en Papel”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
18. Retención de la Información Sobre Violaciones y Problemas de Seguridad	Política: La información que describe todos los problemas de información de seguridad y violaciones debe ser retenida durante tres años.	Políticas Relacionadas: “Análisis de Violaciones y Problemas” y “Reportes Externos de Violaciones”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
12.01.04 Protección de los Datos y Privacidad de la Información Personal				
1. Efectos Personales y Comunicaciones Privadas	Política: Los trabajadores no deben introducir efectos personales a las instalaciones de la Gobernación o hacer uso de los sistemas de la Gobernación para comunicaciones personales sin entender que los mismos pueden ser revisados y monitoreados al azar.	Políticas Relacionadas: “Despidos Inmediatos”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Recopilación de Datos Personales Bajo Pretextos	Política: La Gobernación en ningún momento debe recopilar información personal con falsedades y declaraciones de pretexto relativas a su derecho a recibir tal información.	Políticas Relacionadas: “Uso de Investigadores”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
3. Renuncia a Derechos de Privacidad	Política: La Gobernación debe reservarse el derecho a revelar información confidencial a terceros con el propósito de cobrar cuentas pendientes, o de alguna manera forzar el cumplimiento de condiciones contractuales.	Políticas Relacionadas: “Excepciones a las Políticas” y “Período de Retención de la Información”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
4. Divulgación de Información Privada	Política: Los registros de información privada se deben revelar únicamente al personal que se encuentre activamente involucrado de manera profesional con la persona o cuando la persona lo autorice por escrito.	Políticas Relacionadas: “Bloqueo de Divulgación de Información Privada” y “Uso del Registro Personal”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
5. Recopilación de Información Privada	Política: Los trabajadores de la Gobernación y los sistemas informáticos no deben recopilar información privada, excepto con la previa autorización del departamento Legal de la empresa.	Políticas Relacionadas: “Información de Empleado Potencial” y “Restricciones en Contenido de Mensajes”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Low
6. Información Personal para el Funcionamiento del Negocio	Política: La Gobernación debe recopilar, procesar, almacenar y diseminar sólo la información que es necesaria para el funcionamiento correcto del negocio.	Políticas Relacionadas: “Inventario de Activos — Información” y “Destrucción de Información”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
7. Información Sobre Libertad de Expresión	Política: La Gobernación no debe recopilar información acerca de las opiniones sobre la libertad de expresión de los trabajadores.	Políticas Relacionadas: “Derecho a la Libre Expresión”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
8. Autorización de Recopilación de Información Privada	Política: La necesidad de tener la información debe ser documentada y aprobada por la Gerencia de Recursos Humanos, antes de que los trabajadores de la Gobernación recopilen información privada de los trabajadores, clientes u otras personas.	Políticas Relacionadas: “Información Sobre el Monitoreo del Desempeño” e “Indices de Base de Datos Que Contienen Información Privada”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
9. Recopilación de Datos Privados	Política: La recopilación de información privada por los trabajadores de la Gobernación debe ser realizada a través de medios legales, y sólo con propósitos relacionados con las actividades de la Gobernación.	Políticas Relacionadas: "Autorización de Recopilación de Información Privada" e "Información Personal para el Funcionamiento del Negocio"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
10. Recopilación Furtiva de Información Privada	Política: Los sistemas de computación y comunicaciones no deben recopilar datos privados de clientes o clientes potenciales, sin antes haber logrado un consentimiento claro y sin ambigüedades.	Políticas Relacionadas: "Herramientas de Monitoreo de Sistemas,' "Areas de Monitoreo Electrónico,' "Uso de Tecnología Telefónica para Conferencias o Grabación,'y "Recopilación de Información Privada"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
11. Consentimiento para la Recopilación de Información Privada	Política: La Gobernación debe obtener el consentimiento por escrito de los clientes antes de registrar cualquier información acerca de los mismos en un sistema informático computarizado.	Políticas Relacionadas: "Autorización de Recopilación de Información Privada" y "Recopilación de Información Privada"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
12. Aviso de Recopilación de Información	Política: En cada instancia que se recopile información que identifique a una persona, se debe entregar en el momento y en el lugar de recopilación, una notificación explícita y entendible.	Políticas Relacionadas: "Actividad de Monitoreo y Grabación" y "Anonimato del Cliente"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
13. Recopilación de Información Personal de Menores	Política: Información personal acerca de niños no debe ser recopilada por ninguno de los sistemas informáticos de la Gobernación, sin el consentimiento claro y sin ambigüedades de los padres o representantes.	Políticas Relacionadas: "Acceso a Material Adulto" y "Autorización para Inclusión en Sistemas de Datos Privados"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
14. Distribución de la Información Personal	Política: El acceso a cualquier recopilación de información personal de clientes potenciales y otros con quienes la Gobernación tiene relaciones comerciales, debe ser estrictamente controlada con base en la necesidad de conocer, y sin el debido consentimiento la información no se debe vender, intercambiar o distribuir a terceros.	Políticas Relacionadas: "Recopilación Furtiva de Información Privada"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
15. Recopilación de Información de Clientes	Política: Los procedimientos de soporte computarizado de la Gobernación no deben imponer la condición de suministrar información personal innecesaria para completar una transacción o para proveer productos o servicios.	Políticas Relacionadas: "Autorización de Recopilación de Información Privada"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
16. Métodos de Recopilación de Información Privada	Política: La Gobernación debe emplear los métodos menos intrusivos a su disposición para recolectar información confidencial de sus clientes, prospectos, empleados, y otros asociados con su organización.	Políticas Relacionadas: “Recopilación Furtiva de Información Privada” y “Recopilación de Información de Clientes”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
17. Captura de Información Biométrica	Política: La información personal biométrica no debe ser captada por ninguno de los sistemas de la Gobernación, excepto cuando la persona descrita haya sido previamente notificada y haya acordado su captación.	Políticas Relacionadas: “Autorización de Recopilación de Información Privada” e “Identificación Positiva para Uso del Sistema”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
18. Transferencia de Información Biométrica	Política: Los trabajadores no deben suministrar información biométrica a terceros excepto por requisito de ley.	Políticas Relacionadas: “Captura de Información Biométrica”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
19. Expectativas de Privacidad e Información Almacenada en Sistemas de la Organización	Política: La gerencia de la Gobernación debe notificar a todos los usuarios del sistema informático que en cualquier momento y sin previo aviso, la Gobernación puede examinar el correo electrónico archivado, los directorios de archivos personales, los archivos del disco duro y otra información almacenada en los sistemas informáticos de la Gobernación.	Políticas Relacionadas: “Privacidad en Correo Electrónico,’ “Revisión de la Información Respaldada,’y “Privacidad del Archivo Personal”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
20. Conducta de los Empleados Fuera de la Oficina	Política: La gerencia no debe entrometerse en la vida de los empleados o de alguna manera buscar manejar su comportamiento fuera de la jornada laboral, excepto cuando éste perjudique la capacidad del empleado para la realización de sus tareas de trabajo normales, o si afecta la reputación de la Gobernación de manera significativa.	Políticas Relacionadas: “Derechos de Propiedad Intelectual” e “Información de Empleado Potencial”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
21. Sistemas Secretos	Política: Con excepción de las investigaciones criminalísticas, no debe existir un sistema de registros personales en la Gobernación, cuya existencia sea desconocida para las personas descritas en el mismo.	Políticas Relacionadas: “Inventario de Activos — Información” y “Herramientas de Monitoreo de Sistemas”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
22. Acceso a la Información Personal	Política: Cada persona, al solicitarlo por escrito, debe tener acceso a los registros de la Gobernación que contengan información personal referente a su vida personal o su condición.	Políticas Relacionadas: “Declaración Explicativa del Empleado,’ “Información Personal Incorrecta, ’“Revisión del Archivo del Empleado,’ “Distribución de los Registros del Personal,’ y “Acceso al Archivo del Personal”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
23. Divulgación de Información Privada a Terceros	Política: La divulgación de información de los trabajadores de la Gobernación a terceras personas no debe ocurrir, salvo por mandato de ley, o con el consentimiento explícito e inequívoco del trabajador.	Políticas Relacionadas: “Divulgación de Razón de Cese de Relación Laboral” y “Divulgación de Información a las Autoridades”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
24. Transferencia de Datos Privados	Política: La Gobernación sólo debe divulgar datos privados a organizaciones de terceros que se comprometan por escrito a mantener la información con un nivel adecuado de protección según lo determinado por la gerencia de Seguridad Informática.	Políticas Relacionadas: “Términos y Condiciones para el Acceso de Terceros” y “Diseminación de la Información”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
25. Registros de Divulgación de Información Privada — Detalles	Política: Los trabajadores de la Gobernación que divulguen información confidencial a terceros deben mantener registros de todas las divulgaciones, incluyendo la naturaleza de la información, a quien se divulgó y la fecha de tal divulgación.	Políticas Relacionadas: “Uso de la Información Personal para Nuevos Propósitos,’ “Divulgación de Receptor de Información del Cliente,’ y “Notificación al Cliente de Solicitudes de Registros”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
26. Transferencia Internacional de Información Privada	Política: No se debe realizar ninguna transferencia de información privada a otros países, sin importar la tecnología empleada, a menos que se tenga la autorización de la gerencia de Seguridad Informática, cuando la persona afectada está, o será destinada a cualquier país, o cuando la persona haya solicitado específicamente tal transferencia.	Políticas Relacionadas: “Transferencia de Datos Privados” y “Compromiso en Acuerdos de Confidencialidad”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
27. Bloqueo de Divulgación de Información privada	Política: La Gobernación debe informar a las personas por anticipado que los datos personales en su posesión han sido solicitados por terceros, a menos que sea obligada a divulgarlos por mandato claro y autorizado por ley o reglamento, y a esas personas se les debe dar un plazo razonable de varias semanas para que tengan la oportunidad de cerrar el paso a dicha divulgación.	Políticas Relacionadas: “Consentimiento para Acciones Cuestionables en los Sistemas”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
28. Divulgación de Información de Contacto de Trabajadores	Política: La Gobernación no debe divulgar los nombres, cargos, números de teléfono, ubicaciones, u otra información de contacto de sus trabajadores, excepto cuando sea requerido por razones de trabajo, mandato de ley, o cuando la persona haya autorizado su divulgación con claridad.	Políticas Relacionadas: "Divulgación de Información Privada a Terceros"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
29. Divulgación de Razón de Cese de Relación Laboral	Política: La razón del cese de la relación laboral de los trabajadores no debe ser divulgada a terceras personas, excepto con autorización previa de un alto funcionario de la Gobernación o cuando la divulgación se hace por mandato de ley.	Políticas Relacionadas: "Divulgación de Información Privada a Terceros" y "Divulgación de Cambio de Situación"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
30. Divulgación de Cambio de Situación	Política: La información detallada del cambio de situación de un trabajador es estrictamente confidencial, y no se puede divulgar a ninguna persona, excepto a quienes tienen legítimo derecho de conocerla.	Políticas Relacionadas: "Divulgación de Razón de Cese de Relación Laboral"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
31. Acceso a Divulgación de Registros de Datos Privados	Política: Los trabajadores deben recibir acceso a los registros que reflejen la divulgación de su propia información privada, y se les debe dar suficiente información para que ellos puedan comunicarse para corregir errores o suministrar información adicional.	Políticas Relacionadas: "Registros de Divulgación de Información Privada — Mantenimiento"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
32. Información Sobre Desempeño del Trabajador	Política: La información del desempeño del trabajador no se debe suministrar a otros que no tengan la necesidad legítima de conocerla, relacionada con el negocio.	Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer"	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
33. Privacidad del Archivo Personal	Política: Los expedientes personales en los computadores de la Gobernación y en los escritorios de los trabajadores de la Gobernación se deben manejar como para garantizar que otros trabajadores, inclusive los gerentes y los administradores de sistemas, no los puedan leer, salvo que tal acción sea parte de una investigación iniciada por Seguridad Informática, o un intento por descartar o reubicar los expedientes después del retiro del trabajador de la Gobernación.	Políticas Relacionadas: "Examen de los Datos Almacenados en los Sistemas" y "Privacidad en Correo Electrónico"	Política Dirigida a:Todos	Ambientes de Seguridad: Bajos y medianos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
34. Registros de Divulgación de Información Privada — Mantenimiento	Política: Toda divulgación de información privada a terceros se debe registrar y dichos registros se deben mantener por un período mínimo de cinco años.	Políticas Relacionadas: “Divulgación de Información Privada a Terceros” y “Acceso a Divulgación de Registros de Datos Privados”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
35. Privacidad de la Información del Cliente	Política: La información que pueda ser vinculada directamente a un cliente en específico sólo se debe revelar a terceros cuando el cliente haya dado previo consentimiento por escrito, o si la Gobernación está legalmente obligada a divulgar la información.	Políticas Relacionadas: “Información Estadística de los Registros de los Clientes”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
36. Compartir Información Privada	Política: La Gobernación no debe divulgar información específica de las cuentas de clientes, las transacciones, o las relaciones con terceros no afiliados para su uso independiente, a menos que la divulgación de la información sea para una agencia de información de reputación reconocida, cuando la información esta relacionada con una solicitud del cliente para la ejecución de cierto acto, el cliente solicita la divulgación, la divulgación es requerida o permitida por ley, o el cliente ha sido informado acerca de la posibilidad de tal divulgación para propósitos de mercadeo o similares, y se le ha dado la oportunidad de declinar.	Políticas Relacionadas: “Privacidad de la Información del Cliente” y “Divulgación de la Información del Cliente”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
37. Divulgación de Información Privada a Organizaciones Contratadas	Política: La Gobernación no debe vender, arrendar, o de alguna manera transferir información de clientes a terceras personas en ninguna forma, excepto cuando éstas firmen un acuerdo de confidencialidad a través del cual se les prohíba diseminar y hacer uso de la misma con fines no autorizados.	Políticas Relacionadas: “Privacidad de la Información del Cliente”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
38. Divulgación de la Información del Cliente	Política: La Gobernación no debe divulgar a personas externas la información de sus clientes sin una autorización explicita emitida por escrito.	Políticas Relacionadas: “Privacidad de la Información del Cliente”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
39. Divulgación de Datos Personales	Política: La información personal, incluyendo, sin limitantes, la agregada, resumida, anónima, los estudios de casos individuales, o información que identifica personas, que sea recopilada por la Gobernación no se debe vender, alquilar, transferir, entregar, o de alguna otra manera transferir a terceras personas.	Políticas Relacionadas: “Actividad de Monitoreo y Grabación” y “Aviso de Recopilación de Información”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
40. Divulgación de Receptor de Información del Cliente	Política: Cuando le sea solicitado por escrito, la Gobernación debe divulgar con prontitud, el nombre, dirección y número de teléfono de todas las terceras personas que reciben información privada acerca de cualquier cliente o persona.	Políticas Relacionadas: “Registros de Divulgación de Información Privada — Detalles” y “Acceso a la Información Personal”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
41. Notificación al Cliente de Solicitudes de Registros	Política: La Gobernación no debe liberar los registros de los clientes a terceros a menos que los clientes así lo soliciten, o a menos que se vea obligada a hacerlo por ley o reglamento, y sólo habiendo informado al cliente sobre dicha divulgación con dos semanas de anticipación.	Políticas Relacionadas: “Liberación de Información de la Organización” e “Información Personal de los Clientes”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
42. Aplicación de Política de Privacidad	Política: Toda la información de los clientes debe ser protegida de acuerdo con las políticas de privacidad vigentes para el momento en que se recopile la información, a menos que el cliente autorice otra iniciativa.	Políticas Relacionadas: “Usos de Datos Personales Después de Una Fusión o Adquisición” y “Autorización para Inclusión en Sistemas de Datos Privados”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
43. Privacidad de Información de Contacto de Remitentes	Política: No se deben revelar a terceros las direcciones de correos electrónicos y los números telefónicos de las personas que intercambian información con todos los usuarios de los sistemas informáticos de la Gobernación, a menos que se obligue legalmente a la Gobernación.	Políticas Relacionadas: “Información Personal de los Clientes” y “Registros de Divulgación de Información Privada — Mantenimiento”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
44. Anonimato del Cliente	Política: La Gobernación debe suministrar mecanismos para que los clientes escojan si prefieren mantener su anonimato al utilizar los sistemas de la Gobernación.	Políticas Relacionadas: “Identificadores de Usuarios Anónimos” y “Privacidad de la Información del Cliente”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
45. Identificación de Clientes Famosos	Política: Los trabajadores no deben dar a conocer públicamente la identidad de los clientes famosos cuando éstos estén presentes, no deben hablar sobre estos clientes sino con otros trabajadores de la Gobernación, y no deben revelar la identidad de los mismos a menos que estén realizando una actividad comercial.	Políticas Relacionadas: “Actividad de Monitoreo y Grabación” e “Identificadores de Usuarios Anónimos”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
46. Información Estadística de los Registros de los Clientes	Política: La información estadística que proviene de los registros de los clientes, no se debe revelar a terceros fuera de la Gobernación, a menos que no se pueda identificar al cliente a través de dicha información.	Políticas Relacionadas: “Privacidad de la Información del Cliente” y “Restricciones a la Recopilación de la Información”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
47. Divulgación del Registro de las Actividades del Cliente	Política: Los registros que reflejen las actividades de los usuarios de los computadores o de los que se benefician de estos, no se deben revelar a terceros, a menos que la Gobernación se vea obligada por una orden remitida por un tribunal, por una ley o por una regulación, o mediante una autorización por escrito de los individuos correspondientes.	Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer” e “Información de Registro del Cliente”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
48. Cumplimiento de la Privacidad	Política: Los trabajadores no deben permitir una violación de la privacidad de la Gobernación o dejar de observar el derecho a la privacidad de la Gobernación, a menos que se obtenga una autorización de la alta gerencia.	Políticas Relacionadas: “Acuerdos de Confidencialidad de Terceros” y “Divulgación de Información a las Autoridades”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
49. Consentimiento para Acciones Cuestionables en los Sistemas	Política: Cuando exista inseguridad en el desempeño de una actividad con un computador, los trabajadores de la Gobernación deben informar a los afectados sobre las acciones que piensan llevar a cabo, el propósito de dichas acciones, y los impactos potenciales que estas pueden ocasionar en los receptores de la información, y deben contar con autorización de los afectados o el permiso de un vicepresidente.	Políticas Relacionadas: “Responsabilidad en la Seguridad Informática”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
50. Autorización de Acceso a los Registros Individuales	Política: Los pacientes no pueden ver sus registros médicos personales sin la autorización previa del proveedor de atención médica que generó dichos registros.	Políticas Relacionadas: “Acceso al Archivo del Personal”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
51. Divulgación de Usos Propuestos de Información Personal	Política: Antes de que un cliente coloque una orden o revele alguna información personal, todos los representantes de la Gobernación deben informar a los clientes la forma en que dicha información se va a utilizar.	Políticas Relacionadas: “Opción de Participación en Sistema de Datos Privados”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
52. Acceso al Archivo del Personal	Política: Se debe permitir a los empleados tanto examinar como elaborar una copia de la información que aparece en su archivo personal.	Políticas Relacionadas: “Acceso a la Información Personal,’ “Sistemas Secretos,’ y “Distribución de los Registros del Personal”	Política Dirigida a:Usuarios finales y gerencia	Ambientes de Seguridad: Todos
53. Revisión del Archivo del Empleado	Política: Todos los empleados que deseen revisar su archivo personal, deben someter una petición por escrito a la gerencia de Recursos Humanos, y revisar sus archivos en el momento asignado, durante horas laborables, y en la presencia de un representante de Recursos Humanos.	Políticas Relacionadas: “Distribución de los Registros del Personal” y “Autorización de Acceso a los Registros Individuales”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
54. Declaración Explicativa del Empleado	Política: Si los empleados objetan la exactitud, la importancia o la integridad de la información que aparece en sus archivos personales, se les debe dar una oportunidad para incorporar una declaración adicional.	Políticas Relacionadas: “Acceso a la Información Personal”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
55. Información Personal Incorrecta	Política: Cada vez que se notifique a la Gobernación sobre la existencia de información personal errada en sus registros, esta debe corregir inmediatamente dicha información o anexarle un indicativo de que la misma está en discusión y que se alega su inexactitud.	Políticas Relacionadas: “Acceso a la Información Personal” y “Divulgación de Receptor de Información del Cliente”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
56. Integridad del Registro Personal	Política: La gerencia debe realizar esfuerzos adicionales para garantizar que la información personal que permanece en la Gobernación es correcta, oportuna, relevante e íntegra.	Políticas Relacionadas: “Investigación de Errores” e “Información de Contacto del Empleado”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
57. Manejo del Registro Personal	Política: Se deben establecer procedimientos documentados para manejar la información personal, se debe hacer un seguimiento estricto y actualizar dicha información regularmente.	Políticas Relacionadas: “Revisión de Registros de Operadores de Computadores” y “Procedimientos de Respuesta a Intrusión”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
58. Uso del Registro Personal	Política: La gerencia debe realizar esfuerzos adicionales para garantizar que la información personal se va a utilizar sólo para lo que se diseñó originalmente y que las precauciones para evitar su mal uso son efectivas y apropiadas.	Políticas Relacionadas: “Usos Inaceptables de los Sistemas de Computación y de Comunicaciones”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
59. Registro del Acceso a la Información Privada	Política: Deben establecerse controles de acceso para todo sistema de producción que contenga información catalogada como "privada", de forma tal que todo acceso a dicha información iniciado por un usuario sea registrado, identificando al individuo cuya información fue accedida, al usuario que está haciendo la petición de acceso, la fecha y la hora.	Políticas Relacionadas: “Registros en Sistemas y Aplicaciones Sensibles,’ “Arquitectura de Sistemas para Registro de Actividades,’ y “Originador de Transacciones”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
60. Uso de la Información Personal para Nuevos Propósitos	Política: La información personal acerca de empleados, consultores o contratistas que ha sido recopilada para un propósito, no debe ser utilizada para otro fin sin el claro y manifiesto consentimiento de las partes a las que esta información incumba.	Políticas Relacionadas: “Uso Personal del Teléfono” y “Uso Distinto al Empresarial de la Información de la Organización”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
61. Enlace de Información Anónima	Política: Los sistemas informáticos y el personal de la Gobernación no deben enlazar información anónima con información que permita la identificación personal, a menos que las personas involucradas hayan dado su consentimiento.	Políticas Relacionadas: “Uso de la Información Personal para Nuevos Propósitos,’ “Enlaces con Información Privada,’ y “Uso del Registro Personal”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
62. Información Personal de los Clientes	Política: Todos los registros de los clientes que contengan información personal que se encuentren en poder de la Gobernación deben utilizarse únicamente con fines directamente relacionados con el negocio de la Gobernación y únicamente pueden ser revelados a terceros con el consentimiento del cliente o si la Gobernación ha recibido una citación u orden judicial.	Políticas Relacionadas: "Uso de la Información de Contacto del Cliente"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
63. Acceso del Cliente a Información Personal	Política: A los clientes se les debe dar la oportunidad de obtener una confirmación de la Gobernación de que la información personal acerca de ellos se encuentra almacenada en los sistemas de la Gobernación y una explicación acerca de la naturaleza de esta información.	Políticas Relacionadas: "Recopilación de Información de Clientes" e "Información Personal para el Funcionamiento del Negocio"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
64. Uso de la Información de Contacto del Cliente	Política: La información de contacto recopilada acerca de los clientes o clientes potenciales debe utilizarse únicamente para propósitos internos de la Gobernación.	Políticas Relacionadas: "Información Personal de los Clientes" y "Divulgación de Información Privada a Organizaciones Contratadas"	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
65. Información Personal Incluida	Política: Los sistemas informáticos de la Gobernación no deben emplear números seriales secretos, números de identificación del personal secretos ni cualquier otra clase de mecanismo secreto que pudiera revelar la identidad o las actividades de los clientes.	Políticas Relacionadas: "Enlaces Entre la Información Privada y la Identificadora" y "Cookies para Inicios Automáticos de Sesión"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
66. Identificadores Personales en Ubicaciones Públicas	Política: Con excepción de las claves de cifrado y de los certificados digitales, ningún identificador personal debe aparecer en una ubicación accesible públicamente,	Políticas Relacionadas: "Información Personal Incluida" e "Identidad en Internet"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
67. Inteligencia de Números de Cuentas	Política: La Gobernación no puede utilizar identificadores externos significativos como sus propios números internos de cuenta de los clientes.	Políticas Relacionadas: "Códigos de Identificación para Soporte Técnico" y "Acceso a la Información Personal"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
68. Enlaces Entre la Información Privada y la Identificadora	Política: Debe mantenerse el enlace entre la información de identificación personal y los datos privados únicamente hasta llevar a cabo el propósito para el cual se recopilaron originalmente los datos.	Políticas Relacionadas: “Enlaces con Información Privada,’ “Identificadores de Usuarios Anónimos,’ e “Informes de Incidentes”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos
69. Enlaces con Información Privada	Política: Los sistemas informáticos no deben soportar ningún enlace entre información privada y otros tipos de información relacionada con la misma persona sin la aprobación de la Gerencia de Seguridad Informática.	Políticas Relacionadas: “Enlaces Entre la Información Privada y la Identificadora” y “Enlace de Información Anónima”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
70. Opción de Participación en Sistema de Datos Privados	Política: Antes de proceder a la implantación de un nuevo o sustancialmente modificado sistema informático que maneje datos privados, las personas involucradas deben tener la oportunidad de escoger si desean participar en el nuevo sistema.	Políticas Relacionadas: “Autorización para Inclusión en Sistemas de Datos Privados,’ “Clientes Rechazan Correo Directo No Solicitado,’ y “Divulgación de Usos Propuestos de Información Personal”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
71. Recordatorio de Política de Privacidad	Política: A todos los clientes de la Gobernación se les debe enviar anualmente una copia de la política oficial de privacidad de la Gobernación y las instrucciones informándoles cómo pueden dejar de participar de las actividades de compartimiento de datos de la Gobernación.	Políticas Relacionadas: “Clientes Rechazan Correo Directo No Solicitado” y “Aviso de Cambio en Política de Privacidad”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
72. Autorización para Inclusión en Sistemas de Datos Privados	Política: Para que los individuos interesados puedan ser incluidos dentro de cualquier sistema de la Gobernación que maneje datos privados, deben específicamente elegir participar en el sistema.	Políticas Relacionadas: “Opción de Participación en Sistema de Datos Privados”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
73. Control del Individuo sobre el Uso de sus Datos Personales	Política: Si un individuo o cliente decide revocar el permiso que dio para que la Gobernación utilice sus datos personales, la Gobernación debe actualizar rápidamente sus registros y asegurarle que sus deseos se han cumplido.	Políticas Relacionadas: “Aplicación de Política de Privacidad” y “Opción de Participación en Sistema de Datos Privados”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
74. Uso de Información Específica Respecto de la Ubicación	Política: La Gobernación no utilizará información relativa a la ubicación precisa de sus clientes o empleados con dispositivos inalámbricos o permitirá que otras organizaciones comerciales utilicen esta información con propósitos de mercadeo a menos que exista una autorización específica de cada individuo.	Políticas Relacionadas: “Información Personal de los Clientes” y “Uso de Pequeños Computadores Portátiles”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
75. Remoción de Individuos de la Base de Datos	Política: Si un individuo solicita ser removido de la base de datos de clientes o prospectos de la Gobernación, los empleados deben eliminarlo inmediatamente de la base de datos.	Políticas Relacionadas: “Fuente de Material de Mercadeo por Correo Electrónico” e “Información de Registro del Cliente”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
76. Eliminación de la Información del Cliente o Prospecto	Política: Cuando los clientes o prospectos soliciten que la información acerca de ellos sea eliminada de los registros de la Gobernación, ésta debe rápidamente cumplir este requerimiento a menos que retenga las porciones de los registros de sus transacciones que sean requeridos por autoridades gubernamentales o que puedan ser necesarios para demostrar el cumplimiento de las leyes y las regulaciones.	Políticas Relacionadas: “Retención de la Información Personal” y “Enlaces Entre la Información Privada y la Identificadora”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
77. Bloqueo del Uso de Datos Privados	Política: Los empleados de la Gobernación deben respetar diligentemente el derecho incondicional de los individuos de bloquear los datos acerca de ellos con propósitos de mercadeo, bloquear la venta de estos datos a terceros y eliminar permanentemente estos datos de listas de mercadeo directo.	Políticas Relacionadas: “Registro del Movimiento de Documentos Secretos” y “Distribución de Materiales de Mercadeo”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
78. Compartir Información Personal	Política: La Gobernación no puede vender, alquilar, comerciar, prestar o transferir ninguna información personal de los clientes o prospectos a cualquier otra organización incluyendo, sin limitantes, afiliados, subsidiarias, compañías filiales, casas matrices y socios estratégicos.	Políticas Relacionadas: “Transferencia de Datos Personales” y “Compromiso en Acuerdos de Confidencialidad”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
79. Transferencia de la Información sobre Clientes	Política: Si la Gobernación es cerrada, fusionada, adquirida por otra, u ocurre cualquier otro cambio legal en su estructura organizativa, la Gobernación puede necesitar compartir toda o parte de la información de sus clientes con otra entidad, por lo que éstos deben ser notificados rápidamente.	Políticas Relacionadas: “Usos de Datos Personales Después de Una Fusión o Adquisición”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
80. Transferencia de Datos Personales	Política: La Gobernación no debe compartir la información personal sobre sus clientes con otras organizaciones que no sean subsidiarias, empresas subcontratadas o socios estratégicos de negocios, a menos que la Gobernación esté en quiebra, sea fusionada o adquirida por otra.	Políticas Relacionadas: “Transferencia de la Información sobre Clientes” y “Bloqueo del Uso de Datos Privados”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
81. Usos de Datos Personales Después de Una Fusión o Adquisición	Política: Si la Gobernación o cualquiera de sus bases de datos de información personal son vendidas, fusionadas, adquiridas o de cualquier otra manera transferidas a otra organización, esta información no puede ser utilizada para nuevos y no previstos propósitos a menos que los individuos involucrados aprueben estos nuevos usos.	Políticas Relacionadas: “Aplicación de Política de Privacidad” y “Autorización para Inclusión en Sistemas de Datos Privados”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
82. Cambios en la Estructura del Negocio y la Transferencia de Datos Privados	Política: La Gobernación no puede transferir datos privados de los clientes a terceros, sin importar qué tipo de cambios organizacionales experimente.	Políticas Relacionadas: “Usos de Datos Personales Después de Una Fusión o Adquisición”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
83. Indices de Base de Datos que Contienen Información Privada	Política: La Gobernación debe actualizar e indexar anualmente todas las bases de datos internas y archivos que contengan información privada y hacer que este índice esté disponible a los empleados y terceros descritos estas bases de datos y archivos.	Políticas Relacionadas: “Autorización de Recopilación de Información Privada” e “Inventario de Activos — Información”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
84. Lista de Tipos de Información de Producción Disponibles para Empleados	Política: La Gerencia de Tecnología de la Información debe crear y actualizar anualmente una lista completa de los tipos de información de producción que mantiene la Gobernación, hacer que esta lista esté disponible para todos los empleados e informarles qué tipos de información están a su alcance para su inspección.	Políticas Relacionadas: “Autorización de Recopilación de Información Privada” y “Diccionario de Datos”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
85. Negativa a Proporcionar Información Innecessaria	Política: No se puede negar ningún beneficio de la Gobernación a la persona que se niegue a suministrar información confidencial innecesaria cuando el departamento legal de la Gobernación haya resuelto todas las disputas acerca de la definición de "información confidencial necesaria".	Políticas Relacionadas: “Mal Funcionamiento del Control de Acceso,’ “Resolución de Quejas,’ y “Verificaciones de Historia Crediticia de Empleados Potenciales”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
86. Cifrado de Correo Electrónico Privado	Política: Nunca se debe transmitir a través de correo electrónico información descifrada que haya sido catalogada como privada.	Políticas Relacionadas: “Envío de Información Secreta Vía Fax — Cifrado” e “Información Secreta en Correo Electrónico”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
87. Aviso de Cambio en Política de Privacidad	Política: Los miembros del personal de la Gobernación deben llevar a cabo los pasos razonables para notificar rápidamente a todos los individuos afectados en caso de que exista un cambio sustantivo en sus políticas de privacidad.	Políticas Relacionadas: “Puntos de Recopilación de Datos Personales y la Privacidad” y “Herramientas de Monitoreo de Sistemas”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
88. Resumen de Diferencias en Políticas de Privacidad	Política: Cuando la Gobernación modifica la política de privacidad, todos aquellos que se ven afectados y provistos de un resumen con todos los cambios y su posible impacto.	Políticas Relacionadas: “Importancia de la Política de Privacidad” y “Aviso de Cambio en Política de Privacidad”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
89. Importancia de la Política de Privacidad	Política: La Gobernación debe asegurar que su política de privacidad se encuentra completa, que no existen excepciones y que hace referencia a todas las interacciones con los clientes sin importar los canales de comunicación, los departamentos involucrados dentro de la Gobernación y qué tópicos abarca esta interacción.	Políticas Relacionadas: “Acceso del Cliente a Información Personal”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
90. Puntos de Recopilación de Datos Personales y la Privacidad	Política: Todos aquellos puntos en donde se recopilan datos personales para ser utilizados por los sistemas informáticos de la Gobernación deben incluir una copia de la política de privacidad de la Gobernación aprobada por la Gerencia de Seguridad Informática.	Políticas Relacionadas: “Herramientas de Monitoreo de Sistemas” y “Verificaciones de Historia Crediticia de Empleados Potenciales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
91. Identidad del Recolector de Información Privada	Política: Tanto el nombre legal del recolector de la organización como la información actual de contacto deben ser revelados en cada punto en donde se recopile información privada.	Políticas Relacionadas: “Aviso de Recopilación de Información” y “Recopilación Furtiva de Información Privada”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
92. Explicación del Requerimiento de Información Privada	Política: Cada vez que los trabajadores o los sistemas informáticos de la Gobernación soliciten información privada, deben revelarse las razones completas y detalladas para recopilarla.	Políticas Relacionadas: “Declaración Explicativa del Empleado” y “Conciencia del Usuario Sobre Registros de Violaciones de Seguridad”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
93. Distribución de Políticas de Privacidad	Política: Todas las políticas internas de privacidad de la Gobernación que un cliente potencial o un cliente pueda necesitar saber deben ser posteadas públicamente o distribuidas periódicamente de algún otro modo a estas mismas personas.	Políticas Relacionadas: “Aviso de Cambio en Política de Privacidad” y “Puntos de Recopilación de Datos Personales y la Privacidad”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
94. Revisión de los Archivos Privados de Usuarios	Política: Cada vez que los administradores autorizados del sistema revisan los archivos de usuario privado para atender emergencias u otras necesidades de negocio, se debe notificar con prontitud al usuario mencionado a menos que se esté llevando a cabo una investigación de presuntos actos criminales o de abuso.	Políticas Relacionadas: “Acceso a Información Sensible o Valiosa,’ “Otorgamiento de Acceso a la Información de la Organización,’ y “Privacidad en Correo Electrónico”	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
95. Modificaciones a la Información Personal	Política: Antes de realizar cualquier cambio en los datos personales de los sistemas de producción de la Gobernación basado en una solicitud del cliente, éste debe suministrar la información anterior correcta.	Políticas Relacionadas: “Contraseñas de Servicio al Cliente” y “Códigos de Identificación para Soporte Técnico”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
12.01.05 Prevención del Uso Indebido de las Instalaciones de Procesamiento de Información				
1. Juegos en los Sistemas de Computación de la Organización	Política: No se pueden almacenar o usar juegos en ninguno de los sistemas de computación de la Gobernación.	Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones” y “Copias de Software”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
2. Uso Personal de los Sistemas de Computación y de Comunicaciones	Política: El computador y los sistemas de comunicaciones de la Gobernación deben usarse únicamente para propósitos de negocio, salvo que se haya obtenido un permiso especial del gerente del departamento.	Políticas Relacionadas: “Uso Distinto al Empresarial de la Información de la Organización,’ “Uso Personal del Teléfono,’ “Usos del Sistema de Correo Electrónico,’ “Uso Personal de Internet,’ y “Juegos en los Sistemas de Computación de la Organización”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
3. Uso Personal Incidental de los Sistemas de Comunicación	Política: El computador y los sistemas de comunicación de la Gobernación deben utilizarse únicamente para propósitos de negocio, salvo que su uso sólo consuma una cantidad insignificante de recursos que de otro modo pudiesen emplearse para propósitos de negocio, no interfiera con la productividad del trabajador y no tenga prioridad sobre otras actividades de negocio.	Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones,’ “Uso Personal del Teléfono,’ y “Juegos en los Sistemas de Computación de la Organización”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
4. Uso Personal Razonable de los Sistemas de Computación y de Comunicaciones	Política: El uso personal del computador y de los sistemas de comunicaciones debe ser consecuente con las normas convencionales de conducta cortés y ética.	Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones” y “Uso Personal Incidental de los Sistemas de Comunicación”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
5. Acceso de Usuarios a Internet	Política: Los usuarios que acceden a la Internet con las facilidades de la Gobernación deben estar informados que lo hacen a su propio riesgo y que la Gobernación no se responsabiliza por el material que los usuarios vean, descarguen o reciban a través de la Internet.	Políticas Relacionadas: “Sitios Web No Relacionados con Negocio,’ “Control de Tráfico en Internet,’ y “Comunicaciones Salientes en Internet”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
6. Clasificación del Uso Aceptable de Internet	Política: El uso de Internet debe clasificarse de la siguiente manera: rojo, en los casos cuando está prohibido en todo momento, amarillo, cuando se permite únicamente con la autorización de los gerentes de departamento o verde, cuando se permite en todo momento.	Políticas Relacionadas: “Zonas de Seguridad de la Red” y “Descargas Grandes desde Internet”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
7. Usos Inaceptables de los Sistemas de Computación y de Comunicaciones	Política: Los suscriptores de los servicios de computación y de comunicaciones no deben emplear estas facilidades para ofrecer sus servicios, vender productos o dedicarse de algún modo a actividades comerciales diferentes a las que están expresamente permitidas por la gerencia de la Gobernación.	Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones” y “Usos del Sistema de Correo Electrónico”	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
8. Uso Personal de Internet	Política: Los sistemas informáticos de la Gobernación no deben usarse para acceder a la Internet con fines personales.	Políticas Relacionadas: “Usos Inaceptables de los Sistemas de Computación y de Comunicaciones,’ “Uso Personal de los Sistemas de Computación y de Comunicaciones,’ y “Uso Personal del Teléfono”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
9. Uso Personal de los Servicios de Internet de la Organización	Política: Todos los trabajadores que hacen uso de la Internet por razones personales con las facilidades de Internet de la Gobernación deben hacerlo fuera del horario de trabajo.	Políticas Relacionadas: “Identificadores Personales de Usuario — Responsabilidad” y “Uso Personal de los Sistemas de Computación y de Comunicaciones”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
10. Tiempo de Acceso Personal a Internet	Política: El acceso del trabajador a la Internet por razones personales mientras utilizan las facilidades de Internet de la Gobernación debe realizarse únicamente después del horario normal de trabajo.	Políticas Relacionadas: "Uso Personal de los Sistemas de Computación y de Comunicaciones" y "Uso Personal de Internet"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
11. Restricciones al Uso Personal	Política: El uso personal secundario de los sistemas de computación y de comunicación de la Gobernación debe restringirse a una hora o menos al mes y debe excluir las siguientes actividades: crear o distribuir cartas en cadena, intercambiar información que pudiese considerarse indecente, recibir o reenviar chistes, tener un segundo empleo o buscar otro y participar en juegos de azar o en actividades políticas o benéficas.	Políticas Relacionadas: "Uso Personal de Internet"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
12. Identificadores de Usuario Empleados en Actividades Abusivas	Política: Todos los privilegios del sistema asignados a un identificador de usuario que participe en actividades indebidas o delictuales deben ser revocados de inmediato.	Políticas Relacionadas: "Finiquito de los Privilegios de Acceso" y "Reinicialización de la Contraseña Posterior a la Desactivación"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
13. Herramientas de Prueba de la Seguridad del Sistema	Política: Los trabajadores de la Gobernación no deben adquirir, poseer, intercambiar o utilizar herramientas de software o hardware que pudiesen emplearse para evaluar o comprometer la seguridad de los sistemas informáticos salvo que la gerencia de Seguridad Informática lo autorice expresamente.	Políticas Relacionadas: "Prueba de los Controles del Sistema Informático,' "Divulgación de las Vulnerabilidades del Sistema Informático,' y "Herramientas de Estado de Seguridad del Sistema"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos
14. Uso Distinto al Empresarial de la Información de la Organización	Política: El uso de la información de la Gobernación para algún propósito que haya sido expresamente establecido por la gerencia debe ser aprobado por escrito por el Propietario designado de la información.	Políticas Relacionadas: "Uso Personal de los Sistemas de Computación y de Comunicaciones,' "Uso de la Información,' y "Usos del Sistema de Correo Electrónico"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
15. Examen de los Datos Almacenados en los Sistemas	Política: La gerencia de la Gobernación debe reservarse el derecho de revisar toda la información almacenada o transmitida por sus sistemas de computación y de comunicaciones y debe informar a todos los trabajadores que no deben esperar ninguna privacidad asociada con la información que almacenan o envían a través de estos sistemas.	Políticas Relacionadas: "Derechos de Propiedad Intelectual,' "Monitoreo de Mensajes de Correo Electrónico,' y "Privacidad del Archivo Personal"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
16. Areas de Monitoreo Electrónico	Política: Los trabajadores deben ser informados de que pueden estar sujetos a monitoreo electrónico en áreas donde no hay ninguna expectativa razonable de privacidad mientras se encuentren en las instalaciones de la Gobernación con el objeto de apoyar la medición del desempeño del trabajador y de proteger su propiedad y su seguridad, así como la propiedad de la Gobernación.	Políticas Relacionadas: "Monitoreo de Mensajes de Correo Electrónico" y "Recopilación Furtiva de Información Privada"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
17. Discusiones Utilizando Servicios Computacionales y Comunicacionales	Política: Los sistemas internos de computación y de comunicación no deben emplearse como un foro abierto para discutir los cambios en la organización o los asuntos relacionados con la política de los negocios de la Gobernación.	Políticas Relacionadas: "Derecho a la Libre Expresión" y "Uso Personal de Internet"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
12.01.06 Reglamentación de los Controles Criptográficos				
1. Armamentos en Comercio Internacional	Política: Los usuarios no deben distribuir, directa o indirectamente, software de cifrado ni otras municiones de guerra tal como se define en cualquier reglamentación de comercio internacional de armamentos.	Políticas Relacionadas: "Envío de Información Sensible Vía Fax — No Cifrada"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Medianos y altos
12.01.07 Recopilación de Evidencia				
1. Evidencia de Delito o Abuso Informático	Política: Toda la información relacionada con un supuesto uso indebido o delito, incluyendo sin limitantes, la configuración actual del sistema y a las copias de respaldo de todos los archivos potencialmente comprometidos, debe capturarse y almacenarse de inmediato en forma segura fuera de línea hasta que se otorgue la custodia oficial de la misma a otra persona autorizada o hasta que el asesor legal principal determine que la Gobernación ya no necesita la información.	Políticas Relacionadas: "Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Fuentes de Evidencia Digital	Política: Para cada sistema de computación de producción, el departamento de Seguridad Informática debe identificar las fuentes de evidencia digital que razonablemente pudiesen ser usadas en un juicio e implementar un proceso normalizado de captura, retención y destrucción similar al que se utiliza para los registros demográficos.	Políticas Relacionadas: "Registro de Intentos de Acceso" y "Archivo de Correo Electrónico"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Medianos y altos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
3. Divulgación de Información a las Autoridades	Política: Los usuarios deben dar su consentimiento en el sentido de permitir que toda la información que almacenen en los sistemas de la Gobernación se divulgue a las autoridades a discreción de la gerencia de la Gobernación.	Políticas Relacionadas: "Examen de los Datos Almacenados en los Sistemas,' "Divulgación de Información Privada a Terceros,' y "Monitoreo de Mensajes de Correo Electrónico"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
4. Información Sobre el Monitoreo del Desempeño	Política: La gerencia no debe utilizar los computadores para recopilar en forma automática información sobre el desempeño de los trabajadores, salvo que los trabajadores mencionados hayan acordado colectivamente que dicha información refleja en forma realista su desempeño en el trabajo.	Políticas Relacionadas: "Autorización de Recopilación de Información Privada" y "Uso de Tecnología Telefónica para Conferencias o Grabación"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
5. Permiso para Monitoreo	Política: La Gobernación no debe monitorear las comunicaciones de un empleado sin su permiso, salvo que el permiso por adelantado pueda modificar alguna conducta específica.	Políticas Relacionadas: "Monitoreo de Mensajes de Correo Electrónico"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
6. Monitoreo de las Comunicaciones de los Empleados	Política: La Gobernación no debe participar en el monitoreo general de las comunicaciones de los empleados, salvo que exista una necesidad justificada de negocio que no pueda ser satisfecha por otros medios, el empleado mencionado no está disponible y el factor tiempo sea crucial en una actividad de negocio, exista una causa razonable para sospechar que se está produciendo una actividad delictiva o una violación a la política o el monitoreo sea requerido según la ley, el reglamento o los acuerdos con terceros.	Políticas Relacionadas: "Expectativas de Privacidad e Información Almacenada en Sistemas de la Organización"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
7. Monitoreo o Grabación de Conversaciones Telefónicas	Política: Las conversaciones telefónicas del trabajador de la Gobernación no deben ser monitoreadas o grabadas a menos que se escuche claramente el tono de beep cuando se realice el monitoreo.	Políticas Relacionadas: "Monitoreo del Desempeño"	Política Dirigida a:Todos	Ambientes de Seguridad: Todos
8. Confidencialidad de la Información de las Investigaciones Internas	Política: Todas las investigaciones que se lleven a cabo de supuesta conducta indebida o delictiva debe mantenerse estrictamente confidencial para preservar la reputación de la parte sospechosa hasta que se formulen los cargos o se tomen las medidas disciplinarias correspondientes.	Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías,' "Investigación de Delito Computarizado,' y "Transferencias de Trabajadores"	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
9. Investigaciones Policiacas o Legales	Política: Los trabajadores de la Gobernación no deben revelar ninguna información interna de la Gobernación a través de ningún mecanismo de comunicaciones, a menos que hayan establecido la autenticidad de la identidad del individuo y la legitimidad de la investigación.	Políticas Relacionadas: “Divulgación Telefónica de Información” y “Solicitudes de Información Organizacional”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
10. Participación en Procedimiento Legal	Política: Cualquier empleado de la Gobernación que reciba una citación o que sea llamado para testificar frente a un jurado o una agencia gubernamental, debe notificar este hecho por escrito al asesor legal en jefe.	Políticas Relacionadas: “Infracción de la Ley” y “Manejo de Mensajes de Correo Electrónico”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
11. Provisión de Información en Procedimientos Legales	Política: Los empleados no deben suministrar ningún informe de la Gobernación ni copias de él a terceros fuera de la Gobernación ni a funcionarios gubernamentales, en respuesta a una citación o de cualquier otra manera, ni deben testificar acerca de hechos que conocieron mientras desempeñaban sus cargos en la Gobernación, a menos que previamente se haya obtenido autorización del asesor legal en jefe.	Políticas Relacionadas: “Información de Asuntos Legales” y “Moratoria en Destrucción de Datos”	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
12. Contactos con Autoridades Judiciales	Política: El personal técnico de sistemas informáticos no debe contactar a la policía ni a ningún otro miembro de la comunidad de justicia criminal con relación a algún problema que se le presente en los sistemas informáticos, a menos que tengan autorización del director del departamento Legal.	Políticas Relacionadas: “Interferencia con Reportes de Violaciones y Problemas” y “Cumplimiento de la Privacidad”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
13. Reportes Sobre Situación de la Investigación	Política: El estatus de las investigaciones sobre seguridad informática debe ser comunicado a la gerencia únicamente por el jefe de la investigación o por el representante de la gerencia dentro del equipo de investigación.	Políticas Relacionadas: “Análisis de Violaciones y Problemas” y “Verificación de Cumplimiento de Seguridad Informática”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
14. Información Sobre Investigaciones de Delitos Computarizados	Política: Toda evidencia, idea e hipótesis acerca de delitos de computación que haya sufrido la Gobernación, incluyendo posibles métodos de ataque e intenciones de ataque, debe ser comunicada al asesor legal interno de la empresa y tratada como información restringida y legalmente privilegiada.	Políticas Relacionadas: “Divulgación de Ataques a Sistemas de Computación” y “Reportes Centralizados de Problemas”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
15. Proceso de Análisis Forense	Política: Todo análisis o investigación en el que se utilicen medios de almacenamiento de datos que contengan información que podría en algún momento convertirse en evidencia importante para un juicio sobre un delito o abuso de computación, debe llevarse a cabo con una copia en lugar de utilizar la versión original.	Políticas Relacionadas: "Destrucción de Mensajes de Correo Electrónico" y "Evidencia de Delito o Abuso Informático"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
16. Investigaciones de Seguridad Informática	Política: Todas las investigaciones internas de la Gobernación sobre incidentes de seguridad informática, violaciones y problemas, deben ser conducidas por personal adiestrado por la gerencia de Seguridad Informática.	Políticas Relacionadas: "Revisión de los Archivos Privados de Usuarios" y "Problemas por Accesos No Autorizados"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
17. Equipos de Investigación de Seguridad Informática	Política: Cualquier persona que sea amiga personal o conocida de un sospechoso en una investigación, no debe formar parte del equipo de investigación sobre incidentes de seguridad informática.	Políticas Relacionadas: "Investigaciones de Seguridad Informática" y "Detalles de Investigaciones de Intrusiones"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
18. Investigaciones Internas y Solicitudes Oficiales	Política: Todos los empleados de la Gobernación deben testificar o responder a preguntas relacionadas con investigaciones internas cuando el asesor legal en jefe les indique hacerlo.	Políticas Relacionadas: "Participación en Procedimiento Legal" y "Reportes Sobre Situación de la Investigación"	Política Dirigida a:Usuarios finales	Ambientes de Seguridad: Todos
19. Detalles de Investigaciones de Intrusiones	Política: Los detalles acerca de investigaciones actuales sobre intrusiones en sistemas informáticos no deben enviarse a través del correo electrónico ni deben almacenarse los archivos que describen una investigación actual en sistemas potencialmente interceptables, o en una red en la que puede esperarse que sean vistos por intrusos.	Políticas Relacionadas: "Informes de Violaciones y Problemas" y "Evidencia de Delito o Abuso Informático"	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
12.02 Revisión de Políticas de Seguridad y Cumplimiento Técnico				
12.02.01 Cumplimiento de la Política de Seguridad				
1. Cumplimiento del Discado Telefónico	Política: Las conexiones telefónicas discadas a sistemas internos y redes deben ser revisadas por el departamento que hace la instalación y cualquier desviación de las normas internas publicadas debe ser previamente aprobada por la gerencia de Seguridad Informática.	Políticas Relacionadas: "Conexiones Discadas" y "Acceso Remoto de Terceros"	Política Dirigida a:Usuarios finales y personal técnico	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
2. Responsabilidad por Cese de Trabajador	Política: En el caso de que un empleado, consultor o contratista termine su relación con la Gobernación, el gerente inmediato del empleado debe asegurarse de que devuelva toda la propiedad que estaba en su custodia antes de que abandone la Gobernación, debe notificar a todos los administradores que manejan las cuentas del computador y de comunicaciones utilizadas por el empleado tan pronto como sea conocida su terminación en el cargo y finalizar todos los privilegios relacionados con su trabajo en el momento en que tenga lugar la terminación.	Políticas Relacionadas: “Devolución de Propiedad al Cesar Empleo”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
3. Planes Divisionales para el Cumplimiento de la Seguridad Informática	Política: La gerencia de cada una de las divisiones de la Gobernación debe preparar un plan anual de forma que sus sistemas de computación y de comunicaciones estén conformes con sus políticas y normas publicadas.	Políticas Relacionadas: “Planes de Seguridad Informática”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
4. Normas de Implantación de Controles	Política: La gerencia debe implementar controles de los sistemas informáticos de forma consistente con las prácticas de negocios generalmente aceptadas y con la criticidad, valor y sensibilidad de la información que procesa.	Políticas Relacionadas: “Corrección de Registros de Negocios,’ “Protección de la Información, ’“Variaciones Respecto de Prácticas de Control Generalmente Aceptadas,’ “Revisión de los Controles de los Sistemas Informáticos — Independiente,’ y “Normas de Seguridad Informática Específicas a Cada Industria”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
5. Variaciones Respecto de Prácticas de Control Generalmente Aceptadas	Política: La gerencia debe revelar las variaciones que perciba de las prácticas generalmente aceptadas en los sistemas informáticos de control y es igualmente responsable de llevar a cabo rápidamente la acción correctiva.	Políticas Relacionadas: “Normas de Implantación de Controles” y “Normas de Seguridad Informática Específicas a Cada Industria”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
6. Evaluaciones de Riesgo de los Sistemas	Política: Cada unidad organizacional dentro de la Gobernación que maneje sus propios computadores o redes debe llevar a cabo una evaluación anual de riesgo relacionado con la seguridad de estos sistemas para posteriormente certificar que se han implementado las medidas de seguridad apropiadas.	Políticas Relacionadas: “Excepciones a las Políticas” y “Evaluación de Riesgo de Seguridad Informática en Toda la Organización”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Medianos y altos
12.02.02 Verificación de Conformidad Técnica				

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
1. Auditorías de Respaldo de Producción	Política: La gerencia de Auditoría Interna debe realizar una revisión anual y pruebas aleatorias de los procesos de respaldo de los sistemas de producción.	Políticas Relacionadas: “Revisión del Respaldo” y “Archivos de Sitios Web y Comerciales”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
2. Evaluaciones de Riesgo de la Seguridad de Sistemas Informáticos	Política: Deben realizarse al menos una vez cada dos años evaluaciones de riesgos de seguridad para los sistemas informáticos que manejan información crítica y aplicaciones de producción críticas, y todas las considerables mejoras, actualizaciones, conversiones y demás cambios asociados con estos sistemas o aplicaciones, deben estar precedidas de una evaluación de riesgo definida en el manual de Seguridad Informática.	Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones” y “Planes de Seguridad Informática”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos
3. Evaluación de Riesgo de Seguridad Informática en Toda la Organización	Política: Cada año la gerencia de Seguridad Informática debe dirigir o manejar a un grupo independiente que lleve a cabo una evaluación a lo largo de toda la organización y genere un informe como resultado de este proyecto en el que se encuentre una descripción detallada de los riesgos de seguridad informática que está enfrentando la organización, con recomendaciones específicas para prevenir o mitigar estos riesgos.	Políticas Relacionadas: “Análisis de Violaciones y Problemas” y “Evaluación del Riesgo en los Sistemas de Producción”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos
12.03 Consideraciones sobre Auditoría de Sistemas				
12.03.01 Controles de Auditoría de Sistemas				
1. Atributos de la Integridad de la Información	Política: Dentro de lo posible, la gerencia debe notificar periódicamente acerca de la exactitud, oportunidad, relevancia y demás atributos de integridad informática que describen a la información utilizada para la toma de decisiones.	Políticas Relacionadas: “Naturaleza y Ubicación de la Información de la Organización” e “Información Incompleta u Obsoleta”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Revisión de los Controles de los Sistemas Informáticos — Interno	Política: El Auditor Interno debe revisar periódicamente lo adecuado de los controles respecto de los sistemas informáticos y el cumplimiento de dichos controles.	Políticas Relacionadas: “Registros de Auditoría en los Sistemas” y “Evaluación del Riesgo en los Sistemas de Producción”	Política Dirigida a:Gerencia	Ambientes de Seguridad: Todos

Tema	Política	Políticas Relacionadas	Política Dirigida a:	Ambientes de Seguridad
3. Verificación de Cumplimiento de Seguridad Informática	Política: El Auditor Interno debe llevar a cabo la verificación del cumplimiento de las políticas, normas y procedimientos relacionados con la seguridad informática.	Políticas Relacionadas: “Revisión de los Controles de los Sistemas Informáticos — Interno”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
12.03.02 Protección de los Rastros de Auditoría de Sistemas				
1. Código Fuente del Software de Penetración de Sistemas	Política: El código fuente de programación y sus respectivos análisis técnicos usados para garantizar la seguridad, debe ser divulgado únicamente a aquellas personas que tengan una necesidad demostrable de conocerlos.	Políticas Relacionadas: “Divulgación de las Vulnerabilidades del Sistema Informático,’ “Comprometer Mecanismos de Seguridad para los Clientes,’ y “Presentación de la Imagen Pública”	Política Dirigida a:Gerencia y personal técnico	Ambientes de Seguridad: Todos
2. Identificación de Vulnerabilidades	Política: Todos los sistemas conectados directamente a Internet deben estar sujetos a una verificación automática de riesgo, llevada a cabo a través de software para identificación de vulnerabilidades por lo menos una vez al mes.	Políticas Relacionadas: “Sistemas de Detección de Intrusos,’ “Contraseñas Proporcionadas por Proveedores,’ y “Evidencia de Delito o Abuso Informático”	Política Dirigida a:Personal técnico	Ambientes de Seguridad: Todos