Proceso: Gestión de TI
PROCEDIMIENTO NOTIFICACIÓN Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
Versión: 1
TI.PR.01

1. OBJETIVO

Establecer las actividades a seguir para la notificación, atención y manejo de los incidentes de seguridad de la información que se presenten en la **Agencia Nacional Digital – AND,** con el fin de mitigar los eventos que afecten la seguridad de los activos de información, para que sean comunicados y gestionados oportunamente, implementando las acciones correctivas y oportunidades de mejora correspondientes.

2. ALCANCE

Este procedimiento aplica a todos los trabajadores, contratistas y proveedores que tienen acceso a los activos de información de la Agencia Nacional Digital para notificar y reportar los eventos y/o incidentes que puedan afectar la seguridad de la información.

3. DEFINICIONES

a) **Activo:** Todo lo que tiene valor para la Agencia Nacional Digital. Existen diferentes tipos de activos como: Información, software, físico (como equipo de cómputo, documentos físicos), servicios, personas.

b) **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Organización[1].

c) **Amenaza Persistente Avanzada (APT):** Ataques concretos dirigidos contra la Entidad, con mecanismos muy sofisticados de ocultación, anonimato y persistencia. Habitualmente esta amenaza emplea técnicas de ingeniería social y el uso de procedimientos de ataque conocidos.

d) **Atención de Incidentes de Seguridad de la información:** Es cuando se recibe y resuelve los incidentes de seguridad de acuerdo con las condiciones establecidas.

e) **Defacement a un sitio web:** Es el término que se utiliza cuando existe una desfiguración o cambio producido por un atacante de manera intencional en un sitio web y con propósitos de afectar la reputación de la organización.

f) **Evento de Seguridad de la información:** Actividad sospechosa de seguridad de la información que requiere ser analizada por el oficial de seguridad y el equipo directivo de la Agencia Nacional Digital.

[1] Tomado del Glosario de http://www.iso27000.es/glosario.html

g) Guía: Documento que orienta los pasos técnicos para la gestión de los incidentes de seguridad de la información de la Agencia Nacional Digital.

h) **Incidente de Seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que compromete la operación de la Agencia Nacional Digital.

i) **Ingeniería Social:** Técnica utilizada para obtener información sensible como claves de acceso de la víctima.

j) **Malware:** Es un software malicioso que tiene como objetivo dañar o infiltrarse en un sistema de información.

k) **Recolección Evidencia Digital:** Es cuando se realiza la toma, preservación y documentación de evidencia cuando sea requerida.

l) **Responsable del activo:** Persona o grupo de personas asignadas que hace uso del activo de información.

m) **Rootkit:** Es una herramienta con fines de ocultar actividades ilegítimas en un sistema después de ser instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo.

n) **Ransomware:** Tipo de malware que infecta el equipo y secuestra la información del usuario cifrándola, dejando de forma ilegible y requiere de la contraseña de descifrado. Pide al usuario un rescate económico a cambio de esta contraseña para recuperar la información.

o) **Snifing:** La acción de monitorizar la información que circula por la red con el objeto de capturar información.

p) **Suplantación de identidad:** Un atacante se hace pasar por otra persona o empresa para cometer fraudes.

4. DOCUMENTOS DE REFERENCIA

- Política de Seguridad de la Información de la Agencia Nacional Digital.
- Política de Gestión de Incidentes de Seguridad de la Agencia Nacional Digital.
- ISO 27035:2012
- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información: https://mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- Guía Nacional de Notificación y Gestión de Ciberincidentes. https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

5. NIVEL DE IMPACTO

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE IMPACTO	
NIVEL	**DESCRIPCIÓN**
CRÍTICO	- Afecta a la seguridad nacional. - Afecta a la seguridad y privacidad o intimidad ciudadana, con potencial peligro para la vida de las personas. - Afecta a una infraestructura crítica. - Afecta a sistemas clasificados como CRÍTICOS en la operación de la Entidad. - Afecta a más del 90% de los sistemas de la Entidad. - Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios. - Para resolver se requiere de periodo de un mes. - Con impacto económico muy elevado. - Daños reputacionales muy elevados. - Afecta las actividades operacionales y/o misionales.
ALTO	- Afecta a más del 50% de los sistemas de la Entidad. - Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios. - Para resolverse requiere de 5 a 10 días. - Con Impacto económico alto. - Daños reputacionales de difícil reparación.
MEDIO	- Afecta a más del 20% de los sistemas de la Entidad. - Interrupción en la prestación del servicio superior al 5% de usuarios. - Para resolverse requiere de 1 a 4 días. - Con Impacto económico medio. - Daños reputacionales aceptables.
BAJO	- Afecta a los sistemas de la organización. - Interrupción de la prestación de un servicio. - Para resolver se requiere de un día. - Con Impacto económico bajo. - Daños reputacionales puntuales.

6. EJEMPLOS DE TIPOS DE INCIDENTES SEGÚN SU NIVEL DE IMPACTO

NIVEL DE IMPACTO	TIPO DE INCIDENTE
CRÍTICO	- Amenaza Persistente Avanzada (APT). - Daños en infraestructuras clasificadas como críticas. - Borrado de información en un servidor crítico de la Entidad. - Interrupción de la operación de la Entidad por causa de acceso físico o lógico no autorizado a los activos de información. - Desastre natural con pérdidas totales.

	- Distribución de malware. - Robo de información. - Secuestro de datos.
ALTO	- Denegación de servicio en la Entidad. - Acceso no autorizado y afectación a la información. - Modificación no autorizada de información. - Explotación de vulnerabilidades desconocidas. - Intento de acceso con credenciales vulneradas. - Desastre natural con pérdidas parciales. - Pérdida de datos. - Defacement a un sitio web de la Entidad.
MEDIO	- Ataque de ingeniería social. - Explotación de vulnerabilidades conocidas. - Compromiso de cuentas con privilegios del sistema de la Entidad. - Exposición intencional o involuntaria de información confidencial de clientes. - Uso no autorizado de recursos. - Suplantación de identidad. - Revelación de información. - Sistema vulnerable. - Violaciones a las medidas de seguridad física. - Sistemas operativos mal-configurados o configurados en forma deficiente. - Falla en base de datos. - Instalación de un Rootkit.
BAJO	- Escaneo de redes para obtener información. - Realiza sniffing para el análisis de paquetes con software no autorizado. - Compromiso de cuenta sin privilegios. - Mal uso de los sistemas de información. - Afectación de estaciones de trabajo de la Entidad por infección masiva de virus. - Cuentas de usuarios o de acceso a plataformas bloqueadas después de múltiples intentos fallidos. - Uso inapropiado de los recursos de la red. - Falla de la red de comunicaciones. - Falla en los programas de aplicaciones.

7. DESCRIPCIÓN

ITEM	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	PUNTO DE CONTROL	REGISTRO
1	Reportar el evento y/o incidente ocurrido al Oficial de Seguridad de la información o quien haga sus veces e informar al(la) Subdirector(a) de su área inmediatamente. El activo de información no debe ser utilizado hasta recibir indicaciones del Oficial de Seguridad y Privacidad.	Responsable del Activo	N.A.	N.A.

2	Diligenciar el Formato para reporte de incidentes de seguridad con la información del evento y/o incidente.	Responsable del Activo y/o Subdirector(a) área.	Reporte del incidente.	Formato Reporte de incidentes diligenciado
3	Enviar el formato diligenciado al correo del Oficial de Seguridad de la información o quien haga sus veces, Profesional Jurídica u oficial de datos personales o quien haga sus veces y al Profesional de apoyo administrativo TI inmediatamente se detectó el evento y/o incidente.	Responsable del Activo y/o Subdirector(a) área.	Correo enviado.	Correo enviado.
4	Dar acuse de recibido del formato y definir el tipo de incidente para realizar el correspondiente escalamiento, tomar las acciones según lo establecido en la Guía de incidentes de seguridad de la información y dar respuesta al responsable del activo informando las acciones que debe seguir.	Oficial de Seguridad de la información o quien haga sus veces, Profesional Jurídica u oficial de datos personales o quien haga sus veces y al Profesional de apoyo administrativo TI.	N.A.	Correo respuesta al responsable del activo.
5	Elaborar el reporte de las acciones tomadas en el formato de atención y clasificación de incidentes de seguridad y enviar a la dirección para su conocimiento y toma de decisiones si aplica. **Nota:** En caso de que el incidente de seguridad de la información afecte los Servicios Ciudadanos Digitales informar al Ministerio de Tecnologías de la Información y las Comunicaciones y reportar los incidentes a los ciudadanos titulares de la información afectados. En caso de afectación a información personal, reportar el incidente a la SIC, conforme a lo establecido en el Capítulo Segundo del Título V de la Circular única.	Oficial de Seguridad de la información o quien haga sus veces, Profesional Jurídica u oficial de datos personales o quien haga sus veces y al Profesional de apoyo administrativo TI.	Reporte de las acciones tomadas para la solución del incidente.	Formato de atención y clasificación de incidentes de seguridad diligenciado.
6	Realizar seguimiento de las acciones tomadas para solución del incidente con el propósito de evaluar su efectividad.	Oficial de Seguridad de la información o quien haga sus veces, Profesional Jurídica u oficial de datos personales o quien haga sus veces y al Profesional de apoyo administrativo TI.	Evaluación de la efectividad de las acciones.	Formato listado de chequeo diligenciado
7	Elaborar los planes de mejora que apliquen.	Oficial de Seguridad de la información o quien haga sus veces, Profesional Jurídica u oficial de datos personales o quien haga sus	N/A	Formato de plan de mejora diligenciado

		veces y al Profesional de apoyo administrativo TI.		

8. FORMATOS ASOCIADOS

Los siguientes formatos hacen parte del presente procedimiento:

- TI.GU.01 Guía de Incidentes de seguridad de la Información.
- TI.FT.01 Formato Reporte de incidentes de seguridad.
- TI.FT.02 Formato Atención y clasificación de incidentes de seguridad.
- TI.FT.03 Formato listado de chequeo.
- SM.FT.01 Formato plan de mejora.

9. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
1	16/08/2019	Emisión del documento

Elaboró	Revisó	Aprobó
Germán Darío Baquero Salamanca Profesional de Seguridad y Privacidad	Diana Cristina Gil Cuervo Profesional Jurídica Johanna Catherine Laverde Moncada Profesional de Procesos	Lina María Cruz Silva Subdirectora de Servicios Ciudadanos Digitales Maria Carolina Rodriguez Subdirectora Administrativa y Financiera