La seguridad es de todos

Mindefensa

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2022

UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Oficina de Tecnologías de la Información y las Comunicaciones

CONTENIDO

1. INTRODUCCIÓN

La Dirección de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial a través de la Oficina de Tecnologías de la Información y las Comunicaciones ha establecido una política de Seguridad de la Información con lineamientos claros y orientados a que los activos de información en los que se soportan sus procesos estén debidamente gestionados a lo largo de todas sus etapas.

La Entidad se encuentra en proceso de implementación de su Modelo Integrado de Planeación y Gestión MIPG, así como de la construcción e implementación de su Modelo de Seguridad y Privacidad de la Información MSPI, este último se constituirá en el instrumento de gestión de la seguridad de la información en la Justicia Especial, indicando el tratamiento de la información recogida, producida y gestionada en los procesos misionales, estratégicos, de apoyo y de evaluación y control que se ejecutan para el cumplimiento de su misión y visión.

La Entidad busca con este Plan de Tratamiento de Riesgos de Seguridad, articular su operación en materia de Seguridad de la Información con las entidades coordinadoras a nivel nacional CSIRT Nación y COLCERT para que de forma acompasada y armónica se de tratamiento a los incidentes de seguridad que puedan presentarse y manteniendo la reserva, disponibilidad e integridad de la información.

2. OBJETIVO GENERAL

Generar un Plan de Tratamiento de Incidentes de Seguridad de la Información claro, que siga la metodología para la gestión del riesgo e involucre a los actores, funcionarios, contratistas y entidades externas para el adecuado tratamiento de los incidentes de seguridad de la información que en la Justicia Penal Militar y Policial se puedan presentar.

3. ALCANCE

La gestión de los riesgos de seguridad en la Unidad Administrativa Especial de la Justicia Penal Militar debe ser aplicado a los Registros de Activos de Información teniendo en cuenta los lineamientos de la norma ISO 27001 para el mejoramiento, seguimiento y evaluación permanente.

4. MARCO NORMATIVO

TIPO DE NORMA	NÚMERO	AÑO	Descripción – Epígrafe
Constitución Política de Colombia	Artículo 15	1991	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales
Ley	23	1982	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar
Ley	527	1999	Ley 1273 de 2009, 2016 Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para Marco Normativo Año Descripción la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley	1273	2009	Ley 1273 de 2009, 2016 Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para Marco Normativo Año Descripción la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley	1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Ley Estatutaria	1581	2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley	1474	2011	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley	1712	2014	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto	4632	2011	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Decreto	2609	2012	Por el cual se reglamenta parcialmente la Ley 1581de 2012
Decreto	1377	2013	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto	2573	2014	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto	1494	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto	1008	2019	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital
Resolución	0137	2018	Por la cual se establecen los responsables de la Política de Gobierno Digital
Resolución	500	2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital

TIPO DE NORMA	NÚMERO	AÑO	Descripción – Epígrafe
Norma Técnica Colombiana	ISO/IEC 27001	2013	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa

5. RESPONSABLES

La elaboración del Plan de Tratamiento de incidentes de Seguridad de la Información está a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones y su aplicación estará a cargo de todos los actores involucrados, funcionarios, personal de apoyo, contratistas, personal en comisión y personal externo que en el ejercicio de sus funciones deba conocer información relacionada con la Justicia Especial.

6. DEFINICIONES

Los siguientes términos son utilizados en el contexto de la gestión de la seguridad de la información y aplican para todas sus fases y momentos, incluyendo la gestión de riesgos.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la Entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)

Amenaza: Es la causa potencial de una situación de incidente no deseado por la organización

Causa: Es todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos,

las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo es evaluada.

Control: Medida que modifica el riesgo. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma ISO 27001.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos inaceptables en el marco de la seguridad de la información e implantar los controles necesarios para proteger la misma.

Parte interesada (Stakeholder): Persona u organización que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.

Riesgo en la seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgoparticular.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo[1]

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. DESARROLLO DEL PLAN

7.1. PREPARACIÓN

La etapa de preparación para la atención de incidentes de seguridad está liderada por la Oficina de Tecnologías de la Información y las Comunicaciones a través de sus tres coordinaciones, Sistemas de Información, Plataforma Tecnológica y Redes y Comunicaciones, quienes deberán dentro de las actividades propias del desempeño de sus obligaciones velar por el cumplimiento y conocimiento de la Política de Seguridad de la Información y

[1] ICONTEC Internacional (2011)

el aseguramiento de la infraestructura que soporta la operación de los procesos de la Unidad Administrativa Especial Justicia Penal Militar y Policial.

Dentro de estas actividades de preparación se deberá como mínimo:

- **Realizar una gestión de parches de seguridad** y de actualizaciones de los componentes de software, firmware y demás actividades que permitan tener un aseguramiento frente a las vulnerabilidades detectadas por la industria o el fabricante de los componentes tecnológicos
- **Realizar un aseguramiento de la plataforma,** esta actividad comprende la configuración de los elementos tecnológicos bajo el principio del menor privilegio garantizando que se ofrecen y permiten las funcionalidades y accesos mínimos requeridos para la correcta operación, evitando configuraciones por defecto o funcionalidades, servicios de red o características adicionales que no hacen parte de lo estrictamente necesario para proveer un servicio adecuado sin el compromiso de la disponibilidad, la integridad o la confidencialidad de la información.
- **Seguridad en redes,** tanto las redes de área local LAN, cableadas alámbricas o inalámbricas, como las redes de área amplia WAN, deben ser protegidas de las amenazas que se puedan originar al interior de ellas como de las amenazas que se originen en las redes públicas, de esta forma se debe mantener una política del menor privilegio en el acceso, actualización de listas de control de acceso, listas negras, grises y blancas, actualización de plataformas de protección, antivirus, escudos anti DDoS, firewalls de red, firewalls de aplicación y demás medidas que se consideren necesarias para garantizar la seguridad de las redes de la Justicia Especial.
- **Prevención de código malicioso,** la protección de los activos de información crítica frente a amenazas debe contemplar la prevención frente a código malicioso, proveniente de vectores internos y externos por tanto la Entidad debe protegerse frente a estas manteniendo un conjunto de técnicas y productos actualizados y orientados a detener las amenazas frente a Malware, Trojans, Worms y demás software considerado maligno.
- **Sensibilización y entrenamiento de usuarios,** La Entidad a través de la Oficina de Tecnologías de la Información alentara el aumento y especialización de las capacidades técnicas y operativas en seguridad de la información, ciberseguridad y demás líneas de formación que

permitan que los funcionarios conozcan y se apropien de los estándares de seguridad.

7.1.1. RECURSOS DE COMUNICACIÓN

La Entidad cuenta con recursos de comunicación para la Política de Seguridad y el reporte de posibles eventos de seguridad así:

- **Información de contacto:** a través de la mesa de ayuda de servicios.
- **Información de escalamiento:** a través de los coordinadores de los grupos de la Oficina de Tecnología de la Información y las comunicaciones, quienes coordinaran el personal de la Entidad, proveedores y contratistas para la atención de los posibles incidentes de seguridad.
- **Información de los administradores de la plataforma tecnológica:** Administradores de infraestructura local "on premise", infraestructura en la nube, administradores de equipos de cómputo personal, administradores de infraestructura de red local y perimetral, administradores de los sistemas de información.
- **Contacto con el área de recursos humanos,** a través de la coordinación de recursos humanos y control disciplinario se pondrán en conocimiento de los eventos y sus responsables en el caso de ser necesario.
- **Contacto con entidades interesadas o grupos de interés:** CCP de la Policía Nacional, Fiscalía General de la Nación, Procuraduría General de la Nación.

La comunicación oficial de los eventos que sean catalogados como incidentes de seguridad solo se hará de forma oficial a través del jefe de la Oficina de Tecnologías de la Información y las Comunicaciones o por indicación expresa a través de los coordinadores de los grupos de la Oficina.

7.1.2. HARDWARE Y SOFTWARE

Para la gestión de la plataforma local, la Unidad cuenta con un cortafuegos (Firewall) de próxima generación Fortinet con su respectivo analizador, además de software de control de punto final con su respectiva consola, y software de monitoreo de la red LAN y WAN, Software de respaldo de imágenes de servidores y datos.

Para la gestión de la plataforma de nube pública se cuenta con Web Application Firewall (WAF) para la protección de las aplicaciones, grupos de

seguridad a nivel de los recursos, y herramientas de análisis para los eventos que se puedan presentar.

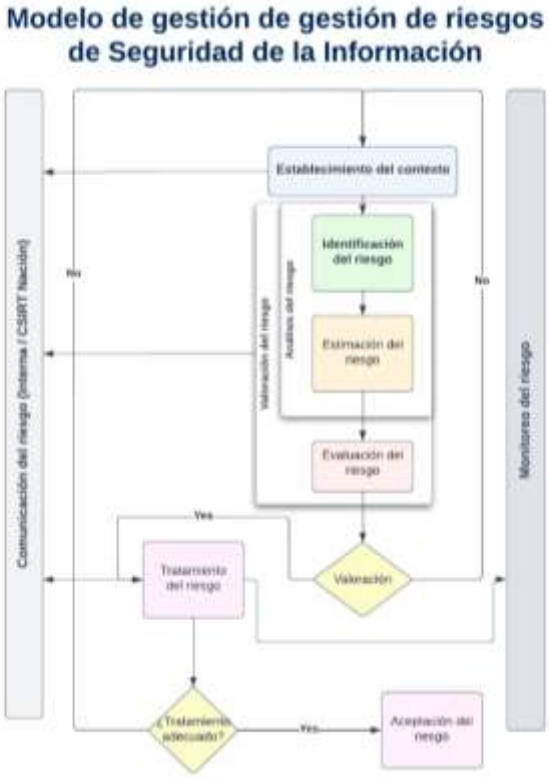
7.1.3. RECURSOS PARA EL ANÁLISIS DE INCIDENTES

Para la recolección de información de los eventos, el analizador FortiAnalyzer cuenta con los reportes y herramientas de análisis con el fin de determinar los posibles ataques en las capas de la red y de los activos que ellas conectan, además de SolarWinds para el análisis de trazas de paquetes de red, la consola de punto final McAfee permite detectar en línea los ataques que se podrían originar en las estaciones de trabajo de los usuarios, tarea a cargo del Grupo de Infraestructura Tecnológica con al apoyo de la mesa de ayuda.

7.1.4. RECURSOS PARA LA MITIGACIÓN Y REMEDIACIÓN

Con el fin de mitigar y remediar el impacto a la infraestructura tecnológica se cuenta con el software de respaldo para la información de los servidores y los servicios de red locales y remotos, y en la nube pública se cuenta con copias de imágenes de los recursos almacenados en zonas geográficas distintas.

7.2. DETECCIÓN, EVALUACIÓN Y ANÁLISIS



7.2.1. DETECCIÓN IDENTIFICACIÓN Y GESTIÓN DE ELEMENTOS INDICADORES DE UN INCIDENTE

Para la detección, diariamente se monitorean los activos a nivel de IPS, SolarWinds, y EPO con el fin de detectar anomalías, lo mismo se tienen alarmas en línea de los recursos en la nube, labor realizada por él ingeniero administrador de la plataforma tecnológica del Grupo de Infraestructura.

7.2.2. ANÁLISIS

Este inicia con el tratamiento de los riesgos cuando son catalogados como “Riesgos de Seguridad Digital” y apoyan a los propietarios de la información a identificar en una fase temprana cual es la gestión adecuada de los incidentes para los activos que han sido catalogados en el Registro de Activos de Información y clasificados con criticidad alta, según sus propiedades de confidencialidad, disponibilidad e integridad.

La criticidad del activo de información fue calculada según la Guía para la Gestión y Clasificación de Activos de la Información del MINTIC [2] en donde se tienen en cuenta los atributos de seguridad de la información de confidencialidad, integridad y disponibilidad

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

7.2.3. EVALUACIÓN

Realizada la valoración del activo de información según cada uno de los anteriores criterios, se clasifica el activo en algunos de los niveles de criticidad ALTA, MEDIA o BAJA según la guía de la siguiente forma:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o en todas las propiedades (confidencialidad, integridad y disponibilidad es alta).
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

El resultado de esta valoración se refleja en el Registro de Activos de la Información, en donde se selecciona el tratamiento a los riesgos de seguridad que se cataloguen con criticidad ALTA.

7.2.4. CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

[2] https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Con lo especificado en la metodología [3] se debe especificar la amenaza de acuerdo con la siguiente tabla de referencia:

Tipo	Amenaza
Daño físico	Fuego
	Agua
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua
	Fallas en el suministro de aire acondicionado
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida
	Espionaje remoto
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
Compromiso de las funciones	Error en el uso o abuso de derechos
	Falsificación de derechos
Pérdida de datos	Fuga de expedientes
	Consulta no autorizada
	Secuestro de expedientes

Tras la identificación y registro de la amenaza se deben especificar las vulnerabilidades especificadas por la metodología de acuerdo con la siguiente tabla de referencia:

[3] https://mintic.gov.co/portal/715/articles-61854_documento.docx

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoria
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
	Expedientes sin perfiles de acceso
	Expedientes sin cifrado
Red	Ausencia de pruebas de envió o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones

Tipo	Vulnerabilidades
	Ausencia de acuerdos de niveles de servicio (ANS/SLA)
	Ausencia de mecanismos de monitoreo para brechas de seguridad
	Ausencia de procedimientos y/o políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio o pantalla limpia entre otros)

7.2.5. PRIORIZACIÓN DE LOS INCIDENTES

La priorización de los incidentes de seguridad se da según la clasificación del activo comprometido y de su criticidad. Según el cuadro de clasificación de la sección 7.2.3.

7.2.6. TIEMPOS DE RESPUESTA

Según la clasificación de criticidad los tiempos de respuesta se darán así:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o en todas las propiedades (confidencialidad, integridad y disponibilidad es alta).	4 horas
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.	8 horas
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja	12 horas

7.2.7. DECLARACIÓN Y NOTIFICACIÓN DE INCIDENTES

La ocurrencia de un evento detectado no se considera por sí mismo un incidente de seguridad de la información, para que se dé tal declaración, se debe seguir el presente plan, y una vez surtido y su criticidad sea ALTA, el

Jefe de la Oficina de Tecnologías de la Información declarará la ocurrencia de un incidente de seguridad y realizará las notificaciones internas al Comité de Gestión y Desempeño de la Unidad a través de medio escrito y seguirá la ruta de notificación al CSIRT Gobierno del Ministerio de Tecnologías de la Información y las Comunicaciones y a las autoridades a las que haya lugar.

Como parte del plan de atención de incidentes de seguridad sí se presenta un incidente con criticidad alta (grave o muy grave) se debe realizar el reporte al CSIRT GOB de acuerdo con el formato establecido a través de los canales oficiales: Línea gratuita, buzón de correo o micrositio.

Una vez reportado el incidente se deberá continuar con la ruta de atención para recuperar los activos y procesos afectados, realizar un balance y hacer un seguimiento para extraer las lecciones aprendidas y tomar las medidas de seguridad y ajustes a los procesos que impidan que el incidente se presente nuevamente. Es importante recordar que sí el incidente se clasifica como un delito se deberá hacer la respectiva denuncia penal por cualquier funcionario de la Entidad una vez recolectadas los elementos probatorios y ante la Fiscalía General de la Nación o la Policía Nacional y/o el reporte a la Superintendencia de Industria y Comercio sí se vulneraron bases de datos que contienen datos personales.

Si es necesario preservar evidencia digital se deben conservar copias crudas, archivos de registro, bases de datos, archivos, logs de acceso, conservación de los discos duros, físicos o virtuales, equipos de cómputo, equipos de comunicaciones, que apoyen la investigación judicial y mantener su reserva a través de la Oficina de Tecnologías de la Información y las Comunicaciones.

[4]

Ilustración 1 Reporte de incidentes ante el CSIRT nación

7.3. CONTENCIÓN ERRADICACIÓN Y RECUPERACIÓN

Dependiendo de los tipos de incidentes de seguridad detectados se dará un tratamiento para su erradicación y posterior recuperación del activo comprometido, a continuación, se listan los eventos considerados y su estrategia de contención.

Incidente	Tipo de evento	Estrategia de contención
Acceso no autorizado	Sucesivos intentos fallidos de ingreso	Bloqueo de cuenta
Código Malicioso	Infección con virus	Desconexión de la red del equipo afectado
Acceso no autorizado	Compromiso del administrador	Apagado del sistema

[4] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/

Reconocimiento	Escaneo de puertos	Incorporación de reglas de filtrado en el firewall

Dependiendo de los tipos de incidentes se presentan las siguientes estrategias de recuperación de los activos comprometidos, estas actividades estarán a cargo del Grupo de Plataforma Tecnológica, el Grupo de Redes de Comunicaciones y el Grupo de Sistemas de Información con el apoyo de los proveedores externos necesarios para el restablecimiento de los activos comprometidos.

Incidente	Tipo de evento	Estrategia de erradicación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparación el sitio web
Intrusión	Instalación de un *"rootkit"*	Reinstalación del equipo y recuperación de datos

Incidente	Tipo de evento	Estrategia de recuperación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparación del sitio web

7.4. ACTIVIDADES POST-INCIDENTE

7.4.1. LECCIONES APRENDIDAS

Una vez realizada la recuperación de los activos de información comprometidos, conservada la información forense, realizadas las notificaciones internas y externas, además puesto en conocimiento de las autoridades competentes los hechos a través de los canales que las mismas dispongan para tal fin, se procederá en un término no mayor a 36 horas una reunión en forma presencial o virtual con los responsables de las infraestructuras tecnológicas, los dueños y responsables de la información para hacer un recuento de la aplicación correcta de los controles de seguridad, de la aplicación de la Política de la Seguridad de la Información, hacer un informe de los fallos ocurridos y de las acciones de mejora a ser aplicadas así como de su seguimiento y evaluación de la efectividad en prevención de incidentes futuros.

7.5. ROLES Y PERFILES NECESARIOS

Para la evaluación post-incidente, se debe contar con los siguientes roles y perfiles necesarios

Perfil / Rol	Descripción
Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones	Jefe de la OTIC de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Coordinador del grupo de Plataforma Tecnológica	Coordinador o a quien el delegue
Coordinador del grupo de Redes de Comunicaciones	Coordinador o a quien el delegue
Coordinador del Grupo de Sistemas de Información	Coordinador o a quien el delegue

Experto en seguridad en redes	Experto externo o interno con conocimiento en el incidente o administrador del recurso tecnológico
Experto en seguridad en plataforma tecnológica	Experto contratado con conocimiento en el incidente o administrador del Firewall o Protección de punto final
Dueño o administrador de la información	Dueño interno, usuario de la información o encargado de recolectarla, mantenerla o consumir la información comprometida

7.6. RECOMENDACIONES FINALES

El presente plan se presenta de manera general siguiendo las buenas practicas y el modelo presentado por el Ministerio de Tecnologías de la Información y las Comunicaciones y presenta las generalidades que se deben seguir al interior de la Entidad para dar respuesta oportuna y reporte a las autoridades cuando se presente un incidente de seguridad que comprometa los activos clasificados como críticos al interior de la Entidad, es importante darlo a conocer a todos los funcionarios y colaboradores de la Justicia Especial, y generar conciencia de la importancia de seguir los protocolos y la Política de Seguridad de la Información y las Comunicaciones.

8. PRESUPUESTO

El siguiente plan hace parte del Modelo de Seguridad y Privacidad de la Información MISP, para la ejecución de este, se presentó proyecto de inversión a ejecutar hasta la vigencia 2025 por valor de 4.100 millones.

9. SEGUIMIENTO Y MEDICIÓN DEL PLAN

Se realizará una reunión de seguimiento semestral hasta la vigencia 2025.

9.1. INDICADORES

A modo de ejemplo, se propone el siguiente indicador para ser incluido en todos los planes:

$$\frac{N° \text{ de Incidentes tratados}}{Nx° \text{ de Incidentes reportados}}$$

Este indicador medirá el cumplimiento del presente Plan a través del resultado del siguiente indicador, para el cual la meta es 95% anual.

La sección de CONTROL DE CAMBIOS será diligenciada por la Oficina Asesora de Planeación, una vez sea aprobado el Plan Institucional por el Comité Institucional de Gestión y Desempeño, para su posterior publicación en la página Web de la Entidad.

CONTROL DE CAMBIOS			
Versión	**Fecha**	**Instancia de Aprobación**	**Descripción**
01	10/06/2022	Sesión 3 Extraordinaria Comité Institucional de Gestión y Desempeño	Versión inicial del documento.