INDICE

PRESENTACIÓN

Cada uno de nosotros realiza día a día un gran esfuerzo para hacer más eficiente la Administración Pública Federal y para construir un Gobierno más transparente. Para lograr estos objetivos, es fundamental que nos distingamos como Servidores Públicos y que seamos capaces de poner el ejemplo al reflejar, en nuestras actividades y en nuestra relación con los demás, el cuidado en la protección de la información, la rendición de cuentas y la responsabilidad, que son atributos de un buen Gobierno.

Este documento es producto de los Servidores Públicos de la CONSAR, quienes en un ambiente de participación lo enriquecieron con sus aportaciones y comentarios. Asimismo, en él se ha detallado un conjunto de lineamientos que deberán ser observados para el aseguramiento de la información.

Es por ello que los invito a adoptar este modelo como una norma de trabajo; que en nuestras responsabilidades diarias nos comprometamos con el aseguramiento de la información; y que este esfuerzo nos ayude a servir mejor a México y a sentirnos orgullosos de pertenecer a una Institución que cultiva valores de integridad, ética y transparencia.

PRESIDENTE DE LA CONSAR

MARCO NORMATIVO

Las políticas de seguridad presentadas en este manual tienen como fundamento legal lo dispuesto en las regulaciones por las que está regida la CONSAR, las cuales se listan a continuación:

Leyes

Constitución Política de los Estados Unidos Mexicanos
DOF 05-02-1917

Ley de los Sistemas de Ahorro para el Retiro
DOF 23-05-1996
Ley de la Propiedad Industrial
DOF 27-06-1991
Ley Federal del Derecho de Autor
DOF 24-12-1996
Ley Federal de Responsabilidades Administrativas de los Servidores Públicos
DOF 13-03-2002
Ley Federal del Trabajo
DOF 01-04-1970
Ley Federal del Transparencia y Acceso a la Información Pública Gubernamental
DOF 11-06-2002
Ley Federal de Archivos
DOF 23-01-2012

Códigos

Reglamentos

Reglamento de la Ley de los Sistemas de Ahorro para el Retiro
DOF 24-08-2009
Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
DOF 11-06-2003
Reglamento de la Ley de la Propiedad Industrial
DOF 23-11-1994

Reglamento de la Ley Federal del Derecho de Autor
DOF 22-05-1998
Reglamento de la Ley Federal de Archivos
DOF 13-05-2014

Decretos

Lineamientos

Lineamientos de Protección de Datos Personales
DOF 30/09/2005
Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto Federal de Acceso a la Información Pública los Índices de Expedientes Reservados
DOF 09/12/2003
Lineamientos para la Elaboración de las Versiones Públicas, por parte de las Dependencias y Entidades de la Administración Pública Federal
DOF 13/03/2006

Estándares Internacionales

ISO/IEC 17799:2005 Tecnologías de Información – Técnicas de Seguridad – Código de Práctica para la Gestión de la Seguridad de Información

Política

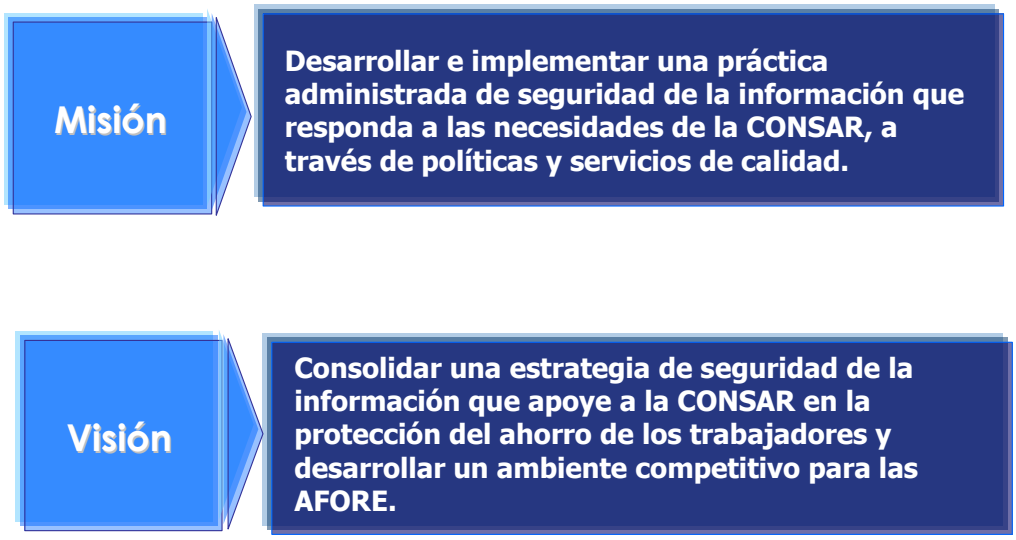
Todos los empleados de la Comisión Nacional del Sistemas de Ahorro para el Retiro están obligados a operar en un ambiente de trabajo que garantice la confidencialidad, integridad y disponibilidad de la información.

El incumplimiento accidental o deliberado de las políticas, estándares, guías y procedimientos descritos en este documento, será considerado una falta y tendrá las consecuencias que correspondan conforme a la normativa aplicable para el caso.

ELABORÓ	REVISÓ	APROBÓ
REPRESENTANTE DEL SGSI	RESPONSABLE DE PROCESO	ALTA DIRECCIÓN

Objetivo

El propósito de la Política General de Seguridad es establecer las directrices para poder cumplir con la misión y visión de seguridad de la información para la CONSAR, las cuales se presentan a continuación:



Misión y Visión del Modelo de Gestión de Seguridad de la Información (MGSI) de la CONSAR.

Los objetivos específicos de la Política General de Seguridad son:

1. Establecer un marco regulatorio de la seguridad de la información congruente con el marco jurídico mexicano y con las disposiciones internas de la CONSAR.
2. Establecer la postura respecto a la seguridad de la información por parte de la CONSAR.
3. Establecer un modelo formal para la administración de riesgos sobre la seguridad de la información.
4. Evaluar, definir e implementar las soluciones tecnológicas, los servicios y las herramientas de protección de la información.
5. Promover una cultura de seguridad y protección de la información a fin de que los datos, bases de datos, herramientas de explotación de información, portales de información y demás elementos relativos a la materia, provean información íntegra, confiable y de fácil acceso a los usuarios autorizados.

6. Definir los planes, programas y presupuestos en materia de seguridad de la información conforme a los objetivos institucionales y al plan estratégico de la CONSAR.

7. Representar a la CONSAR, en materia de seguridad de la información en foros, comités, instituciones, entidades públicas o privadas, tanto nacionales como internacionales, sin que los comentarios o decisiones de los representantes sean vinculatorios para la Comisión, y coordinar los grupos de trabajo internos en dicha materia.

8. Contar con los mecanismos para verificar que la seguridad de la información se está observando con efectividad.

9. Evaluar y proponer adecuaciones a los programas, planes y procedimientos de continuidad de la operación e integridad de los servicios, información y recursos tecnológicos en casos de contingencia o desastre.

Alcance

La Política General de Seguridad de la Información se aplica a todos los servidores públicos, personal por honorarios o terceros como: consultores, empleados eventuales, prestadores de servicio, personal de mantenimiento y/o prestadores de servicio social, que actúen en nombre de la CONSAR o se vinculen con esta, según sea el caso.

La normativa derivada de esta política general se compondrá de los siguientes elementos:

a. **Políticas.** Una política es una declaración de alto nivel, de carácter obligatorio, que describe metas, objetivos y referencias generales sobre tópicos de seguridad de la información.

b. **Lineamientos.** Declaraciones generales de carácter opcional desarrolladas para lograr los objetivos de las políticas.

c. **Procedimientos.** Son las especificaciones de la secuencia de actividades de cómo son implantadas las políticas y los lineamientos en el ambiente operativo de la CONSAR.

Lineamientos.

Propiedad de la Información.

La información que conforme a las facultades de la CONSAR se genere, procese o almacene bajo cualquier concepto será propiedad de la CONSAR o en su caso, del Gobierno Federal; procurando que se observe lo anterior respecto de la información generada por terceros contratados para esos fines.

a. La seguridad de la información debe contemplar la implementación de controles de acuerdo a los siguientes criterios:

   1. Grado de confidencialidad, determinado por el daño o pérdida que puede tener la CONSAR ante un acceso o divulgación de información no autorizada.

   2. Grado de integridad, determinado por el daño o pérdida que puede tener la CONSAR ante la inexactitud de la información.

   3. Grado de disponibilidad, determinado por el daño o pérdida que puede tener la CONSAR frente a la no-disponibilidad de la información cuando ésta sea requerida.

b. El término "*información*" incluye de manera enunciativa más no limitativa los expedientes, reportes, estudios, resoluciones, actas, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, conocimientos adquiridos y/o desarrollados como colaborador de la CONSAR o bien, cualquier otro tipo de registro que documente el ejercicio de las

facultades o de las actividades de la CONSAR, sin importar su fuente o fecha de elaboración.

c. La información que debe protegerse puede estar en cualquier forma o soporte material, incluyendo los electrónicos, que permita su percepción, reproducción u otra forma de transmisión.

d. Esta política se aplica a todas las manifestaciones de la información sin tomar en cuenta la forma ni el formato, así como a todos los recursos para el transporte o transmisión de la misma.

e. El nivel de protección de la información debe establecerse con base en un proceso de análisis que contemple la valoración de amenazas, vulnerabilidades, probabilidad e impacto de los riesgos asociados a ésta.

f. Toda la información utilizada en los procesos de negocio de la CONSAR debe sujetarse a la normativa en materia de seguridad de la CONSAR.

Gestión de la Seguridad

Para lograr una adecuada Gestión de la Seguridad, se debe de:

a. Establecer un plan estratégico de seguridad de la información, el cual deberá ser revisado y actualizado anualmente.

b. Crear un grupo de políticas, estándares, guías y procedimientos de seguridad de la información que estén dirigidos hacía todos los niveles jerárquicos de la CONSAR.

c. Definir un plan de concientización institucional para asegurar el éxito de las iniciativas en materia de seguridad de la información.

d. Establecer un esquema institucional de clasificación de la información para establecer los niveles de protección de ésta.

e. Mantener contacto con grupos especializados en aspectos de seguridad para estar actualizados en dichos temas, como lo pueden ser foros Web de discusión, listas de correo, avisos de correo por parte de fabricantes, páginas Web especializadas en seguridad informática, avisos de correo por parte de proveedores.

f. Asegurar la segregación de funciones en el desempeño de las tareas relevantes de seguridad de la información, para ello se deben establecer los siguientes roles y responsabilidades:

Dueño (Propietario): Tiene la responsabilidad de la clasificación de los activos de información, contando con la autoridad para definir el alcance de acceso a la información, para negar o permitir su consulta, su creación o actualización, su borrado o destrucción.

El dueño de la información debe tener un nivel de Presidencia (PRE), Vicepresidencia (VP), Dirección General (DG), Dirección General Adjunta (DGA) o Dirección de Área (DA).

A continuación se describen las responsabilidades de los dueños de la información en cuanto a seguridad se refiere:

- Identificar y realizar un inventario de los activos de información de su propiedad, mismo que deberá ser actualizado cuando menos una vez al año.
- Clasificar la información con base en su confidencialidad, integridad y disponibilidad.
- Valorar los riesgos asociados a la información.
- Aprobar o rechazar los requerimientos para acceder a la información.
- Impulsar las sanciones para los accesos no autorizados, de acuerdo con su naturaleza y los daños ocasionados.

Custodio de la información. Son las personas que tienen la responsabilidad de establecer y mantener los controles de seguridad adecuados a la información, con base en el nivel de protección requerido por el dueño de la información.

El custodio de la información debe contar con el nivel de Coordinador General de Administración y Tecnologías de la Información (CGATI), Director de Informática (DI), Subdirector de Infraestructura (SI), Jefe de Departamento (JD), Líder de Proyecto (LP) u Operativo (OP).

El Custodio de la información no debe ser el mismo que el dueño de la información y debe estar en un nivel jerárquico abajo del dueño.

A continuación se describen las responsabilidades de los custodios de la información en cuanto a seguridad se refiere:

- Proteger los activos de Información según la clasificación asignada.
- Permitir los accesos a la información solo por el personal autorizado.
- Informar a los usuarios sobre los controles establecidos.
- Llevar a cabo las acciones delegadas por el dueño de la información, para asegurar ésta.

Administrador de Tecnologías de Información. Tiene la responsabilidad de las aplicaciones y sistemas de información y se encarga de mantener la administración de los sistemas donde radica la información. A continuación se describen las responsabilidades de los administradores de Tecnologías de Información (TI) en cuanto a seguridad se refiere:

- Revisar periódicamente las TI a su cargo para detectar las amenazas o vulnerabilidades de seguridad.
- Llevar a cabo el aseguramiento de equipos y actualización de parches de seguridad.
- Dar el soporte para responder ante incidentes de seguridad.

- Mantener la confidencialidad, integridad y disponibilidad de los sistemas de información.

Usuario de la Información. Son las personas que requieren de la autorización de los dueños para acceder a la información y poder realizar su función a través de los recursos asignados y de la normativa existente. A continuación se describen las responsabilidades de los usuarios de la información en cuanto a seguridad se refiere:

- Ser responsables del uso del equipo de cómputo, cuenta y contraseña asignados, y de los medios magnéticos de transmisión de información.
- Obtener la autorización formal del dueño, antes de intentar acceder a cualquier activo de información.
- Utilizar los sistemas de información sólo para actividades de negocio.
- No divulgar información alguna sin autorización del dueño.
- Conocer la clasificación de los activos de información que maneja.

g. La CONSAR debe contar con un Modelo de Gestión de la Seguridad de la Información el cual esté orientado a la creación, mantenimiento, difusión y custodia de la normativa a través de actividades encaminadas a su revisión, implementación, cumplimiento y mejora continua.

h. La CONSAR debe contar con un área encargada de la coordinación, implementación, monitoreo y mantenimiento de los mecanismos de seguridad de la información, asignación de roles y responsabilidades, así como de la generación y difusión oportuna de la normativa de seguridad de la información, definiendo sus procedimientos y relaciones entre las diferentes áreas de la Institución.

Propiedad y Uso de Recursos de Procesamiento de Información.

a. La CONSAR considera los recursos de procesamiento de información como prioritarios para el ejercicio de sus funciones; por lo cual todo el personal interno y externo de la CONSAR es responsable de salvaguardarlos de modificaciones no autorizadas, destrucción e indisponibilidad. Su uso no autorizado se considerará **una falta administrativa y tendrá las consecuencias que correspondan conforme a la normativa aplicable para el caso.**

b. Los recursos de procesamiento de información están diseñados para ser utilizados únicamente con fines relacionados con las actividades de la CONSAR.

c. Al terminar el empleo o trabajo de una persona, los recursos de procesamiento de la información propiedad o en custodia de la CONSAR, deben ser devueltos en buenas condiciones de operación, con toda la documentación original, medios de almacenaje y equipo periférico.

d. Los usuarios de herramientas de procesamiento de información de oficina (hojas de cálculo, procesamiento de palabras, etc.) son los responsables de garantizar la exactitud

e integridad de los resultados obtenidos de dichas herramientas cuando éstas sean utilizadas para dar apoyo a la operación de los procesos de negocio de la CONSAR.

Definición y Actualización de la Política Institucional.

a. La Política General de Seguridad de la Información, se debe revisar y actualizar cuando sea necesario o por lo menos una vez cada dos años.

b. Los cambios y el seguimiento a la normativa de seguridad de la Información para la CONSAR deben definirse con base en un análisis de riesgos para determinar las nuevas vulnerabilidades y deficiencias de control de forma periódica.

Clasificación y Control de Activos de Información.

a. Toda la información utilizada por la CONSAR debe contar con una clasificación de acuerdo a su nivel de confidencialidad, integridad y disponibilidad.

b. La información debe ser etiquetada de acuerdo a su nivel de clasificación.

c. Se debe contar con los mecanismos de control de registro y localización de los medios donde se encuentre la información, así como de su uso, procesamiento, transporte, transferencia, almacenamiento, respaldo y destrucción.

Seguridad para el Personal.

a. Todos los Servidores Públicos de la CONSAR están obligados a guardar la debida discreción sobre la información confidencial o reservada que manejen, observando lo que al respecto dispone la Ley de los Sistemas de Ahorro para el Retiro como las leyes que rigen a los servidores públicos.

b. Respecto a los Terceros que sean contratados por la CONSAR o que tengan acceso a información confidencial o reservada, se procurará establecer cláusulas de confidencialidad en los Convenios o Contratos que se celebren, o, en su caso, un convenio de confidencialidad y uso adecuado de los recursos de la Comisión.

c. Se procurará con lo anterior, garantizar la seguridad, integridad y uso adecuado de la información por quienes tengan acceso a ella. El uso adecuado debe entenderse como la obligación de que cada persona autorizada utilice la información para el cumplimiento de sus funciones, la cual no podrá difundir ni a compañeros ni a terceros sin la autorización correspondiente.

d. La CONSAR debe proporcionar entrenamiento a toda persona que tenga acceso a información sobre las medidas de seguridad de la información necesarias para minimizar riesgos sobre ésta.

e. Todo empleado o personal externo contratado por la CONSAR, debe reportar inmediatamente cualquier incidente que pudiera tener un impacto sobre la seguridad de la información.

f. Los funcionarios públicos de la CONSAR serán sometidos a los procedimientos administrativos para el caso de violaciones a disposiciones que sobre el manejo de información sea aplicable. Asimismo, para los terceros se le harán efectivas las penas y/o responsabilidades que correspondan.

g. La CONSAR procurará en todo momento que al terminar una relación laboral o contractual con los servidores públicos o con terceros respectivamente, regresen todos los activos de información que tengan en su posesión hasta ese momento. Así mismo se deben remover todos los privilegios de acceso que les hayan sido otorgados.

Seguridad Física y Ambiental.

a. El acceso a las instalaciones de la CONSAR debe contar con los mecanismos de control que permitan asegurar que el personal que ingrese cuente con la autorización correspondiente.

b. Los centros de cómputo de la CONSAR deben operar en áreas restringidas, en las cuales sólo puede acceder personal autorizado.

c. Se deben cumplir con las medidas de seguridad física que ayuden a mantener en buen estado los equipos de cómputo y de comunicaciones, así como las instalaciones y los centros de cómputo.

Administración de Redes, Comunicaciones y Operaciones.

a. Deben existir mecanismos de control para proteger toda la información que se opere en la infraestructura tecnológica de la CONSAR, que prevengan y detecten posibles intrusiones o robos de la información, y que de igual forma, protejan toda aquella información con carácter confidencial que por necesidades de la Institución deba transmitirse ya sea dentro de la red interna de la CONSAR, hacia otras redes de Instituciones gubernamentales / paraestatales o hacia Internet.

b. Se deben definir y establecer procedimientos de seguridad que proporcionen las acciones a seguir en caso de eventos no programados, así como medidas que aseguren que los equipos dentro del centro de cómputo cuenten con las características necesarias para satisfacer los requerimientos de procesamiento de información de la CONSAR.

c. Se debe proteger la información residente en los equipos de cómputo de la CONSAR, de cualquier tipo de código móvil y malicioso (virus computacionales, caballos de Troya,

gusanos de red, spyware, malware, entre otros), los empleados de la CONSAR que hagan uso de un equipo de cómputo, deben estar conscientes de todas las medidas para la prevención de virus.

Control de Acceso Lógico.

a. El acceso a la información y a la infraestructura tecnológica de la CONSAR debe contar con mecanismos de control de acceso que permitan contar con los principios de identidad, responsabilidad y rastreabilidad.

b. Cada dueño es responsable del mecanismo de control de acceso que le sea proporcionado [cuenta(s) de usuario(s), contraseña(s), etc.], para acceder a los sistemas de información y a la infraestructura tecnológica de la CONSAR, por lo que deberá mantenerlo de forma confidencial. El mal uso de la cuenta del usuario será responsabilidad del empleado a quien fue asignada la misma.

c. El Responsable del Sistema de Gestión de Seguridad de Información tiene a su cuidado la evaluación, propuesta, certificación de la implementación, supervisión de los resultados, seguimiento del proceso de mejora de todos aquellos mecanismos de control de acceso que prevengan la intrusión no autorizada a la infraestructura de la CONSAR (red, sistemas operativos, bases de datos, aplicaciones, etc.).

d. El derecho de acceso a la información que se encuentra en los sistemas de información y en la infraestructura tecnológica de la CONSAR, debe ser proporcionado por el dueño, con base en el principio de la “necesidad de saber”, considerando la segregación y la rotación de funciones.

Adquisición, Desarrollo y Mantenimiento de Sistemas.

a. Todos los sistemas deben ser desarrollados con base en una metodología probada y apegada a estándares internacionales. Asimismo, se debe contar con procedimientos de control de cambios en los sistemas, así como en el proceso de implantación en producción de los mismos.

b. Los sistemas deben contar con controles de validación y edición de datos, de procesamiento y de salida, que garanticen que únicamente información válida, completa y correcta será procesada.

c. Los sistemas de información desarrollados internamente o adquiridos deben contar con los controles internos que garanticen la seguridad de los datos, y el registro de las actividades que los usuarios realizan en estos.

Manejo de Incidentes de Seguridad de Información.

a. La CONSAR debe contar con un procedimiento para el manejo de incidentes de seguridad de información, que le permita garantizar que los eventos y debilidades de seguridad de información son comunicados de una manera apropiada, permitiendo tomar acciones en tiempo y forma.

b. Se debe considerar un esquema de mejora continua en el manejo de los incidentes de seguridad para aprender de los incidentes ocurridos y mitigar los impactos que éstos ocasionan.

c. Cuando se requiera evidencia de los incidentes ocurridos, se debe recolectar cumpliendo con los requerimientos legales que para el caso se requiera.

Continuidad del Negocio y Recuperación ante Desastres.

a. La CONSAR debe contar con un Plan de Continuidad del Negocio (BCP), que permita garantizar que los procesos críticos de la CONSAR operen en caso de presentarse un desastre o contingencia que imposibilite su operación normal.

b. Se debe nombrar a un coordinador o grupo de trabajo responsable del desarrollo, implementación, ejecución, pruebas y actualización del Plan de Continuidad del Negocio (BCP).

c. Todo el personal de la CONSAR debe conocer la responsabilidad que se le ha asignado en el Plan de Continuidad del Negocio (BCP), así como los procedimientos a ejecutar en dicho plan.

Cumplimiento.

a. Se deben establecer mecanismos de control para certificar el cumplimiento de esta política, en concordancia con la legislación mexicana y los acuerdos Internacionales para el uso de recursos de procesamiento de información, a través de auditorías realizadas por personal interno o externo.

b. Se deben proteger los datos de carácter personal contra accesos y divulgaciones no autorizadas.

c. Todos los recursos de procesamiento de información (el software y hardware adquirido por la CONSAR) es propiedad del Gobierno Federal, independientemente de la asignación de propietario de la PC/estación de trabajo en la que se instale.

d. Bajo ninguna circunstancia una persona puede instalar, utilizar o almacenar juegos u otro tipo de software no autorizado en ninguna PC/estación de trabajo o dispositivo de red de la CONSAR. La piratería de software es una falta que se sancionará conforme a la Ley de

Propiedad Industrial, la Ley Federal del Derecho de Autor y los Códigos Penales según corresponda; sanciones que podrán ser multas e incluso hasta penas privativas de la libertad. La CONSAR no tolerará el uso ilegal de copias o la distribución de software no autorizado bajo ninguna circunstancia. Las copias que se hagan de software autorizado (excepto para fines de respaldo) están estrictamente prohibidas.

Normativa.

La normativa que soporta la presente política se compone de un conjunto de directrices que tienen como objetivo estandarizar y presentar la definición de los componentes para la gestión de la seguridad de la información.

La estructura normativa se compone de los siguientes elementos:

a. **Política.** Declaración de alto nivel, de carácter obligatorio, que describe metas, objetivos y referencias generales sobre tópicos de seguridad de la información.

b. **Lineamientos.** Declaraciones de carácter opcional desarrolladas para lograr los objetivos de las políticas.

c. **Procedimientos.** Especificaciones de la secuencia de actividades de cómo son implementadas las políticas, estándares y guías en el ambiente operativo de la CONSAR.

El orden en que debe aplicarse la normativa es el siguiente:

Jerarquía en la aplicación del Marco Normativo para la Seguridad de la Información.

Código de Conducta Relacionado con el Manejo de la Información.

Todos los empleados de la CONSAR, en forma adicional al Código de Conducta definido por la CONSAR como parte de su Marco Regulatorio, deben observar los siguientes lineamientos de conducta relacionados con el manejo de la información:

- *Asumir el compromiso de actuar conforme a derecho, de acuerdo con los estándares morales y éticos más altos de la CONSAR.*
- *No cometer o formar parte de actos ilícitos o poco éticos que además, puedan llegar a afectar de forma negativa la reputación de la CONSAR.*
- *Asumir el compromiso de notificar por los medios autorizados cualquier actividad relacionada que considere ilícita y cooperar en cualquier investigación que se derive de esta notificación.*
- *Asumir el compromiso de ayudar en los esfuerzos relacionados con el entendimiento y aceptación de las medidas de seguridad adoptadas por la CONSAR.*
- *Asumir el compromiso de proveer servicios competentes a la CONSAR y evitar cualquier conflicto de interés.*
- *Asumir el compromiso de no hacer mal uso de la información y de los recursos durante la ejecución de las actividades.*
- *Mantener la confidencialidad, integridad y disponibilidad de toda la información bajo custodia, que incluye explícitamente la no divulgación de la información y/o conocimientos relacionados con ella en situaciones diferentes a las que sus funciones le asignan, ni a compañeros de la CONSAR ni a terceros.*

Conformación del Marco Normativo.

El marco normativo se compondrá de los siguientes temas organizados en políticas:

Responsabilidades Generales de Seguridad

POLDGI-01 Política General de Seguridad.

Seguridad de Acceso por Terceros y Responsabilidades de Aseguramiento de la Información de Terceros (outsourcing).

POLDGI-02 Política de Seguridad para Terceros.

Clasificación de Información.

POLDGI-03 Política de Clasificación de Información.

Manejo de la Información Clasificada

POLDGI-04 Política de Respaldo y Borrado de Información.

POLDGI-05 Política de Cifrado de Datos.

Responsabilidades de Seguridad de los Empleados de la CONSAR

POLDGI-06 Política de Roles y Responsabilidades.

Responsabilidades de Seguridad en la Operación de Dispositivos Tecnológicos.

POLDGI-07 Política de Protección de Equipos de Cómputo.

POLDGI-08 Política de Equipos Portátiles.

POLDGI-09 Política de Protección de Redes Internas.

POLDGI-10 Política de Protección de Redes Externas.

Entrenamiento de Usuarios Finales y Entrenamiento de Operadores.

POLDGI-11 Política de Seguridad en el Personal.

Respuesta a Incidentes.

POLDGI-12 Política de Incidentes de Seguridad.

Protección Contra Software no Autorizado.

POLDGI-13 Política de Licenciamiento de Software.

POLDGI-14 Política de Antivirus y Código Malicioso.

Administración de cuentas, contraseñas y privilegios.

POLDGI-15 Política de Usuarios y Contraseñas.

Controles de Acceso Lógico.

POLDGI-16 Política de Seguridad Física y Ambiental.

POLDGI-17 Política de Autenticación y Control de Accesos.

Monitoreo para la Seguridad de la Información.

POLDGI-18 Política de Monitoreo de Seguridad**.**

Requerimientos de Seguridad en Sistemas.

POLDGI-19 Política de Adquisición e Implementación de Infraestructura Tecnológica.

POLDGI-20 Política de Administración de Riesgos.

Administración de la Continuidad

POLDGI-21 Política de Administración de la Continuidad.

Realización de Revisiones

POLDGI-22 Política de Cumplimiento.

POLDGI-23 Política de Sanciones.

Responsabilidades de Seguridad en el Desarrollo de Software

POLDGI-24 Política de Desarrollo y Mantenimiento de Sistemas Informáticos.

Responsabilidades de Seguridad en la Administración de Bases de Datos

POLDGI-25 Política de Administración de Bases de Datos.

Responsabilidades de Uso de Medios de Almacenamiento de Información en Internet

POLDGI-26 Política de Uso de Medios de Almacenamiento de Información en Internet.

Control de Cambios

No DE REVISION	FECHA	MOTIVO
07	**Diciembre 2017**	**Se actualizan referencias a los nombres de las áreas internas.** **Se agrega la Política 26 Uso de Medios de Almacenamiento en Internet al Marco Normativo.**
06	Agosto 2016	Se eliminan las referencias al ISO 27001 y se actualizan los datos de las últimas versiones oficiales de los documentos asociados al SGSI.
05	Octubre 2011	Se acota el Marco Normativo debido a que el alcance del SGSI solo aplica a uno de los procesos de la CONSAR.
04	Mayo 2011	Se elimina la personalización del nombre del Presidente en este documento. Se agrega la Política 25 de Administración de Bases de Datos en el Marco Normativo.
03	Septiembre 2007	Se unificó el formato del tipo de letra del Indice respecto al formato del resto del documento. Se modificó el cuadro de firmas que autorizan el documento para homologarlo de acuerdo a lo que marca el PGSI-01. Se agregaron los números de código de documento en todas las referencias a otros documentos asociados del SGSI.
02	Agosto 2007	Adecuaciones de redacción en diferentes puntos del documento, actualización del marco normativo, modificación de la sección de seguridad del personal, inserción de los códigos de identificación de las políticas que se citan en la sección Conformación del Marco Normativo.
01	Diciembre 2006	Se inserta la viñeta “e)” en el apartado “Gestión de la seguridad” en la página 9 de 18 para hacer referencia de los grupos que pueden servir de apoyo en aspectos de seguridad. La viñeta anterior “e)” se recorre a “f)”
00	Agosto 2006	Creación de la Política General de Seguridad.

INDICE

Política

Los equipos de procesamiento de información de la CONSAR, deben contar con los medios de almacenamiento que aseguren la información contenida en éstos, a fin de evitar pérdidas importantes de datos y las posibles consecuencias asociadas. Se deben especificar claramente los tipos de datos que necesitan ser respaldados, los registros de operación críticos y eliminar registros no necesarios.

Objetivo

Establecer los lineamientos de respaldo, recuperación y borrado de información de los sistemas y componentes de red que soportan la operación de la CONSAR.

ELABORÓ	REVISÓ	APROBÓ
REPRESENTANTE DEL SGSI	RESPONSABLE DE PROCESO	ALTA DIRECCIÓN

Alcance

Indicar los requerimientos de los respaldos y recuperación de información, su programación en calendario y el resguardo seguro de los mismos, así como los lineamientos de desecho de información.

Lineamientos de Respaldo de Información.

Generales.

a. Toda la información en formato electrónico sin importar si se clasifica como confidencial, reservada y/o pública en los sistemas de la CONSAR, debe respaldarse periódicamente con base en su criticidad.

b. La Coordinación General de Administración y Tecnologías de la Información, es la encargada de llevar a cabo el proceso de respaldo de la información que se encuentre almacenada dentro de los servidores de los centros de datos.

c. Será responsabilidad de las áreas de la CONSAR solicitar apoyo al personal de la Coordinación General de Administración y Tecnologías de la Información para el respaldo de información contenida en sus equipos y serán éstas las responsables de custodiar los medios de respaldo (CD´s, cintas, etc.). Asimismo serán las áreas quienes verifiquen y validen el contenido de los respaldos.

d. Los procesos de respaldo de información almacenada en los servidores de los centros de datos que implique afectación en la disponibilidad de la información a respaldar, deben efectuarse fuera de los horarios de operación de la organización.

e. Los procesos de respaldo de información almacenada en los equipos de las áreas, se pueden realizar en cualquier momento dentro de los horarios normales de trabajo sin que esto afecte la disponibilidad de la información hacia los usuarios.

f. La Coordinación General de Administración y Tecnologías de la Información con base en la infraestructura tecnológica con la que cuente, la frecuencia de cambio de la información y el volumen de los datos, programará la periodicidad (diaria, semanal o mensual) y el tipo de respaldo a realizar (incremental o completo). Asimismo, controlará la retención de medios de respaldo generados en un lapso de tiempo; decidiendo cuáles respaldos conservar y cuáles depurar. Cuando el dueño de la información proponga cierta periodicidad de respaldo o retención, la Coordinación General de Administración y Tecnologías de la Información tomará la decisión de aceptar o rechazar la propuesta tomando en cuenta los tres criterios antes mencionados, estableciendo las características finales del respaldo en cuestión.

Restauración e Integridad de Respaldos.

a. El personal de la Coordinación General de Administración y Tecnologías de la Información debe realizar pruebas programadas de restauración de información simulando situaciones de contingencia, bajo parámetros de tiempo establecidos, en donde se revise la integridad y funcionalidad de los respaldos de información y debe reportar los resultados al Responsable del Sistema de Gestión de Seguridad de

Información. Las pruebas deberán buscar emular de manera integral los ambientes en producción, siempre que se cuente con la infraestructura necesaria para mantener ambos ambientes en operación. En caso contrario, se deberán realizar pruebas de restauración parciales que permitan corroborar el buen estado de los respaldos y de los medios que los contienen.

Almacenamiento de Información.

a. Se debe evitar que los medios magnéticos utilizados para el almacenamiento de información clasificada como confidencial y/o reservada, se vuelvan obsoletos en cuanto a la tecnología que utilizan. En el caso de que sea inminente la obsolescencia, el personal de la Coordinación General de Administración y Tecnologías de la Información debe asegurarse de la implementación de tecnología vigente y mover los respaldos de los medios en proceso de obsolescencia a medios de tecnología vigente. También se debe buscar utilizar tecnologías de punta que permitan reducir el espacio físico que ocupan estos medios.

b. Los procedimientos de respaldo de información en medios magnéticos (disquete, CD, cintas magnéticas, etc.) deben asegurar que la información sensible, crítica o valiosa almacenada por periodos prolongados de tiempo, no se pierda por deterioro. Por ejemplo, los operadores de la información deben copiar los datos en medios de almacenamiento diferentes, si el medio de almacenamiento original muestra señas de deterioro. Para el caso de información que se etiqueta con un periodo de retención del tipo “permanente” se deberán realizar copias periódicas a medios más recientes y/o respaldarse por duplicado.

c. Los respaldos de información confidencial y/o reservada, deben almacenarse en un sitio protegido contra el medio ambiente y con controles estrictos de acceso que se encuentre en oficinas externas a las de la Comisión y a una distancia razonablemente fuera del alcance de un evento en la zona original.

d. Para cualquier equipo servidor, de escritorio, portátil y de telecomunicaciones que se retire de su sitio original para efectos de mantenimiento o manipulación por terceros, se deberá evaluar si se requiere un respaldo de información previo a la intervención del equipo. Está evaluación estará a cargo del personal de la Coordinación General de Administración y Tecnologías de la Información o bien del operador del equipo. Si se determina que un respaldo es requerido, dicho respaldo deberá permanecer bajo custodia de la Coordinación General de Administración y Tecnologías de la Información o del operador sin que pueda salir de las instalaciones de la CONSAR, a menos que se obtenga la autorización del Responsable del Sistema General de Seguridad de la Información.

Destrucción de Información.

a. La información de la CONSAR debe ser destruida o almacenada en un sitio seguro cuando ya no sea necesaria ni en la operación ni por requerimientos legales. Se debe revisar periódicamente por parte de las áreas correspondientes la continuidad del valor y utilidad de la información. Los procedimientos deberán considerar los siguientes puntos básicos:

- Toda la información confidencial y/o reservada, al no ser utilizada, debe ser eliminada o almacenada, de acuerdo a los criterios que establezcan las áreas competentes.
- Los medios que contengan información se podrán encontrar en las siguientes presentaciones:
  - Documentos impresos.
  - Unidades de almacenamiento magnético removibles (discos duros, discos flexibles, cintas, etc.).
  - Medios de almacenamiento óptico.
- Todo almacenamiento o destrucción de datos debe ser registrada por el operador responsable de esa actividad y ser informada al coordinador de grupo correspondiente.

Destrucción de Medios.

a. Todos los medios que deban ser retirados por obsolescencia, deberán ser migrados a medios magnéticos de reciente tecnología, a excepción de los medios que contengan información que se encuentre en operación y que ya se esté respaldando en tecnologías más recientes.

b. Se debe asegurar que la información de los medios obsoletos fue copiada en su totalidad a los nuevos medios.

c. Se debe solicitar el apoyo a la Coordinación General de Administración y Tecnologías de la Información para que se realice una destrucción segura de medios.

d. La Coordinación General de Administración y Tecnologías de la Información deberá generar la evidencia necesaria para mostrar la destrucción segura de los medios.

Anexos

Documentos Asociados

- PDGI-18 Respaldo de los Servidores
- PDGI-19 Respaldo de Datos de Usuario
- PDGI-37 Dictamen Técnico para Baja de Equipos Informáticos

Control de Cambios

No DE REVISION	FECHA	MOTIVO
05	**Diciembre 2017**	**Se actualizan algunos textos para mejora de su descripción.**
04	Agosto 2016	Revisión y actualización general y eliminación de la referencia a ISO 27001.
03	Octubre 2012	Se actualizan las referencias a los nombres de las unidades administrativas de la CONSAR.
02	Agosto 2009	Se hace referencia que los respaldos deberán mantenerse el medios de tecnología vigente. Se especifica que en los procesos de restauración de los respaldos se deben realizar pruebas emulando los ambientes en producción, siempre que se cuente con la infraestructura necesaria. Se agrega la sección de Destrucción de Medios para establecer las consideraciones a tomar para estos casos.
01	Septiembre 2007	Se unificó el formato del tipo de letra del Indice respecto al formato del resto del documento. Se modificó el cuadro de firmas que autorizan el documento para homologarlo de acuerdo a lo que marca el PGSI-01. Se agregaron los números de código de documento en todas las referencias a otros documentos asociados del SGSI.
00	Agosto 2006	Creación de la Política de Respaldo y Borrado de Información.

INDICE

Política

Contar con mecanismos tecnológicos de cifrado de información, que permitan minimizar los riesgos en el proceso de transportación y almacenamiento de la misma.

Objetivo

Asegurar que la información clasificada como reservada o confidencial reciba un tratamiento especial en el proceso de transportación y almacenamiento, con base en mecanismos que permitan minimizar los riesgos y lograr que el almacenamiento y transmisión de la información sea segura.

ELABORÓ	REVISÓ	APROBÓ
REPRESENTANTE DEL SGSI	**RESPONSABLE DE PROCESO**	**ALTA DIRECCIÓN**

Alcance

Establecer los mecanismos necesarios para la protección de la información, incluyendo los siguientes aspectos:

- Determinación de la información que debe ser cifrada, con base en la política de clasificación de la información.
- Mencionar los procedimientos para manejar las llaves de acceso, incluyendo los métodos para la recuperación de información cifrada en caso de pérdida, compromiso o daño de las mismas.
- Descripción de responsabilidades en el manejo de las llaves cifradas y los niveles a utilizar.

Lineamientos de Cifrado de Información.

Generales.

a. Se debe diseñar y utilizar un estándar para el cifrado de la información de la CONSAR, con previa evaluación y autorización del Comité de Seguridad de la Información.

b. Se deben diseñar y difundir con previa evaluación y autorización del Comité de Seguridad de la Información los procedimientos necesarios para el cifrado de la información de la CONSAR.

c. La Información reservada o confidencial de la CONSAR que sea enviada a través de una red pública, deberá ser cifrada con un método aprobado por el Comité de Seguridad de la Información.

d. La información clasificada como reservada o confidencial transportada en formatos de almacenamiento (CD, medios magnéticos, USB), por cualquier computadora, debe encontrarse cifrada de acuerdo a los procedimientos definidos.

e. La información clasificada como reservada o confidencial de la CONSAR que no se encuentre en uso por largos periodos de tiempo debe estar cifrada.

f. La transferencia de información clasificada como reservada o confidencial vía correo electrónico debe ser cifrada.

g. Se debe exigir a los proveedores cifrado en la transferencia de la información o almacenamiento de la información, siempre y cuando la información que manejen se encuentre clasificada por la CONSAR como reservada o confidencial.

Manejo de Llaves.

a. Las llaves de cifrado utilizadas en la CONSAR no deberán ser comunicadas o compartidas con ningún tercero, a menos que se cuente con la autorización del Responsable del Sistema de Gestión de Seguridad de Información.

b. Los sistemas de la CONSAR deberán diseñarse de tal forma que ninguna persona externa tenga el conocimiento total de ninguna llave de cifrado.

c. Si se utiliza cifrado, la información protegida debe ser transferida por un medio distinto al utilizado para transferir las llaves de descifradoras de la información.

d. Siempre que se utilice cifrado, las llaves y los métodos utilizados para generarlas deben permanecer protegidos y su cuidado debe continuar mientras la información permanezca cifrada con esa llave.

e. Las llaves de cifrado deben ser divididas y cada parte debe ser custodiada por una persona distinta; el almacenamiento de las llaves en formato de texto debe hacerse de forma cifrada. Todos los materiales utilizados para la generación, distribución y resguardo de las llaves de cifrado, deben encontrarse protegidos por personas autorizadas. Cuando ya no sean necesarios, los materiales deberán ser destruidos por métodos aprobados por el Comité de Seguridad de la Información.

f. Si las llaves de cifrado son enviadas por algún medio de comunicación, esto debe hacerse en forma cifrada. El cifrado de las llaves deberá efectuarse con un método más seguro que el utilizado para cifrar otros datos sensitivos.

g. Si los datos en un medio de almacenamiento se encuentran cifrados, las llaves de cifrado deben ser almacenadas en otro medio de almacenamiento separado.

h. Todos los sistemas de cifrado utilizados para proteger la información de la CONSAR, deben tener mecanismos que permitan la desencripción de los archivos protegidos.

i. Siempre que se utilice cifrado, se debe verificar que el archivo cifrado es factible de restablecerse en su forma original. Una vez que lo anterior haya sido demostrado, el archivo original deberá ser borrado.

j. Siempre que se utilice cifrado para proteger información clasificada como reservada o confidencial, el dueño de la información debe, explícitamente, asignar o tener la responsabilidad para el manejo de las llaves de cifrado.

k. Si se utilizan llaves tanto para cifrado como para autenticación de mensajes, ambas llaves deberán ser distintas una de la otra.

l. Si alguna información reservada o confidencial se almacena en un sistema utilizado por varios usuarios, la información deberá ser primero compresa y después cifrada utilizando un algoritmo de cifrado aprobado.

m. Siempre que se utilice cifrado, las llaves empleadas deben ser generadas para que no puedan ser prácticamente replicables y que sean difíciles de adivinar. El uso de llaves de cifrado de mayor número de bits (128 comercialmente) deberá ser el preferido.

n. Las llaves de cifrado utilizadas por la CONSAR deben cambiarse al menos cada 12 meses.

Anexos

Documentos Asociados

- PDGI-44 Controles Criptográficos y Llaves de Encripción

Control de Cambios

No DE REVISION	FECHA	MOTIVO
02	**Agosto 2016**	**Se elimina la referencia al ISO 27001 y se valida la aplicabilidad.**
01	Septiembre 2007	Se unificó el formato del tipo de letra del Indice respecto al formato del resto del documento. Se modificó el cuadro de firmas que autorizan el documento para homologarlo de acuerdo a lo que marca el PGSI-01. Se agregaron los números de código de documento en todas las referencias a otros documentos asociados del SGSI.
00	Agosto 2006	Creación de la Política de Cifrado de Datos.

INDICE

Política

Deben formalizarse las medidas necesarias para el control adecuado de la información sensible alojada en los equipos de cómputo, así como el cuidado de los mismos.

Objetivo

Establecer los requerimientos de seguridad para todos los equipos de cómputo.

ELABORÓ	REVISÓ	APROBÓ
REPRESENTANTE DEL SGSI	RESPONSABLE DE PROCESO	ALTA DIRECCIÓN

Alcance

Esta política aplica para todas las computadoras que procesen, transmitan o almacenen información de la CONSAR. Los lineamientos de esta política deben incluir los siguientes puntos:

- Controles de accesos
- Administración del usuario
- Responsabilidades del usuario
- Seguridad de equipos y aplicaciones
- Software no autorizado y Antivirus
- Reportes de mal funcionamiento

Lineamientos para la Protección de Equipos de Cómputo.

Generales.

a. Los equipos de cómputo deben ser asignados por la Coordinación General de Administración y Tecnologías de la Información y ésta área será la responsable de la instalación, configuración y asignación inicial de los equipos.

b. La Coordinación General de Administración y Tecnologías de la Información, es el área responsable del mantenimiento de los equipos de cómputo y de proporcionar la seguridad adecuada a los mismos con base en esta política.

c. La Coordinación General de Administración y Tecnologías de la Información, es el área responsable de llevar un inventario de los equipos de cómputo y de todos los sistemas y aplicaciones instalados en los mismos.

d. Los usuarios deben reportar a la mesa de ayuda cualquier mal funcionamiento de los equipos de cómputo.

e. Todos los equipos que tenga la CONSAR para su uso, deben contar con antivirus de acuerdo a los lineamientos de la POLDGI-14 Política de Antivirus y Código Malicioso.

f. Si no ha habido actividad en el equipo de cómputo durante un lapso largo de tiempo el sistema debe estar configurado para suspender la sesión y se debe restablecer cuando el usuario introduzca la contraseña adecuada (se debe tener habilitado el protector de pantalla que se active una vez transcurrido el lapso de tiempo definido para su activación).

g. El lapso de tiempo máximo para la activación del protector de pantalla es definido por el Comité de Seguridad de Información (CSI).

h. Los usuarios que se les asigne equipos de cómputo deben ser responsables del uso de los mismos, considerando los siguientes puntos:

- Cuidado físico de los equipos.
- Información contenida.
- Software instalado fuera de las normas dictadas por la Coordinación General de Administración y Tecnologías de la Información.
- Configuraciones fuera de normas dictadas por la Coordinación General de Administración y Tecnologías de la Información.
- Periféricos asignados.

Autorización de Uso de Equipos de Cómputo.

a. La Coordinación General de Administración y Tecnologías de la Información, es el área responsable de proporcionar el entrenamiento necesario a los usuarios para el uso de los mismos, obligando con esto a que los usuarios se responsabilicen de los equipos.

b. No está autorizado que los usuarios reinstalen o cambien la configuración del software y hardware previamente instalado por el personal de la Coordinación General de Administración y Tecnologías de la Información.

c. No está autorizado bajar software de Internet para instalarlo en los equipos de cómputo, ni bajar contenido de Internet que no haya sido autorizado y tampoco el uso de aplicaciones de Internet que sean peer-to-peer (chats, messengers, etc.) que no hayan sido autorizadas por la Coordinación General de Administración y Tecnologías de la Información.

d. Todo el software que sea necesario instalar en los equipos debe ser autorizado por el responsable del área donde se encuentre el equipo de cómputo que tenga al menos nivel Director General o superior y avalado por la Coordinación General de Administración y Tecnologías de la Información.

e. La Coordinación General de Administración y Tecnologías de la Información es el área responsable de asignar, reasignar y retirar el equipo de cómputo a los usuarios, previo a un análisis de uso, desempeño del equipo y cantidad de procesos ejecutados.

Instalación y Configuración Inicial.

a. Es importante que los equipos de cómputo cuenten con controles de acceso para autenticar a los usuarios con base en la política de usuarios y contraseñas.

b. Se debe contar con guías para la configuración de sistemas operativos, desarrolladas por el personal de la Coordinación General de Administración y Tecnologías de la Información y autorizadas por el Responsable del Sistema de Gestión de Seguridad de la Información.

c. Los equipos de cómputo deben contar con las siguientes instalaciones y configuraciones de seguridad:

- Protección para evitar el acceso no autorizado a la configuración de discos duros y sistema operativo.
- Protección para evitar la remoción de discos duros de los equipos.
- Protección para ataques externos.
- Protección contra virus y código malicioso

- Protección contra la instalación y configuraciones inadecuadas.

Áreas Seguras.

a. Las áreas que contengan equipo de cómputo crítico para la operación de la CONSAR, deben contar con la protección física contra posibles amenazas. Tomar en consideración los lineamientos de la POLDGI-16 Política de Seguridad Física y Ambiental.

b. Para remover equipos y componentes físicamente, es necesaria la autorización de la Coordinación General de Administración y Tecnologías de la Información.

Información en los Equipos de Cómputo.

a. La información clasificada como confidencial o reservada de los equipos de cómputo, debe contar con mecanismos para fortalecer el acceso y la seguridad en general. Para la información que se reciba de las entidades relacionadas con el sistema de pensiones (Afores y Siefores, entre otras), debe ser cifrada con base en los lineamientos de la POLDGI-05 Política de Cifrado de Datos.

b. Deben realizarse procesos periódicos de respaldo de información alojada en los servidores del Centro de Cómputo con base en los lineamientos de la POLDGI-04 Política de Respaldo y Borrado de Información. Para el caso de información contenida en los equipos de los usuarios, éstos deberán responsabilizarse del respaldo de la información.

c. Deben revisarse al menos una vez al año por parte de la Coordinación General de Administración y Tecnologías de la Información, las aplicaciones y archivos alojados en los equipos de cómputo; eliminar cualquier aplicación, programa o archivo sospechoso, en coordinación con los dueños de la información con base en los lineamientos del PDGI-06 Revisión Informática.

Servidores.

a. Los servidores de la CONSAR, deben estar protegidos bajo los siguientes lineamientos:

- Los servidores deben estar en áreas seguras.
- Los sitios en donde se encuentren los servidores deben estar en cumplimiento con la POLDGI-16 Política de Seguridad Física y Ambiental.
- En caso de desastre, los servidores que sean clasificados como críticos, deben estar dentro de un plan de continuidad del negocio y de acuerdo a la POLDGI-21 Política de Administración de la Continuidad.

Las consolas de los servidores sólo deben ser utilizadas por usuarios autorizados y contar con controles de accesos.

Equipos Portátiles.

a. Los equipos portátiles de la CONSAR, deben estar protegidos bajo los lineamientos de la POLDGI-08 Política de Equipos Portátiles.

Mantenimiento de Equipos de Cómputo.

a. Los equipos de procesamiento de información deben contar con mantenimientos periódicos de acuerdo a los requerimientos del fabricante.

b. Se deben tener registros sobre las averías a los equipos y los mantenimientos tanto correctivos como preventivos que se efectúen.

c. Es importante contar con equipos de reciente tecnología para optimizar el trabajo de las áreas.

Anexos

Documentos Asociados

- POLDGI-04 Política de Respaldo y Borrado de Información
- POLDGI-05 Política de Cifrado de Datos
- POLDGI-08 Política de Equipos Portátiles
- POLDGI-14 Política de Antivirus y Código Malicioso
- POLDGI-16 Política de Seguridad Física y Ambiental
- POLDGI-21 Política de Administración de la Continuidad
- PDGI-06 Revisión Informática
- PDGI-09 Administración de Usuarios en los Servicios de la Red Local y Otras Aplicaciones
- PDGI-18 Respaldo de los Servidores
- PDGI-19 Respaldo de Datos de Usuario
- PDGI-23 Seguridad de Acceso a Servidores y a Bases de Datos
- PDGI-25 Mantenimiento Preventivo al Equipo de Cómputo
- PDGI-26 Mantenimiento Correctivo al Equipo de Cómputo
- PDGI-27 Mantenimiento Preventivo del Aire Acondicionado
- PDGI-28 Mantenimiento Correctivo del Aire Acondicionado
- PDGI-29 Mantenimiento Preventivo al UPS y Planta de Emergencia
- PDGI-30 Mantenimiento Correctivo al UPS y Planta de Emergencia
- PDGI-31 Mantenimiento Preventivo del Conmutador Telefónico
- PDGI-32 Mantenimiento Correctivo del Conmutador Telefónico
- PDGI-33 Mantenimiento Preventivo al Sistema de Incendios
- PDGI-34 Mantenimiento Correctivo al Sistema de Incendios
- PDGI-35 Mantenimiento Preventivo al Centro de Cómputo
- PDGI-38 Control de Inventarios de Bienes Informáticos
- PDGI-39 Control del Inventario de Software
- PDGI-40 Monitoreo de Servicios Informáticos
- PDGI-48 Plan de Recuperación ante Desastres – DRP

Control de Cambios

No DE REVISION	FECHA	MOTIVO
04	**Agosto 2016**	**Se eliminan las menciones a ISO 27001 y se actualiza el documento.**
03	Octubre 2012	Se actualizan las referencias a los nombres de las unidades administrativas de la CONSAR.
02	Agosto 2009	Se realizan pequeños ajustes en diversas secciones del documento. Se establece a la Dirección General de Informática como responsable de algunas actividades. Se define que la información confidencial o reservada debe ser cifrada y respaldada.
01	Septiembre 2007	Se unificó el formato del tipo de letra del Indice respecto al formato del resto del documento. Se modificó el cuadro de firmas que autorizan el documento para homologarlo de acuerdo a lo que marca el PGSI-01. Se agregaron los números de código de documento en todas las referencias a otros documentos asociados del SGSI.
00	Agosto 2006	Creación de la Política de Protección de Equipos de Cómputo.

INDICE

Política

Formalizar las medidas necesarias para el control adecuado de la información sensible alojada en las unidades de cómputo portátiles, así como el cuidado de las mismas.

Objetivo

Proteger la información sensible alojada en los equipos portátiles, así como procurar su cuidado físico.

ELABORÓ	REVISÓ	APROBÓ
REPRESENTANTE DEL SGSI	**RESPONSABLE DE PROCESO**	**ALTA DIRECCIÓN**

Alcance

Esta política contempla a los equipos portátiles, en donde los lineamientos deben estar enfocados a los siguientes puntos:

- Propiedad y custodia.
- Autorizaciones de uso.
- Protección de información confidencial y/o reservada.
- Intercambio de equipos.

Lineamientos para Equipos Portátiles.

Generales.

a. La Coordinación General de Administración y Tecnologías de la Información, es el área responsable de la instalación, configuración y asignación inicial de los equipos portátiles.

b. La Coordinación General de Administración y Tecnologías de la Información, es el área responsable del mantenimiento de los equipos portátiles.

c. La Coordinación General de Administración y Tecnologías de la Información, es el área responsable de proporcionar la seguridad operativa adecuada a los equipos portátiles. Con base en esta política, la seguridad física de los equipos debe ser coordinada de manera formal y con compromisos escritos con los servicios de control de acceso físico a las instalaciones de la CONSAR así como con el área de seguridad de la Institución.

d. La Coordinación General de Administración y Tecnologías de la Información, es el área responsable de llevar un inventario de los equipos portátiles y de todos los sistemas y aplicaciones instalados en los mismos.

e. La Coordinación General de Administración y Tecnologías de la Información deberá coordinar, monitorear y registrar, los movimientos de los equipos portátiles fuera de las instalaciones de la CONSAR.

f. Los usuarios deben reportar a la mesa de ayuda cualquier mal funcionamiento que se presente en los equipos portátiles.

g. Todos los equipos que tenga la CONSAR para su uso, deben contar con antivirus de acuerdo a los lineamientos de la POLDGI-14 Política de Antivirus y Código Malicioso.

h. Si no ha habido actividad en el equipo de cómputo durante un lapso largo de tiempo, el sistema debe estar configurado para suspender la sesión y se debe restablecer cuando el usuario introduzca la contraseña adecuada (se debe tener habilitado el protector de pantalla que se active una vez transcurrido el lapso de tiempo definido para su activación).

i. El lapso de tiempo máximo para la activación del protector de pantalla es definido por el Comité de Seguridad de Información (CSI).

j. Los usuarios que tengan bajo su resguardo equipo de cómputo portátil, podrán salir de la Comisión con el equipo, siempre que sea para uso del usuario y con fines que competen a las funciones de la CONSAR.

k. Los usuarios que tengan bajo su resguardo equipo de cómputo portátil, deberán mantenerlo dentro de la Comisión mientras se encuentren físicamente dentro de las instalaciones.

l. La Coordinación General de Administración y Tecnologías de la Información podrá retirar a los usuarios, los equipos de cómputo portátil, cuando se detecte que estos son utilizados únicamente con fines personales ajenos a las actividades laborales, o bien, cuando se detecte que los usuarios mantienen el equipo en su hogar u otro sitio ajeno a actividades laborales y al mismo tiempo el usuario se encuentre físicamente en la CONSAR.

m. Los usuarios que se les asignen equipos portátiles deben ser responsables del uso de los mismos considerado los siguientes puntos:

- Cuidado físico de los equipos.
- Información contenida.
- Software instalado fuera de las normas dictadas por la Coordinación General de Administración y Tecnologías de la Información.
- Configuraciones fuera de normas dictadas por los dueños de los activos.
- Periféricos asignados.

Autorización de Uso de Equipos Portátiles.

a. La Coordinación General de Administración y Tecnologías de la Información, debe proporcionar el entrenamiento necesario a los usuarios para el uso de los mismos, obligando con esto a que los usuarios se responsabilicen de los equipos.

b. No está autorizado que los usuarios configuren el software y hardware ya instalado por el personal de la Coordinación General de Administración y Tecnologías de la Información.

c. No está autorizado que los usuarios bajen software de Internet para instalarlo en los equipos portátiles, ni bajar contenido de Internet que no haya sido autorizado y tampoco el uso de aplicaciones de Internet que sean peer-to-peer (chats, messengers, etc.) que no hayan sido autorizadas por la Coordinación General de Administración y Tecnologías de la Información.

d. Todo el software que sea necesario instalar en los equipos debe ser autorizado por el responsable del área donde se encuentre el equipo de cómputo que sea al menos de nivel Director General y avalado por la Coordinación General de Administración y Tecnologías de la Información.

Instalación y Configuración Inicial.

a. Los equipos portátiles deben contar con las siguientes instalaciones y configuraciones de seguridad.

- Protección para evitar el acceso no autorizado a la configuración de discos duros y sistema operativo.
- Protección para evitar el remover discos duros de los equipos portátiles.
- Protección para ataques externos.
- Protección contra virus y código malicioso.
- Protección contra transmisiones wireless (red inalámbrica).
- Contar con cifrado de datos, sólo para los casos en que el equipo cuente con información de carácter confidencial.

Información en los Equipos Portátiles.

a. La información clasificada como confidencial o reservada de los equipos portátiles debe ser cifrada con base en los lineamientos de la POLDGI-05 Política de Cifrado de Datos.

b. Los usuarios deben contar con el respaldo de toda información alojada en los equipos portátiles que se les asignó.

c. La Coordinación General de Administración y Tecnologías de la Información, debe revisar al menos una vez al año los equipos portátiles para eliminar cualquier aplicación, programa o archivo sospechoso, en coordinación con el área dueña de la información que los equipos contengan.

Cuidado Físico de Equipos Portátiles.

a. Debe controlarse estrictamente la entrada y salida de equipos portátiles de las instalaciones de la CONSAR.

b. Deben considerarse los accesorios necesarios para conservar la integridad física de los equipos portátiles; así como su robo o extravío, a través de candados.

c. Debe evitarse el uso de medios de transporte público para la transportación de los equipos portátiles.

d. No está permitido el préstamo o intercambio de equipos portátiles por parte de los usuarios.

Terminación y Reasignación de Equipos Portátiles.

a. Al reasignarse los equipos portátiles o al terminar el uso por parte de los empleados, la Coordinación General de Administración y Tecnologías de la Información, debe reinstalar el sistema operativo y aplicaciones pertinentes.

Comunicación Vía Módem.

a. No está permitido el uso de cualquier módem, para conectarse a redes públicas, mientras se encuentre conectado dentro de la red interna de la CONSAR.

Anexos

Documentos Asociados

- POLDGI-05 Política de Cifrado de Datos
- POLDGI-14 Política de Antivirus y Código Malicioso
- PDGI-09 Administración de Usuarios en los Servicios de la Red Local y Otras Aplicaciones
- PDGI-38 Control de Inventarios de Bienes Informáticos
- PDGI-39 Control del Inventario de Software

Control de Cambios

No DE REVISION	FECHA	MOTIVO
04	**Agosto 2016**	**Se eliminan las referencias a ISO 27001 y se actualiza el documento.**
03	Octubre 2012	Se actualizan las referencias a los nombres de las unidades administrativas de la CONSAR.
02	Agosto 2009	Se define a la Dirección General de Informática como responsable de las acciones mencionadas en este documento. Se agregan nuevos puntos en la sección de Lineamientos para establecer que los equipos tengan antivirus, protector de pantalla con contraseña y que deben mantenerse en la CONSAR cuando los usuarios se encuentren en las instalaciones.
01	Septiembre 2007	Se unificó el formato del tipo de letra del Indice respecto al formato del resto del documento. Se modificó el cuadro de firmas que autorizan el documento para homologarlo de acuerdo a lo que marca el PGSI-01. Se agregaron los números de código de documento en todas las referencias a otros documentos asociados del SGSI.
00	Agosto 2006	Creación de la Política de Equipos Portátiles.

INDICE

Política

Los equipos de la CONSAR deben contar con mecanismos de protección para evitar virus, código malicioso y código móvil que puedan ocasionar daños o mal funcionamiento en la operación.

Objetivo

Establecer la administración de código malicioso, código móvil, virus, gusanos, caballos de Troya, entre otros, que involucren cualquier incidente en los sistemas de información y redes que procesen, almacenen o transmitan información de la CONSAR.

ELABORÓ	REVISÓ	APROBÓ
REPRESENTANTE DEL SGSI	RESPONSABLE DE PROCESO	ALTA DIRECCIÓN

Alcance

Indicar los lineamientos para la protección de equipos servidores de archivos y de correo, equipos de usuarios portátiles y de escritorio, contra virus, código malicioso y código móvil, tomando en consideración los siguientes puntos:

- Responsabilidades de los empleados.
- Archivos y Software.
- Reporte y solución de Incidentes.
- Actualizaciones y mantenimiento.
- Avisos y alerta de virus, código malicioso y código móvil.
- Correo electrónico.

Lineamientos de Antivirus, Código Malicioso y Código Móvil.

Generales.

a. Todos los equipos de escritorio, móviles, personales y servidores utilizados en la operación de la CONSAR, deben manejar un software de antivirus y antispyware que pueda detectar cambios en los archivos de usuario, archivos de configuración, archivos de sistema, aplicaciones y otros recursos.

b. El Responsable del Sistema de Gestión de Seguridad de la Información junto con el Subdirector de Infraestructura, deben verificar que se lleve a cabo una adecuada administración del antivirus, coordinando actividades con el personal de la Dirección de Informática y de Soporte Técnico.

c. Los usuarios son responsables de no desactivar o eliminar el software de antivirus y antispyware en sus equipos y deben notificar cualquier sospecha de contaminación.

d. Los proveedores o personal externo que tengan equipos y que necesiten conectarse a la red de la CONSAR, deben contar con un software de antivirus y antispyware con la última versión liberada, para lo cual el personal técnico de la CONSAR debe confirmar por medio de la aplicación de lo especificado en el procedimiento PDGI-14 Control de Aplicativos y Utilerías en Equipos de Proveedores Varios, que los equipos de los proveedores o del personal externo se encuentren libre de virus, software malicioso, etc.

Reporte de Incidentes.

a. La mesa de ayuda debe atender los incidentes de antivirus, código malicioso y código móvil que sean reportados por los usuarios, hasta llegar a la eliminación de los mismos.

b. Debido a que los virus se han vuelto muy complejos, los usuarios no deben pretender eliminarlos por sí solos. Si los usuarios perciben o sospechan que sus equipos están infectados, inmediatamente tienen que detener el uso del equipo en cuestión y contactar a la mesa de ayuda.

Archivos y Software

a. Los archivos de nueva procedencia deben ser revisados automáticamente por el software de antivirus y antispyware incluyendo:

- Archivos de correo electrónico.

- Archivos provenientes de medios magnéticos (discos floppy, CD, USB, memorias, discos duros externos).
- Archivos de otras PC's.
- Contenido de Internet.

b. Los archivos de correo electrónico deben ser revisados por el software antivirus y antispyware utilizado oficialmente, antes de ser accesible para el usuario.

c. Disquetes o archivos provenientes de entidades externas que sean de uso colectivo, deben ser revisados automáticamente con el software antivirus y antispyware utilizado oficialmente.

d. El software y archivos provenientes de fuentes externas como Internet pueden contener virus (como caballos de Troya, gusanos, etc.) o código móvil (como applets, active X, spyware, etc.), por lo anterior, el software de antivirus y antispyware deberá estar configurado para revisar y limpiar automáticamente, o en último caso, poner en cuarentena cualquier archivo descargado o accedido desde Internet. La herramienta deberá enviar mensajes de alerta al usuario indicándole la peligrosidad del sitio de acuerdo al contenido del mismo; en caso de ser sitios oficiales, el usuario deberá solicitar el apoyo necesario al personal de la Dirección de Informática para poder ingresar a este sitio. En caso de detectarse algún virus o spyware, se debe notificar inmediatamente y no se realizará ningún trabajo sobre el dispositivo infectado hasta que el virus sea eliminado.

e. Todo el software original de los servidores debe ser copiado antes de su uso previo (siempre y cuando las protecciones del mismo lo permitan), y debe ser guardado bajo llave. Esta copia no debe ser usada para uso común, sino sólo para recuperar la versión original que pudiera haber sido dañada por virus, código malicioso o código móvil, daño del disco duro y otros problemas de cómputo.

f. Antes de distribuir un software o archivo en medio electrónico a terceros, los operadores deben revisarlo con el antivirus y antispyware para identificar y eliminar la presencia de alguno de ellos.

g. Queda prohibido instalar y ejecutar cualquier programa o proceso no autorizado para la operación de la CONSAR.

Escaneo y Capacidades del Antivirus.

a. El software de antivirus y antispyware debe estar configurado para desempeñar las siguientes actividades:

- Revisión del sistema al iniciar.
- Revisión del sector de arranque.
- Revisión en tiempo real.
- Revisión al escribir en disco.
- Revisión al leer en disco.
- Revisión de todos los archivos.
- Revisión de programas desconocidos no deseados y troyanos.
- Revisión de virus de macro.
- Los escaneos de servidores de archivos, de correo y críticos deben hacerse por lo menos una vez al día en horarios fuera de operación, mientras que otro tipo de servidores y equipos de escritorio y portátiles por lo menos una vez por semana.
- Revisión de archivos de correo electrónico de entrada y de salida.
- Escaneo de contenidos Web.

b. El software de antivirus y antispyware debe contar con las siguientes capacidades:

- Escaneo automático, manual o programable.
- Limpiar archivos infectados.
- Mantener en cuarentena los archivos que no pueden ser limpiados.
- Proveer la capacidad de actualizaciones automáticas y programables.
- Registrar los incidentes de virus y antispyware y contar con la capacidad de análisis de registro.
- Detección de código malicioso y código móvil.
- Alertas.
- Administración centralizada.

Mantenimiento.

a. Los servidores de antivirus deben contar con mantenimientos periódicos de acuerdo a los requerimientos del fabricante.

b. Se deben llevar acabo las actualizaciones del software de antivirus y antispyware con base en los contratos con el fabricante.

c. El software antivirus y antispyware debe ser actualizado cada vez que se libere una versión, previo a un estudio de validación de aplicaciones.

d. Las definiciones de datos del Antivirus deben actualizarse diariamente.

Reportes y Alertas.

a. El software de antivirus y antispyware debe proporcionar los siguientes tipos de alertas:

- Reporte centralizado de la solución corporativa del antivirus.
- Reportes por medio de correos electrónicos.
- Alertas por medio de mensajes escritos a dispositivos móviles, alarmas visuales o de sonido.

Indicadores.

a. Por lo menos, en forma bimestral se debe generar un reporte global de la situación del antivirus en todos los equipos Windows y Mac de la CONSAR; sean servidores, equipos de escritorio y/o móviles, que muestre el porcentaje de cumplimiento en cuanto a la última versión del antivirus liberada por el fabricante.

Anexos

Documentos Asociados

- MGSI-01 Manual de Gestión de Seguridad de Información (Indicadores).
- PDGI-14 Control de Aplicativos y Utilerías en Equipos de Proveedores Varios.
- PDGI-43 Manejo de Incidentes.

Control de Cambios.

No DE REVISION	FECHA	MOTIVO
06	**Diciembre 2017**	**Se actualizan los nombres de las áreas administrativas y algunos textos para mejora de su descripción.**
05	Agosto 2016	Se eliminan las referencias al ISO 27001 y se actualiza el documento.
04	Octubre 2012	Se actualizan las referencias a los nombres de las unidades administrativas de la CONSAR.
03	Noviembre 2009	Se cambia la frecuencia de elaboración del indicador de “Actualización de Antivirus” de Cuatrimestral a Bimestral.
02	Agosto 2009	Se estipula que se deben aplicar los conceptos de PDGI-14 a equipos de proveedores con necesidad de conexión a la red de la CONSAR. Se agregan algunos puntos a la lista de actividades que deben desempeñar el software antivirus y antispyware. Se cambia la periodicidad de actualización del antivirus y se especifica que se debe realizar un reporte cuatrimestral de actualización de antivirus en todos los equipos.
01	Septiembre 2007	Se unificó el formato del tipo de letra del Indice respecto al formato del resto del documento. Se modificó el cuadro de firmas que autorizan el documento para homologarlo de acuerdo a lo que marca el PGSI-01. Se agregaron los números de código de documento en todas las referencias a otros documentos asociados del SGSI.
00	Agosto 2006	Creación de la Política de Antivirus y Código Malicioso.

INDICE

Política

El incumplimiento accidental o deliberado de las políticas descritas en este documento, será considerado una falta administrativa y tendrá consecuencias laborales y legales, dependiendo de la gravedad de la falta, la cuál será determinada por las áreas competentes.

Objetivo

Proveer un marco de referencia que indique la dimensión de la sanción a la que se hace acreedor quién viole una política de seguridad, evitando en la medida de lo posible, el ejercicio discrecional de las sanciones.

ELABORÓ	REVISÓ	APROBÓ
REPRESENTANTE DEL SGSI	RESPONSABLE DE PROCESO	ALTA DIRECCIÓN

Alcance

Aplicable para todas aquellas violaciones a las políticas y procedimientos incluidos en el Sistema de Gestión de Seguridad de la Información.

Lineamientos de Sanciones.

Generales.

Las sanciones aplicables por violaciones a las Políticas de Seguridad de la Información establecidas por la Comisión serán determinadas por la Coordinación General de Administración y Tecnologías de la Información y/o por el Órgano Interno de Control, de acuerdo a la normatividad aplicable.

Anexos

Documentos Asociados

- Leyes, Reglamentos y Normas del Marco Normativo de la CONSAR.

Control de Cambios

No DE REVISION	FECHA	MOTIVO
05	**Diciembre 2017**	**Se actualizan algunos textos para mejora de su descripción.**
04	Octubre 2016	Se elimina la referencia al ISO 27001.
03	Octubre 2012	Se actualizan las referencias a los nombres de las unidades administrativas de la CONSAR.
02	Agosto 2009	Se hacen modificaciones al Alcance respecto a los documentos incluidos en el Sistema de Gestión de Seguridad de la Información. Se elimina el texto de los Lineamientos de Sanciones y se remite todo a lo indicado en la normatividad aplicable.
01	Septiembre 2007	Se unificó el formato del tipo de letra del Indice respecto al formato del resto del documento. Se modificó el cuadro de firmas que autorizan el documento para homologarlo de acuerdo a lo que marca el PGSI-01. Se agregaron los números de código de documento en todas las referencias a otros documentos asociados del SGSI.
00	Agosto 2006	Creación de la Política de Sanciones.

INDICE

Política

Se establecen los controles y lineamientos para el uso de los medios de almacenamiento de información en Internet para asegurar la información y los servicios de la CONSAR contra el uso indebido y accesos no autorizados.

Objetivo

Establecer los lineamientos generales sobre el uso de medios de almacenamiento en Internet con la finalidad de mantener una adecuada administración para la protección de la información y los servicios de la CONSAR.

ELABORÓ	REVISÓ	APROBÓ
REPRESENTANTE DEL SGSI	RESPONSABLE DE PROCESO	ALTA DIRECCIÓN

Alcance

Indicar los controles para la protección de la información de la CONSAR por el uso de medios de almacenamiento en Internet, bajo los siguientes puntos:

- Titulares de las redes.
- Administración por el uso de medios de almacenamiento de información en Internet.
- Seguridad en el uso de medios de almacenamiento de información en Internet.

Lineamientos de uso de los medios de almacenamiento de información en Internet.

Generales.

a. Toda la información almacenada en los equipos de cómputo y servidores de la CONSAR es propiedad de la Comisión y debe usarse exclusivamente para los propósitos de la misma. A los usuarios se les brinda acceso a la red interna y a los servicios de Internet como ayuda en el desempeño de sus tareas, todos los usuarios tienen la responsabilidad de utilizar los recursos de la red y los servicios de Internet de una manera ética, legal y profesional. El uso indebido de estos recursos será considerado una falta y tendrá las consecuencias que correspondan conforme a la normativa aplicable para el caso.

b. Está estrictamente prohibido conectar los equipos personales a la red interna de datos y hacer uso de transmisión de información a cualquier medio de almacenamiento disponible en la nube usando cualquier servicio para estos fines como : Dropbox, Copy, Google Drive, Box, OneDrive, Mega, CloudMe, Bitcasa, Shared, Adrive, 4Shared, CX, Mediafire, HiDrive, Idrive, Open Drive, Popoplug, Obuntu One, Amazon Cloud Drive, YuuWaa, ElephantDrive, Fiabee, Filesanywhere, Feedrive, Skydrive, Mimus, Memopal, Spideroak, Wuala, Storegate, etc.

c. Si algún usuario tiene necesidad de hacer uso de este recurso de transmisión de información a un medio de almacenamiento en la nube, lo tendrá que solicitar a la Coordinación General de Administración y Tecnologías de la Información, en la que se especifique qué información será copiada, la razón justificable del uso del recurso, características de tipo de información y tamaño de lo que se copiará, horario en que se pretende hacer uso de la herramienta y cualquier otro dato que sea relevante a considerar para la evaluación para su autorización.

d. La Coordinación General de Administración y Tecnologías de la Información, revisará las condiciones técnicas y de seguridad del equipo y de la información antes de permitir conectarlo a la red interna de datos. Una solicitud no contempla que el equipo pueda ser conectado a la red interna de datos cuantas veces requiera el usuario, éste último deberá hacer su solicitud cada que requiera la conexión. De igual modo, ningún proveedor puede irrestrictamente conectar equipos a la red interna de datos, deberá de haber de por medio una solicitud expresa a la Coordinación General de Administración y Tecnologías de la Información.

e. Sólo personal del área de Soporte Técnico y personal de la Coordinación General de Administración y Tecnologías de la Información estará autorizado para hacer movimientos para permitir las conexiones de la red para el uso de estos medios de almacenamiento en la nube.

f. Sólo personal de la Coordinación General de Administración y Tecnologías de la Información podrá ejecutar programas analizadores de protocolos y de muestreo de la red y sólo para propósitos como inventarios, revisión de permisos, búsqueda de equipos, análisis de protocolos, generación de gráficas sobre consumo de ancho de

banda y todas aquellas relacionadas a actividades propias de la Coordinación General de Administración y Tecnologías de la Información.

g. Los usuarios de los servicios de almacenamiento en la nube, son responsables del uso de la misma y debe ser sólo para efectos de la operación de la Institución.

h. Los administradores de la red deben ser los responsables de la administración, configuración y mantenimiento de los componentes de la red de la CONSAR.

i. Queda estrictamente prohibido conectar algún dispositivo inalámbrico a la red interna de datos sin conocimiento y autorización de la Coordinación General de Administración y Tecnologías de la Información.

Administración por el uso de medios de almacenamiento de información en Internet.

a. La Coordinación General de Administración y Tecnologías de la Información, debe tomar las medidas necesarias para asegurar la protección de la red establecidas en la POLDGI-09 Política de Protección de Redes Internas y de la información almacenada, procesada y transmitida vía red.

b. Se debe llevar a cabo un estricto bloqueo de sitios Web que no son necesarios para la operación de la CONSAR, ya que consumen recursos de la red y pueden representar un riesgo para la seguridad de la información de todos los equipos de la CONSAR. Este bloqueo incluye los sitios utilizados para el almacenamiento de información en Internet.

Seguridad en el uso de medios de almacenamiento de información en Internet.

a. Los componentes de la red, deben contar con las configuraciones adecuadas de seguridad.

b. Se debe contar con un monitoreo por parte del Grupo de Monitoreo de la Seguridad, el cual se encargue de detectar cualquier incidente de seguridad en los servicios de red de la CONSAR, para lo cual deberá apoyarse en las bitácoras de los sistemas de seguridad o monitoreo con los que cuente: firewall, aplicaciones de análisis de la red, aplicaciones para filtrado de contenido, entre otros.

c. Se deben considerar controles de seguridad para el uso de medios de almacenamiento en Internet dentro de la red interna de la CONSAR, donde se revisen los siguientes puntos:

- Implicaciones de acceso externo a información contenida en equipos de la red interna de la CONSAR.

- Bloqueo de uso de medios para copiado de información contenida en equipos de la red interna de la CONSAR a repositorios externos.
- Configuración y en su caso bloqueo, de los tamaños máximos de copiado de información contenida en equipos de la red interna a través de cualquier medio de almacenamiento en Internet tanto de entrada como de salida.
- Configuración y en su caso bloqueo, de los tipos de archivos permitidos en el copiado de información contenida en equipos de la red interna tanto de entrada como de salida.

Administración de Riesgos.

a. Se deben llevar a cabo un análisis de riesgos de la red interna de la CONSAR, anualmente para garantizar la integridad, disponibilidad y confidencialidad de la información que viaja por la red.

Anexos

Documentos Asociados

- POLDGI-09 Política de Protección de Redes Internas.
- PDGI-09 Administración de Usuarios en los Servicios de la Red Local y Otras Aplicaciones.
- PDGI-14 Control de Aplicativos y Utilerías en Equipos de Proveedores Varios.
- PDGI-40 Monitoreo de Servicios Informáticos.

Control de Cambios

No DE REVISION	FECHA	MOTIVO
02	**Diciembre 2017**	**Se actualizan algunos textos para mejora de su descripción.**
01	Noviembre 2016	Se elimina la referencia al ISO 27001.
00	Abril 2014	Creación de la Política de Uso de Medios de Almacenamiento de Información en Internet.