ANEXO XII

GESTIÓN DE INCIDENTES DE SEGURIDAD

1. OBJETIVO

Establecer los lineamientos adecuados para la correcta detección, gestión y tratamiento de incidentes en materia de Seguridad de la Información que puedan afectar los activos de información y/o las operaciones esenciales de la S.R.T. viéndose comprometida la confidencialidad, integridad y disponibilidad de los datos y la información que el Organismo administra y gestiona.

2. ALCANCE

Comprende toda la infraestructura de la red tecnológica, así como los dispositivos que están conectados e involucrados en el tratamiento de la información del Organismo.

3. DEFINICIONES

Contención: son acciones encaminadas a contener o paliar los efectos de un incidente detectado y evitar su recurrencia.

Evento 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.

Incidente de seguridad: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa u Organismo.

Mitigación: son aquellas acciones que están encaminadas a reducir y limitar los efectos de un evento de seguridad.

4. RESPONSABILIDADES

El Responsable de Seguridad de la Información (RSI) deberá definir lineamientos para la gestión y el tratamiento de los incidentes de seguridad de la información que puedan afectar a la confidencialidad, integridad y disponibilidad de los datos y de la información almacenada, procesada y transmitida por el Organismo (interna y externa).

Deberá validar la severidad del incidente y acompañar el desarrollo hacia la gestión del incidente para determinar cursos de acción, en caso de ser necesario.

Asimismo, deberá realizar el seguimiento de los estados de situación en torno a la gestión y el tratamiento de incidentes en materia de seguridad de la información, y evaluar de acuerdo a la severidad del evento su escalamiento a las partes interesadas para su conocimiento, incluyendo a la Dirección Nacional de Ciberseguridad (DNC).

Deberá validar con los responsables de los procesos y/o activos, la operatividad de los mismos luego de la ejecución de acciones de contención y/o de mitigación. Y deberá llevar adelante la gestión sobre las lecciones aprendidas y la detección de oportunidades de mejoras.

La Subgerencia de Sistemas (S.S.) deberá notificar al RSI en caso de eventos de seguridad y sobre aquellos incidentes que por su severidad lo amerite.

Deberá ejecutar, en colaboración con el RSI, las acciones de contención y de mitigación del incidente.

En caso de corresponder, la S.S. deberá evaluar factibilidades y debilidades de la ejecución de medidas de contención y de mitigación, y participar de las mismas al RSI. Asimismo, la S.S. deberá mantener comunicación con el personal afectado.

Por otra parte, deberá cerrar el incidente en caso de una resolución positiva del mismo, y comunicarlo a las partes interesadas.

El Comité de Seguridad de la Información deberá ser convocado en los casos que la severidad de un incidente de seguridad lo amerite. Deberá tomar conocimiento del mismo y, en caso que lo considere pertinente, realizará el seguimiento de las acciones preventivas, correctivas y de mitigación ejecutadas ante la ocurrencia del mismo.

Todo el personal de la S.R.T. será responsable de notificar a la S.S. ante un posible evento de seguridad a través de los canales de comunicación habilitados para tal fin, o bien a los Titulares de las Unidades Organizativas.

5. CONTENIDO

Mediante un proceso de gestión de incidentes se deberán adoptar las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar los activos de información de la S.R.T..

5.1 ESTABLECIMIENTO DE MEDIDAS PARA LA GESTIÓN DE INCIDENTES

Se deberán establecer las medidas necesarias para que la gestión de los incidentes de Seguridad de la Información, cuente con los siguientes aspectos:

- La identificación de potenciales debilidades en los procesos donde se gestione información en el Organismo;
- La adopción de medidas preventivas antes potenciales incidentes de seguridad;
- La formalización de procedimientos de gestión de incidentes y su adecuada comunicación a las áreas pertinentes;
- Un ciclo de vida definido, donde se pueda identificar los estados por los que transita un incidente de seguridad;
- Canales de comunicación donde el personal pueda informar potenciales incidentes, y donde se pueda, además, informar a las partes interesadas, proveedores y/o terceros en caso de contar con incidentes críticos;
- Una estrategia de priorización y escalamiento, que incluya la comunicación a las áreas involucradas y autoridades;
- Determinación de la severidad de un incidente, donde se pueda visualizar el impacto que pudiera tener el mismo;
- Procesos para la contención y/ o mitigación de un incidente;
- La recopilación de evidencia de todo el proceso de resolución del incidente, desde que se informa hasta que se soluciona;
- Una base de conocimiento, donde se pueda tomar información que sirva para retroalimentar a la gestión y, de esta manera, lograr una mejora continua.

5.2 DETECCIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD

Se deberá instruir al personal para la prevención, detección y reporte de eventos e incidentes de seguridad, según las responsabilidades correspondientes.

5.2.1 Canales de Comunicación

Durante el proceso de tratamiento y gestión de los eventos e incidentes de Seguridad de la Información, las partes involucradas deberán utilizar canales formales de comunicación, los cuales permitan establecer contacto durante todo el ciclo de vida del evento o incidente y dejar evidencias claras sobre cada uno de los estados por el cual transite.

Por este motivo, es necesario definir y comunicar a todo el personal los canales de comunicación, teniendo en cuenta principalmente las tecnologías utilizadas en el Organismo para dicho fin.

5.2.2 Severidad de los Incidentes

Se deberá definir y establecer criterios para la asignación de la severidad con la que se registrarán los incidentes de seguridad. Para ello, se deberá tener en cuenta:

- Los niveles de impacto definidos por el análisis de riesgos y la clasificación de activos de información;
- El impacto que resulta del incidente, es decir, la cantidad de personal afectado;
- La manera en que se compromete información de la S.R.T..

Asimismo, la severidad definida determinará el tiempo que se requiere para la resolución del incidente y el impacto que tiene el mismo en el Organismo.

Por último, se deberán establecer los criterios que permitan identificar aquellos incidentes cuya severidad sea tal que requiera ser comunicada a las partes interesadas.

5.2.3 Escalamiento de incidentes de seguridad de la información

Se deberá establecer una estrategia clara de priorización y escalamiento, que incluya la comunicación a las áreas involucradas y autoridades, así como a terceros en caso de corresponder. Se deberán contemplar las siguientes medidas:

- De acuerdo a la severidad e impacto del incidente, se evaluará la oportunidad de comunicación con otras áreas de la S.R.T., con terceros, proveedores y otros Organismos;
- De acuerdo a la severidad e impacto del incidente, se pondrá en conocimiento al Comité de Seguridad de la Información;
- De acuerdo a la severidad e impacto del incidente, se notificará a la Dirección Nacional de Ciberseguridad de la ocurrencia de incidentes de seguridad de la información, en un plazo no superior a CUARENTA Y OCHO (48) horas de su detección;
- Se evaluará los potenciales casos en que el incidente de seguridad de la información hubiere afectado activos y/o se haya comprometido información y/o datos personales de terceros, para comunicar públicamente tal evento.

5.3 PROCESOS DE CONTENCIÓN Y DE MITIGACIÓN

Posterior a un análisis de situación se deberá gestionar y tratar los incidentes de seguridad de la información que demandan muchas veces la ejecución de acciones de contención. En el caso de no ser efectivas estas acciones, se deberán ejecutar las acciones correctivas o de mitigación. Para esto, es necesario contar previamente con una planificación que permita identificar qué acciones requieren los incidentes de acuerdo a su tipología, y que sirva de hoja de ruta para todo el proceso de la gestión del mismo.

5.3.1 Procesos de Contención

La gestión de incidentes en materia de Seguridad de la Información deriva en la ejecución de medidas o acciones que contengan la propagación de las amenazas. En este contexto, se deberán tener en cuenta los siguientes aspectos:

- Los canales de comunicación a utilizar con el personal afectado;
- Los canales de comunicación a utilizar con los responsables de los procesos asociados y/o con los terceros, en caso de requerir su intervención;

- Los procedimientos y acciones de contención de las amenazas a ejecutar, evitando su propagación en el resto de la red corporativa de la organización;
- La notificación a los responsables, los propietarios de la información sobre la ejecución de dichas medidas y sus resultados;
- Validaciones sobre las acciones llevadas a cabo, en los casos que amerite.

5.3.2 Procesos de Mitigación

Asimismo, es necesario definir y establecer las acciones de mitigación, para los casos donde la ejecución de las medidas de contención no resulte efectiva. Para ello se deberán tener en cuenta los siguientes aspectos:

- La comunicación con el personal afectado y con los responsables de los procesos asociados, en caso de requerir su intervención;
- La comunicación con terceros, en caso de requerir su intervención;
- Las buenas prácticas en materia de seguridad de la información;
- Evaluaciones sobre las factibilidades y debilidades de la aplicación de las medidas y acciones correctivas o de mitigación;
- Validaciones sobre la operatividad del personal afectado;
- Validaciones de las acciones, en los casos que amerite.

5.4 CAPTURA Y PRESERVACIÓN DE EVIDENCIAS

Durante todo el tratamiento del incidente, se deberá capturar y preservar las evidencias del caso como respaldo ante posibles requerimientos de una auditoría interna o externa a la SRT. Asimismo, se deberá recopilar la evidencia necesaria para la adopción de medidas administrativas o judiciales posteriores, resguardando la cadena de custodia.

Las evidencias pueden provenir de los siguientes ítems:

- Capturas de pantallas de acciones realizadas a lo largo de la gestión y el tratamiento del incidente;
- Pistas de auditoría de las aplicaciones, sistemas o bases de datos afectadas;
- Correos electrónicos;
- Seguimiento del incidente, carga en el sistema de registración de tickets;
- Otros registros que puedan servir de evidencia para la gestión y el tratamiento del incidente.

5.5 GESTIÓN DE LECCIONES APRENDIDAS Y OPORTUNIDAD DE MEJORA

La gestión del incidente además de dejar evidencias respecto de su ejecución deberá dejar constancia de los antecedentes a efecto de retroalimentar una base de conocimiento la cual deberá ser adoptada para optimizar la gestión de incidentes recurrentes o de naturalezas similares en el futuro.

La experiencia recabada traerá asociada la capacitación y concientización, las cuales deberán ser adoptadas como prácticas habituales.

Respecto a la identificación de oportunidades de mejora, las partes involucradas (posterior a la gestión del incidente) deberán revisar de manera habitual la base de conocimiento, relevar acciones tomadas y proceder a corregirlas, en caso de requerirse, para poder optimizar el proceso de gestión y tratamiento del incidente.

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

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66587138-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO XII Gestión de Incidentes de Seguridad-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 5 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:41:28 -03:00

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

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:54:35 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:54:35 -03:00