PROCESO		
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN		
CÓDIGO	**PROCEDIMIENTO**	**VERSIÓN**
PR-TI-22	PROCEDIMIENTO DE GESTION DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACION	3

Procedimiento Gestión de eventos e incidentes de Seguridad

Control de Versiones

Versión	Fecha	Descripción Modificación	Folios
3	2022-04-28	Ajuste de actividades y responsables acorde con la realidad institucional.	24
2	2019-10-09	Ajuste al nuevo formato y la inclusión de conceptos relacionados con lo establecido en las normas ISO 27035 y NIST SP 800-61r2.	25
1	3/10/2016	Versión inicial del documento	25

PROCESO		
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN		
CÓDIGO	**PROCEDIMIENTO**	**VERSIÓN**
PR-TI-22	PROCEDIMIENTO DE GESTION DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACION	3

El documento original ha sido aprobado mediante el SID (Sistema Información Documentada del IDU). La autenticidad puede ser verificada a través del código

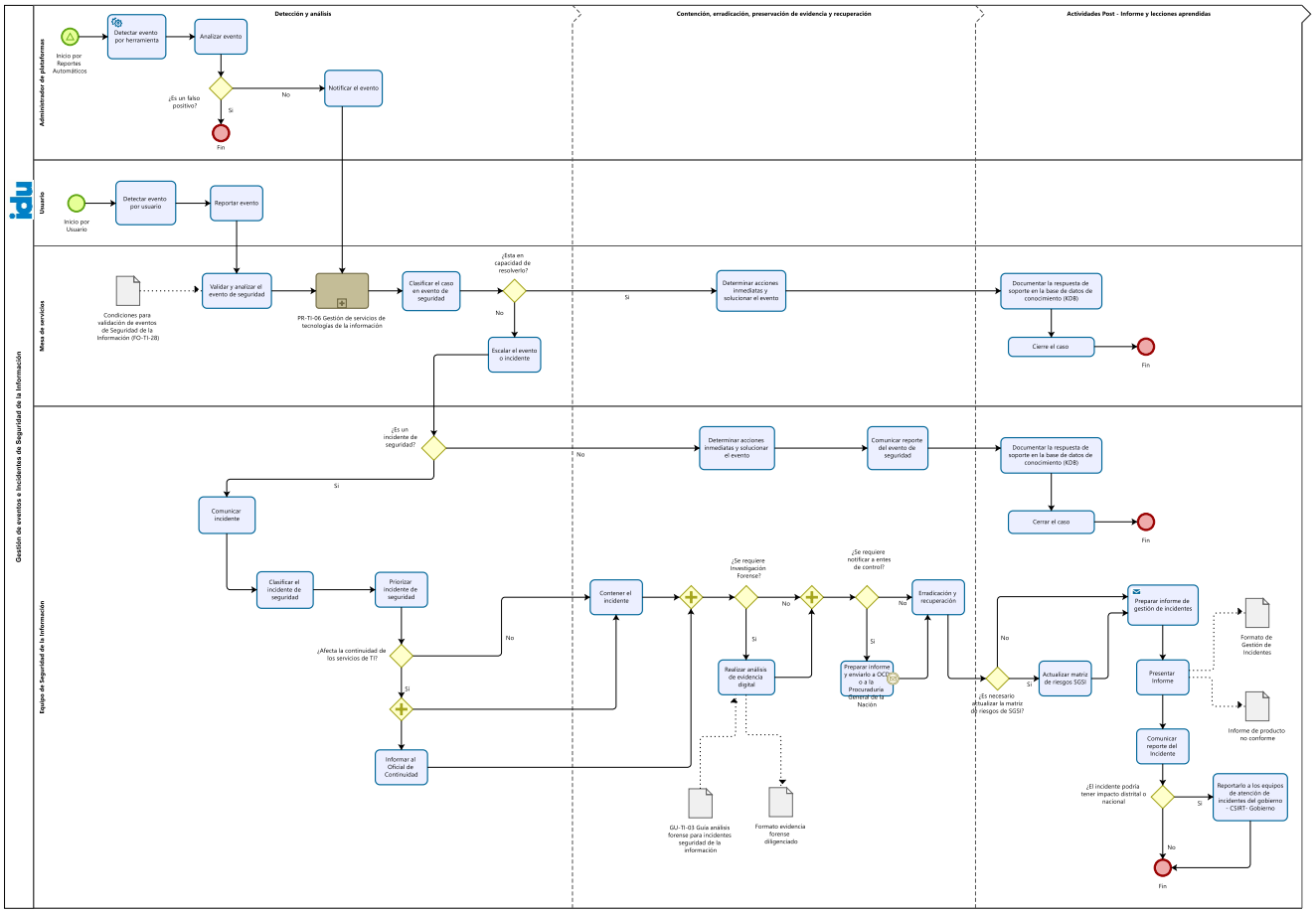
Participaron en la elaboración[1]	**Carlos Fernando Campos Sosa, OAP / Hector Andres Mafla Trujillo, STRT /**
Validado por	**Sandra Milena Del Pilar Rueda Ochoa, OAP Validado el 2022-04-26**
Revisado por	**Arleth Patricia Saurith Contreras, STRT Revisado el 2022-04-27**
Aprobado por	**Arleth Patricia Saurith Contreras, STRT Aprobado el 2022-04-28**

[1]El alcance de participación en la elaboración de este documento corresponde a las funciones del área que representan

Tabla de Contenidos

PROCESO		
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN		
CÓDIGO	**PROCEDIMIENTO**	**VERSIÓN**
PR-TI-22	PROCEDIMIENTO DE GESTION DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACION	3

DIAGRAMA DE FLUJO



1.GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1.1. DESCRIPCIÓN

Participaron en la elaboración: Luis Albeiro Cortés C - STRT, Héctor Andes Mafla T, y Carlos Fernando Campos - OAP.

1.2. OBJETIVO

Formalizar las actividades necesarias para atender cualquier incidente de seguridad de la información relacionado con los activos de información del Instituto, especialmente en las tareas relacionadas con la Gestión de Tecnologías de la Información y Comunicación.

1.3. ALCANCE

Este procedimiento cubre las actividades desde que se detecta un evento de seguridad de la información por parte del usuario final o por reportes automatizados de las consolas de monitoreo y control de los elementos de tecnologías que son administrados con dichos mecanismos y termina con las actividades propias de cierre de los incidentes y documentación de las lecciones aprendidas de los sucesos acontecidos.

1.4. MARCO NORMATIVO

• Ley 1341 de 2009, Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

• Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.

• Ley 1273 de 05 de enero 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”

• Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

• Directiva Distrital 002 de 2002, cuyo asunto es: "formulación de proyectos informáticos y de comunicaciones"

• Directiva Distrital 005 de 2005, Por medio de la cual se adoptan las políticas generales de tecnología de información y comunicaciones aplicables al Distrito Capital.

• Resolución 004 de 2017, Por la cual se modifica la Resolución 305 de 2008 de la CDS.

• Documento CONPES 3854 Política Nacional de Seguridad Digital.

• Resolución IDU 1543 de 2019, "Por la cual se adopta el Manual de Gestión de Políticas de Seguridad de la Información ".

• Resolución interna 1641 de 2019, “Por la cual se adopta el Sistema de Gestión MIPG-SIG del Instituto de Desarrollo Urbano, y se crean los equipos Institucionales”.

• Resolución interna 1909 de 2019, “Por medio de la cual se define la política MIPG-SIG-IDU, se determinan las directrices y objetivos de los Subsistemas de Gestión, y se adopta la versión 4.0 del Manual de Procesos del IDU.”

• Resolución IDU 3807 de 2017, “Por la cual se compilan algunas normas del Sistema Integrado de Gestión-SIG y se dictan otras disposiciones”.

• NTC/ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos Anexo A. Controles del Numeral 16. “Gestión de incidentes de Seguridad de la Información".

1.5. TERMINOS Y DEFINICIONES

Los términos y definiciones aplicables al procedimiento pueden ser consultados en el micro sitio Diccionario de términos IDU (https://www.idu.gov.co/page/transparencia/información-de-interés/glosario)

· 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.[ISO/IEC 27000:2009]

· Incidente de seguridad de la información. Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000:2009].

· KDB: (Knowledge Database) Sigla del idioma inglés que se traduce como base de datos de conocimientos, es un repositorio centralizado y organizado de información referente a las soluciones prestadas a diferentes casos (eventos o incidentes), que al ser analizadas pueden presentarse a la organización como un elemento de retroalimentación para mejorar la prestación de los servicios.

· Mesa de Servicios: es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las TIC.

· Problema: Causa raíz de uno o más incidentes (NTC/ISO 20000-1:2012 Numeral 3.24). La causa raíz usualmente se desconoce en el momento en que se crea el registro de un problema. El procedimiento de la Gestión de Problemas es responsable de la investigación posterior.

· Registro

· Seguimiento

· Servicio

· Verificación

1.6. POLÍTICA OPERACIONAL

1. La duración de las actividades esta expresada en minutos y corresponden a tiempos efectivos de ejecución.

2. Los controles a los riesgos de seguridad de la información se documentarán en la matriz de riesgos del proceso.

3. Los controles a los aspectos e impactos ambientales se documentarán en la matriz de aspectos ambientales del IDU.

4. Los controles a los riesgos laborales se describen en la matriz de peligros y el plan de emergencias del IDU.

5. Las disposiciones de almacenamiento y archivo para los documentos referidos en los procedimientos se definirán en las tablas de retención documental.

6. Los controles a los riesgos de gestión se documentarán en la matriz de riesgos del proceso.

7. El procedimiento debe ser conocido por los diferentes funcionarios, contratistas de la Entidad y empresas de outsourcing interésados que actúan en el sistema.

8. Todas las solicitudes de incidentes o requerimientos realizados por las diferentes áreas, deben ser registradas en el único medio destinado por la STRT "Herramienta Aranda".

9. Todas las solicitudes de incidentes o requerimientos que no estén registrados en el medio destinado por la STRT no serán atendidos hasta que esta política se cumpla

10. Todo incidente o requerimiento debe ser documentado y solucionado a satisfacción del usuario, dando el cierre final en la herramienta destinada para tal fin, por parte del especialista responsable de su atención y solución.

1.7. ELEMENTOS DEL PROCESO

1.7.1. Inicio por Reportes Automáticos

Descripción

Este es un inicio realizado a través de dispositivos tecnológicos o mediante consolas de monitoreo, que al presentar algún evento que no esté acorde con los parámetros normales de funcionamiento (o de control), "dispara" automáticamente una señal (alerta) para indicar el comportamiento diferente del servicio monitoreado.

1.7.2. Detectar evento por herramienta

Descripción

Percibir, detectar, cualquier circunstancia particular sospechosa que no esté acorde con los parámetros configurados de funcionamiento y control de los dispositivos tecnológicos (servidores, elementos de telecomunicaciones, equipos especializados, equipos de control ambiental, equipos de prevención de incendios, entre otros), que muestren un cambio en el comportamiento diario o mal uso de la red o los activos de información o algún ataque informático a los activos de la Entidad o violación a las políticas de seguridad de la información.

Ejecutantes

Asistencial, Técnico, Profesional Universitario

1.7.3. Analizar evento

Descripción

Realizar una revisión de las alertas que han sido reportadas por los diferentes dispositivos o consolas de administración y/o monitoreo que posee el Instituto, y determinar si se está afectando algún servicio de la entidad, si hay variaciones considerables que afectan el tráfico de red, si falta la aplicación de alguna actualización o parche y demás análisis que se considere pertinente respecto al evento presentado. En caso de que se trate de un falso negativo, es decir, cuando algo que se presume como falso o incierto termina siendo real. Por ejemplo: un antivirus no detecta una pieza de malware y la deja pasar, permitiendo que se ejecute en el sistema se debe notificar. Y por el contrario si se trata de un falso positivo, que es cuando un hecho que se presume como cierto o verdadero resulta no ser tal.

Ejecutantes

Técnico, Profesional Universitario, Profesional Especializado

Duración

60.00

1.7.4. ¿Es un falso positivo?

Descripción

Cuando se genera un falso positivo, Por ejemplo cuando un antivirus o sistema de seguridad interpreta que un código, programa, aplicación, dirección web, archivo etc., legítimo está infectado por un malware, sin que en realidad sea así, se termina el proceso.

Flujos

No

Condición

Notificar el evento

Si

Condición

Fin

1.7.5. Notificar el evento

Descripción

El administrador de plataforma en el momento que evidencia alguna circunstancia o actividades que no se están realizando adecuadamente durante las escalas de tiempo acordadas, y de conformidad con las políticas y procedimientos establecidos, debe realizar el análisis del evento ocurrido y tomar las decisiones a que dé lugar para brindar soporte y atención al caso y reportarlo lo más pronto posible a través de la mesa de servicios, utilizando los canales de registro dispuestos por el Instituto para este fin. Independientemente de que el caso corresponda a segundo nivel debe realizarse el reporte y escribir claramente que el caso se esta atendiendo por los ingenieros responsables de la administración con el objeto de tener la traza del evento o incidente. Además, debe informar el caso a través de correo electrónico al equipo de seguridad de la información

Ejecutantes

Profesional Universitario, Profesional Especializado

Duración

30.00

1.7.6. Inicio por Usuario

Descripción

Este es un inicio común al procedimiento de gestión de servicios de TI y al procedimiento de gestión de incidentes, que se presenta cuando una persona o usuario de los activos de información del Instituto, detecta un comportamiento anómalo.

1.7.7. Detectar evento por usuario

Descripción

Percibir, observar, cualquier circunstancia particular sospechosa, o debilidad, que muestre un cambio en las operaciones diarias de la red, servicios de TI o mal uso de algún activo de información, o algún ataque informático a los activos de la entidad, o la violación a las políticas de seguridad de la información.

Ejecutantes

Asistencial, Técnico, Profesional Universitario, Profesional Especializado, Asesor, Directivo

Duración

30.00

1.7.8. Reportar evento

Descripción

Notificar a través de los canales de gestión dispuestos por el Instituto para este fin la circunstancia que se está presentando. Se debe describir en el reporte claramente la siguiente información: Hora de ocurrencia del evento, descripción, activo de información relacionado o afectado por el evento o situación presentada, usuario o usuarios afectados e involucrados. Sí el usuario desea se puede escribir el nombre del usuario que lo reporta, de lo contrario debe quedar como usuario anónimo este aplica principalmente cuando se trata de reporte de denuncia internas respecto al incumplimiento de políticas o procedimientos de seguridad de la información.

Algunas situaciones que se deben considerar para el reporte de eventos de seguridad de la información incluyen:

- un control de seguridad ineficaz;
- violación de la integridad, confidencialidad o disponibilidad de la información;
- errores humanos;

- no conformidades con políticas o directrices;
- violaciones de acuerdos de seguridad física;
- cambios no controlados en el sistema;
- mal funcionamiento en el software o hardware;
- violaciones de acceso.
- indisponibilidad, desempeño o anormal prestación de un trámite o servicio institucional
- se evidencia el recibo o envió de correo(s) electrónico(s) (SPAM)
- se dificulta la prestación de los servicios a la ciudadanía o de los servicios internos / externos.
- otro comportamiento anómalo a un sistema de información, ya que puede ser un indicador de un incidente de seguridad de la información.

Referencia: GTC ISO/IEC 27002:2015, númeral 16.1.2 Reporte de eventos de seguridad de la información y GUÍA DE GESTIÓN DE INCIDENTES

Ejecutantes

Asistencial, Técnico, Profesional Universitario, Profesional Especializado, Asesor, Directivo

Duración

30.00

1.7.9. Validar y analizar el evento de seguridad

Descripción

Realizar la evaluación del evento reportado, diligenciando el formato "Condiciones para validación de eventos de Seguridad de la Información", en donde se listan algunas características que clasifican el evento como un incidente de seguridad de la información y debe escalarse al nivel correspondiente para que se realicen las actividades respectivas para la contención, o por el contrario si el personal de la mesa de servicios está en capacidad de resolver el caso, debe atenderse de acuerdo al procedimiento. Debe informarse al Grupo de seguridad de la información acerca del evento de seguridad reportado, para que realicen seguimiento hasta el cierre del caso.

Ejecutantes

Profesional Universitario, Técnico

Duración

120.00

1.7.10. PR-TI-06 Gestión de servicios de tecnologías de la información

Descripción

Este paso hace referencia al procedimiento establecido de la Gestión de servicios de soporte de TI prestados por la mesa de servicios. Mayor información disponible en documento "PR-TI-06 Gestión de Servicios de TI".

Ejecutantes

Asistencial, Técnico, Profesional Universitario, Profesional Especializado

1.7.11. Clasificar el caso en evento de seguridad

Descripción

Validar las condiciones del caso y determinar si corresponde a un evento o incidente de seguridad de la información.

Ejecutantes

Técnico, Profesional Universitario

Duración

60.00

1.7.12. ¿Esta en capacidad de resolverlo?

Descripción

Una vez analizado y clasificado el evento se debe considerar si la mesa de ayuda puede resolver el evento.

Flujos

Si

Condición

Determinar acciones inmediatas y solucionar el evento ó incidente

No

Condición

Escalar el evento ó incidente

1.7.13. Escalar el evento o incidente

Descripción

En caso de NO tener la capacidad para resolver el incidente, la mesa de servicios debe escalar el evento de seguridad de la información de acuerdo a lo establecido en el procedimiento PR-TI-06 Gestión de servicios de tecnologías de la información. Además, debe informar el caso a través de correo electrónico al equipo de seguridad de la información.

Ejecutantes

Técnico, Profesional Universitario

Duración

30.00

1.7.14. ¿Es un incidente de seguridad?

Descripción

Se realiza un análisis de la situación reportada para determinar si corresponde a un incidente de seguridad de la información, y no a un evento, es decir donde se identifique que efectivamente se materializó un riesgo de seguridad de la información.

Flujos

No

Condición

Determinar acciones inmediatas y solucionar el evento

Si

Condición

Comunicar incidente

1.7.15. Comunicar incidente

Descripción

Comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o a las partes interesadas.

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

60.00

1.7.16. Clasificar el incidente de seguridad

Descripción

El incidente debe enmarcarse en alguna de las siguientes categorías de clasificación :

- acceso no autorizado,
- modificación de recursos no autorizado,
- uso inapropiado de recursos,
- no disponibilidad de los recursos,
- compromiso del sistema,
- multicomponente

y las demás categorías establecidas en la GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Ejecutantes

Profesional Universitario, Profesional Especializado

Duración

60.00

1.7.17. Priorizar incidente de seguridad

Descripción

Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación) se debe determinar el nivel de prioridad del mismo y de esta manera atenderlos según la necesidad, es claro que los incidentes no deben manejarse por orden de llegada, estos deben priorizarse de acuerdo a la criticidad de los activos de información afectados, por tanto, se deben tener en cuenta los niveles establecidos en la GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

60.00

1.7.18. ¿Afecta la continuidad de los servicios de TI?

Descripción

Es un evento de desastre, interrupción o un evento de contingencia

Flujos

No

Condición

Contener el incidente

1.7.19. Informar al Oficial de Continuidad

Descripción

El (la) Subdirector (a) Técnico (a) de Recursos Tecnológicos debe informar al Oficial de Continuidad que se presentó un incidente de seguridad que puede afectar la continuidad de la operación de la Entidad.

Ejecutantes

Directivo, Profesional Especializado

Responsable

Directivo

Duración

20.00

1.7.20. Contener el incidente

Descripción

Esta actividad busca detener o como su nombre lo indica, contener el incidente con el fin de que no se propague y no puedan generar más daños a la información o a la infraestructura tecnológica de la Entidad. Las estrategias/acciones de contención que se pueden considerar son:

1. Aislar el componente, activo o elemento que está afectado.

2. Apagar o mantener encendido el sistema afectado:

3. Bloquear servicios afectados o áreas afectadas

4. Evaluar la posibilidad de implementar o activar un control adicional mientras está en curso el incidente

5. Solicitar apoyo de terceros especializados que puedan aplicar acciones de contingencia, por ejemplo: solicitar al proveedor del servicio de internet - ISP que bloquee tráfico entrante; en caso de incidentes que afecten la infraestructura tecnológica, solicitar el apoyo CSIRT de Gobierno csirtgob@mintic.gov.co, centro cibernético policíal CCP CAI Virtual https://caivirtual.policía.gov.co/ , Fiscalía General de la Nación o al Grupo de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT.)

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

1200.00

1.7.21. ¿Se requiere Investigación Forense?

Descripción

Verificar si existe la necesidad de realizar el análisis de evidencia digital al incidente reportado.

Flujos

No

Si

Condición

Realizar análisis de evidencia digital

1.7.22. Realizar análisis de evidencia digital

Descripción

Como primera medida y de acuerdo al tipo de incidente el primer respondiente (Oficial de seguridad), se recomienda reportar inmediatamente a las autoridades CSIRT Gobierno, COLCERT y/o Fiscalía según sea el caso para apoyo y asesoría para proceder con la atención del incidente y recolección de evidencia forense. Se deben consolidar todas las evidencias posibles del incidente.

Ejecutantes

Profesional Universitario, Profesional Especializado

Duración

2600.00

1.7.23. ¿Se requiere notificar a entes de control?

Descripción

En caso de que el incidente corresponda a la violación de políticas de seguridad por parte de los servidore públicos o contratistas de prestación de servicios de a´poyo a la gestión, se deberá remitir el informe del incidente a la Oficina de Control Disciplinario o a la Procuraduría, según corresponda.

Flujos

Si

Condición

Preparar informe y enviarlo a OCD o a la Procuraduría General de la Nación

No

Condición

Erradicación y recuperación

1.7.24. Preparar informe y enviarlo a OCD o a la Procuraduría General de la Nación

Descripción

Se debe informar del incidente a la Oficina de Control Disciplinario para que se de inicio a la investigación disciplinaria o a la Procuraduría General de la Nación, según corresponda. El informe debe ser enviado por los medios autorizados, teniendo en cuenta la clasificación de la información contenida en el mismo.

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

1440.00

1.7.25. Determinar acciones inmediatas y solucionar el evento

Descripción

Brindar el apoyo para la solución al evento de seguridad

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

480.00

1.7.26. Comunicar reporte del evento de seguridad

Descripción

Comunicar a los usuarios afectados sobre los acontecimientos ocurridos, de tal manera que se promuevan las medidas de prevención y recomendaciones que sean convenientes.

Ejecutantes

Profesional Universitario, Profesional Especializado

Duración

120.00

1.7.27. Documentar la respuesta de soporte en la base de datos de conocimiento (KDB)

Descripción

Documentar la totalidad de las acciones que se tomaron para atender el evento en la base de datos de conocimiento (KDB).

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

240.00

1.7.28. Cerrar el caso

Descripción

Cerrar el caso en la mesa de servicios.

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

60.00

1.7.29. Determinar acciones inmediatas y solucionar el evento

Descripción

Realizar las actividades que corresponda para solucionar el evento

Ejecutantes

Profesional Universitario, Técnico

Duración

480.00

1.7.30. Documentar la respuesta de soporte en la base de datos de conocimiento (KDB)

Descripción

Documentar la totalidad de las acciones que se tomaron para atender el evento en la base de datos de conocimiento (KDB) e informar al grupo de seguridad de la información siempre que se trate de un evento de seguridad de la información. En este caso el equipo de seguridad debe estar informado del caso para tomar las medidas correctivas o preventivas a las que haya lugar.

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

240.00

1.7.31. Cierre el caso

Descripción

Cerrar el caso

Ejecutantes

Profesional Universitario, Técnico

Duración

60.00

1.7.32. Erradicación y recuperación

Descripción

Se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente, por ejemplo:

· Restauración del servicio caído.

· Corrección de efectos producidos.

· Restauración de backups.

· Reparar el sitio web.

· Re-instalación del equipo (PC, servidor o equipo activo de red) y recuperación de datos.

Posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador del sistema o del recurso de TI o quien haga sus veces, debe restablecer la funcionalidad de los sistemas afectados, y realizar un proceso de fortalecimiento (hardening) del sistema que permita prevenir incidentes similares en el futuro.

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

3000.00

1.7.33. Actualizar matriz de riesgos SGSI

Descripción

Verificar si con el incidente presentado se materializaron uno o más riesgos de seguridad de la información, y de ser necesario se debe actualizar la matriz de riesgo para la verificación de los controles existentes y el plan de tratamiento.

Duración

180.00

1.7.34. Preparar informe de gestión de incidentes

Descripción

Esta actividad consiste en recopilar la información más relevante de los eventos e incidentes atendidos, así como los aspectos más relevantes de los resultados obtenidos del incidente de seguridad de la información, con el objetivo de mitigar futuras incidencias que puedan presentar similitud con la incidencia, mantener actualizada la documentación de las "lecciones aprendidas" y fomentar procesos de concienciación sobre seguridad de la información en toda la Entidad.

Ejecutantes

Profesional Universitario, Profesional Especializado

1.7.35. Presentar Informe

Descripción

El equipo de seguridad de la información debe generar un informe lo sucedido en el FORMATO DE INFORME DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN y presentarlo al (a la) Subdirector(a) Técnico(a) de Recursos Tecnológicos.

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

240.00

1.7.36. Comunicar reporte del Incidente

Descripción

Se debe comunicar a las partes interesas involucradas en el incidente sobre los acontecimientos ocurridos, de tal manera que se promuevan las medidas de prevención que sean convenientes.

Uno de los aspectos importantes que se debe tener en cuenta para lograr una comunicación asertiva, es incluir las lecciones aprendidas.

Ejecutantes

Profesional Universitario, Profesional Especializado

Duración

240.00

1.7.37. ¿El incidente podría tener impacto distrital o nacional

Descripción

Tras el análisis del incidente, se verifica si la vulnerabilidad puede afectar a entidades del orden distrital o nacional.

Flujos

No

Condición

Fin

Si

Condición

Reportarlo a los equipos de atención de incidentes del gobierno - CSIRT- Gobierno

1.7.38. Reportarlo a los equipos de atención de incidentes del gobierno - CSIRT- Gobierno

Descripción

En caso de requerir que se reporte el incidente a las terceras partes, ver las relacionadas en la Guía para la atención de eventos e incidentes de seguridad de la información, si se requiere apoyo para la gestión del incidente, o es un caso que podría tener impacto nacional.

Ejecutantes

Profesional Especializado, Profesional Universitario

Duración

120.00

1.7.39. Fin

Descripción

Finaliza procedimiento.

1.7.40. Formato evidencia forense diligenciado

Descripción

Formato para diligenciar las etapas del análisis forense, incluyendo la cadena de custodia. En este caso se puede emplear el formato IDU, el de un proveedor de este servicio o el de cualquier entidad nacional o distrital competente.

1.7.41. GU-TI-03 Guía análisis forense para incidentes seguridad de la información

Descripción

Brindar lineamientos necesarios para asegurar, identificar, recolectar, preservar y presentar la evidencia forense referente a incidentes de seguridad de la información que se presenten en la plataforma tecnológica del IDU,

1.7.42. Condiciones para validación de eventos de Seguridad de la Información (FO-TI-28)

Descripción

Este es un formato de apoyo para los prestadores de soporte de primer nivel, con el fin de identificar sí algún evento en curso o atendido, se considera un evento o posible Incidente de Seguridad de la Información.