1. OBJETO

Gestionar adecuadamente la detección de situaciones no previstas e indeseadas que tienen alta probabilidad de afectar la seguridad de la información y la continuidad de las operaciones del ***Instituto de Financiamiento, Promoción y Desarrollo de Ibagué – INFIBAGUÉ***. Protegiendo la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Inicia con la detección del incidente de seguridad de la información en el ***Instituto de Financiamiento, Promoción y Desarrollo de Ibagué – INFIBAGUÉ,*** determinar su clasificación del incidente utilizando la estrategia de contención y termina con el análisis del Pos-incidente.

3. DEFINICIONES

- **EQUIPO:**
  Es cada uno de los siguientes artículos informáticos: computadoras personales, servidores, computadoras portátiles, monitores, teclados, mouses, impresoras, scanners, unidades de disco (CD ROM, CD, etc.), graficadores, plotters, etc.

- **USUARIO:**
  Es toda la persona que hace uso del equipo, ya sea que esté bajo su resguardo o sin él.

- **ACTIVO DE INFORMACIÓN**:
  Es cualquier elemento que tenga valor para la organización y, en consecuencia, debe ser protegido.

- **AMENAZA:**
  Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.

- **AUTENTICIDAD**:
  Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.

- **AVISO DE IDS SOBRE BUFFER OVERFLOW**:
  Es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada.

- **CADENA DE CUSTODIA**:
  Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma

- **CONTENCIÓN**:
  Evitar que el incidente siga ocasionando daños.

- **ERRADICACIÓN**:
  Eliminar la causa del incidente y todo rastro de los daños.

- **EVENTO DE SEGURIDAD:**
  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]

- **GESTIÓN DE INCIDENTES**:
  Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una Entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.

- **HASH**:
  Función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.

- **IDS**:
  Software de detección de intrusos

- **IMPACTO**:
  Consecuencias que produce un incidente de seguridad sobre la organización.

- **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 27001:2009].

- **LOG'S:**
  Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.

- **RECUPERACIÓN:**

Volver el entorno afectado a su estado natural.

- **SNIFFER**:
  Software que captura los paquetes que viajan por la red para obtener información de la red o del usuario.

- **SSI**:
  Subsistema de Seguridad de la Información.

- **VALIDACIÓN:**
  Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

- **VULNERABILIDAD:**
  Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

4. RESPONSABILIDAD

- La responsabilidad en el desarrollo del presente procedimiento en lo relacionado con la "**PROCEDIMIENTO DE SALIDAS DE EQUIPOS TECNOLOGICOS DEL INSITUTO**", está a cargo de Gestión Tecnológica del ***Instituto de Financiamiento, Promoción y Desarrollo de Ibagué - INFIBAGUÉ.***

- El seguimiento y control en la implementación del presente procedimiento, corresponde a la Oficina Asesora de Planeación.

- El Comité de Coordinación de Control Interno y del SIG, es el responsable de aprobar la documentación que se genere en el marco del Sistema Integrado de Gestión "INTEGRA", previa revisión del Responsable del proceso y su equipo de trabajo.

5. GENERALIDADES

5.1 Tratamiento de los incidentes

La Oficina Asesora De Gestión Tecnológica Y Transformación Digital debe orientar, capacitar, sensibilizar, a funcionarios y contratistas en cuanto al reporte de incidentes de seguridad de la información y vulnerabilidades de los sistemas de información con los que cuenta el Instituto.

Debe mantener constante capacitación y demás partes interesadas, debe hacer énfasis en:

- Los riesgos de un control de seguridad ineficaz.

- Que es la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información.
- Los errores humanos.
- Las no conformidades con políticas o directrices.
- Violaciones de acuerdos de seguridad física.
- El mal funcionamiento en el software o hardware.
- Las violaciones de acceso.

Lo anterior con el propósito que los funcionarios, contratistas y demás partes interesadas del Instituto estén en capacidad de reconocer y reportar incidentes de seguridad.

Debe mantener contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información.

Debe hacer un seguimiento periódico a los incidentes de seguridad presentados.

5.2 Tipos de incidentes de seguridad

La Oficina Asesora De Gestión Tecnológica Y Transformación Digital debe conocer el tipo de incidentes, los cuales pueden afectar al Instituto:

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Ataques dirigidos y no dirigidos.
- Pérdida o robo de la información.
- Modificación no autorizada.
- Información no actualizada.
- Mala gestión del conocimiento.
- Diligenciamiento errado de formatos.
- Perdida o daño de la documentación.
- Daños sobre Activos de información
- Uso indebido de Activos de información
- Uso Indebido de Software.
- Uso Indebido de Usuarios.
- Suplantación de Identidad.

La Oficina Asesora De Gestión Tecnológica Y Transformación Digital responsable y debe atender de manera inmediata el incidente de Seguridad de la Información, de acuerdo a los niveles de criticidad del evento / incidente a fin de darle el tratamiento adecuado.

Urgencia \ Incidente	Alto	Medio	Bajo
Alto	1	2	3
Medio	2	3	4
Bajo	3	4	5

Tabla No. 1

Incidente de Valor 1: Interrumpe seriamente la operación de la entidad, el incidente puede tener velocidad significativa/rápida en su propagación y ocasionar daños de activos. Podría llegar a afectar más de un tipo de activo.

Incidente de Valor 2: Interrumpe en un periodo corto de tiempo los procesos generales de la entidad, el incidente/evento compromete un activo importante.

Incidente de Valor 3: No interrumpe los procesos generales de la entidad, el incidente/evento, se detecta y puede controlar fácilmente con recursos existentes en la entidad.

El área encargada de atender el incidente de Seguridad de la Información, debe conocer la siguiente tabla de escalamiento a fin de darle el tratamiento adecuado.

Incidente	Tratamiento
Alto	Se informa a los proveedores pertinente y si es el caso a las autoridades externas competentes.
Medio	La Oficina Asesora De Gestión Tecnológica Y Transformación Digital y las áreas involucradas.
Bajo	Se diligencia en el formato y se informa al usuario involucrado en caso de ser necesario.

Tabla No 2

La Oficina Asesora De Gestión Tecnológica Y Transformación Digital para preservar la Integridad, Disponibilidad y Confidencialidad de los activos de información debe generar las alertas tempranas mediante las herramientas tecnológicas disponibles así:

6. DESCRIPCION DEL PROCEDIMIENTO

ACTIVIDAD	RESPONSABLE	REGISTRO	PUNTO DE CONTROL
1. REPORTAR DEL INCIDENTE DE SEGURIDAD. Los funcionarios, contratistas y demás partes interesadas con acceso a información del Instituto nota que se está presentando un ataque a los	Los funcionarios, contratistas Oficina Asesora De Gestión Tecnológica Y Transformación Digital		

activos de la entidad, o conoce de que alguna persona está violando las políticas del Manual de seguridad de la información o conoce de riesgos asociados a la información, debe proceder a reportar esta situación como un evento o incidente de seguridad la Oficina Asesora De Gestión Tecnológica Y Transformación Digital, enviando un correo john.aguilar@infibague.gov.co, llamando a la Extensión 124, 125, la página web.			
2. REGISTRAR Y CLASIFICAR EL INCIDENTE. La Oficina Asesora De Gestión Tecnológica Y Transformación Digital toma los datos fecha, hora, y demás datos, realiza el registro correspondiente en el formato, se clasifica o categoriza el incidente, si se puede solucionar inmediato, se procede y se documenta la solución aplicada.	Oficina Asesora De Gestión Tecnológica Y Transforma ción Digital		
3. EVALUAR IMPACTO DE INCIDENTE. En caso que la Oficina Asesora De Gestión Tecnológica Y Transformación Digital no pueda resolver el incidente se pasa al siguiente nivel donde el Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital o quien haga sus veces, evaluara que tipo de incidente es el que se presenta, que activos está afectando, el alcance del mismo, pronóstico de expansión, daños potenciales o reales que se generen. Cuando se afecte más de un activo y/o más de un incidente. Todo se valorara en los niveles establecidos en la tabla Nro. 1 y teniendo en cuenta la importancia del activo.	Oficina Asesora De Gestión Tecnológica Y Transforma ción Digital		
4. IDENTIFICAR LA IMPORTANCIA DEL ACTIVO. De acuerdo a la verificación de los	Oficina Asesora De Gestión Tecnológica Y Transforma		

	ción Digital		

riesgos asociados a los activos de información que se encuentran en la ASGU05 Guía Metodológica De Análisis De Riesgos De Seguridad de la Información, se establecerá la afectación del activo de información, incluyendo el valor económico y la cantidad información relevante para la Entidad contenida en el mismo.			
5. IDENTIFICAR EL NIVEL DEL INCIDENTE. El Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital o quien se delegue haga sus veces, deberá identificar el nivel de afectación del incidente de acuerdo a los Niveles de Criticidad del Evento/Incidente descritos en la Tabla Nro.1	Oficina Asesora De Gestión Tecnológica Y Transforma ción Digital		
6. ESTABLECER LA ACCIÓN DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. Pasa saber cómo actuar el Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital o quien se delegue conforme al nivel del incidente se debe tener en cuenta: • Proceder de acuerdo con las instrucciones de la Brigada de Emergencias y según lineamientos de los cuerpos de socorro, privilegiando la conservación de la vida e integridad de las personas del Instituto y como de los visitantes. Tener en cuenta las autoridades y los grupos de interés descritos en la GGGU01 Guía de contacto con las autoridades y grupos de interés especial. En la medida que haya tiempo y recursos económicos, la Oficina Asesora De Gestión Tecnológica Y Transformación Digital debe adelantar las actividades que tiendan a proteger la información, solicitando autorización y activando la funcionalidad soportada a través del centro alterno de cómputo cambiando la dirección de producción a la dirección contingente, o en caso de no requerirse este tipo de manejo	Oficina Asesora De Gestión Tecnológica Y Transforma ción Digital		

debe seguir con la siguiente actividad de la presente guía.			
7. INICIAR LA ESTRATEGIA DE CONTENCIÓN. El Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital o quien se delegue, deben tener en cuenta los siguientes factores para la contención del incidente o evento • Daño significativo a los recursos a causa del incidente. • Necesidad de Guardado de evidencias. • Tiempo y recursos necesarios para poner en práctica la estrategia. •Efectividad de la estrategia. • Evaluación Crítica de los sistemas afectados. • Características de los posibles atacantes. • Si el incidente es de conocimiento público. • Pérdida económica. • Implicaciones Legales.	Oficina Asesora De Gestión Tecnológica Y Transforma ción Digital		
8. RECOLECTAR DE EVIDENCIA. Para hacer una recolección de evidencias, el Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital o quien se delegue, deben tener en cuenta lo siguientes criterios: • Información basada en la red: Log's de IDSs, logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de servidores de autenticación. • Información Basada en el Equipo: Live data collection: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red. Otra información: Testimonio de funcionario o contratista que reporta el evento o incidente.	Oficina Asesora De Gestión Tecnológica Y Transforma ción Digital		
9. MANEJAR EVIDENCIAS.			

El líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital o a quien se delegue, debe darle un correcto manejo de a los datos y evidencias recolectadas los cuales deben ser archivados para futuras investigaciones e implementación de controles preventivos o de mejoramiento. La información que debe ser archivada y custodiada por el Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital incluyendo: • Cantidad de incidentes presentados y tratados. • Tiempo asignado a los incidentes. • Daños ocasionados. • Vulnerabilidades explotadas. • Cantidad de activos de información involucradas. • Frecuencias de ataques. • Pérdidas. Además, debe cumplir con un control de seguridad que garantice la confidencialidad, integridad y disponibilidad de las evidencias retenidas.El almacenamiento físico seguro de las evidencias estará custodiado por el Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital y el electrónico se almacena en el caso generado en la herramienta de gestión de TI.	Oficina Asesora De Gestión Tecnológica Y Transformación Digital		
10. IDENTIFICAR FUENTES DE ATAQUE. El Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital debe tener identificados las posibles fuentes de ataque: El área encargada de gestionar el incidente de seguridad, debe tener identificadas las posibles fuentes de ataque mencionados: • Empleados Descontentos. • Baja Concientización. • Crecimiento de Redes. • Falta de Previsión de Contingencias. • Falta de Políticas. • Desastres Naturales. • Inadecuada protección de la Infraestructura.	Oficina Asesora De Gestión Tecnológica Y Transformación Digital		

• Confianza creciente en los sistemas • Virus. • Caballos de Troya. • Explotación de Vulnerabilidades, tanto a nivel de host, como de arquitectura de red (vulnerabilidades de la seguridad perimetral). • Falsificación de identificadores (biométricas, de autenticación o de encabezado de paquetes). • Robo de Información confidencial. • Violación a la privacidad. • Ingeniería social. • Denegación de Servicios. Hacking.			
11. ESTABLECER LA ESTRATEGIA DE ERRADICACIÓN. El área encargada de gestionar el incidente de seguridad, debe tener en cuenta para definir/decidir las estrategias de erradicación los siguientes factores: •Tiempo y Recursos necesarios para poner en práctica la estrategia.•Efectividad de la Estrategia.•Pérdida económica.•Posibles implicaciones legales.•Relación costo-beneficio de la estrategia.•Experiencias anteriores.•Identificación de los Procedimientos de cada sistema Operativo comprometido.•Identificación de Usuarios o servicios comprometidos para proceder a desactivarlos.	Oficina Asesora De Gestión Tecnológica Y Transforma ción Digital		
12. APLICA PROCEDIMIENTOS DE RECUPERACIÓN DE INFORMACIÓN. El Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital seguridad o a quien se delegue, para definir las estrategias de recuperación debe tener en cuenta los siguientes factores: • Cargar la copia de respaldo actualizada del sistema de información, configuración o base de datos.	Oficina Asesora De Gestión Tecnológica Y Transforma ción Digital		

• Creación nuevamente de la información digital o física, configuración de sistemas operativos, sistemas de información, cargue manual de la información. • Actualización, instalación de parches de seguridad a los sistemas que se vieron comprometidos. Otras definidas en el Plan de Recuperación de desastres.			
13. ANÁLIZAR POST-INCIDENTES. El Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital o quien se delegue debe garantizar el correcto manejo de las lecciones aprendidas, de la siguiente manera: • Periódicamente el Líder de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital o quien se delegue se reunirá con los demás funcionarios de la Oficina Asesora De Gestión Tecnológica Y Transformación Digital a fin de analizar los eventos e incidentes presentados durante el periodo. Se busca definir esquemas más efectivos para responder ante situaciones que afecten la seguridad de la información en la entidad. Entre las actividades que se realizan está: • Mantener la documentación de los eventos e incidentes de seguridad de la Información. • Mantener actualizada la base de datos de conocimientos. • Integrar los eventos e Incidentes a la Matriz de Riesgos de los Activos. • Realización de Capacitaciones a los Funcionarios de la entidad en lo relacionado a eventos e incidentes de seguridad de la información. • Analizar los Hechos y tomar decisiones	Oficina Asesora De Gestión Tecnológica Y Transforma ción Digital		

7. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS

01	2019/02/13	Aprobación inicial del documento en el Comité Institucional de Gestión y Desempeño
02	2026/06/25	Actualización nombre de La Oficina Asesora De Gestión Tecnológica Y Transformación Digital.