1. PROCESO

Gestión de las Tecnologías de la Información.

2. OBJETIVO

Establecer las actividades, condiciones y acciones para detectar, reportar, evaluar, clasificar, responder, tratar y aprender sobre los eventos e incidentes de seguridad de la información y seguridad digital que se evidencien o presenten con cualquier activo de información de la Unidad de Servicios Penitenciarios y Carcelarios - USPEC, a fin de garantizar el tratamiento oportuno y eficaz para evitar daños o repercusiones que generen o aumenten el impacto.

3. ALCANCE

Inicia con el reporte o notificación del evento de seguridad de la información y finaliza con el cierre del ticket correspondiente al evento o incidente de seguridad de la información.

4. DEFINICIONES

- **Activo:** cualquier elemento que tiene valor para la organización y que para la gestión de riesgos de seguridad de la información se consideran los siguientes: hardware, software, información (física o digital), servicios y recursos humanos.

- **Control:** cualquier acción o elemento del sistema de gestión cuyo propósito es el de prevenir la ocurrencia de un incidente o disminuir la severidad de las consecuencias.

- **Contención:** son aquellas acciones tendientes a evitar la propagación de la amenaza que ocasionó el incidente de seguridad de la información detectado. Algunos ejemplos de actividades de contención son: bloqueo de cuenta después de sucesivos intentos de acceso o la desconexión de la red de un equipo infectado con malware.

- **Erradicación:** consiste en eliminar cualquier rastro dejado por el incidente de tal forma que no sea perceptible el impacto generado por el incidente, ejemplos de esta actividad son: Reparación del sitio web después de un defacement, borrado seguro y restauración de un backup en un equipo infectado por malware, reinstalación del sistema operativo de un equipo de cómputo o servidor y recuperación de datos cuando se detecta un rootkit.

- **Evento de Seguridad de la Información:** es cualquier suceso que en el contexto de seguridad de la información no incide en un impacto sobre las propiedades de un activo de información, pero que pudo haberse materializado si no existiera el respectivo control o salvaguarda. Para efectos de este procedimiento, todo reporte inicialmente es un evento hasta tanto no se clasifique como incidente, o sea, se considere que el evento generó un impacto sobre los activos de información.

- **Incidente de Seguridad de la Información:** es el resultado de un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. Son los eventos que debido al impacto por afectación a las propiedades de seguridad de la información (Disponibilidad, Integridad y Confidencialidad) y su contexto de origen, generan un perjuicio para la entidad que puede estar relacionado a afectación en la calidad de los servicios, en pérdidas económicas, en fuga de información, en temas legales, entre otros.

- **Mitigación:** acciones de prevención de expansión del incidente de seguridad de la información, con el objeto de mitigar el impacto generado hasta cierto punto por la materialización del incidente sobre un activo de información.

- **Vulnerabilidad:** debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

- **Privacidad:** corresponde al derecho que tiene toda persona a conservar de manera reservada y confidencial la información que constituye su ser o que podría dar indicio a su personalidad, religión, estado de salud, preferencias políticas, entre otras que por ningún motivo personas ajenas a su consentimiento deben conocer u obtener.

- **Responsable del activo:** persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El responsable del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

- **Usuario**: personal vinculado a la USPEC o que cuente con acceso a los activos de información de la Entidad o partes interesadas.

- **Vulnerabilidad:** debilidad identificada sobre un activo y que puede ser aprovechada por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

5. DISPOSICIONES GENERALES

5.1. MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Resolución 500 de 2021 (MINTIC)	A través de la cual se establecen los lineamientos y estándares para estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de Información, fortaleciendo la gestión de riesgos e incidentes de seguridad de información.
Resolución 00181 de 2022 (USPEC)	Política de seguridad, privacidad de información y seguridad digital expedida por la USPEC.
Directiva 002 de 2022 (Presidencia de la República)	Lineamientos de seguridad digital. En términos generales trata de las medidas a tomar para mitigar los constantes ataques cibernéticos, incluyendo el fortalecimiento de elementos tales como: contratación de servicios en la nube, actualización de activos de información, implementación de la estrategia de seguridad digital, gestión de riesgos e incidentes entre otros.
Decreto 1008 de 2018 (MINTIC)	Por el cual se establecen los lineamientos generales de la política de gobierno digital y se establece la seguridad de la información como un principio de la política de gobierno digital.
Norma ISO 27001:2013 (Anexo A)	Control A.16 Gestión de incidentes de seguridad de información, tiene como objetivo "*Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades*"
Guía para la gestión y clasificación de incidentes de seguridad de información. (MINTIC)	Este anexo definido por MINTIC, entrega los lineamientos básicos para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren

5.2. GENERALIDADES

Es responsabilidad de todo el personal vinculado a la USPEC o que cuente con acceso a los activos de información de la Entidad o incluso que se considere una parte interesada, reportar cualquier tipo de situación que pueda generar afectación a las propiedades de seguridad de la información (confidencialidad, integridad y disponibilidad) o que vaya en contravía de las políticas, procedimientos y demás lineamientos establecidos por la USPEC en el Sistema de Gestión de Seguridad de la Información – SGSI, así como la normatividad aplicable.

La detección o advertencia de un evento de Seguridad de la Información, también se puede generar a través de herramientas tecnológicas administradas por la OTEC.

En caso requerido, se debe ajustar el mapa de riesgos de seguridad de información con el fin de incluir los incidentes presentados adoptando los controles que resulten pertinentes.

En el formato Registro de Eventos y/o Incidentes de Seguridad de la Información TI-FO-017, se establece la clasificación de los incidentes de seguridad de información, los cuales se catalogan como Graves, Moderados y Bajos.

Todos los incidentes de seguridad de información, deben ser reportados ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno. Para aquellos catalogados como Graves se debe requerir ante el CSIRT apoyo y coordinación en la gestión de estos. Para los catalogados como Moderados o Bajos, deben ser registrados en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.

Si el incidente es catalogado como Grave, se debe realizar planes de mejoramiento, para lo cual el responsable de seguridad de la Entidad supervisa y hace seguimiento a su cumplimiento.

Ante un incidente con un impacto grave, es importante comunicar a las partes interesadas y, en caso de ser necesario, a la Dirección General con el fin que se tomen decisiones que puedan estar fuera del alcance del responsable de seguridad de la información o líder de proceso, con el fin de:

- Informar al personal vinculado a la USPEC acerca de la afectación que está ocurriendo y las precauciones que se deben tener, para que estas sean adoptadas de manera transversal en la Entidad.
- Informar a la Superintendencia de Industria y Comercio - SIC acerca de incidentes que involucren datos personales, de acuerdo a la normativa aplicable.

- Informar a las partes interesadas acerca de la pérdida de la confidencialidad, integridad y disponibilidad de un servicio o activo y el tiempo que tomará restaurarlo, recuperarlo o recrearlo.

- En conceso entre el responsable de seguridad de información, el responsable del activo y la Dirección General se determina la necesidad de informar a los medios de comunicación el impacto generado en los activos de la Entidad ante la materialización de un incidente.

El reporte de eventos y/o incidentes de seguridad de información se pueden realizar a través de alguno de los siguientes canales:

- Correo electrónico mesadeayuda@uspec.gov.co con copia al correo seguridad.informacion@uspec.gov.co

- Extensiones asignadas a la Mesa de Ayuda.

- Herramienta HelpTIC www.helptic.uspec.gov.co

Nota: Todos los eventos y/o incidentes generados con la información institucional de la USPEC, deben ser reportados a través de estos canales, dependiendo del nivel de afectación de los activos la Oficina de Tecnología determina la necesidad de escalarlo para solución a otras instancias.

5.3. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DE INCIDENTES

A continuación se establecen los roles, las responsabilidades y los momentos en que cada uno debe intervenir para llevar a cabo la gestión de incidentes:

ROL	RESPONSABILIDADES
Responsable(s) del SGSI	- Clasificación, evaluación y documentar los eventos e incidentes. - Seguimiento a eventos o incidentes de seguridad de la información. - Reporte de incidentes ante las instancias pertinentes. - Definir, socializar e implementar el procedimiento de Gestión de Eventos e Incidentes de Seguridad de la Información TI-PR-004 en la Entidad. - Ejecutar acciones oportunas para contener, mitigar o erradicar las fuentes de ataque, amenazas o vulnerabilidades explotadas que generen la afectación de los activos de la Entidad. - Realizar el seguimiento a la gestión del incidente a cargo del responsable o custodio del activo implicado en el incidente de seguridad de la información. - Realizar y/o coordinar las acciones correspondientes para recuperar los activos de información o los servicios que hayan sido afectados por el incidente. **Intervención**: Antes, durante y después de un **evento** o **incidente** de seguridad de la información.
Personal adscrito o vinculado a la USPEC	- Reportar cualquier evento que afecte los principios de seguridad de la información institucional a través de los canales establecidos por la OTEC. **Intervención**: En el momento en que se presente o detecte un **evento** o **incidente** de seguridad de la información.
Personal de Mesa de Ayuda	- Escalar e informar oportunamente al responsable de seguridad de la información, los eventos reportados. **Intervención**: Después del reporte de un **evento** o **incidente** de seguridad de la información
Responsable o, custodio del activo afectado.	- Apoyar las gestiones correspondientes a resolución de eventos o incidentes de seguridad de la información sobre los activos a su cargo. - Realizar la evaluación y el impacto del evento o incidente y realizar las gestiones necesarias para socializar en su proceso o dependencia las acciones correctivas en caso de requerirse. - Promoción y socialización de los riesgos asociados a incidentes de seguridad de la información de manera general a su proceso o equipo de trabajo. **Intervención**: Antes, durante y después de un **evento** o **incidente** de seguridad de la información.

Control interno disciplinario	- Tramitar las acciones disciplinarias correspondientes cuando los eventos o incidentes sean generados por personal de la entidad bajo cualquier índole. **Intervención**: Después de un **evento** o **incidente** de seguridad de la información, siempre y cuando el material probatorio haya sido debidamente recolectado y presentado y su vez se encuentre correctamente custodiado.
Control interno	- Realizar seguimiento a las acciones correctivas implementadas o definidas en el proceso contención, mitigación o erradicación de los incidentes de seguridad de la información. - Dar parte, sobre la efectividad de las acciones tomadas durante y después de un evento o incidente de seguridad de la información. - Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. **Intervención**: Después de un **evento** o **incidente** de seguridad de la información.

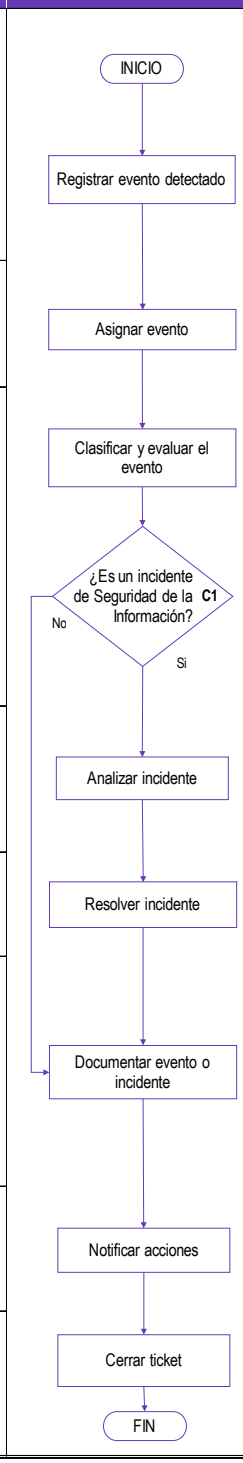
5.4. DIRECTORIO CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS

En el caso de aquellas situaciones en las que se evidencie compromiso de algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la USPEC, o de una fuga o afectación a la privacidad de la información de la Entidad o ciudadanos, el responsable de seguridad de la información debe realizar el reporte a las autoridades competentes (en caso requerido consultar el directorio de autoridades y/o grupos de interés con la Oficina de Tecnología).

En caso requerido es importante hacer una recolección y manejo adecuado de la evidencia; para ello, la entidad puede contactar al ColCERT. Si el Equipo de Seguridad de la USPEC lleva a cabo la recolección de evidencia, se debe tener en cuenta el Manual del Sistema de Cadena de Custodia[1] de la Fiscalía General de la Nación o las guías de MinTIC, ColCERT y el CCP para recolección, tratamiento y gestión de evidencias digitales, las cuales se argumentan de acuerdo a la norma técnica colombiana NTC ISO/IEC 27035 vigente.4599-1861-5045-9481

[1] https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf

6. DIAGRMA DE FLUJO

N°.	FLUJOGRAMA	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTROS
1		Registrar detalladamente el evento en la herramienta HelpTIC, incluyendo en lo posible evidencias que sustenten la situación. Nota: si el reporte es realizado a través de otro medio diferente a la herramienta el personal de Mesa de Ayuda debe registrar el ticket en la herramienta HelpTIC. Si un mismo evento es reportado por más de un usuario, solo se tendrá en cuenta el primer reporte, sin embargo, en la Matriz Consolidado Eventos e Incidentes de Seguridad de la Información, se debe documentar que el evento fue reportado por la cantidad total de personas y sus correspondientes dependencias, procesos o terceros (partes interesadas) para la Entidad.	Usuarios Responsable SGSI Mesa de Ayuda	Correo electrónico Herramienta HelpTIC Matriz Consolidado Eventos e Incidentes de Seguridad de la Información
2		A través de la herramienta HelpTIC se asigna el evento al personal responsable, notificando a través de correo. **Nota:** en el inventario de activos de información de cada proceso, se puede consultar el responsable del activo afectado.	Mesa de Ayuda	Correo electrónico Herramienta HelpTIC
3		Clasificar y evaluar el evento con el fin de determinar si corresponde a un evento o un incidente de seguridad de la información. **Nota:** se debe registrar en la herramienta HelpTIC el resultado de esta actividad. **Punto de Control** **C1:** verificar si es un incidente de seguridad de la información de acuerdo a lo establecido en las disposiciones generales.	Responsable activos de información Responsable SGSI Mesa de Ayuda	Herramienta HelpTIC
4		Analizar el incidente para determinar el origen, amenazas, posibles motivos o consecuencias, documentando los hallazgos (logs de sistema y/o fotos y/o videos y/o correos electrónicos y/o documentos evidencia). Nota: las evidencias se deben documentar y salvaguardar en caso de requerir reaizar denuncias, acciones disciplinarias o legales.	Responsable activos de información Responsable SGSI	Registro de Eventos y/o Incidentes de Seguridad de la Información TI-FO-017
5		Resolver el incidente de seguridad tomando las medidas correspondientes para contener, mitigar o erradicarlo, teniendo como referencia el análisis previo.	Responsable activos de información Responsable SGSI	N/A
6		Documentar todas las acciones y actividades que se hayan ejecutado en la gestión del reporte de evento o incidente de seguridad de la información, de acuerdo a lo solicitado en el formato TI-FO-017 Registro de Eventos y/o Incidentes de Seguridad de la Información. Registrar el evento o incidente de Seguridad de la Información en la matriz Consolidado Eventos e Incidentes de Seguridad de la Información. **Nota:** para todos los incidentes se les debe registrar las lecciones aprendidas en la matriz Consolidado eventos e incidentes de seguridad de información.	Responsable activos de información Responsable SGSI	Registro de Eventos y/o Incidentes de Seguridad de la Información A3TI-FO-017 Matriz Consolidado Eventos e Incidentes de Seguridad de la Información
7		Informar a las partes interesadas la solución del incidente y las lecciones aprendidas. **Nota:** cuando el responsable de seguridad de información lo considere pertinente se socializarán las lecciones aprendidas con toda la Entidad y con las entidades del sector.	Responsable del SGSI	Correo Electrónico
8		Cerrar el ticket en la herramienta HelpTIC, adjuntando la documentación generada del evento o incidente.	Mesa de Ayuda	Herramienta HelpTIC

RESUMEN DE CAMBIOS:

Versión	Fecha	Numerales	Descripción de la modificación
01	22/08/2016	Todos	Se crea el documento.
02	29/06/2020	Todos	Se cambia el nombre "Gestión de Incidentes de Seguridad de la Información" por "Gestión de Eventos e Incidentes de Seguridad de la Información". Se actualiza todo el documento.
	04/10/2021	N/A	Se ajustan los códigos de los documentos de acuerdo con la actualización del Mapa de Procesos Institucional. La versión del documento se mantiene debido a que su contenido no se modificó.
03	17/11/2022	Todos	Se actualiza objetivo, disposiciones generales, glosario y actividades, diagrama de flujo teniendo en cuenta los lineamientos establecidos en la resolución 500 de 2021 establecido por MINTIC.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Nombre: Mayra Alexandra Agudelo Carvajal	Nombre: Camilo Alejandro Romero González	Nombre: Imelda Muñoz Mancipe
Cargo: Profesional Especializado	Cargo: Coordinador Grupo Comunicaciones	Cargo: Jefe Oficina de Tecnología
Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología