1. OBJETIVO

Gestionar los eventos o incidentes de seguridad de la información, con el fin de responder a ellos de forma oportuna evaluando el impacto que pueda llegar a presentar en la entidad referente a confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Inicia con el reporte del evento o incidente de seguridad y finaliza con la notificación de la solución del incidente.

3. ENTRADAS

A continuación, se definen las entradas necesarias para la atención de solicitudes de incidentes de seguridad:

✓ Reporte de incidentes de seguridad a través de la mesa de ayuda.
✓ Reporte de advertencias o alertas tempranas de seguridad de entidades de control externas.

4. LINEAMIENTOS DE OPERACIÓN

- El oficial de seguridad o quien haga sus veces debe mantener actualizados los contactos de grupos de interés de seguridad con el fin de prevenir incidentes de seguridad en la información y a los cuales sea posible acudir en caso de que estos incidentes se materialicen.
- El oficial de seguridad es responsable de inscribirse a boletines, comunicados, foros y participar en charlas, capacitaciones o talleres que realicen los grupos de apoyo como COLCERT, CSIRT, Centro Cibernético de la policía, MINTIC, entre otros; así mismo recibir y notificar a los servidores públicos avisos anticipados de alertas o vulnerabilidades detectadas por los grupos de apoyo con la finalidad de prevenir incidentes de seguridad en el instituto.
- Los eventos o incidentes de seguridad deben ser reportados a través de la mesa de ayuda para su debida identificación y gestión teniendo en cuenta la siguiente catalogación:
  - Hacer uso de la información del instituto con el fin de obtener beneficio propio o de terceros.
  - Transferir, divulgar o publicar información reservada del instituto sin previa autorización del responsable.
  - Descargar software que no sea licenciado a través de internet sin la debida autorización del área de Tecnología.
  - Robo de información sensible del instituto.
  - Robo o pérdida de equipos de cómputo y medios removibles con información sensible del instituto.
  - Accesos no autorizados a sistemas de información.
  - Accesos no autorizados a bases de datos.
  - Cambios o modificaciones de los registros de la base de datos sin previa autorización o que no esté definido a través de un control de cambios.
  - Envío de cualquier comunicación electrónica fraudulenta.
  - Denegación de acceso a los servicios como aplicaciones, sitios web, equipos en la red, afectando las labores diarias de los funcionarios y contratistas.

- Denegación del servicio por la ejecución de virus que se propago por la red generando vulnerabilidades.
- Amenazas a través del correo electrónico institucional que generen un impacto sobre la seguridad de la información del instituto.
- Generación, descarga o distribución de código malicioso.
- Fallas o caídas de los sistemas de información y pérdida prolongada de servicios a cargo del ICANH.
- Realizar copias no autorizadas de software o información.
- Sustraer equipos de cómputo con información sensible sin autorización del área de Almacén, y Tecnología.

- Los funcionarios y contratistas deben reportan los eventos o incidentes de seguridad a través de la mesa de ayuda medio por el cual se realiza la debida gestión y tratamiento en caso de que pueda ser un riego potencial.
- El oficial de seguridad o quien haga sus veces es el responsable de validar si el incidente de seguridad reportado se puede catalogar o no como un incidente de seguridad y según lo identificado se debe dar respuesta al usuario.
- El oficial de seguridad o quien delegue procede a determinar el tipo de incidente de seguridad según lo establecido en la **guía de incidentes de seguridad de la información,** y clasificarlo como corresponda en el formato establecido de registro de incidentes o eventos de seguridad.
- Cuando se identifique que un incidente de seguridad es real, el oficial de seguridad o quien haga sus veces debe evaluarlo en función del impacto que puede causar en el Instituto, en cuanto a: Confidencialidad en la información, credibilidad o imagen, legal y operativo según lo establecido en el plan de tratamiento de riesgos.
- El oficial de seguridad es el encargado de definir la solución o el tratamiento al incidente reportado, en caso de que no sea posible encontrar una solución, debe contactar a los grupos de apoyo y autoridades en el tema.
- Realizar campañas de sensibilización de seguridad a los funcionarios y contratistas para prevenir riesgos en ocurrencias de incidentes de seguridad los cuales pueden generar afectación para el instituto.
- El oficial de seguridad o designado para la solución del incidente debe identificar las lecciones aprendidas para realizar planes de mejora, definiendo medidas de seguridad fuertes y para ello se debe identificar lo siguiente:

  - Qué sucedió, en qué momento, quien y como se gestionó el incidente.
  - Detalle de las medidas y acciones que se realizaron para facilitar la recuperación eficientemente.
  - Documentar la gestión realizada y que debería realizarle la próxima vez que ocurra un incidente similar.
  - Establecer acciones correctivas que pueden prevenir incidentes similares en el futuro según lo aprendido.
  - Cuáles herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

- El oficial de seguridad debe determinar si el incidente de seguridad amerita recolección de la evidencia, en dado caso, se procede a realizar la recolección ya sea física o digital, procurando no realizar ninguna alteración de esta y cumpliendo con lo establecido en la guía para la gestión de incidentes de seguridad.
- Dado el caso, que en el análisis de las evidencias realizado por Control interno disciplinario y el oficial de seguridad del instituto, se determine necesario iniciar una acción legal, se debe iniciar un proceso disciplinario.

5. DEFINICIONES

- **Activo de información:** Un activo es aquello que tiene valor para la organización y es importante salvaguardar
- **Ciberseguridad:** Es el proceso de proteger activos de información que son almacenados, procesados y transportados a través de los sistemas de información.
- **COLCERT:** Es el grupo de respuesta a emergencias cibernéticas de Colombia, cuyo propósito es coordinar las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.
- **CSIRT:** Es el equipo de respuesta a incidentes de seguridad informática de la Policía Nacional CSIRT-PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática.
- **Denegación de servicios:** Un ataque de denegación de servicios inhabilita el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática.
- **Eventos de seguridad:** Es un cambio que se presenta en la operación de red o de servicios de tecnología indicando que una política de seguridad pudo haber sido vulnerada o una protección de seguridad definida ha fallado
- **Incidentes de seguridad:** Es el intento de acceso, uso, modificación, destrucción de la información sin autorización, accesos y/o bloqueos de la infraestructura tecnológica y violación al manual de políticas de seguridad de la información.
- **Protocolo:** Es un conjunto de reglas o pasos a seguir para solventar una situación.
- **Seguridad de la información:** Son medidas o actividades establecidas para proteger los activos de información de la organización, reduciendo riesgos o mitigando amenazas posibles.
- **Vulnerabilidad:** Es una afectación causada por la debilidad de un software o hardware que puede ser explotada por un ataque cibernético para acceder de forma no autorizada a un sistema.

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro resultado (Documento Evidencia)	Punto de Control
1.	Reportar evento o incidente de seguridad	Reportar mediante mesa de ayuda o correo electrónico (para entes de control externos) al área de TI el evento o incidente de seguridad de la información junto con las evidencias del caso (imágenes, videos documento físico, etc.).	Funcionarios y Contratistas, entes de control externas (COLCERT, CSIRT, Comando Cibernético de la Policía)	Tiquete mesa de ayuda, correo.	
2.	Registrar el evento o incidente de seguridad	Realizar el registro del evento o incidente de seguridad de la información en el formato dispuesto para el mismo.	Oficial de seguridad / Área de tecnología.	Formato de registro de incidentes o eventos de seguridad.	
3.	Verificar el incidente reportado	Si el incidente reportado se puede catalogar como un incidente de seguridad para continuar en la siguiente actividad, de lo contrario pasar a la actividad No. 12.	Oficial de seguridad / Área de tecnología.	Formato de registro de incidentes o eventos de seguridad	Revisar que el incidente contenga toda la información y evidencia necesaria para así mismo poder catalogarlo y darle un tratamiento acorde al mismo.
4.	Asignar una prioridad de atención.	Catalogar el tipo de evento o incidente para dar el tratamiento adecuado según la prioridad asignada y el impacto que puede generar en la entidad: a) Confidencialidad de la información, b) Credibilidad o imagen, c) Legal y operativo Según lo establecido en el **plan de tratamiento de riesgos.**	Oficial de seguridad / Área de tecnología.	Formato de registro de incidentes o eventos de seguridad	Revisar que el incidente contenga toda la información y evidencia necesaria para así mismo poder catalogarlo y darle un tratamiento acorde al mismo.
5.	Divulgar incidente	Mediante correo electrónico del área de TI o memorando interno se debe informar a las instancias pertinentes (Dirección General, Líder del área funcional de TI y Jefe del área o dependencia involucrada) el incidente, su criticidad e impacto. NOTA: De acuerdo al análisis del incidente se debe analizar si es necesario informar mediante el correo electrónico del área de TI, a toda la entidad sobre el impacto y la duración del evento.	Oficial de seguridad / Área de tecnología.	Correo o memorando interno.	
6.	Dar un tratamiento adecuado al evento o incidente de seguridad.	Atender el evento o incidente de seguridad de la información según lo dispuesto en la **"Guía de gestión de incidentes de seguridad"** con la finalidad de dar una adecuado tratamiento y solución.	Oficial de seguridad / Área de tecnología.	NA	
7.	Verificar si se puede dar solución al incidente.	Si el incidente no se puede solucionar internamente se debe continuar en la siguiente actividad, de lo contrario se debe pasar a la actividad No.8.	Oficial de seguridad / Área de tecnología.	Documento del incidente de seguridad	

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro resultado (Documento Evidencia)	Punto de Control
8.	Solicitar apoyo con entidades externas.	Contactar mediante correo a los grupos de apoyo y autoridades en el tema para la solución del incidente y continuar en la actividad No.11.	Oficial de seguridad / Área de tecnología.	Documento del incidente de seguridad, correo.	
9.	Solucionar incidente internamente.	Documentar y generar el reporte de tratamiento y solución del evento o incidente de seguridad de la información en caso de que ocurrencia.	Oficial de seguridad / Área de tecnología.	Documento del incidente de seguridad	
10.	Analizar si se requiere iniciar proceso disciplinario.	Si el incidente amerita iniciar proceso disciplinario para continuar en la siguiente actividad, de lo contrario finalizar en la actividad No.12.	Oficial de seguridad / jefe Oficina Control Disciplinario Interno.	Análisis del caso.	
11.	Iniciar proceso disciplinario.	Cuando el análisis del incidente y la evidencia física o digital amerite iniciar un proceso legal, dado el incumplimiento de requisitos por parte del funcionario o contratista, se debe iniciar el proceso disciplinario pertinente acorde con lo documentado en el **Proceso Control Disciplinario.**	Oficial de seguridad / jefe Oficina Control Disciplinario Interno.	Análisis del caso.	
12.	Notificar estado del incidente.	Notificar al funcionario, contratista, externo y a las instancias que corresponda lo pertinente al estado y clasificación del incidente.	Oficial de seguridad / Área de tecnología.	Correo electrónico	

7. DIAGRAMA DE FLUJO

N.A.

8. REGISTROS (Documentos que generan evidencia de la ejecución del procedimiento)

Registro	Almacenamiento
Correo electrónico	Unidad compartida del área de tecnología/Seguridad Información/año
Memorando	Unidad compartida del área de tecnología/Seguridad Información/año
Tiquete mesa de ayuda	Unidad compartida del área de tecnología/Seguridad Información/año
Evidencias físicas o digitales	Unidad compartida del área de tecnología/Seguridad Información/año
Documento de análisis incidente de seguridad	Unidad compartida del área de tecnología/Seguridad Información/año

9. ANEXOS

Formato de registro de incidentes o eventos de seguridad.
Guía de gestión de incidentes de seguridad.
Plan de tratamiento de riesgos.

10. CONTROL DE CAMBIOS

Versión	Fecha	Descripción general del cambio
01	2022-12-09	Se actualiza el documento de acuerdo con el nuevo formato, en el cual se incluyen los lineamientos de operación, las entradas y registros que se generan como evidencia de la ejecución del procedimiento.

ELABORÓ	REVISÓ	APROBÓ
Cargo: Profesional Área de Tecnología y Sistemas de Información.	**Cargo:** Oficial de Seguridad Jefe Oficina Asesora de Planeación	**Cargo:** Líder del Área de Tecnología y Sistemas de Información
Fecha: 2022-11-11	**Fecha:** 2022-11-22	**Fecha:** 2022-12-09