1. OBJETIVO

Ampliar la descripción de las tareas para realizar la gestión de incidentes de seguridad de la información; en complemento al flujograma de gestión de incidentes de seguridad de la información y digital.

2. ALCANCE

Aplica para los funcionarios, contratistas y terceros que gestionen información de la CGN.

3. CONSIDERACIONES

La gestión de incidentes de seguridad de la información es un proceso dinámico con el propósito de detectar, reportar, evaluar, responder, tratar y aprender de los eventos e incidentes de seguridad en la CGN.

Este instructivo está alineado con la Guía para la Gestión y Clasificación de Incidentes de seguridad de la Información[1] de MinTic.

4. DEFINICIONES

Activo de información: recurso esencial para el funcionamiento de una organización; puede ser tangible o intangible y está relacionado con la creación, almacenamiento, manejo o transmisión de información.

Contención de incidente: consiste en la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, como, por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.

Información confidencial: información que se debe proteger de la indisponibilidad, el acceso no autorizado, la modificación o la divulgación pública debido a posibles efectos adversos en una persona, organización, seguridad nacional o seguridad pública.

Interrupción: incidente ya sea anticipado o imprevisto, que causa una desviación negativa y no planificada de la entrega prevista de productos y servicios según los objetivos de una organización.

[1] articles-5482_G21_Gestion_Incidentes.pdf (mintic.gov.co)

Gusano Informático: es un tipo de programa de software malintencionado cuya función principal es infectar otros equipos mientras permanece activo en los sistemas infectados.

Keylogger: es un tipo de tecnología de vigilancia utilizada para monitorear y registrar cada pulsación de tecla escrita en el teclado de una computadora específica. Este tipo de software malicioso también está disponible para su uso en teléfonos inteligentes, como iPhone de Apple y dispositivos Android.

Phishing: el phishing es una forma de fraude en la que el atacante intenta obtener información como credenciales de inicio de sesión o información de cuenta, haciéndose pasar por una entidad o persona de buena reputación en correo electrónico, mensajería instantánea u otros canales de comunicación.

Política: intenciones y dirección de una organización, expresadas formalmente por su alta dirección.

Ransomware: el ransomware es un software malicioso utilizado por cibercriminales para secuestrar los datos de la víctima y pedir un pago para la recuperación de los mismos. El pago es generalmente exigido a través de BitCoins u otras monedas virtuales para ocultar la identidad del cibercriminal.

Tailgating: también conocido como piggybacking, es una violación de seguridad física en el que una persona no autorizada sigue a un individuo autorizado con el fin de obtener acceso a un área restringida.

Violación de la seguridad de la información: compromiso de seguridad de la información que conduce a la destrucción, pérdida, alteración, divulgación o acceso no deseados a, información protegida, transmitida, almacenada o procesada de otro modo.

5. CONTENIDO

5.1. LINEAMIENTOS DE OPERACIÓN

a. Exigir a los funcionarios y contratistas que utilizan los servicios tecnológicos y sistemas de información proporcionados por la CGN que identifiquen y denuncien cualquier debilidad o vulnerabilidad que comprometa la seguridad de la información, al correo electrónico seguridadinformatica@contaduria.gov.co.

b. Mantener el equipo de respuesta a incidentes de seguridad de la información conformado por:

- Oficial de seguridad de la información o quien haga sus veces.
- Líder de la mesa de servicio.
- Administrador del recurso afectado.
- Coordinador del GIT Apoyo Informático.

c. Adelantar medidas para la prevención de incidentes tales como:

- Análisis periódico de riesgos de seguridad de la información.
- Auditorías internas periódicas.
- Realizar campañas periódicas de sensibilización a funcionarios y contratistas acerca de las políticas de seguridad de la información, procedimiento de seguridad de la información y lecciones aprendidas producto de la gestión de incidentes de seguridad de la información y digital.
- Administración de actualizaciones de software.
- Aseguramiento de servidores expuestos hacia internet.
- Seguridad en la red.
- Protección contra código malicioso.
- Gestión de vulnerabilidades técnicas.
- Retroalimentar en función de las lecciones aprendidas de los eventos e incidentes de seguridad de la información y digital para reducir la probabilidad o impacto de incidentes futuros.

d. Diligenciar el formato GTI10-FOR01 – registro de incidentes de seguridad de la información, incluyendo las lecciones aprendidas del incidente reportado en los campos correspondientes, evidenciando la

experiencia y las mejoras aplicadas identificando las deficiencias que lo generaron.

e. Ejecutar las acciones previstas en el flujograma "Gestión de incidentes de seguridad de la información".

5.2. IDENTIFICACIÓN DEL INCIDENTE O EVENTO

Para determinar si el evento reportado es un incidente de seguridad de la información, se deben tener en cuenta las siguientes definiciones:

Evento de Seguridad de la Información: es la presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información, la falla de las salvaguardas o una situación desconocida previamente que puede ser pertinente para la seguridad. En resumen, el evento se clasifica como "Evento de seguridad" cuando la confidencialidad, integridad o disponibilidad de la información no se ha comprometido aún o su probabilidad de afectar negativamente la información del negocio es baja.

Incidente de Seguridad de la Información: un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer (o ya ha comprometido) de forma negativa las operaciones del negocio y de amenazar la seguridad de la información.

Ejemplos:

- Interrupción de los servicios tecnológicos (o petición de servicio), comunicada por usuario o generada automáticamente por aplicaciones
- Fallo de sistema de almacenamiento, falla en equipos de seguridad perimetral, caída del canal WAN, entre otros.
- Presencia de código malicioso, virus o comportamiento anómalo de los equipos.
- Fuga, pérdida o robo de información.
- Acceso físico y lógico no autorizado.

5.3. ANÁLISIS DEL INCIDENTE

Las categorías para clasificar incidentes de seguridad de la información, que se describen a continuación, se basan en los criterios de integridad, confidencialidad y disponibilidad

5.3.1 Clasificación del incidente

- **Acceso lógico no autorizado.** Acceso no autorizado a sistemas de información, servidores, equipos de cómputo o dispositivos de red de la Entidad.

- **Acceso físico no autorizado.** Acceso a las instalaciones de la CGN sin autorización o sin el debido registro en la recepción.

- **No disponibilidad de servicios o sistemas.** Es un evento no planificado que afecta la disponibilidad de la información dentro de una organización. Se produce cuando los servicios informáticos o los sistemas no están disponibles para su uso previsto debido a problemas técnicos, errores humanos, ataques maliciosos u otras causas. Esto puede resultar en la interrupción parcial o total de la operación de los servicios de TI, lo que puede causar pérdidas financieras, daño a la reputación y afectar la satisfacción del usuario interno o externo.

- **Modificación de recursos no autorizado.**Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.

- **Uso inapropiado de recursos.** Violaciones a las políticas de uso aceptable de los activos.

Es frecuente que existan múltiples incidentes concurrentes, razón por la cual es necesario determinar un nivel de prioridad para la resolución de estos. El nivel de prioridad se basa esencialmente en dos parámetros, impacto y urgencia:

5.3.2. Impacto

Será definido por el valor del activo de información o activos afectados. Para ello, se tendrá en cuenta la valoración de dicho activo según el inventario de

activos de información.

- **Menor.** El incidente afecta activos de información con nivel de importancia bajo, que no impacta directamente los objetivos estratégicos de la CGN.

- **Moderado.** El incidente afecta activos de información con valoración media, que puede afectar los objetivos de un proceso o de seguridad de la información.

- **Mayor.** El incidente afecta activos de información con nivel de importancia alto, impactando directamente los objetivos estratégicos y/o de seguridad de la información.

- **Bloqueante.** El incidente afecta activos de información con nivel de importancia crítico, impactando directamente los objetivos estratégicos y/o de seguridad de la información. Se incluyen en esta categoría aquellos incidentes que afecten la imagen, reputación o que involucren aspectos legales.

5.3.3 Urgencia

Depende del tiempo máximo en el cual se debe resolver el incidente:

- **No urgente.** El incidente no afecta el normal funcionamiento de la CGN y el tiempo de espera puede ser prolongado.

- **Normal.** El tiempo de espera por parte de los afectados es moderado, dado que interrumpe actividades que no son críticas para la entidad y afecta a una persona o a un grupo pequeño de personas.

- **Urgente.** El tiempo de espera por parte de los afectados es corto, dado que afecta gravemente la seguridad de la información e involucra uno o varios procesos de la CGN.

- **Crítica.** El tiempo de espera por parte de los afectados es mínimo, dadoque afecta gravemente la seguridad de la información e involucra a terceros (por ejemplo, entes de control, ciudadanos).

Prioridad y Tiempos de atención del incidente

La prioridad del incidente determina los tiempos de atención, ésta se calcula en función de la urgencia y el impacto del incidente, como se muestra en la siguiente tabla:

PRIORIDAD						
URGENCIA	Crítica	4	4	8	12	16
	Urgente	3	3	6	9	12
	Normal	2	2	4	6	8
	No urgente	1	1	2	3	4
			1	2	3	4
			Menor	Moderado	Mayor	Bloqueante
			IMPACTO			

PRIORIDAD	TIEMPO DE ATENCIÓN
Crítica	Antes de 1 hora
Alta	Entre 1 y 3 horas
Media	Entre 3 y 12 horas
Baja	Entre 12 y 24 horas

5.3.4 Escalamiento de Incidentes de seguridad de la información

Para la atención de incidentes de seguridad de la información, la Entidad cuenta con los siguientes niveles:

- **Primer Nivel.** Es la atención a eventos e incidentes brindada por Soporte Técnico y que en primera instancia se puedan solucionar mediante validaciones y asistencias remotas.

- **Segundo Nivel.** Atención especializada por parte de los Administradores TICs que pertenecen al GIT de Apoyo Informático de

la Entidad.

- **Tercer Nivel.** Comprende la atención especializada asumida por el proveedor (comunicaciones, desarrollo, infraestructura tecnológica, hosting) o personal especializado, por ejemplo, analistas forenses.

5.4. CIERRE DEL INCIDENTE

Las actividades post-incidentes se componen del reporte apropiado del incidente, de la identificación y registro de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias.

Las lecciones aprendidas deben identificarse y documentarse después de un incidente grave, y periódicamente después de los incidentes menores, siendo útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes, facilitando las siguientes actividades:

- Conocer exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Validar los procedimientos documentados.
- Establecer que debería hacerse la próxima vez que ocurra un incidente similar.
- Implementar acciones correctivas que puedan prevenir incidentes similares en el futuro.
- Identificar cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.