DEPARTAMENTO ADMINISTRATIVO

DE LA DEFENSORÍA DEL ESPACIO PÚBLICO

Guía de roles y responsabilidades de seguridad de la información

Código: 127-GUIGI-04

Vigencia desde: 19/03/2019

Versión: 1

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ MEJOR PARA TODOS

CONTENIDO

Lista de Tablas

Lista de Ilustraciones

1. INTRODUCCIÓN

La continua evolución de las tecnologías de la información y las comunicaciones – TIC´s, han permitido que las entidades o empresas de cualquier tipo logren alcanzar los objetivos propuestos con mayor eficiencia y eficacia haciendo uso de los recursos tecnológicos como agente de transformación. En contraprestación al uso y apropiación de nuevos componentes tecnológicos, se encuentra el incremento y materialización de riesgos, eventos e incidentes que comprometen y atentan contra la confidencialidad, integridad y disponibilidad de los datos e información que es almacenada, procesada y transmitida en los distintos sistemas de información, servicios y demás recursos tecnológicos, razón por la cual surge la necesidad de implementar controles para el tratamiento amenazas que afectan la seguridad de la información en las organizaciones.

Por esta razón, la gestión de incidentes de seguridad de la información requiere la implementación de recursos tecnológicos, esfuerzos humanos, así como la ejecución de actividades que logren una adecuada detección, evaluación, análisis, contención, erradicación y recuperación de los eventos e incidentes en función de que la materialización de amenazas generen el menor impacto posible de afectación sobre los activos de información de las organizaciones.

2. OBJETIVO

Proponer lineamientos y actividades para la prevención, detección, contención y recuperación de los activos de información como resultado de eventos e incidentes adversos que afectan la seguridad de la información del DADEP.

OBJETIVOS ESPECIFICOS

- Definir roles y responsabilidades para la atención de incidentes de seguridad de la información.
- Gestionar de manera oportuna los eventos de seguridad de la información que puedan comprometer la seguridad de la información.
- Gestionar de manera idónea los incidentes de seguridad de la información mitigando el impacto.
- Documentar las lecciones aprendidas y las actividades post incidente que prevengan la ocurrencia de futuros incidentes.
- Definir mecanismos de monitoreo que permitan la identificación de vulnerabilidades que de forma anticipada eviten la materialización de eventos de seguridad de la información.

3. ALCANCE

El alcance de la guía de gestión de incidentes de seguridad informática inicia con las medidas para la detección oportuna de vulnerabilidades, amenazas, eventos e incidentes que afectan la seguridad de la información y culmina con la contención, erradicación y recuperación de los activos de información que fueron afectados.

4. DEFINICIONES Y SIGLAS

Para la adecuada gestión de riesgos de seguridad de la información se debe manejar con propiedad los siguientes términos:

- Activo: En relación a la seguridad de la información, se entiende como cualquier información o elementos tecnológicos que tienen relación directa con la información (sistemas de información, servicios tecnológicos, archivos físicos, archivos digitales, infraestructura tecnológica incluso personas) que tenga valor para la organización.

- Confidencialidad de la información: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- CSIRT: "Computer Security Incident Response Team" Equipo de Respuesta a Incidentes de Seguridad Informática

- Disponibilidad de la información: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- Evento de seguridad: Se entiende como cualquier evento relacionado con la seguridad de la información que pueda llegar a afectar uno o varios activos de información.

- Incidente de Seguridad Es la materialización de un evento de seguridad que afecta la integridad, disponibilidad o confidencialidad de la información.

- Integridad de la información: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

5. ¿QUÉ ES UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN?

Un Incidente de Seguridad de la Información es la violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita. También se puede expresar como la materialización de uno o varios eventos no deseados o inesperados que comprometen o impactan la disponibilidad, integridad y confidencialidad de la información en los recursos informáticos.

6. ¿QUÉ ES LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN?

Es la capacidad de administrar recursos tecnológicos y demás mecanismos para la detección, diagnostico, reporte, evaluación, contención, tratamiento, respuesta y documentación de los incidentes de seguridad de la información causados en el DADEP.

7. ROLES Y RESPONSABILIDADES

Dentro de las actividades de gestión de incidentes de seguridad informática deben intervenir varios cargos a nivel estructural de la entidad y unos roles junto con responsabilidades a desempeñar, los cuales se describen en el documento **127 – GUIGI - 02 Guía de Roles y Responsabilidades de Seguridad de la Información** que hace parte del Sistema Integrado de Gestión, en el proceso Seguridad de la Información.

8. MODELO DE GESTIÓN DE INCIDENTES

Para la elaboración de la guía se adoptó el modelo de gestión de incidentes que establece el **MinTIC** cuya definición de actividades se encuentran alineadas con el estándar internacional **ISO 27035:2013** Gestión de Incidentes de Seguridad de la Información

Ilustración 1. Ciclo de Vida Gestión de Incidentes de Seguridad de la Información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

El modelo de gestión de incidentes de seguridad de la información se desarrolla por medio de cuatro fases descritas a continuación

Fase de Preparación

La fase de preparación contempla la formulación estratégica de actividades que permiten responder a los problemas producto de la materialización de eventos de seguridad, así como la capacidad para detectar de manera oportuna vulnerabilidades y amenazas a fin de prevenir la afectación en los sistemas de información, redes de comunicaciones y demás información alojada en dispositivos electrónicos.

Con este fin, resulta oportuno conformar un equipo de respuesta a incidentes de seguridad informática el cual se encargue de gestionar y ejecutar las actividades como resultado de la materialización de posibles eventos adversos e inesperados que se presentan producto de controles fallidos e inexistentes. Razón por la cual, el CSIRT por sus siglas en inglés Computer Security Incident Response Team o su equivalente en español Equipo de Respuesta a Incidentes de Seguridad Informática debe actuar como parte importante de la estrategia de seguridad de la información coadyuvando a incrementar los niveles de protección de los activos de información y actuando en la prevención, detección y recuperación de los incidentes que comprometen la confidencialidad, integridad y disponibilidad de la información.

En esta etapa se debe contar con el apoyo de la Oficina de Sistemas, quienes implementarán buenas prácticas, controles operacionales y herramientas para el aseguramiento de los sistemas de información, redes de comunicaciones y demás recursos tecnológicos entre las que se encuentran:

- Políticas de gestión a incidentes de seguridad de la información.
- Procedimientos para la gestión de incidentes de seguridad de la información.
- Aseguramiento de redes, aplicaciones y sistemas operativos (incluye administración de parches, servidores, bases de datos, frameworks de desarrollo, reglas de firewalls, actualización de dispositivos como IDS o IPS, prevención contra código malicioso entre otros).
- Toma de conciencia y entrenamiento a los funcionarios para la prevención y respuesta a incidentes.
- Selección de herramientas que mejoren la seguridad.

Las actividades mencionadas anteriormente contribuyen de manera eficaz a la prevención de incidentes de seguridad de la información, por lo que de manera proactiva se debe trabajar en estas actividades de manera transversal logrando salvaguardar los activos de información del DADEP.

Adicionalmente, es necesario establecer distintos canales directos de comunicación con los funcionarios que hacen del equipo de respuesta a incidentes de seguridad informática, ingenieros de la oficina de sistemas, el área de asuntos disciplinarios cuando en el incidente se identifique que hubo participación de funcionarios o contratistas y finalmente, tener comunicación con la policía nacional, la Fiscalía y el CSIRT de Gobierno nacional.

La selección de herramientas en esta fase se hacen necesarias para poder responder a los incidentes de seguridad informática, por lo que se hace necesario la selección de herramientas licenciadas y de código libre que permitan una adecuada respuesta a los incidentes entre los cuales se encuentran: equipos forenses, analizadores de protocolos, software para la recolección de evidencias, kit de respuesta a incidentes, software de análisis forense y medios de almacenamiento.

Por su parte, los recursos para el análisis de incidentes de seguridad informática contemplan la mayor recolección posible de información acerca de la configuración de redes que incluye el diagrama o topología de red, puertos, protocolos, tráfico y direcciones de IP´s; también se debe contar con información de los servidores como configuraciones, servicios, sistemas operativos y aplicaciones a fin de poder gestionar los incidentes presentados. Finalmente, se deben contemplar las medidas de mitigación y remediación como backup´s, imágenes de servidores y demás información que permita reestablecer el funcionamiento y disponibilidad del recurso afectado.

Fase de Detección Evaluación y Análisis

En el desarrollo de esta fase se realizar un trabajo de observación, monitoreo y levantamiento de información o eventos que con antelación alerten la posibilidad de presentarse un incidente. Para esto, se realiza la recolección de alertas o logs en sistemas de seguridad (firewall, antivirus, analizadores de vulnerabilidades, sistemas de prevención y/o detección de intrusos), caídas de servidores, reportes de usuarios realizados y demás eventualidades que impidan el normal funcionamiento de los sistemas de información, páginas web y servicios tecnológicos.

Las actividades de análisis del incidente de seguridad involucran componentes tecnológicos, operacionales y de información por tanto se hace necesario contar indicadores, métricas de desempeño y tableros de control en donde se pueda observar el comportamiento de la red, sistemas de información, infraestructura tecnológica y demás recursos que permitan realizar un análisis completo del incidente que se esté presentando. Adicionalmente, es una buena práctica contar con bases de conocimiento con información acerca de la identificación de nuevas vulnerabilidades, servicios que se encuentren habilitados y lecciones aprendidas con incidentes ocasionados con anterioridad.

La detección y análisis de los incidentes se simplifica cuando el origen se identifica con la mayor precisión y se logra determinar el alcance del incidente (redes, infraestructuras o sistemas de información afectadas), identificar quién o cuál fue al fuente del incidente así como los recursos o herramientas empleadas para realizar el ataque y las vulnerabilidades que se están explotando para determinar cómo está ocurriendo el incidente.

Para la evaluación de los incidentes se debe establecer el nivel de severidad de acuerdo a la afectación presentada en los activos de información y el análisis de incidentes realizado; Esta severidad se presenta de acuerdo a los siguientes niveles de impacto:

- **Alto impacto:** Son incidentes que afectan con severidad los activos de información que hacen parte de los procesos misionales o de los objetivos propuestos por la entidad. Sobre este nivel de impacto quedan asociados todos los incidentes que afecten la reputación y buen el nombre o que comprometan aspectos legales.

- **Medio Impacto:** Se consideran así a los incidentes que afectan con moderación algún proceso o procedimiento determinado.

- Bajo Impacto: Se catalogan incidentes de impacto bajo, los que afectan activos de información que tienen una criticidad leve y que su afectación no compromete con consideración el desarrollo de los procesos y objetivo de la entidad.

La evaluación contempla la clasificación del incidente que haya tenido afectación contra la confidencialidad, integridad y disponibilidad de los datos, información y sistemas informáticos, por lo que su clasificación debe estar sujeta a los siguientes delitos establecidos en la ley 1273 de 2009:

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMAS DE INFORMÁTICO.

- Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIONES.
- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.
- Artículo 269D. DAÑO INFORMÁTICO.
- Artículo 269E. USO DE SOFTWARE MALICIOSO.
- Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.
- Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.
- Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.
- Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.
- Artículo 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.

En seguida de la clasificación del incidente, los esfuerzos deben estar orientados a la priorización y tiempos de respuesta del incidente de acuerdo a la prioridad, la criticidad del impacto, el impacto actual y futuro descritos a continuación:

- **Nivel de Prioridad:** Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los activos de información.

Tabla 1. Niveles de Criticidad de Impacto

NIVEL DE CRITICIDAD	VALOR	DEFINICIÓN
Inferior	0.10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0.25	Sistemas que apoyan a una sola dependencia o proceso de una entidad
Medio	0.5	Sistemas que apoyan más de una dependencias o proceso de la entidad.
Alto	0.75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1.0	Sistemas Críticos.

Fuente: MinTIC

- **Impacto Actual y Futuro:** Es la cantidad de daño ocasionado en el momento de ser detectado el incidente y la cantidad de daño puede ocasionar antes de ser contenido o erradicado el incidente.

Tabla 2. Niveles de Impacto Actual y Futuro

NIVEL DE CRITICIDAD	VALOR	DEFINICIÓN
Inferior	0.10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	0.25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	0.5	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Alto	0.75	Impacto moderado en uno o más componentes de más de un sistema de información
Superior	1.0	Impacto alto en uno o más componentes de más de un sistema de información.

Fuente: MinTIC

- **Nivel de Prioridad:** Se realiza un cálculo para determinar el nivel de prioridad con que se debe atender el incidente.

  - **Formula:** Nivel Prioridad = (Impacto actual ***** 2.5) + (Impacto futuro ***** 2.5) + (Criticidad del Sistema ***** 5).

En seguida se comparan los valores obtenidos con los descritos en la tabla de niveles de prioridad del incidente

Tabla 3. Niveles de Prioridad del Incidente

Nivel de Prioridad	Valor
Inferior	0 – 2.49
Bajo	2.5 – 3.74
Medio	3.75 – 4.99
Alto	5 – 7.49
Superior	7.5 – 10.00

Fuente: MinTIC

Luego de identificar el nivel de prioridad, se debe asignar tiempos para la gestión o respuesta del incidente en relación a la criticidad e impacto causado, En la tabla número 4 se describen los tiempos en que se deben ser atendidos los incidentes:

Tabla 4. Tiempos máximos de atención a incidentes

Nivel de Prioridad	Tiempo de Respuesta
Inferior	3 Horas
Bajo	1 Hora
Medio	30 Minutos
Alto	15 Minutos
Superior	Inmediata

Fuente: MinTIC

Como última actividad que hace parte de la fase de Detección Evaluación y Análisis es necesario notificar el incidente con el ánimo de minimizar la probabilidad de ocurrencia, así como de ejecutar con mayor desempeño las actividades de recuperación y contención del incidente siempre buscando minimizar la perdida de información y la interrupción de los sistemas de información y de los servicios.

Las actividades que hacen parte de esta fase se describen con detalle en el procedimiento definido como **127-PRCGI-05 "**Procedimiento de Gestión a Incidentes de Seguridad Informática".

Fase de Contención, Erradicación y Recuperación

Una vez analizado y priorizado el incidente se debe contener su acción para evitar que su propagación impida su erradicación afectando la confidencialidad, integridad y disponibilidad de los datos e información de otros sistemas de información, servidores, servicios tecnológicos y demás recursos de tecnologías de la información.

Cada incidente tiene su propia forma de contención, por lo que debe ser estudiada, definida y adoptada por el equipo de respuesta a incidentes. A continuación se lista algunos ejemplos de estrategias para contención de incidentes:

Tabla 5. Estrategias para la contención a incidentes

INCIDENTE	EJEMPLO	ESTRATEGIA
Acceso no autorizado	Sucesivos intentos fallidos de login	Bloqueo de cuenta
Código Malicioso	Infección con Virus	Desconexión a la red del equipo afectado
Acceso no autorizado	Compromiso del Root	Apagado del Sistema
Reconocimiento	Scanning de Puertos	Incorporación de reglas de filtrado en el firewall
Daño informático	Secuestro de información	Desconexión a la red del equipo afectado
Interceptación de datos	Fuga de información	Suspender el servicio web o recurso de TI
Uso de Software Malicioso	Acceso remoto	Desconexión a la red del equipo afectado

Fuente: Elaboración Propia y MinTIC

Luego que el incidente de seguridad informática fue contenido, es necesario realizar actividades de erradicación para eliminar los componentes y todo rastro que fueron empleados para el desarrollo del mismo. Sin embargo, se puede presentar que en algunos incidentes no se realiza erradicación del mismo sino que el incidente es eliminado mediante actividades y procedimientos de recuperación.

En esta fase se ponen a prueba la efectividad de los recursos operacionales y tecnológicos a disposición, se ejecutan las actividades descritas en el procedimiento definido como **127-PRCGI-05** "Procedimiento de Gestión a Incidentes de Seguridad Informática", al igual que entra en ejecución de ser necesario el Plan de Continuidad de Negocio **BCP** y/o Plan de Recuperación de Desastres **DRP** para proceder a restaurar los sistemas de información, servicios tecnológicos y demás recursos de TI que fueron afectados.

Fase de Post-Incidente

De cada incidente de seguridad informática ocasionado es necesario realizar un aprendizaje que permita la identificación de nuevas amenazas, vulnerabilidades y oportunidades de mejora para la protección de los activos de información. Adicionalmente en esta fase además de reportar el incidente y de aplicar medidas disciplinarias o penales cuando el incidente lo requiera, se debe identificar qué exactamente sucedió y ocasiono el incidente, evaluar el desempeño del equipo de respuesta a incidentes y los directivos, realizar la documentación necesaria de la resolución del incidente y determinar qué acciones y recursos son necesarios para contribuir a la detección, análisis, contención y mitigación de futuros incidentes de seguridad que afecten las disponibilidad, integridad y confidencialidad de los datos e información contenida en los recursos de TI

NADIME AMPARO YAVER LICHT

Directora

Defensoría del Espacio Público

Proyectó: Carlos Rojas Villamil, Contratista, Oficina de Sistemas
Elaboró: Carlos Rojas Villamil, Contratista, Oficina de Sistemas
Revisó: Hugo Roberto Hernández Díaz Profesional Oficina de Sistemas
Isaías Sánchez Rivera Jefe Oficina Asesora de Planeación - Luis Fernando Arango Vargas Profesional Oficina Asesora de Planeación
Aprobó: Julio Alexander Hernández Martínez Jefe Oficina de Sistemas
Código de archivo: 140155

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE MODIFICACIÓN**
1	26/03/2019	N/A