ANEXO VIII

SEGURIDAD OPERATIVA

1. OBJETIVO

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información para minimizar el riesgo de pérdida o alteración de datos.

2. ALCANCE

Comprende todas las instalaciones de procesamiento de información de la S.R.T..

3. DEFINICIONES

Ambiente de Producción: Se refiere al entorno que contiene toda la infraestructura de hardware y software, requeridos para que se ejecute el software utilizado por el personal.

Entorno: Aquella condición extrínseca que un sistema informático requiere para poder funcionar de manera correcta. Por ejemplo, a un tipo de programación, un aparato específico, un lenguaje determinado, etc.

Eventos de Seguridad: Ocurrencia o cambio detectado en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

Malware (o código malicioso/dañino): Es un software que compromete la operación de un sistema al realizar una función o proceso no autorizado. Acorde a la ISO/IEC, fue diseñado específicamente para dañar o interrumpir un sistema sin conocimiento ni consentimiento del propietario. Tipos de malware conocidos hasta el momento: virus informático, gusano informático, troyano, spyware, adware, ransomware.

Operaciones: Conjunto de actividades y procesos que se realizan para apoyar el funcionamiento de los sistemas de información del Organismo.

Vulnerabilidades técnicas: Debilidad de un activo o de un control sobre ese activo, que puede ser explotada por una o más amenazas.

4. RESPONSABILIDADES

El Responsable de Seguridad de la Información (RSI) deberá establecer criterios de aprobación para nuevos sistemas de información respecto a la seguridad de la información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Asimismo, deberá verificar que dichos procedimientos de aprobación de software, incluyan aspectos de seguridad para todas las aplicaciones.

Por otro lado, el RSI definirá procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información y verificar su cumplimiento, de manera que no afecten la seguridad de la información.

El RSI deberá definir lineamientos para la administración de los medios de almacenamiento, así como también para el resguardo y recuperación de la información y controlar que se lleven a cabo las pruebas sobre la recuperación de la información.

Asimismo, al RSI le corresponderá definir y documentar controles para la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes de la S.R.T..

Por su parte, la Subgerencia de Sistemas (S.S.) tendrá que implementar todos los procedimientos de operaciones necesarios para el cumplimiento de la política, evaluar el posible impacto operativo de los cambios previstos en el sistema y equipamiento y verificar su correcta implementación;

asignar responsabilidades; administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento; monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios de los usuarios.

La S.S. deberá realizar las copias de resguardo de información, así como la prueba periódica de su restauración. Por otro lado, implementará el registro de las actividades realizadas por el personal operativo, para su posterior revisión.

La S.S. deberá implementar las estrategias de seguridad definidas respecto a software malicioso y accesos no autorizados.

Finalmente, la SS definirá e implementará procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, pendrives e informes impresos y para su eliminación segura.

5. CONTENIDO

5.1 LINEAMIENTOS Y PROCEDIMIENTOS PARA LA SEGURIDAD OPERATIVA

5.1.1 Documentación de los procesos operativos

Se deberán documentar y mantener actualizadas las metodologías, procesos y procedimientos operativos para la gestión y la operación de todas las instalaciones de procesamiento de información. Para la elaboración de dichos documentos, se deberán considerar los siguientes aspectos:

a) Responsabilidades para la gestión y operación para las instalaciones de procesamiento;
b) Lugar de procesamiento y tipo de información a procesar;
c) Interdependencias entre sistemas e información;
d) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas;
e) Restricciones en el uso de utilitarios de los sistemas;
f) Soporte para contactar en caso de dificultades operativas o técnicas imprevistas;
g) Gestión de la recuperación en caso de producirse fallas en el sistema.

Adicionalmente, se deberá elaborar documentación referida a las siguientes actividades:

a) Instalación y mantenimiento de equipamiento y de las plataformas para el procesamiento de información y comunicaciones;
b) Monitoreo del procesamiento y de las comunicaciones;
c) Inicio y finalización de la ejecución de los procesos en los sistemas;
d) Programación y ejecución de procesos;
e) Gestión de servicios;
f) Resguardo de información;
g) Gestión de la configuración de los ambientes de producción.

5.1.2 Planificación de la capacidad

Se deberá monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello, se tendrán en cuenta, además, los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información de la S.R.T. para el período estipulado de vida útil de cada componente.

Asimismo, se deberán informar las necesidades detectadas para que se puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la continuidad del procesamiento y puedan planificar una adecuada acción correctiva.

5.2 SEGURIDAD DE LOS SISTEMAS E INSTALACIONES

5.2.1 Gestión de cambios en entornos productivos

Se deberán definir los procedimientos para la gestión de los cambios en el ambiente de producción. Todo cambio debe ser evaluado previamente, de manera que no afecten la seguridad de sus componentes ni de la información que contienen. Del mismo modo, se deberá evaluar el posible impacto operativo de los cambios previstos y verificar su correcta implementación.

Por último, se deberá impulsar una gestión que incluya un registro con toda la información relevante de cada cambio implementado.

5.2.2 Separación de ambientes de desarrollo, testing y producción

Los ambientes de desarrollo, testing y producción deberán estar separados, preferentemente en forma física y se deben definir y documentar las reglas para la transferencia de software entre cada uno de esos ambientes. Para ello, se tendrán en cuenta los siguientes aspectos:

a) Ejecutar el software en los diferentes ambientes controlando los permisos de acceso a cada ambiente;
b) Separar las actividades de desarrollo y testing, en entornos diferentes;
c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción, cuando no sean indispensables para su funcionamiento;
d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Las interfaces de los sistemas deben identificar claramente a qué instancia se está realizando la conexión;
e) El personal que lleve a cabo tareas de desarrollo de software no debe tener acceso al ambiente productivo. Para los casos donde se requiera dicho acceso, se deberá establecer un procedimiento para la autorización, documentación y registro. El mismo deberá contemplar la debida justificación donde quede reflejada la necesidad del acceso requerido.

5.2.3 Control de software en ambientes productivos

Se tendrán que definir los controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas, teniendo en cuenta que se deberá:

a) Evitar que el programador pueda acceder a los ambientes de producción;
b) Coordinar la implementación de modificaciones o nuevos sistemas en el ambiente de producción;
c) Asegurar que los sistemas en uso, en el ambiente de producción, sean los autorizados y aprobados de acuerdo con las normas y procedimientos vigentes;
d) Instalar las modificaciones, controlando previamente la recepción de la prueba;
e) Rechazar la implementación para el caso de encontrar defectos y/o si faltara la documentación estándar establecida;

Otros posibles controles a definir podrán ser:

a) Guardar sólo los ejecutables en el ambiente de producción;
b) Llevar un registro de las actualizaciones realizadas;
c) Retener las versiones previas del sistema, como medida de contingencia;

d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformidades pertinentes, las pruebas previas a realizarse, etc.;
e) Se deberá establecer un proceso de gestión de actualizaciones de todo el software utilizado en la S.R.T, incluyendo también aquellos casos en los que el mismo sea provisto por terceros.

5.3 PROTECCIÓN CONTRA CÓDIGO MALICIOSO (MALWARE)

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos. Es imprescindible proteger la integridad del software y la información que procesa, almacena y transmite, por lo que se requiere establecer estrategias de detección y prevención para evitar y detectar la potencial introducción de códigos maliciosos a los sistemas de información del Organismo.

Por este motivo, se deberán implementar las herramientas necesarias y definirse los procedimientos para realizar controles tendientes a evitar, detectar y eliminar los códigos maliciosos. Las estrategias a definir deberán considerar establecer lineamientos y procedimientos formales que contemplen las siguientes acciones:

a) Prohibir la instalación y uso de software no autorizado por la S.R.T.;
b) Emitir criterio con el fin de evitar los riesgos relacionados con la obtención de archivos y software a través de redes externas, o por cualquier otro medio (ej.: dispositivos portátiles), señalando las medidas de protección a tomar;
c) Instalar y actualizar periódicamente software de detección y reparación de malware, examinando computadoras y medios informáticos, como medida precautoria y rutinaria;
d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si los mismos implican cambios críticos a los sistemas);
e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la S.R.T., investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas;
f) Concientizar al personal acerca de los posibles ataques de virus y de cómo proceder frente a éstos;
g) Redactar lineamientos relativos a la protección y habilitación de puertos de conexión.

5.4 RESGUARDO Y RECUPERACIÓN DE LA INFORMACIÓN (BACKUP)

Es necesario mantener la integridad y disponibilidad de la información y sus medios de procesamiento. Por este motivo, se deberán establecer los lineamientos y procedimientos necesarios a fin de implementar una estrategia para las copias de respaldo de los datos y practicar su restauración oportuna.

En ese sentido, es necesario establecer los criterios para llevar a cabo un esquema de resguardo para todos los activos de información en función de su criticidad. Asimismo, se deberá contemplar la disposición y control sobre la realización de dichas copias, así como la prueba periódica de su restauración e integridad. Para esto se debe contar con instalaciones de resguardo que garanticen que el esquema propuesto sea realizado.

Los sistemas de resguardo deben probarse periódicamente. Por este motivo, se deberán definir procedimientos para el resguardo de la información, considerando los siguientes puntos:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente;

b) Establecer un esquema de remplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo con lo indicado por el proveedor y asegurando la destrucción de los medios desechados;
c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de éstas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal;
d) Asignar a la información de resguardo, un nivel de protección física y ambiental;
e) Establecer periodos de prueba de los medios de resguardo;
f) Ejercer un monitoreo sobre las acciones de resguardo de la información;
g) Definir un tiempo de resguardo para la información.

5.5 REGISTRO Y MONITOREO

Es necesario que el procesamiento de información se realice de manera segura. Por este motivo, se implementará un monitoreo continuo sobre la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del Organismo. Por otro lado, corresponderá registrar las fallas que surgieran, para así asegurar que se identifiquen los problemas en los sistemas de información. Por último, se deberá utilizar el monitoreo del sistema para corroborar la efectividad de los controles adoptados respecto a criterios de acceso.

5.5.1 Registro de eventos de seguridad

Se deberán definir, crear y mantener registros sobre eventos de seguridad de la información, que permitan la detección e investigación de incidentes. En cada caso, se deberá evaluar la pertinencia del registro de la siguiente información:

a) Identificación de las/los usuarias/os afectados;
b) Identificación del equipo o la ubicación, si es posible;
c) Registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;
d) Cambios a la configuración del sistema;
e) Uso de privilegios;
f) Uso de utilitarios y aplicaciones de sistemas;
g) Archivos accedidos y el tipo de acceso;
h) Direcciones de redes y protocolos;
i) Alarmas que son ejecutadas por el sistema de control de accesos;
j) Activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.

5.5.2 Registro del Administrador y del Operador

Se deberá llevar adelante un proceso de registro y monitoreo de las actividades de los administradores y operadores. En dicho registro, se deberá evaluar la conveniencia de contar con la siguiente información:

a) Cuenta de administración u operación involucrada;
b) Momento en el cual ocurre un evento (éxito o falla);
c) Información acerca del evento (por ejemplo, los archivos manipulados) o las fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);
d) Procesos involucrados.

5.5.3 Sincronización de Relojes de los servidores

Se deberá tener una correcta configuración de los relojes a fin de garantizar la exactitud de los registros. Para ello, debe disponerse de un proceso de verificación de los mismos contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

5.6 IDENTIFICACIÓN Y GESTIÓN DE VULNERABILIDADES

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

5.6.1 Gestión de vulnerabilidades

Se deberá obtener información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, para evaluar la exposición de la S.R.T. a tales vulnerabilidades y realizar las acciones necesarias para tratar los riesgos asociados.

El proceso de gestión de vulnerabilidades deberá comprender:

a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;
b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;
c) Identificación de los riesgos asociados a la instalación de parches;
d) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;
e) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;
f) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;
g) Seguimiento y evaluación regular del proceso de gestión de vulnerabilidades para garantizar su efectividad y eficiencia;
h) Gestión de los reportes de vulnerabilidades y recomendaciones de actualización.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66585142-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO VIII Seguridad Operativa-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 7 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:40:35 -03:00

Diego Maximiliano Segovia
Subgerente
Subgerencia de Sistemas
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:52:17 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:52:18 -03:00