I. INFORMACIÓN GENERAL

1. LIDER DE PROCESO: Jefe de la Oficina de Tecnologías de la Información

1.1 OBJETIVO DEL PROCEDIMIENTO: Formalizar el conjunto de lineamientos que se deben ejecutar para la gestión de eventos e incidentes de seguridad de la información, a través de las actividades de preparación, detección y atención de posibles eventos e incidentes de seguridad de la información en la Secretaría de Cultura, Recreación y Deporte - SCRD

1.2 ALCANCE DEL PROCEDIMIENTO: Comienza con el reporte de eventos o incidentes de seguridad y termina con la divulgación de las lecciones aprendidas una vez terminada la gestión del evento o incidente de seguridad de la información en la Secretaría de Cultura, Recreación y Deporte- SCRD.

1.3 RESPONSABLE DEL PROCEDIMIENTO: Jefe de la Oficina de Tecnologías de la Información

1.4 CORRESPONSABLES DEL PROCEDIMIENTO: Jefe de la Oficina de Tecnologías de la Información

2. GLOSARIO:

Activo de Información: Es aquel activo que mantiene, resguarda, almacena o procesa información. Dentro de estos se puede encontrar el software, hardware, personas, información física y digital, servicios de información, servicios de comunicación, servicios de almacenamiento y la imagen de la entidad.

CSIRT: Equipo de Respuesta de Incidentes de Seguridad, este puede ser de orden Nacional o Distrital (cuando se encuentre operativo)

Confidencialidad: Es uno de los pilares de la seguridad de la información y este implica el acceso a la información por parte únicamente de quienes están autorizados.

Disponibilidad: Es uno de los pilares de la seguridad de la información y este indica que la información pueda estar accesible y utilizable cuando lo requiera un usuario autorizado.

DOS: Denegación de Servicios.

DRP: Plan de Recuperación de Desastres tecnológico (cuando se encuentre operativo)

Evento de Seguridad de la Información: Acontecimiento identificado en el estado de un sistema, servicio o red que indica un posible incumplimiento o falla en las políticas o controles de seguridad de la información o de una situación desconocida que puede ser relevante para la seguridad.

Incidente de Seguridad de la Información: Uno o una serie de eventos de seguridad de la información inesperados o no deseados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información

Integridad: Es uno de los pilares de la seguridad de la información y este conlleva el mantenimiento de la exactitud y completitud de la información.

OTI: Oficina de Tecnologías de la Información

Requerimiento: Este proceso se refiere a todas las solicitudes que generan los usuarios y que no están asociadas a un incidente en un servicio de TI.

3. POLÍTICAS DE OPERACIÓN:

3.1 Preparación

Define que durante el estado previo a la declaración de un ciberincidente es necesario que la SCRD esté preparada para cualquier suceso que pueda presentarse. La anticipación y entrenamiento previo pueden marcar la diferencia entre una gestión eficaz o un desastre en el momento de gestionar el incidente, esta preparación debe estar enfocada en los 3 componentes fundamentales (personas, procedimientos y tecnología). Por tal razón el presente procedimiento establece 5 actividades preliminares que deben establecerse antes de la ejecución del procedimiento:

- **Conformar el equipo de respuesta a incidentes:** El Jefe de la OTI (Oficina de Tecnologías de la Información) en conjunto con el equipo de seguridad, deben conformar un equipo interdisciplinario que pueda atender de forma oportuna los posibles incidentes de seguridad de la información que se pudieran presentar en la operación de los diferentes procesos institucionales de la Secretaría de Cultura, Recreación y Deporte - SCRD o durante la prestación de los servicios soportados en soluciones tecnológicas que son ofrecidos a las diferentes partes interesadas. En principio, este equipo debe ser conformado por lo menos con un representante de cada equipo de trabajo de la OTI:
    - Mesa de servicios de la OTI
    - Infraestructura de TI
    - Desarrollo de soluciones de TI
    - Apoyo a la gestión TIC
    - Seguridad de la Información y la Ciberseguridad.

- **Realizar actividades de formación, entrenamiento y Sensibilización**: El jefe de la OTI y el equipo de seguridad debe convalidar los perfiles de los miembros en razón a su formación, experiencia y capacidad, con el propósito de identificar las necesidades de formación y entrenamiento que permitan desarrollar las capacidades necesarias para implementar este procedimiento y para dar oportuna respuesta ante un incidente de seguridad de la información o ciberincidente. El resultado de esta actividad será un documento que describa las actividades, metas, entregables, fechas y responsables de ejecución para desarrollar un plan de formación y entrenamiento para el equipo de respuesta y atención de incidentes.

  El equipo de seguridad, debe diseñar espacios de sensibilización respecto a la importancia del oportuno reporte de cualquier debilidad de los controles de ciberseguridad desplegados o sobre las oportunidades de mejora de los mismos. Estas jornadas deben ser convocadas y presentadas para todos los colaboradores y se deben desplegar mecanismos de valoración de su efectividad

- **Definir escenarios probables:** El equipo de seguridad, tomando como base la información de la gestión de incidentes de seguridad de la información de años anteriores, así como también los datos consignados en la herramienta de apoyo a la gestión de la mesa de servicios de TI y la experiencia del equipo de atención de incidentes de seguridad y ciberseguridad, se debe identificar las amenazas (físicas, lógicas y cibernéticas), información proveniente de fuentes externas especializadas en ciberseguridad y con los resultados de la gestión de riesgos de seguridad de la información se deben diseñar y documentar los posibles escenarios de materialización de riesgos de seguridad y de esta manera poder establecer la actuación del equipo de atención de incidentes. Para elaborar escenarios adecuados, es necesario tener en consideración al menos los siguientes elementos expuestos por el CSIRT (Equipo de Respuesta de Incidentes de Seguridad) del Gobierno:

    - Características de la afectación en los sistemas de información o en la infraestructura de TI
    - Patrones de comportamiento detectados y
    - Afectación de los pilares de seguridad de información (confidencialidad, integridad o disponibilidad).

- **Asistir a eventos de sensibilización**: Los usuarios deben asistir, participar, entender, comprender apropiar e interiorizar las buenas prácticas de seguridad originadas en los espacios de sensibilización y formación definidos por el equipo de seguridad, con el fin de aplicarlas en la cotidianidad de sus actividades, tanto para prevenir la ocurrencia de posibles eventos negativos o incidentes de seguridad de la información, o para reconocer los canales de reporte y atención de estos.

- **Reportar eventos sospechosos:** Los usuarios deben reportar a través de los diferentes canales de comunicación de la mesa de servicios de TI del Grupo TIC de la Secretaría de Cultura, Recreación y Deporte - SCRD, que se están presentando eventos, anomalías o incidentes en el entorno de trabajo (físico o lógico) al cual tiene acceso, bien sea de forma cotidiana o de forma ocasional. Los usuarios o colaboradores pueden reportar todos los eventos, incidentes,

debilidades o situaciones sospechosas que consideren que están ocurriendo, estos informes o reportes, serán tratados de forma confidencial y serán debidamente gestionados desde los diferentes equipos de la mesa de servicios de TI, atención y respuesta de incidentes, el equipo de seguridad o cualquier miembro competente del Grupo TI de la entidad. A continuación, se presentan los canales de comunicación para el debido reporte.

- Plataforma de Mesa de servicios de la OTI.
- Correo electrónico de cualquier funcionario de la OTI.
- Presencial acercándose a la oficina de la OTI.

3.2 Detección y Análisis del Evento o Incidente

A partir del momento del reporte del evento o incidente se inicia la fase de detección y análisis, en donde la identificación de lo ocurrido juega un papel imprescindible por lo cual bajo el principio de “necesidad de conocer” bajo estricta confidencialidad y compartiendo la información solamente con aquellas personas implicadas que realmente necesiten conocerla.

El responsable de la mesa de servicios de la OTI verificará la situación e indicará si se trata de un evento o incidente de seguridad teniendo como base de conocimiento las siguientes preguntas:

- ¿Se han reportado alertas en los sistemas de seguridad y vigilancia?
- ¿Se detecta “caída” de alguno de los servidores del centro de cómputo?
- ¿La consola del software antivirus está mostrando informes de alerta?
- ¿Se evidencian funcionamientos fuera de lo normal de los sistemas de información?
- ¿Se identifica que el evento fue intencional?
- ¿Se afecta alguno de los procesos misionales de la Secretaría de Cultura, Recreación y Deporte - SCRD?
- ¿Se afecta disponibilidad o acceso a un servicio o activo crítico?
- ¿Afecta la prestación de servicios de uso crítico para los ciudadanos o las entidades adscritas?
- ¿Se incumple alguna norma legal?
- ¿Se incumple alguna política interna o control de seguridad de la información?
- ¿Afecta a un usuario VIP (Secretaría, directores, Asesores, Jefes de Oficina)?
- ¿Afecta a una dependencia crítica?
- ¿Afecta a más de 10 colaboradores de la entidad (funcionarios y/o contratistas)?
- ¿Afecta la imagen institucional?
- ¿Hay divulgación de información no autorizada?
- ¿Hay robo, pérdida o interceptación de activos de información?
- ¿Hay daño de activos de información?
- ¿Afecta la disponibilidad, desempeño o normal prestación de un servicio?
- ¿Afecta la disponibilidad, integridad o confiabilidad de la información?
- ¿Se presenta modificación no autorizada de algún servicio, bases de datos y/o sistema de información?
- ¿Hay acceso no autorizado a un sistema, aplicación, bases de datos o información?
- ¿Hay uso inadecuado de los recursos tecnológicos y/o activos de información?
- ¿El evento se ha presentado previamente, en condiciones similares, durante el último mes?
- ¿Es un evento desconocido?

Una vez identificada la situación se procede con la determinación y criticidad de la misma.

Si es un EVENTO:

Si la situación presentada se considera un evento de seguridad de la información, las acciones a realizar se determinarán de acuerdo con las siguientes escalas:

- **Eventos de Criticidad Baja**: Son eventos que no comprometen la operación normal de los activos de información, procesos o servicios, es decir, que pueden ser controlados en forma paralela a la operación por parte del ingeniero especialista.

- **Eventos de Criticidad Media**: Posibles anomalías o situaciones detectadas por los sistemas de información y/o personas que puedan ser relevantes para la seguridad de la información. Con el fin de evitar que el evento vuelva a ocurrir se deberá implementar controles y/o realizar concientizaciones correspondientes según el caso.
- **Eventos de Criticidad Alta**: Implica el daño de un activo y el posible incumplimiento de una política de seguridad pero que no presenta resultados negativos en cuanto a la afectación de los pilares de seguridad de la información. Con el fin de evitar que el evento vuelva a ocurrir se deberá realizar una solicitud de acción de mejora.

El evento deberá ser reportado en la mesa de servicios de TI y se deberá dar un tratamiento preventivo por parte del responsable encargado de seguridad de la información.

Si es un INCIDENTE:

Resulta imposible disponer de procedimientos para gestionar todos los ciberincidentes que pueden llegar a materializarse, sin embargo, existen unos vectores de ataque comunes que ayudan a identificar un incidente de seguridad, determinar su alcance y los sistemas afectados. Como elementos de apoyo para la mesa de servicio, se presentan algunos vectores utilizados en la taxonomía del Colcert (Grupo de Respuesta a Emergencias Cibernéticas de Colombia):

TAXONOMÍA		
Clasificación	**Definición**	**Tipo de Incidente**
Contenido Abusivo	Ataques destinados a dañar la imagen de la Entidad o utilizar su contenido dañino en recursos electrónicos para usos ilícitos (como publicidad, extorsión o ciberdelincuencia en general)	Spam, Delito de odio, materiales de abuso / explotación sexual infantil, contenido sexual violento o inadecuado
Contenido Dañino	Incidentes relacionados con actividades maliciosas, aplicaciones y archivos dañinos para obtener acceso no autorizado al sistema para sustraer, exfiltrar, eliminar, modificar información privada o afectar la integridad de la información.	Sistema infectado, servidor comprometido (comando y control), distribución y configuración de malware
Obtención de información	Incidentes relacionados con la identificación y recopilación de información de personas, infraestructura tecnológica y activos de información de la entidad a través de técnicas no autorizadas con fines delictivos.	Escaneo de redes (scanning), análisis de paquetes (sniffing), ingeniería social
Intento de Intrusión	Incidentes relacionados con la utilización de técnicas que intentan atacar una infraestructura tecnológica o un activo de información aprovechándose de una vulnerabilidad para obtener el control y privilegios administrativos o de ejecución.	Explotación de vulnerabilidad conocidas, intento de acceso con vulneración de credenciales, ataque desconocido
Intrusión	Ataques que aprovechan las vulnerabilidades de diseño, funcionamiento o configuración de las diferentes tecnologías, para entrar de forma fraudulenta a los sistemas de una organización.	Compromiso de cuenta con y sin privilegios, compromiso de aplicaciones, robo físico.
Disponibilidad	Interrupción de la capacidad de procesamiento y respuesta de los sistemas y redes para dejarlos inoperativos, acción premeditada para dañar un sistema, interrumpir un proceso, cambiar o borrar información.	DOS (Denegación de Servicios), mala configuración, sabotaje, Interrupciones.
Compromiso de información	Incidentes relacionados con el acceso, filtraciones (confidencialidad), la modificación o el borrado (integridad) de información.	Acceso o modificación no autorizado a información, Pérdida de datos.
Fraude	Incidentes relacionados con la pérdida de bienes causada con intención fraudulenta o deshonesta en procura de un beneficio económico para sí mismo u otra persona o entidad.	Uso no autorizado de recursos, derechos de autor, suplantación, phishing.

Si la situación presentada se considera un evento o incidente de seguridad de la información o ciberseguridad se deberá indicar el impacto de acuerdo con los siguientes NIVELES/IMPACTOS:

NIVEL/IMPACTO	DESCRIPCIÓN
CRÍTICO	Eventos de seguridad que implican un paro total o suspensión de las operaciones de la entidad por un tiempo prolongado
MAYOR	Eventos de seguridad que comprometen la operación normal de algunos procesos de la entidad pero que pueden ser controlados en forma paralela al desarrollo de las demás actividades de la Secretaría de Cultura, Recreación y Deporte - SCRD
MODERADO	Eventos que comprometen la integridad, confidencialidad o disponibilidad de las operaciones de la entidad de forma muy leve, y que por lo tanto no requieren una acción inmediata
MENOR	Eventos que comprometen la integridad, confidencialidad y/o disponibilidad a un grupo localizado de usuarios o que causen un impacto muy limitado de las operaciones de la entidad, y que por lo tanto no requieren una acción inmediata
SOPORTE	Eventos que no comprometen las operaciones del negocio y que afectan a solo un usuario y que por lo tanto pueden tramitarse como un REQUERIMIENTO O SOLICITUD DE TIC.

En caso de que la situación reportada sea un incidente repetitivo o definido como problema, el **responsable de seguridad de la información** deberá escalar el caso al Jefe de la OTI, quien deberá realizar las actividades necesarias para establecer la causa raíz del incidente.

Una vez clasificado el incidente según su impacto, y si su clasificación se encuentra entre menor y crítico, deberá asignarse al responsable encargado de la gestión de incidentes de seguridad.

3.3 Gestión del Incidente

En la gestión de incidentes se encuentran 3 tipos de actividades descritas a continuación:

- **Actividades de Contención:** Es la fase en la que se toman las decisiones de forma rápida y oportuna ya que el tiempo es un factor determinante y la reputación o la continuidad de la Entidad estarán a prueba, por lo tanto dependerá de las acciones asertivas. La documentación de cada paso que se tome o cada actividad que se observe o ejecute durante esta fase resulta de gran importancia para incluir en la herramienta de gestión de la mesa de servicios de TI. Es preciso señalar que se debe tener a la mano información relevante relacionada a la operación tecnológica de la Secretaría de Cultura, Recreación y Deporte - SCRD, la cual debe incluir diagramas de relación y/o de dependencia en donde se identifican los elementos de configuración necesarios para que cada servicio crítico pueda operar normalmente además de listas de responsables de operación y despliegue, contactos claves de los usuarios funcionales.

  Algunas de las actividades de contención podrían ser las siguientes:
  - Revisar si la situación se ha presentado consultando la base de datos de conocimiento y ejecutar las tareas allí documentadas.
  - Si es una nueva situación, se debe definir un plan de acción y ejecutarlo.
  - Desconectar el equipo o aislarlo del segmento de red.
  - Solicitar el aislamiento de red de un segmento específico.
  - Desconectar físicamente dispositivos de la red local.
  - Deshabilitar servicios.
  - Implementación y colocación de equipos o servicios complementarios de seguridad perimetral.
  - Reubicar el recurso comprometido en una VLAN aislada.
  - Considerar la aplicación de técnicas de DNS para controlar tráfico malicioso
  - Bloqueo de determinados correos electrónicos
  - Aplicar reglas en los Firewall
  - Bloquear acceso a unidades compartidas

- Contactar a las entidades externas que puedan ofrecer ayuda en la contención. Los proveedores de servicio de Internet pueden aplicar filtros o activar medidas de protección, el COLCERT o el CSIRT de gobierno puede ofrecer información adicional y coordinación a nivel sectorial, nacional e internacional con otros posibles implicados en el incidente.

- **Actividades de Mitigación o Erradicación:** Una vez que se ha logrado contener el incidente y con ello su propagación se procede a definir las actividades de mitigación las cuales podrían ser las siguiente:
  - Realizar un borrado seguro de los equipos o medios de almacenamiento comprometidos. Esto solo deberá ocurrir si el equipo de la atención del incidente considera que no es pertinente preservar la evidencia digital del incidente.
  - Reinstalar el sistema a través de las copias de seguridad recientes.
  - Consultar a los proveedores de los elementos de la seguridad perimetral las recomendaciones pertinentes para una eventual mitigación del incidente
  - Revisar los registros de auditoría de los elementos de configuración afectados.
  - Establecer las causas del incidente.
  - Gestionar las vulnerabilidades realizando actividades de remediación.
  - Aplicar parches de seguridad
  - Actualizar los sistemas operativos.

- **Actividades de Recuperación**: La finalidad de la fase de recuperación consiste en devolver el nivel de operación de TI a su estado normal y que las diferentes dependencias de la entidad afectadas puedan retomar su actividad y brindar sus servicios misionales. Es preciso prestar especial atención a los sistemas comprometidos durante la puesta en producción y buscar cualquier signo de actividad sospechosa como procesos inusuales, cuentas de usuario no autorizadas, nuevas entradas en el registro, conexiones no identificadas, cualquier síntoma que pueda indicar que el problema está volviendo a ocurrir.

  Existe la posibilidad de que durante la puesta en producción del sistema restaurado se reproduzca el problema original o algún otro que tenga como objetivo alguno de los activos de nuestro dominio. En estos casos será necesario volver a aplicar las medidas de contención y erradicación que se definan en la Secretaría de Cultura, Recreación y Deporte - SCRD

  Una vez ejecutadas las acciones necesarias para contener, erradicar y recuperar el incidente, se deberá iniciar con el monitoreo de este, para verificar que la situación ha sido controlada adecuadamente, el monitoreo del incidente se deberá realizar según lo determine el responsable encargado de seguridad de la información. Si el incidente se presenta nuevamente se deberá volver a gestionar el mismo hasta encontrar nuevas soluciones y la verdadera causa raíz.

3.4 Gestión Post Incidente:

La finalidad de esta etapa es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar que pueda volver a repetirse; además se evalúan los procedimientos de actuación, la cadena de mando, las políticas de seguridad, en pocas palabras, se evalúa el ciclo de respuesta surtido o ejecutado por el equipo designado y por todos los actores claves vinculados al incidente. Cada miembro del equipo implicado en la gestión del incidente o ciberincidente debe aportar sus anotaciones o papeles de trabajo y todas deben ser tenidas en cuenta en la documentación del incidente, así como también los tiempos de ejecución de cada una de sus acciones. Una buena práctica es la realización del informe post-incidente el cual debe incluir un breve resumen ejecutivo y anexos técnicos para ser socializado a la alta dirección de la Secretaría de Cultura, Recreación y Deporte - SCRD, así como también al equipo técnico de esta manera aporta valor para la base de datos de conocimiento definida en la herramienta de gestión y apoyará la atención de eventos o incidentes similares en un futuro. Como producto de esta fase también se encuentran las siguientes actividades:

- **Documentar lecciones aprendidas:** El responsable encargado de la gestión de incidentes, junto con el equipo responsable de la atención del mismo, deberá determinar si existen lecciones aprendidas o un aprendizaje incluyendo los siguientes aspectos:

  - Número de incidente de seguridad: Se debe relacionar el ID del incidente creado en la herramienta de Mesa de servicios de la OTI o en la base de datos de conocimiento.

- Palabra clave: Nombre con el cual se pueden consultar los incidentes respecto a un tema determinado.
- Descripción del incidente: Que fue lo que ocurrió para que se evidenciara el incidente.
- Causa Raíz: Cuál fue la causa raíz que ocasionó el incidente
- Acciones realizadas para la solución: Cómo se logró restablecer el servicio o solucionar el incidente.
- Acciones que no se realizaron y se debieron realizar oportunamente
- Acciones que se ejecutaron y que al final no aportaron para la solución del incidente y las cuales no se deberían repetir.
- Lecciones aprendidas: Cuáles son las acciones que se deben seguir para evitar que el incidente se vuelva a presentar o para minimizar el impacto de la ocurrencia.

Si el incidente puede ser utilizado a modo de concientización, se comunicará a todos los funcionarios de la Secretaría de Cultura, Recreación y Deporte - SCRD con el fin de evitar su recurrencia.

3.5 **Reglas específicas**

Es responsabilidad de la totalidad de los colaboradores de la Secretaría de Cultura, Recreación y Deporte - SCRD, reportar todos los eventos de seguridad de la información y ciberseguridad, los cuales se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

Durante la atención de un evento reportado, las únicas personas autorizadas a emitir comunicaciones respecto a esta situación será el Jefe de la OTI y aquellos que él designe formalmente para esta actividad, cualquier información o reporte sobre el incidente deberá ser aprobado por él. Cualquier otro tipo de información no autorizada, no será considerada como válida y quien la emita puede ser sujeto a investigación.

Se debe llevar un control detallado de las actividades emprendidas para atender el evento y las mismas se verán reflejadas en la herramienta de mesa de servicios de TI.

El equipo de atención y respuesta a incidentes de seguridad dispondrá al menos de un equipo de cómputo configurado con las herramientas suficientes y necesarias para adelantar tareas de diagnóstico y/o conexión a los diferentes recursos tecnológicos desplegados en la Secretaría de Cultura, Recreación y Deporte - SCRD, sin que esto excluya la posibilidad de hacer uso de cualquier equipo de cómputo asignado a cualquier usuario, en los casos de emergencia tecnológica declarada.

Este procedimiento será activado cuantas veces sea necesario para atender cualquier evento que pueda afectar el normal funcionamiento de los procesos institucionales o algún recurso tecnológico de la Secretaría de Cultura, Recreación y Deporte - SCRD.

El objetivo principal del procedimiento y de quienes intervienen en él, es que la causa que provocó el incidente no se vuelva a presentar, sin embargo, en la medida de lo posible se debe procurar conservar evidencia de la situación presentada en cada elemento (imágenes forenses, respaldos, registros fotográficos, registros de auditoría) de tal forma que sea posible, en una etapa posterior hacer análisis más detallados y/o conformar un “acervo probatorio” válido para instaurar un proceso legal.

La documentación del incidente será la base para la construcción de una base de datos de conocimiento (KDB), y fuente principal para la atención de futuros eventos de características similares, además de aportar una fuente de información importante para realizar una gestión preventiva de problemas o fallas y también una fuente de datos para la medición de la disponibilidad de la plataforma tecnológica.

Independientemente a las capacidades que se logren con el despliegue del procedimiento de gestión de incidentes de seguridad y la conformación del equipo de atención y respuesta a incidentes de seguridad, todos los procesos institucionales deberán contar con planes de contingencia para sus actividades y servicios más críticos.

4. RELACIÓN CON OTROS PROCEDIMIENTOS Y PROCESOS:

Procesos que se requieren como proveedor	Que insumos requiere del proveedor	Procedimiento	Que se obtiene del procedimiento	Para quien va dirigido el servicio o producto

GESTION DE TECNOLOGIAS DE LA INFORMACIÒN Y LAS COMUNICACIONES	Reporte de eventos o incidentes de seguridad de la información en la herramienta de mesa de servicios de TI.	Procedimiento de soporte y mantenimiento en las soluciones y servicios tecnológicos.	Registro y gestión de soporte y mantenimiento de las soluciones y servicios tecnológicos.	Usuarios de la entidad

II. ACTIVIDADES Y PUNTOS DE CONTROL

NO.	Actividad	Descripción	Responsable	Tiempo	Documento o Registro
1.	Reportar eventos sospechosos	Esta actividad consiste en reportar a la mesa de servicios de TI de la OTI de la Secretaría de Cultura, Recreación y Deporte - SCRD, a través de la herramienta GLPI o a través de un mensaje de correo electrónico, que se está presentando un evento o anomalía en el entorno de trabajo (físico o lógico) al cual tiene acceso, bien sea de forma cotidiana o de forma ocasional.	Usuarios	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI o correo electrónico
2.	Recopilar datos	Con el reporte recibido, el colaborador de la mesa de servicios de TI, en la medida de lo posible, debe empezar a recopilar datos básicos de ubicación del usuario, del activo, del servicio entre otros datos que permitan adelantar las validaciones correspondientes. Entre otros datos que se pueden recopilar se encuentran: Del usuario: - Nombre completo - Cuenta de usuario - Dependencia - Puesto de trabajo actual (Secretaría de Cultura, Recreación y Deporte - SCRD o remoto) Del activo - Identificador del activo (Placa de inventario para activos fijos, ID del inventario para activos de información) - Tipo de activo - Descripción del activo - Especificaciones técnicas (si se tienen) - Ubicación del activo - Propietario y Usuario Del servicio - Nombre del servicio - Tipo de servicio - Direccionamiento (URL o IP) - Responsable del servicio en GTIC	Profesional Mesa de servicios de TI	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
3.	Validar sucesos o eventos	Esta actividad es propia de los colaboradores de la mesa de servicios de TI, en donde se debe revisar e identificar el evento que ha sido reportado, bien sea por una consulta en la herramienta correspondiente o con una validación personalizada del caso. Con los elementos confrontados, se debe proceder a clasificar y priorizar o re direccionar a un colaborador del grupo de solucionadores. **¿Es un incidente de seguridad?** Tomando como base el resultado de la identificación del evento, debilidad o incidente, se determina si es probable que se esté presentando un incidente de seguridad. Si: Continuar con actividad 5.	Profesional Mesa de servicios de TI	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI

NO.	Actividad	Descripción	Responsable	Tiempo	Documento o Registro
		No: Continuar con actividad 4			
4.	Gestionar los Servicios TI	Realizar las actividades respectivas conforme al procedimiento TIC-PR-02 Soporte y mantenimiento en las soluciones tecnológicas. FIN DEL PROCEDIMIENTO.	Profesional de Mesa de servicios de TI	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
5.	Marcar evento como incidente de seguridad	Con una probable situación de un incidente de seguridad en curso, se procede a marcar el caso en la herramienta de gestión de mesa de servicios TI, bajo la categoría correspondiente, a fin de llevar a cabo los controles y registros correspondientes.	Profesional de Mesa de servicios de TI	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
6.	Clasificar incidente por escenario	De acuerdo con las definiciones revisadas por el equipo de atención y respuesta a incidentes de seguridad y el equipo de seguridad de la información, se debe clasificar el incidente en alguna de las categorías allí expuestas. Si los escenarios propuestos no se ajustan al incidente que se está gestionando, se debe informar a estos equipos, para que se hagan los ajustes correspondientes. **Ver Taxonomía.** **¿El incidente es Mayor o crítico?** Si en el ejercicio de clasificación y asociación con escenario o impacto, se identifica que es un incidente Mayor o Crítico (**Ver Nivel / Impacto**), este se debe reportar al CSIRT - ColCERT, de lo contrario continua la gestión interna. Si Continuar con actividad 7. No: Continuar con actividad 14.	Profesional de Mesa de servicios de TI	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
7.	Informar al Jefe de la OTI y al Profesional encargado de la Seguridad de la Información.	Indistintamente de la clase del incidente de seguridad o ciberseguridad, es necesario informar al responsable del proceso de Gestión de Tecnologías de la Información y las Comunicaciones y al Profesional encargado de la Seguridad de la Información lo anterior debido a que previamente a reportar al ColCERT - CSIRT, dichos líderes deben tener conocimiento de la situación. Este reporte enviado mediante correo electrónico, se convierte en una constante retroalimentación de las acciones subsecuentes, los hallazgos, las hipótesis y la recepción de necesidades de apoyo (interno o externo) que se vayan presentando.	Equipo de respuesta a incidentes	1 día	Correo electrónico
8.	Reportar al ColCERT (CSIRT Gobierno)	Para dar adecuado cumplimiento a los requisitos emitidos por las autoridades competentes, todos los incidentes deben ser reportados, sin embargo, para los casos de aquellos que se clasifican como Graves o Muy Graves, se debe remitir un informe preliminar de la situación al ColCERT - CSIRT a través de los siguientes canales: Buzón de correo: contacto@colcert.gov.co Línea directa: +57 601 344 2222	Equipo de respuesta a incidentes	1 día	Reporte al CSIRT en el formato predefinido

NO.	Actividad	Descripción	Responsable	Tiempo	Documento o Registro
		Sitio web: https://www.colcert.gov.co -https://www.colcert.gov.co/800/w3-article-198656.html#formulario_i__form_ReporteIncidentes_1			
9.	Contener el evento o incidente y validar la acciones realizadas	El propósito principal de esta actividad es ejecutar la acciones de contención para detener el incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI o a la operación de la Secretaría de Cultura, Recreación y Deporte - SCRD en cualquiera de sus dependencias. Además se genera el registro de las actividades realizadas en la herramienta de mesa de servicios TI. **Ver Actividades de contención, citadas en el numeral 3.3 Gestión de incidentes de las Políticas de operación de este procedimiento.** **Punto de Control** El profesional del equipo de respuesta a incidentes verifica que las acciones adoptadas hayan evitado su propagación. **¿Fue contenido el incidente?** Si: Continuar con la actividad 11. No: Continuar con la actividad 10.	Equipo de respuesta a incidentes	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
10.	Aplicar mitigaciones	Tomando como base la documentación disponible de la configuración del servicio, se deben activar regiones más detalladas para identificar las afectaciones presentadas y los niveles de propagación del evento. En caso de ser necesario, se debe validar la disponibilidad de acceso a la copia de seguridad más reciente de cada elemento de configuración afectado. En caso de tener elementos de software se pueden restaurar estos respaldos, pero si se trata de equipamiento físico será necesario contactar al proveedor de soporte para validar acciones de remediación posibles. Se debe generar el registro de las actividades realizadas en la herramienta de mesa de servicios TI. Ver **Actividades de Mitigación o Erradicación citadas en el numeral 3.3 Gestión de incidentes de las Políticas de operación de este procedimiento.**	Equipo de respuesta a incidentes	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
11.	Erradicar el evento o incidente	Para facilitar este proceso de erradicación, en primer lugar, se deben revisar los registros de auditoría de los elementos de configuración del servicio afectado y en segundo lugar se debería realizar una revisión de las verdaderas causas, para lo cual se recomienda usar alguno de los métodos de “análisis de causa raíz” con que cuente la Secretaría de	Equipo de respuesta a incidentes	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI

NO.	Actividad	Descripción	Responsable	Tiempo	Documento o Registro
		Cultura, Recreación y Deporte - SCRD y con base en los resultados de dichas acciones adoptar o sugerir las medidas pertinentes. Se debe generar el registro de las actividades realizadas en la herramienta de mesa de servicios TI.			
12.	Gestionar amenazas y vulnerabilidades	Paso seguido, se deben aplicar acciones de gestión debidamente documentadas en la herramienta de gestión de mesa de servicios TI para cada componente afectado. Es necesario validar sí se deben ejecutar acciones de borrado seguro, sanitización o retorno a configuración de fábrica de cada elemento de configuración para validar la integridad e incrementar el nivel de seguridad para el restablecimiento de la operación	Equipo de respuesta a incidentes	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
13.	Analizar causa raíz y verificar erradicación del incidente	Los resultados del análisis de causa raíz deben permitir validar que se hayan cubierto todas las posibilidades de afectación derivadas del incidente. Estos resultados serán un insumo posterior para validar la eficiencia de los controles desplegados y para ajustar la valoración de los riesgos materializados durante la gestión del incidente de seguridad. Se debe generar el registro del análisis de causa raíz en la herramienta de mesa de servicios TI. **Punto de Control** El profesional del equipo de respuesta a incidentes verifica la erradicación y gestión de todas las posibles causales del evento. **¿El incidente fue erradicado?** Si: Continuar con la actividad 14. No: Volver a la actividad 11.	Equipo de respuesta a incidentes	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
14.	Evaluar resultados	El equipo de atención del incidente tiene la responsabilidad de lograr que la documentación de cada incidente sea de la mejor calidad posible para que sea útil en la Gestión de Incidentes y en la misma operación TIC de la Secretaría de Cultura, Recreación y Deporte - SCRD, razón por la cual será indispensable que los resultados obtenidos estén debidamente sustentados y soportados con evidencias que faciliten la óptima ejecución de estas actividades ante la posible ocurrencia de otro incidente de características similares. Ante los resultados obtenidos se evalúa sí las acciones remediaron definitivamente el incidente o solamente se alcanzó el nivel de operación en contingencia, mientras se alcanza la solución definitiva.	Equipo de respuesta a incidentes	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI

NO.	Actividad	Descripción	Responsable	Tiempo	Documento o Registro
		Se debe registrar la evaluación en la herramienta de mesa de servicios TI. **¿El incidente fue resuelto?** Si: Continuar con la actividad 16. No: Continuar con la actividad 15.			
15.	Activar DRP	En el caso de no contar con una solución definitiva, se deben empezar las acciones que permitan activar el Plan de Recuperación ante Desastres DRP, con el propósito de entregar a la Secretaría de Cultura, Recreación y Deporte - SCRD un nivel de operación que le permita alcanzar los mínimos compromisos que son atendidos a través de los servicios afectados por el incidente. El esquema de Gobierno de TI para la ejecución del DRP recibirá la información necesaria para empezar este despliegue y permitir que el equipo de atención y respuesta a incidentes, pueda continuar con las tareas de remediación y restauración de la operación tecnológica normal, mientras se prestan los servicios en el esquema alterno. La Declaratoria de desastres con la cual se activa el DRP, se puede originar por cualquiera de los diferentes canales establecidos en la Entidad (correo electrónico, comunicación oficial en página Web, Orfeo entre otros).	Equipo de respuesta a incidentes	1 día	Declaratoria de desastres
16.	Restablecer operación normal	Determinar si los esfuerzos de recuperación ya permiten hacer uso de los recursos y procesos normales de operación. Es necesario que las herramientas de monitoreo y demás instrumentos de control se vuelvan a activar para que se tenga control y visibilidad de cada componente que se haya visto involucrado en el incidente de forma directa o indirecta. Se debe registrar el restablecimiento normal de la operación de TI en la herramienta de mesa de servicios TI.	Equipo de respuesta a incidentes	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
17.	Evaluar ciclo respuesta	Evaluar los resultados presentados, los anexos, scripts, diagnósticos externos y demás evidencias que se hayan generado, con el propósito de conocer al detalle los hechos presentados y cuando sea pertinente adoptar medidas específicas. Lo anterior se debe registrar en la herramienta de mesa de servicios TI.	Equipo Seguridad	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI
18.	Documentar acciones y tiempos	Revisar la documentación efectuada en la herramienta de gestión de la mesa de servicios de TI del caso atendido y determinar si surge la necesidad de actualizar alguno de los controles existentes. Además, es necesario preparar informe ejecutivo, que será enviado por ORFEO, en el que refleje los elementos más relevantes del incidente atendido, la	Equipo Seguridad	1 día	Herramienta de apoyo a la gestión de la mesa de servicios de TI Informe

NO.	Actividad	Descripción	Responsable	Tiempo	Documento o Registro
		documentación suministrada, conclusiones y sugerencias remitidas por el líder del equipo de respuesta a fin de generar un documento de resumen No Técnico, para presentar a la Alta Dirección de la Secretaría de Cultura, Recreación y Deporte - SCRD y para remitir al ColCERT - CSIRT Gobierno			ejecutivo del incidente radicado en ORFEO.
19.	Actualizar la Base de Datos de Conocimiento	Todos los resultados de las acciones emprendidas deben quedar en el repositorio centralizado de gestión de incidentes y las acciones de remediación validadas contra la documentación previamente construida y donde sea pertinente adelantar las actualizaciones y socializaciones con los diferentes equipos de trabajo. Las herramientas y utilitarios que fueron usados en modalidad de investigación o de prueba deben ser relacionados y los resultados entregados, debidamente sustentados..	Equipo Seguridad	1 día	Base de Datos de Conocimiento actualizada la cual se encuentra en la Herramienta de apoyo a la gestión de la mesa de servicios de TI
20.	Realizar la divulgación de lecciones aprendidas	La información más relevante del incidente, se debe socializar al interior de la Secretaría de Cultura, Recreación y Deporte - SCRD y aquellas medidas de prevención desplegadas deben ser presentadas, así como las causas reales que permitieron que el incidente se materializa, con el propósito de evitar que se vuelvan a presentar esas condiciones por desconocimiento u omisión de parte de los colaboradores de la Entidad.	Equipo Seguridad	1 día	Correo electrónico, acta de reunión, listados de asistencia, tips de seguridad, charlas de sensibilización etc.

III. DOCUMENTOS ASOCIADOS Y ANEXOS

DOCUMENTOS ASOCIADOS:	
CÓDIGO	**NOMBRE**
TIC-PR-06-FR-01	Formato Reporte de incidentes
ANEXOS (Si aplica)	
1	Diagrama de flujo del procedimiento

IV. CONTROL DE CAMBIOS Y APROBACIONES

CONTROL DE CAMBIOS		
Versión	**Fecha de Emisión**	**Cambios realizados**
1	**31/12/2024**	Ver solicitud de creación, modificación o eliminación de documentos radicada en GLPI con el consecutivo número 112253 de fecha 27/12/2024

FLUJO DE ELABORACIÓN, REVISIÓN Y APROBACIÓN			
Elaboró *Persona(s) responsable(s) de crear, proyectar la modificación y/o ajuste del documento*	**Aprobó** *Líder del Proceso quién debe hacer cumplir el contenido establecido en el documento*	**Validó** *Persona(s) de la OAP responsable(s) de verificar que el documento contenga los lineamientos establecidos*	**Avaló** *Jefe de la Oficina Asesora de Planeación*
NOMBRE: Nidia Patricia Rodriguez R Yadir Guillermo Molina Mora	NOMBRE: Fabio F. Sánchez S.	NOMBRE: Nelson Javier Velandia Castro	NOMBRE: Luis Fernando Mejía Castro
CARGO: Contratista OTI Contratista OTI	CARGO: Jefe OTI (E)	CARGO: Profesional universitario	CARGO: Jefe Oficina Asesora de Planeación
FIRMA: Firmado Electrónicamente	FIRMA: Firmado Electrónicamente	FIRMA: Firmado Electrónicamente	FIRMA: Firmado Electrónicamente

Radicado: **20241600572053**
Fecha 30-12-2024 15:42

El Documento 20241600572053 fue firmado electrónicamente por:	
Luis Fernando Mejia Castro	**Jefe Oficina Asesora de Planeación**, Oficina Asesora de Planeación, ID: 79558456, luis.mejia@scrd.gov.co, Fecha de Firma: 31-12-2024 09:06:28
Nelson Javier Velandia Castro	**Profesional Universitario**, Oficina Asesora de Planeación, ID: 79905104, nelson.velandia@scrd.gov.co, Fecha de Firma: 31-12-2024 08:41:00
Fabio Fernando Sánchez Sánchez (E)	**Jefe Oficina de Tecnologías de la Información (E)**, Oficina de Tecnologías de la Información, ID: 19495495160, fabio.sanchez@scrd.gov.co, Fecha de Firma: 30-12-2024 16:57:15
Yadir Guillermo Molina Mora	**Contratista**, Oficina de Tecnologías de la Información, ID: 91017144, yadir.molina@scrd.gov.co, Fecha de Firma: 30-12-2024 16:48:21
Nidia Patricia Rodriguez Rodriguez	**Profesional Especializado**, Oficina de Tecnologías de la Información, ID: 51930241, nidia.rodriguez@scrd.gov.co, Fecha de Firma: 30-12-2024 15:51:24
f8bb6820b4f5132370c4231c6227ee62ecb368147661360908b9f0e162ed6846 Codigo de Verificación CV: 636eb	

Anexos: 2 folios