PROPÓSITO

Establecer los lineamientos para gestionar los incidentes de seguridad y privacidad de la información, mediante su oportuna identificación, atención y respuesta con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la Unidad Nacional de Protección UNP.

ALCANCE

Es responsabilidad de todos los funcionarios, contratistas, colaboradores y partes interesadas de la UNP, reportar cualquier tipo de incumplimiento a las políticas y procedimientos del SGSI, de manera oportuna para buscar el tratamiento adecuado evitando que se comprometa la confidencialidad, disponibilidad e integridad de los activos de información.

RESPONSABILIDADES

RESPONSABLES	RESPONSABILIDADES
Funcionarios, contratistas, colaboradores, proveedores y terceros	Reportar eventos, solicitudes o posibles amenazas que afecten la seguridad y privacidad de la información.
Punto de contacto	Recepción y categorización de los incidentes de seguridad y privacidad de la información, a través de los siguientes canales definidos. Correo Electrónico: XXXXXXXXX@unp.gov.co Aplicación de la mesa de servicios Tel: XXXXXXX Ext xxxxx.
Responsables de los activos de información.	. **Preparación, reporte y registro de eventos e incidentes** • Establecer las características de la actividad normal de la operación de la entidad, de este modo, se pueden detectar cambios que puedan ser indicadores o advertencias de incidentes. • Verificar que el incidente de seguridad sea válido. • Activar el tratamiento de incidentes de seguridad. • Clasificar y calificar los incidentes. • Actualizar la documentación del incidente.

Equipo de Incidentes de Seguridad de la información y seguridad informática (ing. Lideres de Servicios T.I)	**Detección y análisis.** • Determinar la criticidad del incidente y describir los detalles del incidente. • Determinar grado de daño causado a los recursos o información y documentar hallazgos y daños detectados. • Determinar posibles causas del incidente. • Determinar las posibles consecuencias o impacto. **Contención, erradicación, recuperación, en la (infraestructura).** Las estrategias para evitar que el incidente siga sucediendo (contención), varían dependiendo del tipo de incidente e impacto. En las actividades para la eliminación de la causa del incidente o eliminación de todo rastro de los daños (erradicación), se realiza la eliminación de aquellos componentes asociados al incidente para resolverlo o prevenir futuras ocurrencias. Las siguientes actividades son una de las maneras de hacerlo: • Aislar los servicios, servidores y en general los recursos. informáticos afectados. • Bloquear el acceso al sistema cuando sea necesario. • Instalar los parches de seguridad, cambios de reglas del firewall o de listas de acceso en dispositivos de red. • Analizar información resultante del incidente. • Definir plan de acción para la implantación de acciones correctivas para evitar reincidencias. • Identificar amenazas a partir del incidente presentado. • Notificar sobre disponibilidad de los sistemas. • Ejecutar las acciones adicionales que se consideren pertinentes. **Investigación** Se deben recoger evidencias de los incidentes para su utilización con fines de análisis y como posibles pruebas en caso de ser requerido el

	inicio de acciones legales. Las evidencias pueden ser de sistemas de información (archivos, imágenes de discos, equipos) o cualquier otra que se considere relevante para el análisis del incidente o para inicio de procedimientos legales. Hay que tener en cuenta los siguientes aspectos en el momento de recolectar evidencias: AUTENTICIDAD: Quien haya recolectado la evidencia debe poder probar que es auténtica. CADENA DE CUSTODIA: Debe existir un registro detallado del tratamiento de la evidencia, incluyendo quiénes, cómo, dónde y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma. **Actividades Post-Incidentes.** • Notificar al Líder de seguridad de la información acerca de las acciones realizadas. • Documentar el incidente. **Cerrar incidente.**
Oficial de seguridad de la Información	El oficial de seguridad debe verificar el cumplimiento del procedimiento de gestión de incidentes de seguridad de la información y su documentación, para ello debe asegurar que se cumplan las siguientes actividades: • Recibir reportes de incidentes. • Analizar la documentación disponible del incidente. • Clasificar el nivel de criticidad. • Realizar la planificación general de la investigación. • Verificar la evidencia. • Asegurar el adecuado manejo de la evidencia. • Entregar copia de la información solicitada al responsable de la investigación. • Coordinar la ejecución de los planes de tratamiento dependiendo del tipo de incidente e impacto. • Verificar que el reporte del incidente se cierre adecuadamente.

Responsable de procesos disciplinarios	En caso de requerirse, se debe realizar la investigación pertinente para el incidente de seguridad de la información a nivel interno, cuando se encuentre involucrado un empleado.
Autoridades externas y/o entes de control.	En caso de requerirse, debe realizar la investigación pertinente para el incidente de seguridad de la información a nivel externo, cuando se encuentre involucrado un funcionario, contratista, colaborador, proveedor o tercero dado el caso en el incidente.

DEFINICIONES	
TERMINO	**DEFINICIÓN**
Activo de Información	Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensitivos o críticos para los objetivos de la entidad.
Amenaza informática	La aparición de una situación potencial o actual donde una persona tiene la capacidad de generar una agresión cibernética contra la población, el territorio, la organización política del Estado (Ministerio de Defensa de Colombia).
Activos tecnológicos	Recursos del sistema de información o relacionados con éste, necesarios para que la entidad funcione correctamente y alcance los objetivos propuestos por su dirección. Se pueden estructurar en las siguientes categorías: software, hardware, servicios, datos, comunicaciones, entre otros.
Base de datos de conocimiento en seguridad de la información	Repositorio central con información de operación de la seguridad tales como reportes, informes, investigación de incidentes, manejo de alertas entre otros.
Cadena de custodia	Registro detallado del tratamiento de la evidencia, incluyendo quiénes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma
Caso de soporte	Servicio de asistencia a equipos tecnológicos, a nivel de hardware y software.

Clasificación de la Información	Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.
Confidencialidad	La propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.
Contención	Evitar que el incidente siga ocasionando daños.
Control	Medida que permite garantizar la reducción del nivel de un riesgo específico o mantenerlo dentro de límites aceptables.
CSIRT.	Por sus siglas 'Computer Security Incident Response Team`, equipo de respuesta de incidentes de seguridad.
Custodia de la información	Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, con base en los controles de seguridad existentes en la Entidad.
Datos personales sensibles	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
Disponibilidad:	Garantía que los usuarios y procesos autorizados tengan acceso a los activos de información cuando los requieran.
Erradicación:	Eliminar la causa del incidente y todo rastro de los daños.
Evento de seguridad de la información:	Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de

	las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
Gestión de Incidentes:	Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una entidad, minimizando su impacto en el negocio y la probabilidad que se repita.
Incidente de seguridad de la información:	Un incidente de seguridad de la Información está indicado por **un único evento o una serie de eventos de Seguridad de la Información indeseados o inesperados**, que tienen una probabilidad significativa de comprometer las operaciones de la entidad y de amenazar la seguridad de la información".
Información:	La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.
Modelo de seguridad y privacidad de la información- MSPI	Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información". Fue creada por el Ministerio de Tecnologías de
Plan de Continuidad de Negocio (BCP, por sus siglas en inglés):	Procedimientos documentados que guían a las entidades para responder, recuperar y restaurar a un nivel predefinido de operación, debido a la interrupción.
Propietario de la información	Es la persona que crea un activo de información y por ende tiene la facultad de definir su clasificación y los derechos de acceso que tienen los demás usuarios.
Recursos tecnológicos	Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases

	de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento.
Repositorio de control de almacenamiento de evidencia:	Inventario centralizado para el control de la evidencia almacenada incluyendo ubicación física, responsables, custodios entre otros.
Seguridad de la Información:	Preservación de la integridad, confidencialidad y disponibilidad de la información.
SIC.	Superintendencia de Industria y Comercio.
TI	Tecnologías de Información
Vulnerabilidades	Son las debilidades, hoyos de seguridad o falencias inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por las amenazas, las cuales se constituyen en fuentes de riesgo.

MARCO LEGAL

Ley 527 de 1999. *"Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las Entidades de certificación y se dictan otras disposiciones".*

Ley 1150 de 2007. *"Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos"*

Ley 1273 de 2009. *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*

Ley 1581 de 2012. *"Por la cual se dictan disposiciones generales para la protección de datos personales"*

Decreto 1377 de 2013, por el cual se reglamenta parcialmente la ley 1581 de 2012.

Decreto 2573 de 2014. *"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".*

MARCO LEGAL

Decreto 1008 de 2018. *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".*

CONPES 3701 de 2011.Lineamientos de Política para Ciber-seguridad y Ciber-defensa

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

CONSIDERACIONES GENERALES

POLÍTICAS DE OPERACIÓN

El proceso de gestión de incidentes está enmarcado en la mejora continua. Los resultados de la gestión de incidentes deben ser documentados, esto permitirá analizar y realizar mejoras a controles existentes o implementar nuevos.

El Oficial de Seguridad de la Información debe coordinar las acciones con las partes interesadas para la atención de incidentes.

ROLES Y RESPONSABILIDADES

En las fases de la atención de incidentes de seguridad participan diferentes personas, que tienen asignados roles y responsabilidades, los cuales fueron identificados y descritos en el cuadro de Responsabilidades

REPORTE DEL INCIDENTE

Los funcionarios, contratistas, colaboradores, proveedores y terceros de la UNP, cuando identifiquen amenazas que puedan comprometer la confidencialidad, disponibilidad e integridad de la información a través de un ataque contra los activos de información o un incumplimiento de la política de seguridad y privacidad de la información o del SGSI, deben reportar de forma inmediata el incidente a la mesa de servicios, usando los canales oficiales establecidos por la entidad.

Correo Electrónico: XXXXXXXXX@unp.gov.co
Aplicación de la mesa de servicios
Tel: XXXXXXX Ext xxxxx.

Para la gestión del incidente se debe diligenciar el formato XXXXXXXX Incidentes de Seguridad de la información, que hace parte integral del SGSI.

CLASIFICACION DEL INCIDENTE DE SEGURIDAD

La priorización del incidente será tenida en cuenta con base en la siguiente tabla, la cual indica el nivel de impacto en la compañía.

Clasificación	Descripción
Intolerable (5)	• Impacto alto en uno o más componentes de los activos críticos. • Interrupción total de las operaciones. • Se comprometió la confidencialidad, integridad y disponibilidad de información confidencial (datos personales, secretos comerciales o industriales, entre otros) de la organización. • Sistemas de información Core totalmente comprometidos y/o vulnerados. • Amenaza a la integridad de las personas. • Intervención por parte de un ente de control u otro ente regulador. • Imagen institucional afectada por incumplimiento al código de ética corporativo
Importante (4)	• Compromiso importante en los sistemas pertenecientes al área de tecnología y estaciones de trabajo de usuarios con funciones críticas. • Afectación importante de activos de información con controles operativos y/o administrativos. • Interrupción parcial de las operaciones. • Pérdida o robo de información catalogada con secreto comercial o industrial. • Imagen institucional afectada por incumplimiento al código de ética corporativo. • Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.
	• Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo. • Afectación parcial de activos de información con controles operativos y/o administrativos.

	Moderado (3)	• Compromete medianamente el buen nombre de la empresa. • Afecta medianamente a las personas. • Impacta un número moderado de sistemas o personas • Reprocesos de actividades y aumento de carga operativa. • Imagen institucional afectada por incumplimientos en la prestación del servicio a los usuarios o ciudadanos. • Investigaciones penales, fiscales o disciplinarias.
	Toreable (2)	• No afecta la integridad o la vida de las personas. • Impacta un número mínimo de activos no críticos. • Afecta a sistemas o servicios que apoyan a una sola dependencia o proceso no critico de la empresa. • Interrupción de las operaciones de la empresa por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
	Trivial (1)	• No hay interrupción de las operaciones. • No genera sanciones económicas y/o administrativas. • No afecta las relaciones con los clientes. • No afecta la confidencialidad, integridad o disponibilidad de la información.

Con el propósito de hacer una adecuada gestión de los incidentes de seguridad y como lo exige la Super intendencia de Industria y Comercio, se deben identificar los incidentes relacionados con afectación a datos personales. En la siguiente tabla se presenta una lista de incidentes en los que se incluyen aquellos exigidos por la SIC y que tienen afectación sobre datos personales.

TIPOS DE INCIDENTES DE SEGURIDAD

Ley 1581	Tipo de incidente
S	Afecta la confidencialidad de los datos personales
S	Afecta la disponibilidad de los datos personales
S	Afecta la Integridad de los datos personales
S	Afecta confidencialidad y disponibilidad de los datos personales
S	Afecta confidencialidad e Integridad de los datos personales
S	Afecta disponibilidad e Integridad de los datos personales
S	Afecta la confidencialidad, disponibilidad e integridad de los datos personales
N	Acceso no autorizado a la información.
N	Divulgación de información confidencial.
N	Denegación del servicio.
N	Daño de la información.
N	Ataques externos o internos.
N	Ataques dirigidos.
N	Pérdida o robo de la información.
N	Modificación no autorizada.
N	Información no actualizada.
N	Mala gestión del conocimiento.
N	Diligenciamiento errado de formatos.

N	Perdida o daño de la documentación.
N	Daños sobre activos de información
N	Uso indebido de activos de información.
N	Uso indebido de software.
N	Uso Indebido de cuentas de usuario.
N	Uso indebido de información crítica
N	Uso prohibido de un recurso informático o de red de la UNP.
N	Divulgación no autorizada de información personal.
N	Intrusión física.
N	Destrucción no autorizada de información.
N	Robo o pérdida de información.
N	Interrupción prolongada en un sistema o servicio de red.
N	Modificación, instalación o eliminación no autorizada de software.
N	Acceso o intento de acceso no autorizado a un sistema informático.
N	Suplantación de Identidad
N	Ingeniería social, fraude o phishing.
N	Modificación no autorizada de un sitio o página web de la UNP.
N	Eliminación insegura de información.
N	Modificación o eliminación no autorizada de datos.

N	Anomalía o vulnerabilidad técnica de software.
N	Amenaza o acoso por medio electrónico.
N	Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.)

CAUSAS (VULNERABILDIADES) DE LOS INCIDENTES DE SEGURIDAD.

En la siguiente tabla, se listan las causas en los incidentes de seguridad de la información que tienen que ver con datos personales.

Causas de incidentes que afectan datos personales - SIC

Causas de los incidentes que afectan datos personales
Fraude interno
Fraude externo
Daño a activos físicos
Falla de tecnología informática
Ejecución y/o administración de procesos
Falla por negligencia o actos involuntarios de los titulares

Fuente: SIC

Otras causas de los incidentes

Otras causas de los incidentes
Carencia de procedimientos adecuados de reutilización de medios y computadores.
Contratos vencidos o falta de contratos con soportes

Demoras en la asignación de presupuesto para operación y mantenimiento de TI, y dificultad para su ejecución
Desactualización del antivirus
Desconocimiento o falta de capacitación en seguridad de la información
Equipos de cómputo desatendidos
Errores en la asignación de permisos
Errores en la definición de roles en las aplicaciones
Falta Consideraciones de la seguridad en los acuerdos con terceras partes
Falta de aplicación de buenas prácticas en la configuración de aplicaciones.
Falta de capacitación de los usuarios de acuerdo con su rol.
Falta de capacitación en el uso de los aplicativos.
Falta de capacitación en seguridad de la información
Falta de capacitación para las funciones asignadas
Falta de conciencia respecto a la seguridad de la información.
Falta de control con el uso de dispositivos de almacenamiento externos.
Falta de controles contra código malicioso.
Falta de controles de acceso a la información
Falta de definición de procedimientos para el almacenamiento y comprobación de las copias de seguridad.

Falta de definición y ejecución de procedimientos de mantenimiento.
Falta de documentación de los servicios y/o aplicaciones
Falta de Documentación de pruebas.
Falta de estrategias de escalabilidad.
Falta de mantenimiento.
Falta de oportunidad de negocio
Falta de planes de recuperación.
Falta de planes de sensibilización en seguridad de la información
Falta de políticas / normas / procedimientos de seguridad de la información
Falta de políticas de actualización en el software base.
Falta de políticas de clasificación de la información.
Falta de políticas de seguridad
Falta de políticas de transmisión de documentos
Falta de políticas para el manejo de contraseñas
Falta de políticas para el tratamiento de la información
Falta de políticas para el uso de dispositivos de almacenamiento externos.
Falta de políticas para inactivación de usuarios
Falta de políticas que rijan el uso de los activos de información.

Falta de políticas, normas y procedimientos de seguridad de la información.
Falta de procedimientos para el manejo de la información
Falta de Procedimientos para el tratamiento de la información.
Falta de protección contra virus y código malicioso.
Falta de revocación de los derechos de acceso al activo de información una vez el funcionario cambie de rol o se retire de la organización
Falta de segregación de las funciones
Falta de sensibilización en seguridad de la información
Falta de soporte
Falta mecanismos de monitorización de la red.
Inadecuada clasificación de activos de información.
Inadecuada prevención y detección de incendios.
Inadecuado control de acceso lógico y/o físico a los activos de información
Inexistencia de respaldo y/o custodia de los activos de información.
No existencia de un proceso de gestión de incidentes
Seguimiento y control de pago a proveedores.
Trabajo de personal externo o de mantenimiento no supervisado.
Usuarios por defecto en las configuraciones.

Fuente: Propia UNP

TIPO DE INFORMACIÓN

Información comprometida

Información comprometida	Descripción
Toda la base de datos	
Algunos datos	Datos generales
	Datos de identificación
	Datos de ubicación
	Datos sensibles
	Datos de contenido socioeconómico
	Otros datos
Otra información	

Fuente: SIC

DESCRIPCIÓN DEL PROCEDIMIENTO			
RESPONSABLE	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGSITRO Y PUNTOS DE CONTROL**
Detección y reporte del incidente			
Funcionarios, contratistas, colaboradores, proveedores o terceros.	1. Reporta el incidente de seguridad de la información.	Reportan la situación que podría derivar en un incidente de seguridad de la información. El reporte se hace utilizando los canales definidos por la entidad para este tipo de situación	Se genera a través de los canales de comunicación

			definidos por la entidad.
Punto de contacto.	2. Se recibe y registra la información básica del incidente.	Se recibe el caso y se registra en el formato establecido para ello.	Registro del número del incidente en el formato SEG-FT-008 XXXXX Incidentes de seguridad de la información. Numeral 1 y 2.
Descripción y categorización del incidente			
Oficial de seguridad Responsable del activo de información. Equipo de Incidentes de Seguridad de la información y seguridad informática (ing. Líderes de Servicios T.I)	3. Realizan de manera conjunta con el responsable del activo las siguientes actividades.	Realizan de manera conjunta con el responsable del activo las siguientes actividades. describe el incidente de seguridad. • Se categoriza el incidente de seguridad. • Se determina el grado de criticidad del incidente de seguridad.	Registro de la descripción y categorización del incidente en el formato SEG-FT-008 Incidentes de seguridad de la información, numerales 3, 3.1 y 3.2.
Tratamiento del incidente			

Oficial o líder de seguridad de la información. Responsable del activo de información Equipo de Incidentes de Seguridad de la información y seguridad informática (ing. Líderes de Servicios T.I)	4. Registrar en el formato las siguientes actividades relacionadas con el tratamiento del incidente.	Registrar en el formato las siguientes actividades relacionadas con el tratamiento del incidente. ✓ Registrar los responsables o especialistas designados por el responsable del activo de información, para el tratamiento del incidente. ✓ Describir las actividades a ejecutar para el tratamiento del Incidente de seguridad por cada uno de los responsables o especialistas, designados por el responsable del activo de información.	Registro del tratamiento del incidente en el formato SEG-FT-XXX Incidentes de seguridad de la información, numerales 4, 4.1 y 4.2.
Investigación			
Oficial o líder de seguridad de la información. Responsable del activo de información. Equipo de Incidentes de Seguridad de la información y seguridad informática (ing.	5. Registrar las conclusiones sobre el incidente, teniendo en cuenta las siguientes variables.	Registrar las conclusiones sobre el incidente, teniendo en cuenta las siguientes variables. ✓ Daños identificados (activos comprometidos). ✓ Consecuencias del incidente. ✓ Probabilidad. ✓ Impacto. ✓ Nivel de criticidad riesgo. Adicionalmente se debe registrar: ✓ Las causas reales del incidente.	Registro del tratamiento del incidente en el formato SEG-FT-XXX Incidentes de seguridad de la información, numeral 5.

Líderes de Servicios T.I)		✓ Las observaciones frente a las consecuencias generadas. ✓ La manera como se dio solución al incidente. Recomendaciones.	
Oficial de seguridad de la información. Responsable del activo de información. Equipo de Incidentes de Seguridad de la información y seguridad informática (ing. Líderes de Servicios T.I)	6. Dependiendo del nivel de criticidad y las consecuencias del incidente, se debe establecer si se requiere recolectar evidencia y mantener la cadena de custodia para entregarla a las autoridades internas o externas	Dependiendo del nivel de criticidad y las consecuencias del incidente, se debe establecer si se requiere recolectar evidencia y mantener la cadena de custodia para entregarla a las autoridades internas o externas. ✓ Registra qué tipo de evidencia se está conservando a través de la cadena de custodia. (Si aplica) ✓ Describir las actividades realizadas una vez recibido el informe forense. (Si aplica) En lo que respecta a la recolección de evidencia digital, es importante reconocer las capacidades que tiene La UNP para realizar esta actividad, si no se tienen las herramientas y conocimiento adecuado, se debe contratar a un profesional en esta rama.	Registro del tratamiento del incidente en el formato SEG-FT-XXX Incidentes de seguridad de la información, numeral 6. (Tener en cuenta la guía de recolección de evidencia digital SEG-GU-002 Evidencia digital).

Oficial de seguridad de la información.	7.	Realizar de manera conjunta con el responsable del activo las siguientes actividades:	Describir las razones por las cuales se tuvo que establecer contacto con las autoridades. Internas (Procesos disciplinarios) o Externas (CSIRT, COLCERT, Fiscalía, Contraloría, especialistas forenses o consultores.	Registro del tratamiento del incidente en el formato SEG-FT-XXX Incidentes de seguridad de la información, numeral 7.
Cierre del incidente				
Oficial de seguridad de la información Responsable del activo de información.	8.	Una vez gestionado el incidente, este debe ser cerrado por el responsable del activo con la supervisión del oficial de seguridad, indicando:	Una vez gestionado el incidente, este debe ser cerrado por el responsable del activo con la supervisión del oficial de seguridad, indicando: ✓ La fecha y hora de cierre. ✓ Nombre de quien cierra el incidente. Descripción de las lecciones aprendidas, estas deben ser socializadas con todos los empleados, contratistas, proveedores y terceros según corresponda, como ejemplos de lo que podría ocurrir, cómo responder a estos incidentes y cómo evitarlos en el futuro.	Registro del tratamiento del incidente en el formato SEG-FT-008 Incidentes de seguridad de la información, numeral 8.
Responsable del activo de información. Oficial de seguridad de la información.	9.	Se debe relacionar los documentos que soportan la gestión del incidente.	Se debe relacionar los documentos que soportan la gestión del incidente. Ejemplo: correos electrónicos, comunicaciones con entes externos, imágenes, fotos, entre otros.	Registro del tratamiento del incidente en el formato SEG-FT-008 Incidentes de seguridad de la

			información, numeral 9.

CONTROL DE CAMBIOS			
VERSIÓN INICIAL	**DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO**	**FECHA**	**VERSIÓN FINAL**
00	• Se crea procedimiento de acuerdo a las necesidades del Grupo de Gestión de las Tecnologías de la Información.	XX/03/2020	**01**