1. **PROCESO:** Gestión de las Tecnologías de la Información.

2. **SUB PROCESO:** N/A.

3. OBJETIVO

Establecer las actividades, condiciones y acciones para detectar, reportar, evaluar, clasificar, responder y aprender sobre los eventos e incidentes de seguridad de la información 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.

4. 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.

5. DISPOSICIONES GENERALES

5.1. GENERALIDADES

Es responsabilidad de todo el personal vinculado a la USPEC o que cuente con acceso a los activos de información de la Entidad, reportar cualquier tipo de situación que pueda generar afectación a las propiedades de seguridad de la información (confidencialidad/privacidad, integridad y disponibilidad) o que vaya en contravía de las políticas, procedimientos y demás lineamientos establecidos por USPEC en el Sistema de Gestión de Seguridad de la Información - SGSI o por la regulación Colombiana en cuanto a Privacidad de la información.

No obstante, una persona jurídica o persona natural, ajena a la USPEC y que se considere parte interesada para la Entidad, puede realizar el reporte de un posible incidente de seguridad de la información, a lo cual la USPEC está en la obligación de tratar dicho reporte bajo las mismas condiciones que se establecen en este procedimiento para los reportes o detecciones por parte de personal con vínculo directo con la entidad.

Es importante resaltar que un evento o incidente de seguridad de la información no afecta únicamente activos digitales, estas situaciones también se pueden materializar sobre activos físicos como, por ejemplo: documentos impresos, planos arquitectónicos impresos, dispositivos de almacenamiento o cifrado (token), carpetas de proyectos o de contratación, carpetas de historias laborales, carpetas de facturación o pagos y equipos o dispositivos físicos, estos últimos en cuanto a daños físicos.

5.2. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DE INCIDENTES

Los roles y responsabilidades en la gestión de eventos o incidentes de seguridad de la información se activan en función del impacto que generen o que pudiesen presentar estas situaciones. De acuerdo a esto, se establece el siguiente cuadro en el que se expone cada rol con las probables responsabilidades y el o los momentos en los que debe intervenir:

ROL	RESPONSABILIDADES	MOMENTO DE INTERVENCIÓN
Responsable(s) del SGSI	- Promoción y socialización de los riesgos asociados a incidentes de seguridad de la información de manera transversal a todas las dependencias. - Clasificación y evaluación de un evento para determinar si corresponde o no a un incidente y su impacto. - Seguimiento a eventos o incidentes de seguridad de la información. - Reporte a Jefatura de Tecnología o a la Dirección General de los eventos o incidentes de seguridad de la información que una vez evaluados obtengan un impacto alto para la entidad, en cualquier ámbito. - Documentar los eventos e incidentes de seguridad de la información.	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 gestionada o tratada por USPEC.	En el momento oportuno en que se presente o detecte un **evento** o **incidente** de seguridad de la información.
Personal de Mesa de Ayuda	- Registrar los eventos de seguridad de la información en la herramienta de gestión de tickets. - Escalar e informar oportunamente al primer respondiente o al responsable de seguridad de la información o al responsable del SGSI, los eventos reportados.	Después del reporte de un **evento** o **incidente** de seguridad de la información.
Responsable, custodio o delegado para los activos.	- Reportar cualquier evento que afecte los principios de seguridad de la información de los activos a su cargo o gestión. - Apoyar las gestiones correspondientes a resolución de incidentes de seguridad de la información sobre los activos a su cargo. - Coadyuvar en la clasificación y evaluación de los eventos que se detecten sobre los activos de información a su cargo. - Documentar o coadyuvar en la documentación de los eventos e incidentes de seguridad de la información.	Antes, durante y después de un **evento** o **incidente** de seguridad de la información.

Primer respondiente en la gestión de incidentes de seguridad de la información (Personal técnico de seguridad informática, cibernética y/o de la información).	- Propender por ser el primero en dar gestión sobre el reporte de un evento o incidente de seguridad de la información desde cualquier ámbito, ejecutando acciones oportunas para contener, mitigar o erradicar las fuentes de ataque, amenazas o vulnerabilidades explotadas que permitan la afectación a las propiedades de seguridad de la información de los activos de la entidad. - Coadyuvar en el seguimiento o trazabilidad de la gestión del incidente de seguridad 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 de seguridad de la información. - Documentar los eventos e incidentes de seguridad de la información.	Durante y después de un **evento** o **incidente** de seguridad de la información.
Directivos y Jefes de Oficina o quien estos designen	- Promoción y socialización de los riesgos asociados a incidentes de seguridad de la información de manera general a su proceso o equipo de trabajo. - 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.	Durante y después de un **evento** o **incidente** de seguridad de la información que implique a más de 10% del personal del área o dependencia donde se origine.
Control interno disciplinario	- Tramitar las acciones disciplinarias correspondientes cuando los eventos o incidentes sean generados por personal de la entidad bajo cualquier índole.	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.	Después de un **evento** o **incidente** de seguridad de la información.

5.3. DESARROLLO Y DETALLES EN LA GESTIÓN DE EVENTOS O INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

5.3.1 Fases en la gestión de un evento de seguridad de la información:

- **Detección:** la detección o advertencia de un evento de Seguridad de la Información, se puede generar a través de herramientas especializadas, indicadores de estado, o por parte del personal (de forma visual).

- **Notificación o reporte:** concierne a todo personal vinculado a la USPEC o que cuente con acceso a los activos de información de la Entidad, ente, sistema u organización, notificar o reportar la detección o la sospecha de un evento de seguridad de la información.

- **Registro:** implica crear un número (ticket) que permita hacer seguimiento al reporte.

- **Asignación:** asignar y escalar o remitir el ticket a las personas que tengan procedencia sobre el activo o servicio implicado en el evento de Seguridad de la Información.

- **Evaluación:** clasificar y evaluar el evento de seguridad de la información, según el tipo de evento o incidente y/o la criticidad del mismo, respectivamente.

- **Análisis:** determinar el origen, motivo y consecuencias del incidente. Buscar, reunir y analizar las evidencias documentándolas y salvaguardándolas en caso de requerir realizar las denuncias, acciones disciplinarias o legales por el incidente.

- **Resolución:** establecer y ejecutar las medidas a tomar tras la obtención de las evidencias para dar la solución al evento o incidente.

- **Documentación:** documentar las medidas tomadas y aplicadas junto con la evidencia recolectada.

- **Aprendizaje:** tomar el incidente como un aprendizaje y añadir medidas de prevención para futuras manifestaciones similares.

- **Socialización:** socializar o notificar a las partes interesadas la solución del incidente y las lecciones aprendidas.

- **Cierre:** hacer el cierre oficial del evento o incidente y reunir la documentación, registros, evidencias y demás documentación relacionada a la gestión realizada, guardando en todo caso la información de quienes intervinieron, acciones y procesos realizados por cada uno.

5.3.2 Medios de reporte y comunicación.

La entidad pone a disposición los siguientes medios para reportar los eventos de seguridad de la información en función de quien lo detecte:

ORIGEN DEL REPORTE	MEDIO DE REPORTE	DETALLE
Personal adscrito o vinculado a la USPEC.	Correo electrónico institucional	Para: mesadeayuda@uspec.gov.co CC seguridaddigital@uspec.gov.co
	Teléfonos	Extensiones asignadas a la Mesa de Ayuda.
	Herramienta HelpTIC	URL: helptic.uspec.gov.co
Partes interesadas (persona jurídica o persona natural ajena a la USPEC)	Correo electrónico institucional	Para: mesadeayuda@uspec.gov.co CC seguridaddigital@uspec.gov.co
	Teléfonos	Extensiones asignadas a la Mesa de Ayuda.
	Funcionario o contratista de USPEC.	Reportar el evento a través del correo personal, telefónicamente o verbalmente a algún funcionario o contratista de la USPEC con quien se tenga contacto, quien a su vez retransmitirá el reporte por medio de los mecanismos ya definidos anteriormente y a su alcance.

Para el caso de Personal vinculado directamente a la USPEC, si el evento de seguridad impide el uso de la herramienta HelpTIC y otros mecanismos de reporte tecnológico, se debe reportar el evento por medio alterno, solicitando apoyo a un compañero o de manera personal, en todo caso, es obligatorio el reporte de eventos e incidentes de seguridad de la información por parte del personal de la USPEC. Cualquier omisión será considerada una falta a los protocolos de seguridad de la información y podría repercutir en sanciones disciplinarias e incluso dependiendo del impacto del incidente en sanciones legales.

Si el evento de seguridad es detectado por una persona jurídica o persona natural ajena a la USPEC (partes interesadas), la cual no tiene acceso a los medios de comunicación institucionales, esta puede reportar por cualquier medio la situación detectada al servidor público que autorizó su ingreso a la Entidad, o con cualquier servidor público de la Oficina de Tecnología.

Durante todo el ciclo de vida del evento o incidente es obligatorio actualizar la información de la gestión realizada en el Ticket registrado en la herramienta HelpTIC de la USPEC, con el propósito de brindar información y establecer comunicación constante a quien lo requiera, para seguimiento sobre el estado del evento o incidente.

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, primer respondiente 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/privacidad, integridad y disponibilidad de un servicio o activo y el tiempo que tomará restaurarlo o recuperarlo o recrearlo.

5.3.3 Recepción, registro y atención ante eventos e incidentes de seguridad de la información.

La recepción, registro y atención ante los reportes de eventos de seguridad de la información es fundamental para asegurar una gestión oportuna de estos, por lo tanto, el personal de Mesa de Ayuda, el responsable de seguridad de la información, el primer respondiente y el responsable o custodio del activo deben dar prioridad a las gestiones que correspondan ante el reporte de un evento, con el fin de evaluarlos y dar inicio a las acciones que se consideren.

El personal de Mesa de Ayuda debe tener en cuenta que para los casos donde el evento sea reportado por un medio diferente a la herramienta HelpTIC, se debe registrar el evento manualmente en dicha herramienta. Cada reporte debe tener asignado un número de 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 documentación de trazabilidad del ticket en la herramienta HelpTIC 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.

5.3.4 Detalles ante el reporte.

Es importante que quien realice el reporte lo haga con el mayor detalle posible en la descripción del evento e incluya, de ser posible, evidencias tales como capturas de pantallas o fotos relacionados al evento de seguridad de la información que se reporta. En la medida de lo posible, esto debe ser informado por quien hace el reporte o en dado caso documentado por quien lo recibe (personal de Mesa de Ayuda). Es fundamental que el reporte sea oportuno, procurando que la fecha y hora de la detección coincida en no menos de 10 minutos con el reporte o notificación.

Luego del reporte, es fundamental documentar en el ticket, el detalle de las posibles acciones que desencadenaron o dieron preámbulo al evento, la información que debe ser suministrada por quién reporta el evento o cualquier otro testigo, por ejemplo, se debe considerar realizar preguntas como las siguientes dependiendo del evento: ¿a qué sitios web en específico se accedió antes de detectar el evento?, ¿se abrió o dio respuesta a un correo electrónico desconocido?, ¿se omitió o pasó por alto un mensaje o notificación del sistema?, ¿se recibió una llamada solicitando información?, ¿se visualizó personal desconocido o sospechoso en áreas restringidas o de circulación exclusiva establecidas en la USPEC?, ¿el documento extraviado contiene información sensible, secreta o que afecte la privacidad?.

Si quien reporta, desconoce el origen del evento, debe informar la situación inmediatamente es detectada, con el fin de dar una atención oportuna al caso e investigar las evidencias de su origen.

5.3.5 Asignación del evento desde la herramienta HELPTIC.

El personal de Mesa de Ayuda, una vez reciba el reporte del evento a través de la herramienta HelpTIC, debe asignar el responsable de dar inicio a la actividad de evaluación, clasificación y gestión del evento. Esta asignación la debe realizar teniendo en cuenta el responsable o custodio del activo, para tal caso el personal de Mesa de Ayuda puede soportarse o solicitar ayuda a los responsables del SGSI para determinar el responsable o custodio del activo implicado. El evento debe ser asignado al primer respondiente quien se encargará de realizar las gestiones de seguimiento en conjunto con el responsable del activo implicado.

5.3.6 Clasificación y evaluación de un evento de seguridad de la información.

Un evento de seguridad de la información no será considerado un incidente hasta tanto no se realice la clasificación por parte del responsable del SGSI o el primer respondiente en la gestión de incidentes. En caso que estos responsables no estén presentes en el momento de requerir gestión del evento, esta clasificación la debe asumir el responsable del activo o activos implicados en el evento y ante esta situación, un responsable SGSI deberá dar orientación sobre cómo evaluar el evento de manera remota (vía telefónica, chat o mail), es decir, dará las indicaciones sobre el impacto del evento y con dicha información la decisión deberá ser tomada por el responsable o custodio del activo, esta evaluación deberá ser registrada en el ticket generado en el reporte.

Todo proceso de evaluación de un evento de seguridad de la información, debe realizarse con una validación previa de la matriz "Consolidado Eventos e Incidentes de Seguridad de la Información", para determinar si el incidente de Seguridad de la Información tuvo un precedente, es decir, si anteriormente se había gestionado un incidente similar, en este caso, se opta por abordar las lecciones aprendidas o reforzar el control implementado para la solución del evento o incidente de seguridad de la información, esto junto con el responsable del activo.

La evaluación de los eventos reportados se realiza bajo los criterios para la gestión, atención y respuesta a incidentes de seguridad de la información establecidos por la Oficina de Tecnología.

5.3.7 Análisis del incidente.

Durante la evaluación de lo que se presumió como un incidente de seguridad de la información ya clasificado como tal, se puede dar la situación que el incidente corresponde a un falso positivo. En tal sentido, el personal de Mesa de Ayuda debe cambiar el estado del ticket a "falso positivo" y el responsable del SGSI o el primer respondiente en la gestión de incidentes, debe documentar las razones por las cuales se determinó de esa manera en el Formato Registro de eventos y/o incidentes de seguridad de la información TI-FO-017, sección 4. Evento de seguridad de la información o Falso Positivo.

Durante el análisis del incidente, toda evidencia del origen, destinos, herramientas usadas por la amenaza, posibles motivos o consecuencias relacionadas deben ser reunidas, documentadas, analizadas y salvaguardadas, para realizar las denuncias o acciones disciplinarias o legales según corresponda. En el caso de aquellos incidentes donde se deba recopilar evidencia digita se debe tener en cuenta los lineamientos y directrices establecidos por la Oficina de Tecnología correspondiente a las acciones de obtención y salvaguarda de evidencia o material probatorio digital.

5.3.8 Documentación del evento e incidente de seguridad de la información.

Una vez el evento o incidente es resuelto, o sea, la amenaza o afectación no está presente sobre el activo de información, y el mismo fue recuperado en dado caso que llegase a presentarse una afectación total o parcial en alguna de sus propiedades, toda las acciones, evidencias, registros y demás documentación relacionada al evento o incidente, deben ser documentadas en el Formato Registro de eventos y/o incidentes de seguridad de la información TI-FO-017 y adjuntar los documentos que soporten la gestión del evento y las acciones que permitieron dar la solución de manera detallada.

La trazabilidad de los reportes se registra en la matriz "Consolidado Eventos e Incidentes de Seguridad de la Información". Los eventos que no sean clasificados como incidentes deben ser registrados en el Formato

Registro de eventos y/o incidentes de seguridad de la información TI-FO-017 en la sección 4. con su correspondiente descripción de la evaluación.

Todos los eventos que se clasifiquen como incidentes de seguridad de la información deberán ser documentados con lecciones aprendidas y registrados en la matriz Consolidado Eventos e Incidentes de Seguridad de la Información. Los reportes clasificados como eventos, no tendrán que documentarse con lecciones aprendidas ni los demás datos relacionados exclusivamente para incidentes.

6. 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.

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.

Falso positivo: son los eventos que se originan como un incidente de seguridad de la información, ya que se presumió una afectación de las propiedades de un activo de información, sin embargo, luego del análisis, se determinó que no correspondía a una amenaza o aprovechamiento de una debilidad (Vulnerabilidad) si no a una detección incierta.

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.

Contener: se busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI. 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.

Notificación: acción de informar por medio de algún canal de comunicación la recepción o generación y recepción satisfactoria de un reporte.

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.

Reporte: acción de dar aviso sobre algún evento o situación sospechosa.

Recuperación: restauración de los sistemas y/o servicios afectados para restablecer la funcionalidad de los mismos, y realizar un endurecimiento (hardening) del sistema que permita prevenir incidentes similares en el futuro.

Riesgo: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización).

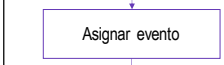
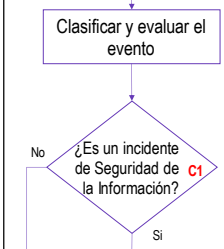
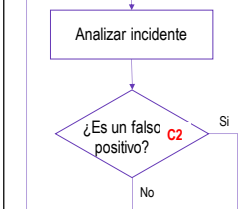
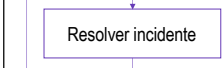
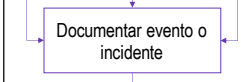
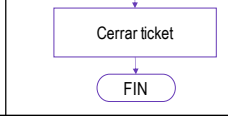
Usuario: personal vinculado a la USPEC o que cuente con acceso a los activos de información de la Entidad o partes interesadas.

VLAN: red de área local virtual, es un método para crear redes lógicas independientes dentro de una misma red física.

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.

7. FLUJOGRAMA, DESCRIPCIÓN DE ACTIVIDADES Y PUNTOS DE CONTROL

GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

N°.	FLUJOGRAMA	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTROS
1		Registrar el evento en la herramienta HelpTIC. 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.	Usuarios/ Mesa de Ayuda	Correo electrónico/ Ticket HelpTIC
2		Asignar el reporte. La herramienta HelpTIC genera automáticamente un correo electrónico, notificando al personal responsable.	Mesa de Ayuda	Ticket 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:** registrar en la herramienta HelpTIC el resultado de la evaluación, estableciendo si se trata de un evento o un incidente. **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 Primer Respondiente Mesa de Ayuda	Ticket HelpTIC
4		Analizar el incidente para determinar el origen, amenazas, posibles motivos o consecuencias, documentando los hallazgos (ver numeral 5.3.7). **Punto de Control** **C2:** verificar si es un falso positivo de acuerdo a lo establecido en las disposiciones generales.	Responsable activos de información Responsable SGSI Primer Respondiente	Logs de sistema y/o fotos y/o videos y/o correos electrónicos y/o documentos evidencia
5		Resolver el incidente de seguridad tomando las medidas correspondientes para contener, mitigar o erradicarlo, tomando como referencia el análisis previo.	Responsable activos de información Responsable SGSI Primer Respondiente	NA
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 Registro de eventos o incidentes de seguridad de la información TI-FO-017. Registrar el evento o incidente de Seguridad de la Información en la matriz Consolidado Eventos e Incidentes de Seguridad de la Información.	Responsable activos de información Responsable SGSI Primer Respondiente	Registro de eventos y/o incidentes de seguridad de la información TI-FO-017 Matriz Consolidado Eventos e Incidentes de Seguridad de la Información
7		Cerrar el ticket en la herramienta HelpTIC, adjuntando la documentación generada del evento o incidente e informar a los implicados a través de correo electrónico sobre la gestión realizada.	Mesa de Ayuda	Ticket HelpTIC Correo Electrónico

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.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma:	Firma:	Firma:
Nombre: Fernando A. Vargas Herrera	Nombre: Diana Paola Cárdenas Huertas Mayra Alexandra Agudelo Carvajal Oscar Javier Suárez Ramos	Nombre: Oscar Javier Suárez Ramos
Cargo: Técnico Operativo	Cargo: Profesional Universitario Profesional Especializado Jefe Oficina de Tecnología	Cargo: Jefe Oficina de Tecnología
Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología