POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Disposición ONTI N° 1/2015

1

INTRODUCCIÓN

1.1. Alcance

El objeto es gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo.

1.2 ¿Qué es seguridad de la información?

Es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo de la operación y la operación normal del organismo.

1.3 ¿Por qué es necesario?

La información y los procesos, sistemas y redes de apoyo son activos importantes. Definir lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una eficacia en la operación de las actividades del organismo

1.4 Requerimientos de seguridad

Todo comienza con identificar los requerimientos de seguridad. Esto se puede hacer a través de: Evaluación del riesgo; Requerimientos legales, reguladores, estatutarios y contractuales; Conjunto de principios, objetivos y requerimientos funcionales para el procesamiento de la información.

1.5 Evaluación de los riesgos de seguridad

Ayudan a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos.

1.7 ¿Cómo empezar?

Se pueden considerar un número de controles como un buen punto de inicio para la implementación de la seguridad de la información.

1.8 Factores críticos de éxito

2

TERMINOS Y DEFINICIONES

2.1 Seguridad de la Información

Es la preservación de las siguientes características: Confidencialidad, Integridad, Disponibilidad, Autenticidad, Auditabilidad, Protección a la duplicación, No repudio, Legalidad, Confiabilidad de la Información,

2.2 Evaluación de Riesgos

Es la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

2.2 Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

2.2 Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

2.4 Comité de Seguridad de la Información

Es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.5 Responsable de Seguridad de la Información

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

2.6 Incidente de Seguridad

Es un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información.

2.7 Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto

2.8 Amenaza

Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

2.9 Vulnerabilidad

Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

2.10 Control

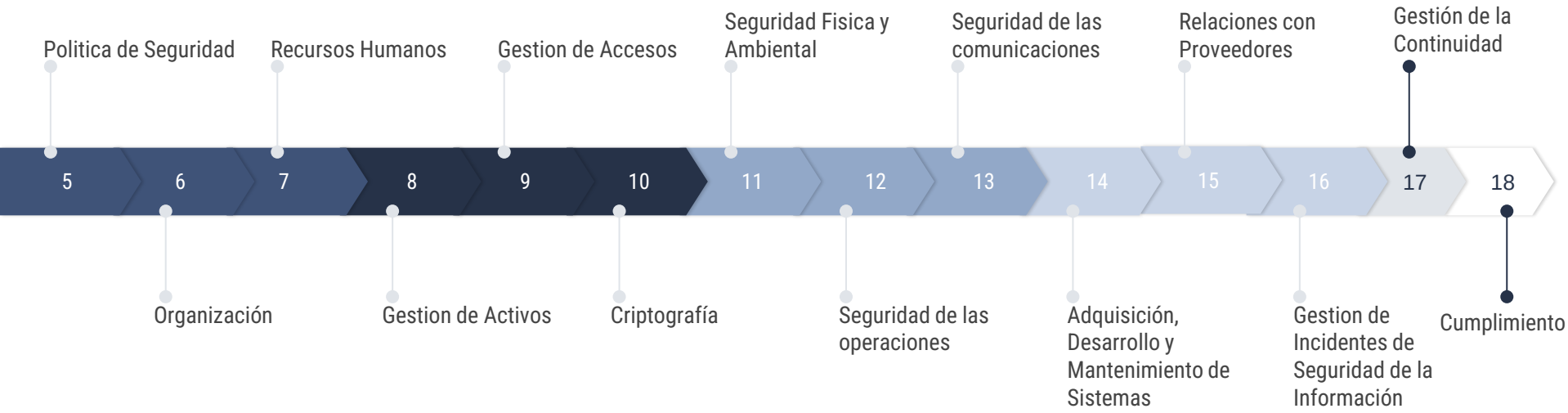
Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

3

ESTRUCTURA DE LA POLITICA MODELO

CUATRO CAPITULOS INTRODUCTORIOS Y CATORCE CLÁUSULAS

Cláusulas



Cada cláusula contiene un número de categorías o grupo de controles de seguridad principales. Por cada categoría, se establece un objetivo y contiene uno o más controles a realizar.

4

TRATAMIENTO DE RIESGOS DE SEGURIDAD

OBJETIVO: *Conocer los riesgos a los que se expone el Organismo en materia de seguridad de la información. Generar información de utilidad para la toma de decisiones en materia de controles de seguridad.*

RESPONSABILIDAD: *El Comité de Seguridad de la Información será responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo.*

4.1 Evaluación de los riesgos de seguridad

El Organismo evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo. Asimismo, se debe efectuar la evaluación cada vez que ocurran cambios significativos.

4.2 Tratamiento de riesgos de seguridad

El Organismo debe decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento.

MITIGAR	ACEPTAR
EVITAR	TRANSFERIR

5

CLÁUSULA: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:

- Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

- Asegurar la implementación de las medidas de seguridad comprendidas en esta Política.

- Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

5.1 Categoría: Política de Seguridad de la información

Objetivo:

- Proporcionar a la Dirección Superior la dirección y soporte para la seguridad de la información en concordancia con los requerimientos y las leyes y regulaciones relevantes. La gerencia debe establecer claramente la dirección de la política en línea con los objetivos

Controles

5.1.1 Control: Documento de la política de seguridad de la información

5.1.2 Control: Revisión de la política de seguridad de la información

6

CLÁUSULA: ORGANIZACIÓN

Objetivo:

- Administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

- Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

6.1 Categoría: Organización interna

Objetivo:

- Manejar la seguridad de la información dentro del organismo.
- Establecer un marco referencial gerencial o político, para iniciar y controlar la implementación de la seguridad de la información dentro del organismo.
- Aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en todo el organismo.

Controles

6.1.1 Control: Compromiso de la dirección con la seguridad de la información

6.1.2 Control: Coordinación de la seguridad de la información

6.1.3 Control: Asignación de responsabilidades de la seguridad de la información

6.1.4 Control: Autorización para Instalaciones de Procesamiento de Información

6.1.5 Control: Acuerdos de confidencialida

6.1.6 Control: Contacto con otros organismos

6.1.7 Control: Contacto con grupos de interés especial

6.1.8 Control: Revisión independiente de la seguridad de la información

6.2 Categoría: Dispositivos móviles y trabajo remoto

Objetivo:

- Asegurar la seguridad de la información cuando se utiliza medios de computación y teletrabajo móviles.

Controles

6.2.1 Control: Dispositivos Móviles

6.2.2 Control: Trabajo Remoto

7

CLÁUSULA: RECURSOS HUMANOS

Objetivo:

- Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos de confidencialidad a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.
- Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.
- Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

7.1 Categoría: Antes del empleo

Objetivo:

- Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Controles

7.1.1 Control: Funciones y responsabilidades

7.1.2 Control: Investigación de antecedentes

7.1.3 Control: Términos y condiciones de contratación

7.2 Categoría: Durante el empleo

Objetivo:

- Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Controles

7.2.1 Control: Responsabilidad de la dirección

7.2.2 Control: Concientización, formación y capacitación en seguridad de la información

7.2.3 Control: Proceso disciplinario

7.3 Categoría: Cese del empleo o cambio de puesto de trabajo

Objetivo:

- Asegurar que los usuarios empleados, contratistas y terceras personas salgan del Organismo o cambien de empleo de una manera ordenada.

Controles

7.3.1 Control: Responsabilidad del cese o cambio

7.3.2 Control: Devolución de activos

7.3.3 Control: Retiro de los derechos de acceso

8

CLÁUSULA: GESTIÓN DE ACTIVOS

Objetivo:

- Garantizar que los activos de información reciban un apropiado nivel de protección.
- Clasificar la información para señalar su sensibilidad y criticidad.
- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación

8.1 Categoría: Responsabilidad sobre los activos

Objetivo:

- Todos los activos deben ser inventariados y contar con un propietario nombrado.

Controles

8.1.1 Control: Inventario de activos

8.1.2 Control: Propiedad de los activos

8.1.3 Control: Uso aceptable de los activos

8.2 Categoría: Clasificación de la información

Objetivo:

- Asegurar que la información reciba un nivel de protección apropiado.

Controles

8.2.1 Control: Directrices de clasificació

8.2.2 Control: Etiquetado y manipulado de la información

8.3 Categoría: Gestión de medios

Objetivo:

- Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades. Los medios se debieran controlar y proteger físicamente

Controles

8.3.1 Control: Administración de Medios Informáticos Removibles

8.3.2 Control: Eliminación de Medios de Información

8.3.3 Control: Seguridad de los Medios en Tránsito

9

CLÁUSULA: GESTIÓN DE ACCESOS

Objetivo:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

- Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

9.1 Categoría: Requerimientos para la Gestión de Acceso

Objetivo:

- Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos sobre la base de los requerimientos del organismo y de seguridad. Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información.

Controles

9.1.1 Control: Política de Gestión de Accesos

9.1.2 Control: Reglas de Gestión de Acceso

9.2 Categoría: Administración de Gestión de Usuarios

Objetivo:

- Controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Controles

- 9.2.1 Control: Registración de Usuarios
- 9.2.2 Control: Gestión de Privilegios
- 9.2.3 Control: Gestión de Contraseñas de Usuario
- 9.2.4 Control: Administración de Contraseñas Críticas
- 9.2.5 Control: Revisión de Derechos de Acceso de Usuarios

9.3 Categoría: Responsabilidades del Usuario

Objetivo:

- Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

Controles

9.3.1 Control: Uso de Contraseñas

9.4 Categoría: Control de Acceso a Sistemas y Aplicaciones

Objetivo:

- Evitar el acceso no autorizado a los servicios de la red.

Controles

9.4.1 Control: Política de Utilización de los Servicios de Red

9.4.2 Control: Camino Forzado

9.4.3 Control: Autenticación de Usuarios para Conexiones Externas

9.4.4 Control: Autenticación de Nodos

9.4.5 Control: Protección de los Puertos (Ports) de Diagnóstico Remoto

9.4.6 Control: Subdivisión de Redes

9.4.7 Control: Acceso a Internet

9.4.8 Control: Conexión a la Red

9.4.9 Control: Ruteo de Red

9.4.10 Control: Seguridad de los Servicios de Red

9.5 Categoría: Control de Acceso al Sistema Operativo

Objetivo:

- Evitar el acceso no autorizado a los sistemas operativos.

Controles

9.5.1 Control: Identificación Automática de Terminales

9.5.1 Control: Identificación Automática de Terminales

9.5.3 Control: Identificación y Autenticación de los Usuarios

9.5.4 Control: Sistema de Administración de Contraseñas

10

CLÁUSULA: CRIPTOGRAFÍA

Objetivo:

- Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, no repudio, la autenticidad y/o la integridad de la información.

10.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo:

- Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. Se debe desarrollar una política sobre el uso de controles criptográficos. Se debe establecer una gestión clave para sostener el uso de técnicas criptográficas

Controles

- 10.1.1 Control: Política de Utilización de Controles Criptográfico
- 10.1.2 Control: Cifrado
- 10.1.3 Control: Firma Digital
- 10.1.4 Control: Servicios de No Repudio
- 10.1.5 Control: Protección de claves criptográfica
- 10.1.6 Control: Protección de Claves criptográficas: Normas y procedimientos

11

CLÁUSULA: FÍSICA Y AMBIENTAL

Objetivo:

- Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.
- Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.
- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.
- Implementar medidas para proteger la información manejada por el personal en las oficinas en el marco normal de sus labores habituales.
- Proporcionar protección proporcional a los riesgos identificados

11.1 Categoría: Áreas Seguras

Objetivo:

- Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales del Organismo.

Controles

- 11.1.1 Control: Perímetro de seguridad física
- 11.1.2 Control: Controles físicos de entrada
- 11.1.3 Control: Seguridad de oficinas, despachos, instalaciones
- 11.1.4 Control: Protección contra amenazas externas y de origen ambiental
- 11.1.5 Control: Trabajo en áreas seguras
- 11.1.6 Control: Áreas de acceso público, de carga y descarga

11.2 Categoría: Seguridad de los equipos

Objetivo:

- Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades del Organismo.
- Proteger el equipo de amenazas físicas y ambientales.

Controles

11.2.1 Control: emplazamiento y protección de equipos

11.2.2 Control: Instalaciones de suministro

11.2.3 Control: Seguridad del cableado

11.2.4 Control: Mantenimiento de los equipos

11.2.5 Control: Seguridad de los equipos fuera de las instalaciones

11.2.6 Control: Reutilización o retiro seguro de equipos

11.2.7 Control: Retirada de materiales propiedad del organismo

11.2.8 Control: Políticas de Pantallas Limpias

11.2.9 Control: Políticas de Escritorios Limpios

12

CLÁUSULA: SEGURIDAD EN LAS OPERACIONES

Objetivo:

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

- Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones

12.1 Categoría: Procedimientos y Responsabilidades operativas

Objetivo:

- Asegurar la operación correcta y segura de los medios de procesamiento de la información.
- Establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.

Controles

12.1.1 Control: Documentación de los Procedimientos

12.1.2 Control: Cambios en las Operaciones

12.1.3 Control: Planificación de la Capacidad

12.1.4 Control: Separación de entornos de desarrollo, pruebas y operacionales

12.2 Categoría: Protección contra el malware (código malicioso)

Objetivo:

- Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. Los usuarios deben estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, los gerentes deben introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

Controles

12.2.1 Control: Control contra el malware (código malicioso)

12.2.2 Control: Código Móvil

12.3 Categoría: Resguardo (backup)

Objetivo:

- Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.
- Establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia (ver también Cláusula 17.1 Categoría: Gestión de Continuidad del Organismo) para tomar copias de respaldo de los datos y practicar su restauración oportuna.

Controles

12.3.1 Control: Resguardo de la Información

12.4 Categoría: Registro y Monitoreo

Objetivo:

- Detectar las actividades de procesamiento de información no autorizadas.
- Monitorear los sistemas y reportar los eventos de seguridad de la información.

Controles

- 12.4.1 Control: Registro de eventos
- 12.4.2 Control: Protección del registro de información
- 12.4.3 Control: Registro del Administrador y del Operador
- 12.4.4 Control: Sincronización de Relojes

12.5 Categoría: Control de Software Operacional

Objetivo:

- Garantizar la seguridad de los archivos del sistema.
- Controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI.

Controles

12.5.1 Control: Instalación de software en sistemas operacionales

12.6 Categoría: Administración de vulnerabilidades técnicas

Objetivo:

- Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

Controles

12.6.1 Control: Administración de vulnerabilidades técnicas

12.6.2 Control: Restricciones en la instalación de software

12.7 Categoría: Consideraciones sobre la auditoría de los sistemas de información

Objetivo:

- Asegurar el cumplimiento de minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

Controles

12.7.1 Control: Controles de auditoría de los sistemas de información

13

CLÁUSULA: GESTIÓN DE COMUNICACIONES

Objetivo:

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

13.1 Categoría: Gestión de la Red

Objetivo:

- Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

Controles

13.1.1 Control: Redes

13.1.2 Control: Seguridad de Servicio de red

13.2 Categoría: Transferencia de información

Objetivo:

- Mantener la seguridad en el intercambio de información dentro del Organismo y con cualquier otra entidad externa.

Controles

13.2.1 Control: Procedimientos y controles de intercambio de la información

13.2.2 Control: Acuerdos de Intercambio de Información

13.2.3 Control: Seguridad de la Mensajería

13.2.4 Control: Acuerdos de confidencialida

14

CLÁUSULA: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Objetivo:

- Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

- Definir los métodos de protección de la información crítica o sensible.

14.1 Categoría: Requerimientos de Seguridad de los Sistemas

Objetivo:

- Garantizar que la seguridad sea una parte integral de los sistemas de información.

Controles

14.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad

14.1.2 Control: Seguridad de servicios aplicativos en redes públicas

14.1.3 Control: Protección de servicios de aplicativos

14.2 Categoría: Seguridad en los Sistemas de Aplicación

Objetivo:

- Establecerán controles y registros de auditoría, verificando:
  - a) La validación efectiva de datos de entrada.
  - b) El procesamiento interno.
  - c) La autenticación de mensajes (interfaces entre sistemas)
  - d) La validación de datos de salida.

Controles

- 14.2.1 Control: Validación de Datos de Entrada
- 14.2.2 Control: Controles de Procesamiento Interno
- 14.2.3 Control: Autenticación de Mensajes
- 14.2.4 Control: Validación de Datos de Salidas

14.3 Categoría: Seguridad de los Archivos del Sistema

Objetivo:

- Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

Controles

14.3.1 Control: Software Operativo

14.3.2 Control: Protección de los Datos de Prueba del Sistema

14.3.3 Control: Cambios a Datos Operativos

14.3.4 Control: Acceso a las Bibliotecas de Programas fuentes

14.4 Categoría: Seguridad de los Procesos de Desarrollo y Soporte

Objetivo:

- Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte dado a los mismos

Controles

14.4.1 Control: Procedimiento de Control de Cambios

14.4.2 Control: Revisión Técnica de los Cambios en el sistema Operativo

14.4.3 Control: Restricción del Cambio de Paquetes de Software

14.4.4 Control: Canales Ocultos y Código Malicioso

14.4.5 Control: Desarrollo Externo de Software

14.5 Categoría: Gestión de vulnerabilidades técnicas

Objetivo:

- Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

Controles

14.5.1 Control: Vulnerabilidades técnicas

15

CLÁUSULA: RELACIONES CON PROVEEDORES

Objetivo:

- Establecer y mantener el nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor.

15.1 Categoría: Seguridad de la información en las relaciones con el proveedor

Objetivo:

- Garantizar y asegurar la protección de la información del organismo que es accedida por los proveedores, cumpliendo con el nivel de seguridad establecido.

Controles

15.1.1 Control: Política de seguridad de la información para las relaciones con el proveedor

15.1.2 Control: Abordar la seguridad dentro de los acuerdos del proveedor

15.1.3 Control: Cadena de suministro de tecnologías de la información y comunicaciones

15.2 Categoría: Administración de prestación de servicios de proveedores

Objetivo:

- Garantizar el mantenimiento del nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor.

Controles

15.2.1 Control: Supervisión y Revisión de los servicios del proveedor

15.2.2 Control: Gestión de cambios a los servicios del proveedor

16

CLÁUSULA: GESTIÓN DE INCIDENTES DE SEGURIDAD

Objetivo:

- Garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

16.1 Categoría: Informe de los eventos y debilidades de la seguridad de la información

Objetivo:

- Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

Controles

16.1.1 Control: Reporte de los eventos de la seguridad de información

16.1.2 Control: Reporte de las debilidades de la seguridad

16.1.3 Control: Comunicación de Anomalías del Software

16.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad de la información

Objetivo:

- Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

Controles

16.2.1 Control: Responsabilidades y procedimientos

16.2.2 Control: Aprendiendo a partir de los incidentes de la seguridad de la información

16.2.3 Control: Procesos Disciplinarios

17

CLÁUSULA: GESTIÓN DE LA CONTINUIDAD

Objetivo:

- Impedir Minimizar los efectos de las posibles interrupciones de las actividades normales del Organismo y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.
- Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan las siguientes etapas: Notificación/Activación; Reanudación; Recuperación.

17.1 Categoría: Gestión de continuidad del Organismo

Objetivo:

- Contraatacar las interrupciones a las actividades del organismo y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

Controles

- 17.1.1 Control: Proceso de Administración de la continuidad del Organismo
- 17.1.2 Control: Continuidad de las Actividades y Análisis de los impactos
- 17.1.3 Control: Elaboración e implementación de los planes de continuidad de las Actividades
- 17.1.4 Control: Marco para la Planificación de la Continuidad de las Actividades del Organismo
- 17.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Organismo

17.2 Categoría: Redundancias

Objetivo:

- Asegurar la continuidad de la información y que esté integrada a los sistemas de gestión

Controles

17.2.1 Control: Disponibilidad de las instalaciones de procesamiento de la información

18

CLÁUSULA: CUMPLIMIENTO

Objetivo:

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.
- Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.
- Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.
- Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.
- Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Organismo.

18.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo:

- Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

Controles

- 18.1.1 Control: Identificación de la Legislación Aplicable
- 18.1.2 Control: Derechos de Propiedad Intelectual
- 18.1.3 Control: Protección de los Registros del Organismo
- 18.1.4 Control: Protección de Datos y Privacidad de la Información Personal
- 18.1.5 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información
- 18.1.6 Control: Regulación de Controles para el Uso de Criptografía
- 18.1.7 Control: Recolección de Evidencia
- 18.1.8 Control: Delitos Informáticos

18.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad Técnica

Objetivo:

- Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

Controles

18.2.1 Control: Cumplimiento de la Política de Seguridad

18.2.2 Control: Verificación de la Compatibilidad Técnica

18.3 Categoría: Consideraciones de Auditorías de Sistemas

Objetivo:

- ❑ Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.
- ❑ Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

Controles

18.3.1 Controles de Auditoría de Sistemas

18.3.2 Control: Protección de los Elementos Utilizados por la Auditoría de Sistemas

18.3.3 Control: Sanciones Previstas por Incumplimiento