| Control de Cambios | | |
|---|---|---|
| **Versión** | **Fecha** | **Descripción de la Modificación** |
| 1 | 30/05/2024 | Versión inicial del documento |
| | | |

| Elaboró | Revisó | Aprobó |
|---|---|---|
| Francisco Daza Cardona<br>Contratista<br><br>Carmenza González Vargas<br>Profesional Universitario | Claudia Marcela Ladino<br>Jefe Oficina TIC | Claudia Marcela Ladino<br>Jefe Oficina TIC<br><br>Nelson Jairo Rincón Martínez<br>Jefe Oficina Asesora de Planeación |

## 1. OBJETIVO

Entregar los lineamientos necesarios con el fin de detectar, reportar, evaluar y dar respuesta a los eventos o incidentes de seguridad y privacidad de la información que se presenten en la plataforma tecnológica e identificar las lecciones aprendidas con el fin salvaguardar la confidencialidad, integridad y disponibilidad de los activos.

## 2. ALCANCE

Inicia desde el reporte o caso de un evento o incidente que comprometa la confidencialidad, integridad y disponibilidad de la información del IDIGER hasta el cierre de este. Su nivel de aplicación es en todas las dependencias del IDIGER.

## 3. DEFINICIONES

**Analista del Operador de Mesa de Servicio:**
Recibe la información de los Colaboradores del IDIGER, registra los casos en la herramienta de Mesa de Servicio y es el primer contacto para la Gestión de los Incidentes de Seguridad de la Información.

**Aprovechamiento de vulnerabilidades Informáticas:**
Aprovechamiento de vulnerabilidades de los sistemas de información, tales como configuraciones, protocolos y programas, para obtener información sobre el IDIGER.

**Antivirus:**
Programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

**Base de Conocimiento:**
Es un tipo de base de datos para la gestión del conocimiento. Provee los medios para la recolección, organización y recuperación computarizada de conocimiento.

**Botnet:**
Grupo de computadores reclutados en redes, controlados centralmente por el autor del Bonet, se forman deliberadamente para infectar masivamente los computadores en redes, crear denegación de servicios, envió de spam, etc.

**Código malicioso:**
Es un término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso.

**Escalamiento:**
Cuando un recurso que recibe una solicitud que no puede solucionar por si solo y requiere la ayuda de una persona o grupo con mayor conocimiento del tema específico.

**Escaneo de redes:**
Uso de software para escaneo de redes y así adquirir información acerca de las configuraciones de red, puertos, servicios y vulnerabilidades existentes.

**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.

**Evento de seguridad de la información:**
Un evento de seguridad de la información es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.

**Gestor de Incidentes:**
Es el rol responsable de identificar, priorizar y analizar la información referente al incidente y toma la decisión de coordinar un equipo de respuesta. Realiza el seguimiento de las acciones emprendidas para la contención y/o erradicación del incidente.

**Gusano de red:**
Tipo de programa maliciosos que se disemina y replica automáticamente a través de las redes, aprovechando las vulnerabilidades de los sistemas de información en las redes.

**Herramienta de Gestión de Servicios:**
Aplicación que ayudan a la gestión de TI del IDIGER; para el caso del IDIGER, es el software en donde se documentan los servicios de gestión tecnológica como Incidentes, Requerimientos, Problemas, Controles de Cambios, entre otros.

**Impacto:**
Es un efecto que ocurre a causa de la materialización de un riesgo y que va en detrimento de uno o más de los recursos importantes del negocio (Recursos: Financiero, Imagen, Ambiental, Humano, entre otros).

**Incidente Crítico:**
Es un evento que representa una seria amenaza para la entidad, y afecta de forma inmediata a uno o más recursos muy importantes o pone en peligro información sensitiva o confidencial del IDIGER, se considera crítica para la misión del IDIGER.

**Incidente de seguridad de la información**:
Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.

**Malware:**
Programa de software que introducido en los equipos y sistemas de una organización los bloquea o controla, "secuestra" información, roba o elimina datos, causa pérdidas millonarias y conlleva graves riesgos legales y de reputación. Los virus y programas ocultos en páginas webs, en ficheros o en el software sin licencia amenazan seriamente el funcionamiento y la seguridad de las empresas.

**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 Tecnologías de la Información y la Comunicación

**Phishing:**
Convencer a los usuarios para que divulguen información importante, tal como detalles de cuentas bancarias y usuarios y contraseñas, mediante el uso de correos electrónicos engañosos.

**Ransomware:**
Es un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.

Respuesta a incidente:
Permite solucionar o dar respuesta aceptable para un Incidente de Seguridad de la Información, puede ser registrado en la Base de Conocimiento.

**Spyware:**
Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

**Virus informático:**
Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.

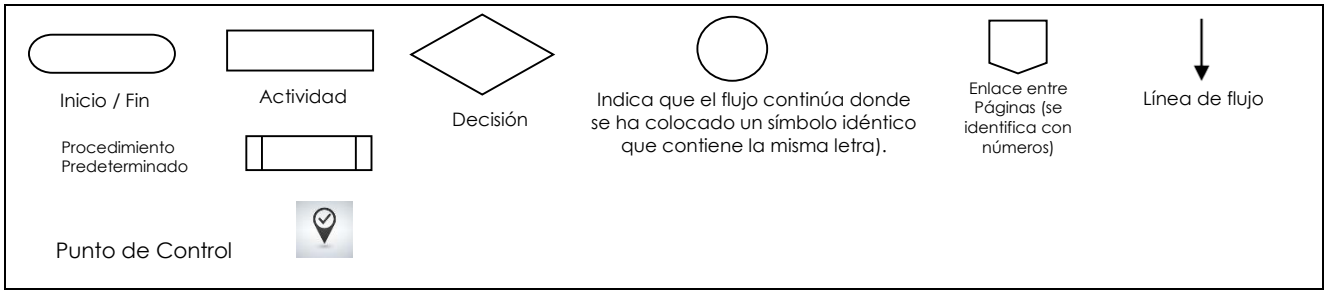
## 4. POLÍTICAS DE OPERACIÓN

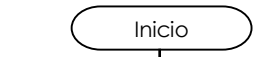
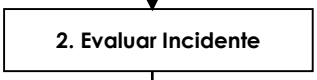
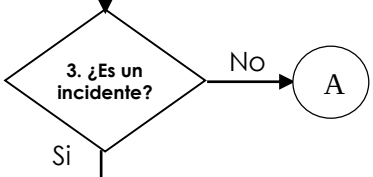
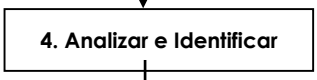
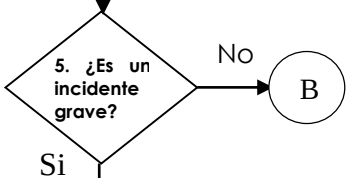
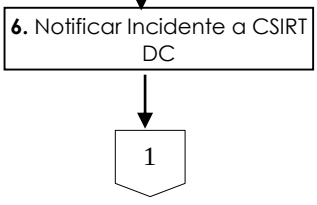
Se deben tener en cuenta los siguientes lineamientos para cada fase de un incidente. Adicionalmente se recomienda realizar un simulacro para poner a prueba los lineamientos y el desarrollo de las actividades.

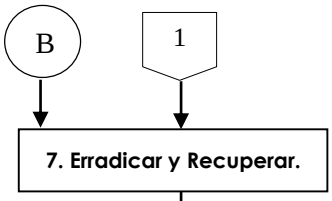
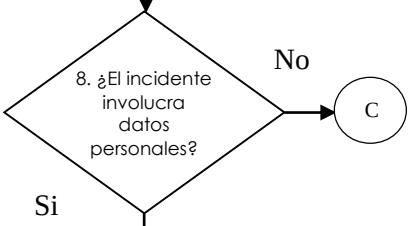
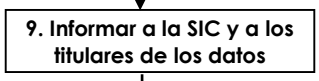
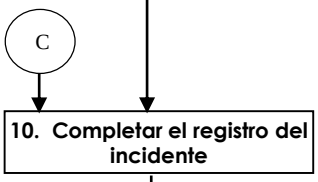
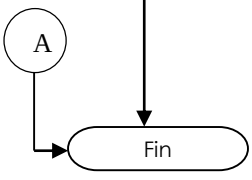
1. Preparación: Elaborar y mantener un plan de respuesta a incidentes, que incluya roles y responsabilidades claros.
2. Detección y notificación: Implementar sistemas de monitoreo para detectar actividades sospechosas y asegurar que existan procedimientos para notificar incidentes de manera oportuna.
3. Análisis: Evaluar rápidamente el alcance y el impacto del incidente para entender la naturaleza del ataque y los sistemas afectados.
4. Contención: Tomar medidas inmediatas para limitar la extensión del daño. Esto puede incluir aislar segmentos de la red o desactivar cuentas comprometidas.
5. Erradicación: Identificar y eliminar la causa raíz del incidente, como malware o accesos no autorizados, para prevenir futuras recurrencias.
6. Recuperación: Restaurar los sistemas y servicios afectados a su operación normal de manera segura y en el menor tiempo posible.
7. Lecciones aprendidas: Después de resolver el incidente, realizar una revisión post-mortem para identificar mejoras en el proceso de respuesta a incidentes.

Adicionalmente, remitirse al documento *TC-GU-04 Guía Incidentes de Seguridad de la Información* de la Entidad para más detalle.

## 5. DESARROLLO



| FLUJOGRAMA | ACTIVIDAD | RESPONSABLE | DOCUMENTO O REGISTRO |
|---|---|---|---|
|  | Identificar un evento de seguridad | Colaboradores, Proveedores y demás Partes Interesadas. | N/A |
|  | 1. Reportar el evento al punto interno de contacto en la entidad. Se debe reportar el posible incidente de seguridad de la información a la herramienta mesa de servicios | Colaboradores, Proveedores y demás Partes Interesadas. | Notificación de incidente (verbal, llamada, correo, caso en la mesa de servicios) |
|  | 2. La entidad evalúa el evento. | Equipo de Respuesta a Incidentes - Oficina TICs | Registro documentando el activo de información afectado (imágenes, fotos) |
|  | 3. Es un incidente?<br>Si: Continua en la actividad 4<br>No: Fin del Procedimiento. | Equipo de Respuesta a Incidentes - Oficina TICs | N/A |
|  | 4. Analizar, determinar el impacto y documentar el incidente. | Equipo de Respuesta a Incidentes - Oficina TICs | Documento con registro del incidente. |
|  | 5.¿Es un incidente grave?<br>Si: Pasar a actividad 6.<br>No: Pasar a actividad 7. | Equipo de Respuesta a Incidentes - Oficina TICs | N/A |
|  | **6.** Notificar Incidente a CSIRT DC. Al completar el registro del incidente determinar si aplica denunciar ante la Fiscalía y Reportar al CSIRT DC las acciones realizadas. | Equipo de Respuesta a Incidentes - Oficina TICs | Reporte a CSIRT DC y Fiscalía (Si aplica) |

| FLUJOGRAMA | ACTIVIDAD | RESPONSABLE | DOCUMENTO O REGISTRO |
|---|---|---|---|
|  | **7.** Contener, Erradicar y Recuperar. | Equipo de Respuesta a Incidentes - Oficina TICs | Documento con registro del incidente actualizado. |
|  | 8.¿El incidente involucra datos personales?<br>Si: Continuar en la actividad 9<br>No: Continuar en la actividad 10 | Equipo de Respuesta a Incidentes - Oficina TICs | N/A |
|  | 9. Informar a la SIC y a los titulares de los datos. | Equipo de Respuesta a Incidentes - Oficina TICs | Reporte a CSIRT y Titulares. |
|  | 10. Completar el registro del incidente con las actividades realizadas. | Equipo de Respuesta a Incidentes - Oficina TICs | Documento con registro del incidente actualizado. |
|  | Fin del Procedimiento. | N/A | N/A |

## 6. DOCUMENTOS EXTERNOS

| Nombre | Fecha de Publicación o Versión | Entidad que lo Emite | Medio de Consulta |
|---|---|---|---|
| Gestión de Incidentes | V 4.0 de Octubre 2021 | MINTIC | Digital |
| Computer Security Incident Handling Guide | Revision 2 | NIST | Digital |