

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Vigencia 2023

Elvis Yonjan Cortés García  
Director

INTRODUCCIÓN	2
ALCANCE Y APLICABILIDAD	2
DEFINICIONES	2
OBJETIVO	7
Objetivo General	7
Objetivo Especifico	7
POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	7
POLÍTICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	9
RECURSOS	18
RESPONSABLE	18
METODOLOGIA DE IMPLEMENTACION	18
ACTIVIDADES	18
CUMPLIMIENTO DE IMPLEMENTACION	18
CRONOGRAMA	20

## 1. INTRODUCCION

El presente Plan se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente **Eje Temático de la Estrategia en Seguridad y Privacidad de la Información**, el cual busca guardar la información, garantizando la seguridad de la misma.

El Plan define los lineamientos y políticas que deben adoptar todos los funcionarios, contratistas, proveedores, visitantes y todo personal externo que preste sus servicios o tenga algún intercambio de información con el IDERF.

Las políticas de seguridad y privacidad descritas en este manual se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y siguiendo las buenas prácticas de seguridad de la información descritas en la norma ISO 27001:2013.

A partir de las políticas descritas en este Plan se promueve la implantación de controles, procedimientos y lineamientos para salvaguardar los activos de información del IDERF.

## 2. ALCANCE Y APLICABILIDAD

Las políticas y lineamientos descritos en este documento aplican a todos los funcionarios, contratistas, terceros y la ciudadanía en general, que en el desempeño de sus funciones y labores, compartan, utilicen, recopilen, procesen, intercambien o consulten información de IDERF.

Las políticas y lineamientos dispuestos en este documento y su implementación son aplicables a toda la información creada, procesada o utilizada por el IDERF, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

Con la definición del presente Manual de Políticas de Seguridad y Privacidad de la Información no se contempla el control de incidentes a nivel de la ciudadanía, usuarios externos o entidades externas a IDERF, sin embargo, con los medios disponibles se buscará promover la sensibilización sobre la existencia de la gestión de la seguridad de la información dentro de la empresa de cara a la ciudadanía y otros actores externos

## 3. DEFINICIONES:

- **Acceso a la Información Pública:**

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **Activo:**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:**

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.



- **Archivo:**

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenazas:**

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:**

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría:**

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- **Autorización:**

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Bases de Datos Personales:**

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Ciberseguridad:**

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio:**

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control:**

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos:**

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones



públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales:**

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:**

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados:**

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos:**

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:**

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Declaración de aplicabilidad:**

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad:**

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).



- **Encargado del Tratamiento de Datos:**

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- **Gestión de incidentes de seguridad de la información:**

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada:**

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada:**

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Plan de continuidad del negocio:**

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos:**

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad:**

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Responsabilidad Demostrada:**

Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.



- **Responsable del Tratamiento de Datos:**

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo:**

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:**

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información (SGSI):**

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información:**

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Trazabilidad:**

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

#### 4. OBJETIVOS:

##### 4.1. Objetivo General:

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes en el IDERF, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

##### 4.2. Objetivos Específicos:

Establecer un Manual de Políticas de Seguridad y Privacidad de la Información junto con los mecanismos y controles que permitan asegurar la integridad, disponibilidad y confidencialidad de los activos de información del IDERF.

#### 5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección del IDERF, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Seguridad de la Información (SGSI) buscando fortalecer la confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la empresa.



Para el IDERF, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a todos los funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones sobre seguridad de la

información estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la empresa.
  - Cumplir con los principios de seguridad de la información.
  - Cumplir con los principios de la función administrativa.
  - Mantener la confianza de sus clientes, socios y funcionarios.
  - Apoyar la innovación tecnológica.
  - Proteger los activos tecnológicos.
- 
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- 
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del IDERF.
- 
- Garantizar la continuidad del negocio frente a incidentes relacionados con seguridad de la información.

A continuación, se establecen los 11 lineamientos que soportan el MSPI (Modelo de Seguridad y Privacidad de la Información) y el SGSI (Sistema de Gestión de Seguridad de la Información) de IDERF:

1. El IDERF ha decidido definir, implementar, operar y mejorar de forma continua un MSPI (Modelo de Seguridad y Privacidad de la Información) y en conjunto el SGSI (Sistema de Gestión de Seguridad de la Información), ambos soportados en lineamientos y criterios alineados con las necesidades del negocio, y con los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades, compromisos frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
3. El IDERF protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la información. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. El IDERF protegerá su información de las amenazas originadas por parte del personal.
5. El IDERF protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.



6. El IDERF controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

7. El IDERF implementará control de acceso a la información, sistemas de información, aplicaciones y recursos de red.

8. El IDERF garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

9. El IDERF garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

10. El IDERF garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos de seguridad y debilidades asociadas.

11. El IDERF garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la presente política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa del IDERF, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

## **6. POLÍTICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

### **6.1. Políticas para Seguridad de la información**

Las políticas específicas relacionadas con la seguridad y privacidad de la información deben brindar orientación y apoyo por parte de la dirección del IDERF, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

- Se deben definir un conjunto de políticas específicas para la seguridad y privacidad de la información, aprobadas por la gerencia, publicadas y comunicadas a los funcionarios y partes externas pertinentes.

- Las políticas específicas para la seguridad y privacidad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas. Como buena práctica se recomienda realizar dicha revisión como mínimo cada año.

### **6.2. Políticas para la Organización de la seguridad de la información.**

Organización interna: Es necesario que El IDERF establezca los lineamientos para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

- El IDERF debe definir y asignar todas las responsabilidades de la seguridad de la información.



- Los deberes y áreas de responsabilidad que presenten conflicto de interés se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de información de la empresa.
- Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
- La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.

Dispositivos móviles y teletrabajo: Entendiendo la regla de negocio de llevar a cabo el trabajo de manera presencial, frente a cualquier situación de riesgo que amenace la ejecución de las actividades de manera presencial y se deba recurrir a la opción de teletrabajo, El IDERF debe garantizar la seguridad del teletrabajo, además de garantizar el uso correcto de los dispositivos móviles en cualquier escenario de trabajo.

- Se deben implementar medidas y lineamientos de seguridad y privacidad para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realizan labores en modalidad de teletrabajo.
- Se deben identificar y gestionar los riesgos introducidos por el uso de dispositivos móviles en cualquier escenario de trabajo.

### 6.3. Políticas para la Seguridad de los recursos humanos

Antes de asumir el empleo: El IDERF debe asegurar que los funcionarios y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, incluyendo las responsabilidades con respecto a la seguridad de la información.

- Los acuerdos contractuales con los funcionarios y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad y privacidad de la información.

Durante la ejecución del empleo: El IDERF debe asegurar que los funcionarios y contratistas tomen conciencia de sus responsabilidades frente a la seguridad y privacidad de la información y las cumplan durante el desempeño de sus labores.

- La secretaria general del IDERF debe exigir a todos los funcionarios y contratistas la aplicación de la seguridad y privacidad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

- Todos los funcionarios del IDERF, y en donde sea pertinente, los contratistas, deberán recibir la educación y formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

- El IDERF debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra funcionarios, contratistas, proveedores y partes externas que hayan cometido una violación a la seguridad y privacidad de la información.



Terminación o cambio de empleo: El IDERF debe proteger sus intereses como parte del proceso de cambio o terminación del contrato de los funcionarios, contratistas, proveedores y partes externas.

- Las responsabilidades y deberes de seguridad y privacidad de la información que permanecen vigentes después de la terminación o cambio de un contrato se deben definir y comunicar al funcionario, contratista, proveedor y partes externas, y se deben hacer cumplir. Se recomienda que la aceptación se dé desde antes del inicio del empleo.

#### 6.4. Políticas para la Gestión de activos

Responsabilidad por los activos: El IDERF debe identificar los activos organizacionales y activos de información y definir las responsabilidades de protección apropiadas para asegurar su uso y gestión adecuados.

- Se deben identificar los activos de información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
- Los activos mantenidos en el inventario deben tener un propietario asignado para asignar las responsabilidades sobre la protección, gestión y buen uso.
- Se deben identificar, documentar e implementar reglas para el uso aceptable de la información, los activos de información e instalaciones de procesamiento de información.
- Todos los funcionarios, contratistas, proveedores, y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

Clasificación de la información: El IDERF debe asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia y relevancia para la empresa.

- El IDERF debe clasificar la información y activos de información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- Se debe desarrollar e implementar un procedimiento para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la empresa.
- Se debe desarrollar e implementar un procedimiento para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la empresa.
- Se debe implementar un procedimiento para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la empresa.
- Se debe disponer en forma segura de los medios cuando ya no sean requeridos, utilizando procedimientos formales.



- Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

#### 6.5. Políticas para el Control de acceso

Requisitos del negocio para control de acceso: En El IDERF se debe limitar el acceso a información y a instalaciones de procesamiento de información.

- Se debe establecer, documentar y revisar los lineamientos de control de acceso con base en los requisitos del negocio y de seguridad de la información.

- Solo se debe permitir el acceso a la red y a los servicios de red para los usuarios (internos, externos) que hayan sido autorizados específicamente.

Gestión de acceso de usuarios: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

- Se debe implementar un procedimiento de gestión de accesos para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.

- Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado, por medio de un procedimiento de gestión de accesos.

- Los propietarios de los sistemas y servicios deben revisar los derechos de acceso de los usuarios, a intervalos regulares, preferiblemente cada año.

- Los derechos de acceso de todos los funcionarios y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios a la contratación.

Responsabilidades de los usuarios: El IDERF debe hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

- Se debe exigir a los usuarios que cumplan las prácticas y lineamientos de la empresa para mantener confidencial cualquier información de autenticación (tales como credenciales de acceso, etc).

Control de acceso a sistemas y aplicaciones: El IDERF se debe evitar el acceso no autorizado a sistemas y aplicaciones.

- El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con los lineamientos y procedimiento de gestión de acceso, que asegure asignación de credenciales para el ingreso seguro. Como mínimo se debe considerar: Control de acceso basado en roles, niveles de acceso, permisos para leer, escribir, eliminar y actualizar información.

- Garantizar que las credenciales (usuario y contraseña) sean de calidad, que cumplan con el nivel requerido y se apliquen de manera consistente para garantizar niveles óptimos de seguridad y protección.

#### 6.6. Políticas para la Seguridad física y del entorno



Áreas seguras: Se debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la empresa.

- Se debe asegurar que solamente se permite el acceso a personal autorizado mediante controles de entrada apropiados para las instalaciones de la empresa, que incluya la asignación de credenciales temporales y registro en un sistema de información.
- Se deben establecer controles de ingreso y permanencia en instalaciones y centros de datos. El centro de datos debe contar preferiblemente con control de acceso biométrico para evitar ingreso de personal no autorizado.
- Se debe restringir el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.
- Las áreas con acceso restringido deben estar claramente demarcadas para evitar ingresos no autorizados.

Equipos: Se debe prevenir la pérdida, daño, robo o compromiso de activos de información, y la interrupción de las operaciones de la empresa.

- Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, asimismo se debe evitar comer, beber y fumar cerca del equipo para evitar daños o evitar que los funcionarios estén en contacto con los equipos si no están trabajando en ellos.
- En el centro de datos e instalaciones de tecnología el cableado de potencia y de telecomunicaciones deben estar separados para evitar interferencias, asimismo, el cableado alrededor del centro de datos debe estar aislado de forma segura para evitar la conexión de dispositivos no autorizados.
- Se deben seguir las recomendaciones del fabricante y realizar mantenimiento a los equipos para asegurar su disponibilidad e integridad continuas, esto incluye que solo el personal autorizado debe realizar dicho mantenimiento y se debe llevar registro del mantenimiento. Cuando sea necesario, la información sensible debe mantenerse a salvo antes de realizar el mantenimiento a un equipo.
- Los equipos, información o software no se deben retirar de su sitio sin autorización previa.

En caso de requerirse el retiro temporal se debe identificar claramente al personal autorizado para realizar el retiro, y llevar registro de los equipos, información o software retirados.

- Se deben mantener el escritorio limpio de documentos y medios de almacenamiento removibles, y mantener la pantalla limpia en los equipos; además de bloquear pantalla y sesiones de aplicaciones cuando no estén en uso.

#### 6.7. Políticas para la Seguridad de las operaciones



Procedimientos operacionales y responsabilidades: Se deben asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

- El procedimiento para la operación, uso y responsabilidad de los equipos debe estar documentado y ser socializado con todos los usuarios que tengan equipos a su disposición.
- Para asegurar el desempeño requerido de la infraestructura, sistemas de información y redes de datos, se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones sobre la capacidad futura. Se recomienda que se haga seguimiento anual.

Protección contra códigos maliciosos: Debe asegurarse que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

- Se deben implementar controles y/o herramientas para la detección, prevención y recuperación, incluyendo la toma de conciencia y socialización de las responsabilidades de los usuarios para la protección contra códigos maliciosos.

- Se debe restringir la conexión de medios extraíbles u otros dispositivos no autorizados para evitar la introducción de códigos maliciosos o material riesgoso.
- Copias de respaldo: Se debe asegurar la protección contra la pérdida de datos.

- Se deben hacer copias de respaldo de la información de los usuarios, y ponerlas a prueba regularmente de acuerdo con las necesidades de recuperación de cada tipo de información.

- La ubicación de las copias de seguridad debe ser diferente a la ubicación original de la información para aumentar la seguridad ante posibles riesgos.

- Se debe mantener un registro de las copias de seguridad realizadas para asegurar que la información salvada se mantiene vigente
- Registro y seguimiento: Se debe llevar registro de los eventos sobre los sistemas de información y redes de datos.

- Se debe contar con una herramienta / sistema / procedimiento de monitoreo de sistemas de información y redes de datos que permita generar, conservar y revisar regularmente los registros sobre las actividades de los usuarios y administradores, excepciones, fallas y eventos de seguridad de la información.

- Se deben identificar oportunamente las vulnerabilidades técnicas de los sistemas de información y redes de datos; evaluar la exposición de la empresa a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. Se recomienda que la identificación de vulnerabilidades técnicas se realice cada año.

- Solo los funcionarios autorizados deben realizar instalación de software y configuraciones en los equipos de los usuarios. Cualquier instalación de software y/o configuración no autorizada deberá tramitarse como un proceso disciplinario por la Oficina de Control Disciplinario y demás que se consideren apropiadas.



Consideraciones sobre auditorías de sistemas de información: Se deben realizar auditorías a los sistemas de información para asegurar que son adecuados al uso y propósito.

- Se deben establecer actividades de auditoría previamente planificadas para la verificación de los sistemas de información. Debe incluir la revisión de: la correcta asignación de privilegios para los usuarios, estabilidad y confiabilidad de la infraestructura que soporta los sistemas de información, suficiente capacidad de los sistemas de información e infraestructura que los soporta (memoria, procesamiento, almacenamiento, ancho de banda, etc.), oportunidades de mejora, desempeño, disponibilidad, mantenimiento, monitoreo.

#### 6.8. Políticas para la Seguridad de las comunicaciones

Seguridad de las redes: Se deben gestionar las redes de datos de la empresa.

- Se deben aplicar controles para gestionar la seguridad de las redes de datos, tales como el inventario de los elementos físicos de red, monitoreo de las redes de datos, y control de los privilegios de acceso a la red para establecer medidas correctivas.
- Se deben establecer y monitorear Acuerdos de Nivel de Servicio para los servicios de red (aunque sean subcontratados con un proveedor externo), con el fin de monitorear la disponibilidad de la red y evaluar los riesgos a los que estamos expuestos con dichos servicios ya que de ellos depende la operatividad de los sistemas de información.

Intercambio de información: Se debe mantener la seguridad de la información transferida dentro de la empresa y la información intercambiada con cualquier Entidad externa (contratista, proveedor, etc.)

- Se debe contar con un procedimiento que permita proteger la transferencia / entrega / intercambio de información considerando los requisitos legales que sean aplicables (p.e. Ley de tratamiento de datos o acuerdos de confidencialidad).
- Todos los funcionarios deben acceder a su correo electrónico corporativo desde las redes de datos del IDERF, en caso que algún usuario requiera acceso externo o desde redes públicas externas, debe ser notificado a la Secretaria General para dar el tratamiento necesario.
- Se deben firmar los acuerdos de confidencialidad y de deber de secreto antes de iniciar una transferencia de información y/o ejecución de labores. Esto es aplicable para todos los funcionarios de la empresa, contratistas, practicantes, proveedores, y cualquier ente externo.

#### 6.9. Políticas para la Adquisición, desarrollo y mantenimiento de sistemas

Requisitos de seguridad de los sistemas de información: Se debe asegurar que la seguridad de la información es parte integral al adquirir o contratar sistemas de información.

- Desde contratación se deben considerar requisitos de seguridad al adquirir o contratar sistemas de información, tales como: criterios de evaluación de riesgos, períodos de prueba de producto, configuraciones adicionales requeridas, homologación y aceptación de producto.



- Se debe contar con certificados de seguridad en los sistemas de información, aplicaciones y/o pasarelas de pago que operen o sean accedidos desde redes públicas externas por los usuarios de la empresa, y que manejen información sensible como datos personales o financieros.

Seguridad en los procesos de desarrollo y soporte: El IDERF debe asegurar que la seguridad de la información sea implementada por los proveedores o contratistas externos que suministran sistemas de información, aplicaciones o servicios de tecnología.

- Se debe asegurar que el proveedor o contratista externo cuenta con una política y/o procedimiento de seguridad de la información en el desarrollo, mantenimiento y soporte de software y sistemas.

- Se debe asegurar que el proveedor o contratista externo cuenta con un procedimiento de gestión de cambios a los sistemas de información, aplicaciones o servicios de tecnología, que incluya plazos de respuesta y escalamientos si aplican.

- Cuando el proveedor o contratista externo aplique cambios a sistemas de información, aplicaciones o servicios de tecnología, se debe realizar pruebas para garantizar que los cambios no afecten la operación del IDERF. Estas pruebas deben ser planeadas y coordinadas previamente con la Dirección y áreas/departamentos que se vean impactados por el cambio.

- Antes de implementar actualizaciones o nuevos sistemas de información, aplicaciones o servicios de tecnología, en conjunto con el proveedor o contratista se debe establecer un cronograma de pruebas para la aceptación y de esta manera evitar fallos en la operación.

#### 6.10. Políticas para la Relación con los proveedores

Seguridad de la información en las relaciones con los proveedores: Se debe asegurar la protección de los activos de información que sean accesibles por los proveedores o contratistas externos.

- En los contratos con proveedores o contratistas externos se deben establecer las condiciones y cláusulas de confidencialidad para el manejo adecuado de la información del IDERF de acuerdo con los requisitos de seguridad definidos en el presente Manual de políticas.

- En caso que el proveedor o contratista externo incumpla con las condiciones y cláusulas de confidencialidad descritas anteriormente, se debe iniciar un proceso legal desde la Oficina Jurídica, por lo que el funcionario, equipo, área o departamento que identifique el incumplimiento debe notificarlo inmediatamente a la Secretaría General.

- En caso que el proveedor o contratista externo identifique algún riesgo al incumplimiento en las condiciones y cláusulas de confidencialidad en su cadena de suministro debe notificarlo inmediatamente a la Secretaría General para iniciar el proceso legal correspondiente.

Gestión de la prestación de servicios con los proveedores: El IDERF debe verificar que el proveedor o contratista externo cumple y mantiene el nivel acordado de



seguridad de la información y de prestación del servicio de acuerdo a los compromisos contractuales.

- Desde la Secretaría General y la Misional y en conjunto con el funcionario, equipo, área o departamento que mantenga relación con el proveedor o contratista externo, se debe establecer una revisión frecuente a los contratos, condiciones y cláusulas pactadas, incluyendo la solicitud de informes mensuales al proveedor o contratista externo sobre el nivel de servicio prestado.

6.11. Políticas para la Gestión de incidentes de seguridad de la información Gestión de incidentes y mejoras en la seguridad de la información: Se debe realizar una gestión adecuada de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y vulnerabilidades.

- Se debe contar con un procedimiento de seguridad que defina los roles y responsabilidades, y las actividades detalladas para la gestión de los incidentes de seguridad de la información que incluya reporte de eventos, análisis y diagnóstico, mecanismos de respuesta a incidentes, y gestión del conocimiento relacionado con los incidentes de seguridad de la información.

- Todos los funcionarios, contratistas, practicantes del IDERF que usan los servicios y sistemas de información de la empresa, deben informar cualquier debilidad o situación sospechosa que pueda afectar los sistemas o servicios.

- Anualmente se debe realizar un análisis de vulnerabilidades técnicas que permita identificar los riesgos a los que se encuentran expuestos los sistemas de información y redes de datos, de manera que se puedan definir las medidas correctivas y preventivas que reduzcan los incidentes de seguridad de la información.

6.12. Políticas para Aspectos de seguridad de la información en la gestión de continuidad de negocio Continuidad de seguridad de la información: Se debe considerar la continuidad de la seguridad de la información ante alguna situación que pueda afectar la continuidad de negocio de la empresa.

- Se debe definir un plan con las medidas que permitan restablecer la disponibilidad, integridad y confidencialidad de la información ante una situación de parada o de emergencia que pueda afectar los distintos servicios (energía, comunicaciones, red de datos, colapso de infraestructuras, etc.)

- Ante una situación de parada de los distintos servicios se debe realizar un análisis de impacto en los requisitos de seguridad de la información, para activar las medidas de respuesta y restablecimiento.

- Anualmente se deben revisar y poner a prueba el plan para restablecer la disponibilidad, integridad y confidencialidad de la información, y revisar las medidas de respuesta definidas anteriormente, para asegurar la vigencia y correspondencia con las necesidades de la empresa.

Redundancias: Se debe asegurar la disponibilidad de instalaciones de procesamiento de información.

- Se debe identificar qué sistemas de información, software, aplicaciones, redes de datos, infraestructura y servicios de tecnología deben contar con redundancia para



asegurar la continuidad de negocio, luego se debe analizar la viabilidad de las redundancias y realizar pruebas del buen funcionamiento de las mismas.

## 7. RECURSOS:

- Humano: Dirección, secretaria general, técnico en Soporte y Mantenimiento de Equipos.
- Físico: PC's, Servidor y equipos de comunicación.

## 8. RESPONSABLES:

- Director.
- Secretaria general-
- Técnico en Soporte y Mantenimiento de Equipos.

## 9. METODOLOGÍA DE IMPLEMENTACIÓN:

Para llevar a cabo la implementación del (MSPI) Modelo de Seguridad y Privacidad de la Información en el IDERF, se implementa la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Aplicar
4. Verificar
5. Realizar

## 10. ACTIVIDADES:

1. Realizar Diagnóstico.
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
3. Realizar la Identificación de los Riesgos en las diferentes áreas de la Empresa.
4. Valorar del riesgo y del riesgo residual.
5. Realizar Mapas de calor donde se ubican los riesgos.
6. Plantear al plan de tratamiento de riesgo aprobado por la gerencia y Técnico en Soporte y Mantenimiento de Equipos.

## 11. CUMPLIMIENTO DE IMPLEMENTACIÓN:

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación.

- Revisión y/o Modificación de la actual Política de Seguridad.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones



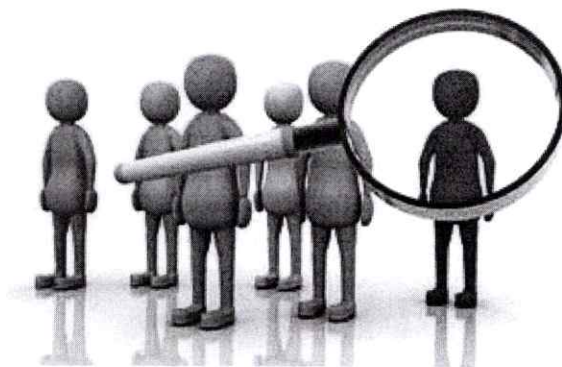
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

## 12. CRONOGRAMA:

ACTIVIDAD	CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION																											
	Mayo				Junio				Julio				Agosto				Septiembre				Octubre							
	9	16	23	30	6	13	20	27	4	11	18	25	8	15	22	29	5	12	19	26	3	10	17	24				
Realizar Diagnóstico.																												
Elaborar el Alcance del Plan del Tratamiento de Riesgos de Seguridad y Privacidad de la Información.																												
Realizar la Identificación de los Riesgos con los Encargados del Proceso,																												
Reunión con los Encargados del Proceso.																												
Valoración del riesgo residual.																												
Mapas de calor donde se ubican los riesgos.																												
Mapas de calor donde se ubican los riesgos.																												
Seguimiento y control.																												



# **Plan de Contingencia y Políticas de Seguridad de Sistemas de Información 2023**



**Elvis Yonjan Cortés García**  
**Director**

## TABLA DE CONTENIDO

### INTRODUCCIÓN

1. OBJETIVOS
- 1.1. ALCANCE Y COBERTURA
2. NORMATIVIDAD
3. DEFINICIONES
4. CONDICIONES GENERALES
- 4.1. ESQUEMA GENERAL
- 4.2. PLAN DE RESPALDO
- 4.3. PLAN DE EMERGENCIA Y RECUPERACIÓN DE DESASTRE
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
6. REPORTE DE PROBLEMA Y SOLICITUD DE MEJORA
- 6.1. CUADRO DE ESCALAMIENTO
- 6.2. CUADRO DE NIVELES DE SERVICIO
- 6.3. CUADRO DE NIVELES DE ATENCIÓN
7. PLAN DE CONTINGENCIA PARA LA PRESTACIÓN DEL SERVICIO
8. DESCRIPCIÓN DE LA ACTIVIDAD
- 8.1. REPORTE DE PROBLEMA
- 8.2. SOLICITUD DE MEJORA Y CONTROL DE CAMBIO
- 8.3. PROCESO DE RECUPERACIÓN EN CASO DE INTERRUPCIÓN DEL SERVICIO
- 8.4. PROCEDIMIENTO DE COPIA DE SEGURIDAD (BACKUP)
9. ANEXOS



## INTRODUCCION

El Instituto Deportivo y recreativo de Fusagasugá - IDERF en su Plan de Contingencia y Políticas de Seguridad de Sistemas de Información, concibe la necesidad de estar a la vanguardia de los avances tecnológicos para lograr ejercer su cometido con resultados eficientes y eficaces, de ahí que se hace fundamental el presente Manual debe ser aplicado en todos los sistemas de información de la Entidad incluyendo aquellos que se implementen en un futuro.

Independientemente de la cobertura y medidas de seguridad que se hallen implantadas, puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencia cuente también con un Plan de Recuperación en caso de desastres, el cual tendrá como objetivo restaurar los servicios de los sistemas de información de forma rápida, eficiente y con el menor costo y pérdidas de tiempo posible.

Como mínimo, los diferentes planes de contingencia que hacen parte del presente documento han sido construidos considerando que el Instituto Deportivo y recreativo de Fusagasugá - IDERF tenga soluciones de continuidad en su operación diaria, aunque ello implique una posible reducción en su capacidad de proceso.

### 1. OBJETIVOS

Los objetivos principales del presente documento son los siguientes:

- Contar con una estrategia planificada compuesta por un conjunto de procedimientos que garanticen la disponibilidad de una solución alterna que permita restituir rápidamente los sistemas de información de la Entidad ante la eventual presencia de siniestros que los paraliquen parcial o totalmente.
- Garantizar la continuidad en los procesos de los elementos críticos necesarios para el funcionamiento de las aplicaciones del IDERF.
- Identificar las acciones que se deben llevar a cabo y los procedimientos a seguir en el caso de la presencia de un siniestro que restrinja el acceso a los sistemas de información.
- Establecer las secuencias que se han de seguir para organizar y ejecutar las acciones de control de emergencias.
- Minimizar las pérdidas asociadas a la presencia de un siniestro relacionado con la gestión de los datos.
- Proveer una herramienta de prevención, mitigación, control y respuesta a posibles contingencias generadas en la ejecución del proyecto.

#### 1.1.2 ALCANCE Y COBERTURA

El plan de contingencias es un análisis de los posibles riesgos y eventuales siniestros a los cuales puede estar expuesto equipos de cómputo, programas, archivos y Bases de Datos, cualquiera que sea su residencia. En este Manual se hace un análisis de los riesgos y siniestros a los cuales se halla sujeta el área de sistemas de información del IDERF, cómo reducir su posibilidad de ocurrencia y los procedimientos apropiados en caso de la presencia de cualquiera de tales situaciones.



El alcance del plan de contingencia incluye los elementos básicos y esenciales, componentes y recursos informáticos que conforman los sistemas de información que maneja el IDERF, y que se relacionan a continuación:

- **Datos:** En general se consideran datos todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (Bases de Datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colecciones de bits.
- **Aplicaciones:** Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la entidad.
- **Tecnología:** Incluye los equipos de cómputo como computadores de escritorio, servidores, cableados, switches, etc. en general, conocidos como hardware y los programas, archivos, bases de datos, etc. denominados software para el procesamiento de información.
- **Instalaciones:** Lugares físicos de la Entidad donde se encuentren el software.
- **Personal:** Los individuos con conocimientos y experiencia específicos que integran el área de sistemas de la Entidad que dentro de sus funciones deban programar, planificar, organizar, administrar y gestionar los sistemas de información.

El presente Manual debe ser aplicado en todos los sistemas de información de la Entidad incluyendo aquellos que se implementen en un futuro.

Independientemente de la cobertura y medidas de seguridad que se sean implantadas, puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencia cuente también con un Plan de Recuperación en caso de desastres, el cual tendrá como objetivo restaurar los servicios de los sistemas de información de forma rápida, eficiente y con el menor costo y pérdidas de tiempo posible.

Como mínimo, los diferentes planes de contingencia que hacen parte del presente documento han sido construidos considerando que el IDERF tenga soluciones de continuidad en su operación diaria, aunque ello implique una posible reducción en su capacidad de proceso.

## 2. NORMATIVIDAD

La operación de los sistemas de información y los procedimientos establecidos en el presente Manual está sujeta al cumplimiento de las siguientes normas legales vigentes en el estado colombiano:

Tipo	Número	Título	Fecha
N.D.	N.D.	N.D.	N.D.

## 3. DEFINICIONES

**Acceso:** Es la lectura o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta una Base de Datos, los datos son primero accedidos y suministrados a la computadora y luego transmitidos a la pantalla del equipo.

**Amenaza:** Cualquier evento que pueda interferir con el funcionamiento de un computador o causar la difusión no autorizada de información confiada a un computador. Ejemplo: Fallas del suministro eléctrico, virus, saboteos o descuido del usuario

**Ataque:** Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a un computador.



**Base de Datos:** Es un conjunto de datos organizados, entre los cuales existe una correlación y que además están almacenados con criterios independientes de los programas que los utilizan. Entre sus principales características se encuentran brindar seguridad e integridad a los datos, proveer lenguajes de consulta, de captura y edición de los datos en forma interactiva, proveer independencia de los datos.

**Datos:** Los datos son hechos y/o valores que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos en el presente documento. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y Bases de Datos, textos (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), videos (secuencia de tramas), etc.

**Golpe (Breach):** Es la violación exitosa de las medidas de seguridad, como el robo de información, la eliminación de archivos de datos valiosos, el robo de equipos, PC, etc.

**Incidente:** Cuando se produce un ataque o se materializa una amenaza se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de eliminación de un archivo protegido.

**Integridad:** Los valores consignados en los datos se han de mantener de tal manera que representen la realidad y su modificación debe ser registrada en bitácoras del sistema que permitan la auditoría de los acontecimientos. Las técnicas de integridad sirven para prevenir el ingreso de valores errados en los datos sea esta situación provocada por el software de la Base de Datos, por fallas de los programas, del sistema, el hardware o, simplemente, por errores humanos.

**Privacidad:** Se define como el derecho que tiene EL IDERF para determinar, a quién, cuándo y qué información de su propiedad podrá ser difundida o transmitida a terceros.

**Seguridad:** Se refiere a las medidas que toma EL IDERF con el objeto de preservar la integridad de sus datos o información procurando que no sean modificados, destruidos o divulgados ya sea en forma accidental, no autorizada o intencional. En el caso de los datos e información contenidos en los sistemas de información EL IDERF, la privacidad y seguridad guardan estrecha relación entre sí, aunque la diferencia entre ellas radica en que la primera se refiere a la distribución autorizada de información y la segunda al acceso no autorizado.

**Sistemas de Información:** Es el término empleado en el ambiente del procesamiento de datos para referirse al almacenamiento de los datos de una organización y ponerlos a disposición de su personal. Pueden ser registros simples como archivos de Word y Excel, o pueden ser complejos como una aplicación de software con base de datos.

**Cortafuegos (Firewall):** Es un sistema diseñado para bloquear el acceso no autorizado de comunicaciones. Se trata de un dispositivo configurado para permitir, limitar, cifrar y descifrar el tráfico de mensajes entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos se utilizan para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

## 4. CONDICIONES GENERALES

### 4.1 ESQUEMA GENERAL

En el presente Manual se indican los procedimientos y actividades generales que se deben tener en cuenta para la correcta ejecución del plan de contingencia que aplica para cualquier sistema de información en el IDERF



TIPO DE RIESGO	FACTOR DEL RIESGO	PREVENCIÓN Y MITIGACIÓN
<b>El Fuego:</b> destrucción de equipos y archivos.	Bajo	Extintores, pólizas de seguros.
<b>El robo común:</b> pérdida de equipos y archivos.	Medio	Seguridad Privada, Alarma, Seguro contra todo riesgo y copias de respaldo (Back up).
<b>El vandalismo:</b> daño a los equipos y archivos.	Medio	Seguro contra todo riesgo, copias de respaldo.
<b>Fallas en los equipos:</b> daño a los archivos.	Medio	Mantenimiento, equipos de respaldo, garantía y copias de respaldo.
<b>Equivocaciones:</b> daño a los archivos.	Bajo	Capacitación, copias de respaldo, políticas de seguridad.
<b>Acción de Virus:</b> daño a los equipos y archivos.	Medio	Actualizaciones del sistema operativo, Antivirus actualizados, copias de respaldo.
<b>Terremotos:</b> destrucción de equipo y archivos.	Medio	Seguro contra todo riesgo, copias de respaldo. Las sedes cumplen con las normas antisísmicas.
<b>Accesos no autorizados:</b> filtrado no autorizado de datos.	Bajo	Cambio de claves de acceso mínimo cada seis meses. Política de seguridad para acceso a personal competente.
<b>Robo de datos:</b> difusión de datos sin el debido cubrimiento de su costo.	Bajo	Cambio de claves de acceso mínimo cada seis meses, custodia de las copias de respaldo.
<b>Fraude:</b> modificación y/o desvío de la información y fondos de la institución.	Bajo	Sistemas de información seguros con dos usuarios para autorizar transacciones, procedimiento de control y registro de transacciones en tablas de auditoría.

El área de Sistemas del IDERF, está conformada por profesionales con conocimientos de sistemas de información quienes prestan asesoría técnica sobre el presente procedimiento y supervisan su correcto desarrollo en caso de requerirse. Adicionalmente se deben contar con contratos de mantenimiento vigentes para las diferentes plataformas informáticas, con profesionales especializados que prestarán soporte técnico de acuerdo a los niveles de servicio exigidos. Ver anexo 9.4.

Debido a que la tecnología es muy volátil, es posible que algunos sistemas de información dejen de operar por encontrarse obsoletos o al ser reemplazados por unos más modernos. De acuerdo con lo anterior, los programas que dejen de operar por ser reemplazados por otros o por ser obsoletos, deben permanecer instalados durante los tres (3) meses siguientes en forma simultánea para emplearlos en caso de contingencia y una vez concluido este período el funcionario responsable debe realizar una copia de seguridad completa de la información en Unidad Extraíble, CD, DVD o BD y enviarla al área de sistemas para su verificación y custodia en diferentes oficinas de la entidad, de acuerdo con lo establecido en la tabla de retención documental.

A continuación se describe la metodología para el desarrollo y aplicación del plan de contingencia de los sistemas de información del IDERF por parte del área de sistemas:

#### 4.2 PLAN DE RESPALDO

Para asegurar que se consideran todas las posibles eventualidades, se relacionan las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los riesgos conocidos.

N°	ACTIVIDAD	ELEMENTOS	RESULTADO
1	Copias de seguridad de la información y documentos residentes en los discos duros de los computadores del IDERF	Documentos en formatos Word, Excel, PDF, artes, imágenes, audio y correos electrónicos	Una copia de seguridad en la nube en línea opcional, una Copia de seguridad anual obligatoria de todos los documentos.



			<b>Responsable:</b> funcionarios que manejen información de gran importancia para la Entidad.
2	Copias de seguridad de los sistemas de información y Bases de Datos del IDERF	Aplicaciones WEB e intranet de información. Aplicaciones y Bases de Datos de los procesos y archivos.	Copia de seguridad semanal de los sistemas de información activos de la Entidad. Los servicios de Hosting en Datacenter contratados incluirán el servicio de Back up para las aplicaciones del IDERF. <b>Responsable:</b> Personal con conocimientos de sistemas de información
3	Contar mínimo con un kit de instalación para restaurar los archivos del sistema operativo y aplicaciones de un computador o servidor en caso de falla o virus.	Sistema operativo (Windows, Linux, etc.) Paquetes de ofimática y diseño. (Office, Corel) Bases de datos (Sql, MySql, FoxPro, etc.) Drivers y utilitarios de impresoras, redes, computadores, etc.	Contar con mínimo un medio de instalación por cada oficina del IDERF. Una copia u original del instalador en custodia de sistemas. <b>Responsable:</b> Personal con conocimientos de sistemas de información
4	Mantener descentralizados los sistemas de información del IDERF, de acuerdo a sus necesidades.	Sitio WEB, Base de Datos del IDERF, aplicaciones fuera de línea en seccionales.	Aplicaciones instaladas en diferentes localizaciones físicas, computadores o servidores. <b>Responsable:</b> Personal con conocimientos de sistemas de información
5	Mantener pólizas de seguros vigentes, asegurando por el valor real, contra todo riesgo los equipos y bienes del IDERF.	Equipos eléctricos y/o electrónicos, móviles, portátiles, software y equipos de comunicación.	Póliza vigente contra todo riesgo de daño y/o pérdida física por cualquier causa. <b>Responsable:</b> Profesional de Gestión Administrativa.
6	Mantenimientos, revisiones preventivas y correctivas de equipos de computación y comunicación, extintores, alarmas y sistemas contra incendio, para mantenerlos en óptimas condiciones.	Equipos de computación y comunicación periféricos, sistemas eléctricos UPS, Aire acondicionado, Alarmas, Sistemas contra incendio, Extintores.	Contratos anuales de mantenimiento, garantías vigentes y control del mantenimiento de los equipos. <b>Responsable:</b> Profesional de Gestión Administrativa y/o supervisor asignado al contrato de mantenimiento.
7	Actualizar las claves o contraseña de acceso a las aplicaciones y bases de datos del IDERF.	Base de Datos, y sistemas de información del IDERF.	Mínimo cada seis meses o cuando se requiera por el usuario o por reemplazos del cargo. <b>Responsable:</b> Todos los funcionarios de la Entidad que manejen sistemas de información.
8	Mantener actualizados los sistemas operativos, antivirus y aplicaciones del IDERF.	Sistemas operativos de equipos de cómputo, antivirus y aplicaciones del IDERF.	Entrega de una actualización cada vez que salga una nueva versión de las aplicaciones. Configuración de actualizaciones automáticas en los sistemas operativos. <b>Responsable:</b> Personal con conocimientos de sistemas de información
9	Mantener los equipos en condiciones ambientales óptimas de tal forma que no se deterioren por uso inadecuado.	Equipos de computación y comunicación.	Contrato vigente de mantenimiento preventivo y correctivo para los equipos de cómputo. <b>Responsable:</b> Servicios generales e inventarios, responsable de los contratos de mantenimiento de la Entidad.
10	Mantener como respaldo un inventario adicional con equipos de cómputo, repuestos, consumibles, para	Equipos de computación y comunicación de la Entidad.	Reducción del tiempo de respuesta a fallas de hardware y sistemas de información.

con la FUERZA de la



	su reemplazo inmediato en caso de falla.		<b>Responsable:</b> Responsable de servicios generales e inventarios de la Entidad.
11	Disponibilidad de redundancia de recursos para evitar la interrupción de la prestación del servicio en los sistemas de información de la Entidad.	<b>Concepto n+1:</b> UPS, Planta eléctrica, almacenamiento, conexiones, líneas, equipos de cómputo adicional y servidores con ambiente de prueba.	Evitar la suspensión del servicio a los usuarios teniendo una alternativa adicional, contratando servicio de hosting en datacenter que garanticen la disponibilidad. <b>Responsable:</b> Personal con conocimientos de sistemas de información

Los responsables están relacionados en el cuadro anterior de acuerdo con la ubicación de las oficinas de la Entidad, el cumplimiento de las actividades descritas en el cuadro anterior se debe verificar por lo menos una vez al año de acuerdo con los formatos del proceso de gestión de Sistema y Tecnologías.

Los registros que se generen con la aplicación de este documento se deben conservar y archivar de acuerdo con lo establecido en la Tabla de Retención Documental.

#### 4.3 PLAN DE EMERGENCIA Y RECUPERACIÓN POR DESASTRE

En el presente numeral se definen los procedimientos y planes de acción para el caso de una falla, siniestro o desastre en el área informática, considerando como tal todas las áreas y usuarios que procesan información en los equipos de cómputo del IDERF. Para lo anterior se recomiendan esquemas de virtualización de servidores.

Cuando ocurra un desastre, es esencial que se conozca al detalle el motivo que lo originó y el daño producido para permitir recuperar en el menor tiempo posible el proceso perdido.

Los procedimientos de recuperación y verificación son de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos. En estos procedimientos están involucrados todos los funcionarios del IDERF.

Las actividades previas a la presencia de un desastre o falla son aquellas relacionadas con el planeamiento, preparación, entrenamiento y ejecución de actividades de resguardo de la información, que aseguren un proceso de recuperación con el menor costo posible para EL IDERF.

En la fase de planeamiento se debe tener la siguiente información disponible para proceder:

##### 4.3.1 SISTEMAS DE INFORMACIÓN

EL IDERF debe tener una relación de identificación actualizada de los Sistemas de Información con los que cuenta, tanto los desarrollados por el área de sistemas como los contratados por la entidad con otras empresas contratistas.

La relación de los sistemas de información deberá detallar los siguientes datos:

N°	INFORMACIÓN	DESCRIPCIÓN
1	CRITICIDAD	El nivel de importancia estratégica que tiene la información de este Sistema para EL IDERF. (Ranking)
2	NOMBRE DEL SISTEMA	Nombre del Sistema, denominación y sigla
3	LENGUAJE DESARROLLO	Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
4	PROCESOS Y ÁREAS	Procesos y áreas (internas/externas) donde se encuentra instalado el sistema y las áreas que los usan.
5	TAMAÑO	El volumen de los archivos que trabaja el sistema en megabytes o gigabytes.
6	TRANSACCIONES	El volumen de transacciones diarias y mensuales que maneja el sistema
7	EQUIPAMIENTO	El equipamiento con el cual está funcionando el sistema.



8	EQUIPAMIENTO MÍNIMO		Equipamiento mínimo necesario para que el sistema pueda seguir funcionando.
9	ACTIVIDADES RECUPERACIÓN	DE	Actividades por realizar para volver a contar con el Sistema de Información (actividades de Restauración).
10	TIEMPO RECUPERACIÓN	DE	Tiempo estimado en horas o días, para que El IDERF pueda funcionar adecuadamente, sin disponer de la información del Sistema.

Con la lista priorizada, se procede a recuperar la operatividad de los sistemas de información en los cuales hubo pérdida causada por el desastre o falla. La información anterior debe estar permanentemente actualizada por el área de sistemas en los formatos del proceso de gestión de Sistemas y Tecnologías.

#### 4.3.2 EQUIPOS DE CÓMPUTO:

EL IDERF debe llevar el inventario actualizado de los equipos de manejo de información (computadores, lectoras de códigos de barras, impresoras, escáneres, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación.

N°	INFORMACIÓN
1	Las Pólizas de Seguros, parte de la protección de los Activos del IDERF, deben incluir en casos de siniestros la restitución de los computadores o equipos siniestrados con actualización tecnológica, siempre y cuando esté dentro de los montos asegurados.
2	Identificar los computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo, los servidores y los computadores con información importante o estratégica.
3	Tener el inventario actualizado de los computadores y equipos del IDERF, con las especificaciones de cada uno de ellos.
4	Los equipos deben estar identificados con una placa que los identifique como activo del IDERF y un código de barras para identificar el responsable y área a la que pertenece.

Con la lista priorizada, se procede a recuperar la operatividad de los sistemas de información en los cuales hubo pérdida causada por el desastre o falla. La información anterior debe estar permanentemente actualizada por el área de sistemas en los formatos del proceso de gestión de Sistemas y Tecnologías.

#### 4.3.3 SERVICIOS DE CÓMPUTO Y PERSONAL DEL ÁREA DE SISTEMAS

Mantener actualizado un listado de proveedores contratados por El IDERF, referente a servicios de cómputo y comunicaciones que requiere la Entidad para su funcionamiento, especificando lo siguiente:

N°	INFORMACIÓN
1	Empresa Contratista.
2	Contacto técnico: Nombres, dirección, teléfono, celular y ciudad.
3	Objeto Contractual o Funciones del cargo (Servicio de Hosting, Mantenimiento, Internet, etc.)
4	Vigencia del contrato: Fecha de inicio y fecha de terminación. No aplica para funcionarios.
5	Tipo de contrato y Cuantía. La cuantía no aplica para funcionarios.
6	Estado del contrato: Vigente o Liquidado.

Con la lista priorizada, se procede a recuperar la operatividad de los sistemas de información en los cuales hubo pérdida causada por el desastre o falla. La información anterior debe estar permanentemente actualizada por el área de sistemas en los formatos del proceso de gestión de Sistemas y Tecnologías.

#### 4.3.4 COPIAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN (BACKUPS)

Las copias de seguridad tienen por objeto proveer el respaldo de la información actualizada de cada sistema de información de acuerdo con los siguientes criterios:



N°	ACTIVIDAD	FRECUENCIA	RESPONSABLES	MEDIDAS DE CONTROL
1	Copias de seguridad de la información y documentos de los discos duros de los computadores del IDERF. (Incluye archivos de Word, Excel, PDF, Power Point y de edición gráfica)	<b>Período:</b> Anual de todos los documentos del IDERF. <b>Medio:</b> DVD o CD, Nube, Memoria USB <b>NOTA:</b> No incluye archivos de uso personal.	Todos funcionarios los del IDERF.	Verificación anual de la aplicación de los procedimientos establecidos. Custodia según tabla de retención documental. Registro en el libro de control de Backups. (Ver Anexo 9.5)
2	Copias de seguridad de información importante de los discos duros de los computadores del IDERF.	<b>Período:</b> Diaria de los documentos más importante del IDERF. <b>Medio:</b> Memoria USB	Funcionarios responsables manejo información importante del IDERF.	Requiere instalación de programa que realiza una copia de seguridad automática de los archivos modificados recientemente a la memoria USB. Custodia de la información por el funcionario responsable. No requiere registro en el libro de control de Backups. (Ver Anexo 9.5)
3	Copias de seguridad de los sistemas de información y bases de datos del IDERF.	<b>Período:</b> Semanal <b>Medio:</b> DVD o CD, BD	Ingeniero sistemas del IDERF.	Pruebas y simulacro de recuperación anual del sistema de información.
4	Contar mínimo con un kit de instalación para restaurar los archivos del sistema operativo y aplicaciones de un computador o servidor en caso de falla o virus.	<b>Período:</b> Semanal <b>Medio:</b> DVD o CD - BD Mínimo un medio de instalación por cada oficina del IDERF. Una copia o el original de instalación en custodia de sistemas.	Responsable del Área de Sistemas y Secretarios Seccionales.	El Secretario Seccional debe tener en custodia mínimo un medio de instalación de cada equipo de las oficinas del IDERF.

Con la lista priorizada, se procede a recuperar la operatividad de los sistemas de información en los cuales hubo pérdida causada por el desastre o falla. La información anterior debe estar permanentemente actualizada por el área de sistemas en los formatos del proceso de gestión de Sistemas y Tecnologías.

#### 4.3.5 INVENTARIO DE LICENCIAS DE SOFTWARE DE EQUIPOS DE CÓMPUTO DEL IDERF.

El área de sistemas del IDERF deberá llevar un listado actualizado con el inventario de licencias de software de los equipos de cómputo de la entidad en el formato con el objeto de mantenerlo disponible para prestar soporte técnico en la configuración o reinstalación de software (Sistema Operativo y Ofimática) en los equipos de cómputo de la entidad en coordinación con el supervisor del contrato de mantenimiento.

### 5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El IDERF en el presente manual establece las políticas de seguridad de la información en materia de informática, las cuales se clasifican de la siguiente manera:

#### POLÍTICA 1: ACCESO A LA INFORMACIÓN

Todos los funcionarios y contratistas que laboran para EL IDERF deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. El área de sistemas del IDERF



y los responsables de la información deben autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas.

Las claves de acceso compartidas asignadas a los funcionarios de los sistemas información de la Entidad tienen únicamente carácter de consulta, estas no permiten modificación de la información, no deben divulgarse hacia el exterior de la entidad, se cambiarán anualmente o cuando se requiera y exclusivamente se utilizarán para la gestión de la Entidad, por ejemplo, la clave de acceso de Intranet del IDERF.

Todos los accesos y claves de usuarios para el uso de los sistemas de información del IDERF, deberán ser desactivados o cambiados después de que el funcionario, contratista, supernumerario o proveedor cese de prestar sus servicios a IDERF.

Mediante los trabajos de auditoría en los diferentes sistemas de información se podrá efectuar un seguimiento a los accesos y cambios realizados por los usuarios a la información del IDERF, con el objeto de minimizar el riesgo de pérdida o integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se debe documentar y realizar las acciones tendientes a su solución.

## **POLÍTICA 2: ADMINISTRACIÓN DE CAMBIOS**

Toda solicitud de mejora (Creación y modificación de programas, pantallas y reportes) o reporte de falla que afecte los sistemas de información del IDERF, debe ser requerido por los usuarios del sistema y para su actualización en el Proceso o formatos establecidos para el Proceso de Gestión de Sistemas y Tecnología según sea el caso.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

## **POLÍTICA 3: SEGURIDAD DE LA INFORMACIÓN**

Los funcionarios y contratistas del IDERF son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad y por la Ley para protegerla, evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma. Así mismo no deben suministrar información de la Entidad a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice la infraestructura tecnológica del IDERF, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está clasificada como confidencial y/o crítica.

## **POLÍTICA 4: SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS**

El sistema de correo electrónico, grupos de charla y utilidades deben ser usados únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades del IDERF, manteniendo un lenguaje claro y respetuoso para su uso.

Los funcionarios del IDERF no deben utilizar versiones escaneadas de firmas personales para dar la impresión de que un mensaje de correo electrónico ó cualquier otro tipo de comunicación electrónica hayan sido firmados por la persona que la envía.

La propiedad intelectual desarrollada o concebida mientras el funcionario se encuentre en el sitio de trabajo, es propiedad exclusiva del IDERF. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado con la FUERZA de la



en memorandos, planes, estrategias, productos, software, códigos fuentes, documentación y otros materiales.

## **POLÍTICA 5: SEGURIDAD EN RECURSOS INFORMÁTICOS**

Los recursos informáticos deben cumplir como mínimo con lo siguiente:

**Administración de usuarios:** Establece cómo deben ser utilizadas las claves de ingreso a los recursos informáticos, longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

**Rol de Usuario:** Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberá permitir la asignación a cada usuario de diferentes roles, así como existir un rol para la administración de usuarios.

**Registros de auditoría:** Hace referencia a la verificación en trabajo de auditoría o registros de los sucesos relativos a la operación.

El control de acceso a todos los sistemas de computación de la Entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario. Las palabras contraseñas o claves de acceso a los recursos informáticos asignados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

Toda la información del servidor de la base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de cifrado para garantizar su inutilidad en caso de ser descubierta.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

## **POLÍTICA 6: SEGURIDAD EN COMUNICACIONES**

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información confidencial.

Todas las conexiones a redes externas tiempo real que accedan a la red interna de la Entidad, debe pasar a través de un *cortafuegos*, denominado sistema de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un documento de formalización.

## **POLÍTICA 7: SOFTWARE UTILIZADO**

Todo software que utilice EL IDERF será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad.



Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios públicos y contratistas de las implicaciones que tiene el instalar software ilegal en los computadores del IDERF.

### **POLÍTICA 8: ACTUALIZACIÓN DE HARDWARE**

Cualquier cambio que se requiera realizar en los equipos de cómputo de la Entidad (cambios de procesador, monitor, teclado, mouse, adición de memoria o tarjetas) debe tener previamente una evaluación técnica del área de sistemas, el supervisor del contrato de mantenimiento y la autorización del Profesional de Gestión Administrativa o el responsable de los inventarios para la actualización de seriales, responsables y hojas de vida de los equipos.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado, previa autorización del supervisor del contrato de mantenimiento y la autorización del Profesional de Gestión Administrativa o el responsable de los inventarios.

Los equipos de cómputo (PC, servidores, comunicaciones, etc.) no deben moverse o reubicarse sin la aprobación previa del Profesional de Gestión Administrativa o el responsable de los inventarios.

### **POLÍTICA 9: ALMACENAMIENTO Y RESPALDO**

La información que es soportada por la infraestructura de tecnología informática del IDERF deberá ser almacenada y respaldada de tal forma que se garantice su disponibilidad. El almacenamiento de la información se debe realizar interna y/o externamente a la Entidad, de acuerdo con su importancia.

Los funcionarios públicos son responsables de los respaldos de la información de cada uno de los computadores asignados, de acuerdo con el procedimiento descrito.

La información de copias de seguridad (BACKUP) en Unidad Extraíble, CD-R, DVD-R, TAPE o BD, debe enviarse al área de sistemas para su custodia, consolidación y archivo de acuerdo a la Tabla de Retención Documental, de tal forma que garantice que la información no sea manipulada por ninguna persona externa o interna durante su transporte y custodia de la misma, estas copias de seguridad permitirán hacer seguimiento de control en una auditoría o en caso de requerirse recuperar la información de los procesos.

### **POLÍTICA 10: CONTINGENCIA**

El área de sistemas del IDERF debe preparar, actualizar periódicamente y probar anualmente un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.

Las crisis suelen provocar "reacciones de pánico" que pueden ser contraproducentes y a veces incluso más dañinas que las provocadas por el incidente que las causo. Por ello en el presente documento se establece claramente las responsabilidades y funciones del personal así como los protocolos de acción correspondientes.

### **POLÍTICA 11: LOG DE AUDITORIA**

Todos los sistemas automáticos que operen y administren información sensible, valiosa o crítica para la Entidad como son los aplicativos en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar un libro con la bitácora de auditoría de las tareas principales (adición, modificación, borrado).



El libro de bitácora de auditoría debe proporcionar suficiente información para apoyar el monitoreo, control y auditorías.

Los archivos de auditoría deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.

Todos los computadores del IDERF deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoría sea correcto.

## **POLÍTICA 12: SEGURIDAD FÍSICA**

La oficina debe contar con los mecanismos de control de acceso tales como vigilancia privada, identificación de visitantes, sistema de alarmas, circuito cerrado de televisión, etc, y en los sitios donde existan sistemas de información, equipos de cómputo y comunicaciones considerados críticos por la Entidad deben contar mínimo con seguridad de acceso con guardia, sistemas de detección y extinción de incendio, circuito cerrado de televisión con cámaras, redundancia de recursos y alta disponibilidad.

Los visitantes de las oficinas del IDERF deben ser escoltados durante todo el tiempo por un funcionario autorizado. Esto significa que se requiere de un escolta tan pronto como un visitante entra a un área y hasta que este mismo visitante sale del área controlada. Todos los visitantes requieren una escolta incluyendo clientes, antiguos empleados, miembros de la familia del funcionario.

Los centros de cómputo o áreas que la Entidad considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente de un funcionario del IDERF.

En los centros de cómputo o áreas que El IDERF considere críticas deberán existir elementos de control de incendio, inundación, alarmas y estar demarcados como zona restringida. Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Los equipos de cómputo (Computadores, servidores, impresoras, equipos de comunicación, entre otros) no deben moverse o reubicarse sin la aprobación previa del Profesional de Gestión Administrativa o el responsable de los inventarios.

Los funcionarios se comprometen a NO utilizar la red regulada de energía (tomacorrientes naranja o UPS) para conectar equipos eléctricos diferentes a su computador, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que implique una mayor carga sobre esa red.

Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no están autorizados para utilizar los recursos informáticos de la Entidad.

## **POLÍTICA 13: ESCRITORIOS LIMPIOS**

Sobre los escritorios u oficinas abiertas y durante la ausencia de los funcionarios del IDERF no deben permanecer a la vista documentos en papel, dispositivos de almacenamiento como CDs, memorias USB, con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

## **POLÍTICA 14: ADMINISTRACIÓN DE LA SEGURIDAD**

Cualquier brecha en la seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, o los recursos informáticos de cualquier nivel (local o institucional) debe



ser comunicada por el funcionario que la detecta en forma inmediata y confidencial al área de Administrativa del IDERF.

Los funcionarios y contratistas que realicen las labores de administración del recurso informático son responsables por la implementación y permanencia de los controles sobre los recursos tecnológicos.

## **POLÍTICA 15: PRÁCTICAS DE USO DE INTERNET**

Los virus informáticos son una de los principales riesgos de seguridad para los sistemas, por tal razón se deben tomar las siguientes precauciones de seguridad sobre la utilización de Internet:

1. No utilizar canales de chat o grupos sociales como Facebook, Messenger, etc, en horario laboral con fines personales sin previa autorización del IDERF.
2. No descargar de Internet, ni alojar en los discos duros de los equipos de cómputo, música, videos, ni cualquier tipo de software sin licenciamiento.
3. No abrir ningún mensaje, sitio web, ni archivo de fuente desconocida o muy poco conocidas. En caso de personas conocidas, se deben tomar precauciones, asegurándose de que esa persona es la responsable del envío y ante cualquier duda, borrar el mensaje, para evitar la contaminación de un virus.
4. Todos los funcionarios del IDERF, tienen la obligación a dar cumplimiento a la Ley 679 de 2001, acatando las prohibiciones que le han sido impuestas. Por con siguiente se obligan a no utilizar los servicios, redes y sistemas del IDERF que impliquen directa o indirectamente, bajar o consultar información de actividades sexuales y/o material pornográfico.
5. El spam o correo basura son los mensajes no deseados que hacen referencia a publicidad pudiendo además contener virus; estos mensajes deben eliminarse sin ser leídos para evitar el aumento de la cantidad del correo basura en el buzón así como la posibilidad de intrusión de virus en el sistema.
6. Usar regularmente un programa antivirus y verificar periódicamente su actualización, el área de sistemas presta el soporte que se requiera para tal fin.
7. No bajar nada de sitios web de los que no se tenga referencias de seriedad, o que no sean medianamente conocidos. Si se bajan archivos, copiarlos a una carpeta y revisarlos con un antivirus actualizado antes de abrirlos.
8. Se debe suministrar el correo electrónico asignado por El IDERF con moderación, ya que podrían enviar publicidad no deseada.
9. No utilizar la cuenta de correo electrónico suministrada por El IDERF, para asuntos personales.
10. Activar las actualizaciones automáticas (Windows y Office), las cuales pueden proteger los equipos de ataques de virus proveniente de Internet.

## **6. REPORTE DE PROBLEMA Y SOLICITUD DE MEJORA**

Los funcionarios del IDERF pueden solicitar la solución de un problema presentado o realizar una solicitud de mejora del sistema de información, comunicándolo al área de sistemas o quiénes son los encargados de gestionar cualquier solicitud por parte de los usuarios finales, presentando una solución de acuerdo con el nivel de importancia y los niveles de servicio del numeral 6.1.

Dependiendo de su clasificación, la solicitud de mejora deberá ser aprobada. Si es un cambio mayor que afecte la disponibilidad de las aplicaciones o la infraestructura, pasa para aprobación al Comité del Sistema de Gestión Calidad; si es un cambio menor, es aprobado por el jefe inmediato. Una vez aprobado el cambio se implementa y aprueba registrando los resultados de la actividad.

### **6.1 CUADRO DE ESCALAMIENTO**

NIVEL	PUNTO DE ESCALAMIENTO
1	Secretaria Administrativa
2	Ingenieros de desarrollo contratistas.



Especialistas consultores externos.
-------------------------------------

## 6.2 CUADRO NIVELES DE SERVICIO

N°	DESCRIPCIÓN GENERAL DEL PROBLEMA	NIVEL DE SERVICIO REQUERIDO
1	Incremento de la capacidad en cualquier capa computacional de hardware o software.	Nivel 2: Hasta 60 días calendario.
2	Denegación de servicios por fallas del software que afecten de forma general el sistema que impida el acceso a los servicios con impacto significativo operacional, entre un 95% al 100% de los usuarios. PRIORIDAD DE SOLUCIÓN ALTA.	Nivel 1: 30 minutos hábiles Nivel 2: 10 horas hábiles
3	Degradación de servicios por fallas sobre las estructuras de datos y software que NO impida el acceso a los servicios con impacto operacional medio-alto, entre un 70% al 94% de los usuarios. PRIORIDAD DE SOLUCIÓN MEDIA.	Nivel 1: 4 horas hábiles Nivel 2: 12 horas hábiles
4	Degradación de rendimiento sobre los servicios y problemas de forma que NO se impida el acceso a los servicios con impacto operacional bajo, entre el 1% al 69% de los usuarios. PRIORIDAD DE SOLUCIÓN BAJA.	Nivel 1: 2 días hábiles Nivel 2: 15 días hábiles
5	Solicitud de mejora o creación de un nuevo módulo de software.	Dependiendo su complejidad, tiempo acordado mediante formato y se escala de acuerdo con la especialidad cuadro 6.1.

El tiempo de solución establecido en el anterior cuadro de niveles de servicio, según la prioridad y niveles de escalamiento, corresponde al tiempo transcurrido entre la comunicación oficial del problema y la solución del problema en el servidor de producción.

Si en el proceso de pruebas, los usuarios identifican que el problema persiste, o se generan nuevos problemas, el tiempo transcurrido se reactiva hasta que nuevamente se entregue la solución del problema encontrado y así sucesivamente, hasta obtener una solución definitiva.

## 6.3 CUADRO DE NIVELES DE ATENCIÓN

NIVEL	NIVEL DE ATENCIÓN
1	<b>ATENCIÓN PRIORITARIA:</b> Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información. <b>Ejemplo:</b> Workflow (Trámites, Radicación, Conectividad, Impresoras de radicación, Procesos Certificados de Vigencia y Antecedentes Disciplinarios, Peticiones y Reclamaciones, Etc.)
2	<b>ATENCIÓN NORMAL:</b> Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. <b>Ejemplo:</b> Impresoras, Procesos Disciplinarios, Sistemas que no requirieran Conectividad y que cuenten con mayor plazo para la consulta y disponibilidad de información, etc.

## 7. PLAN DE CONTINGENCIA PARA LA PRESTACIÓN DEL SERVICIO

Los funcionarios del IDERF deben continuar con la prestación del servicio a los usuarios externos en caso de que ocurra una interrupción del servicio en los sistemas de información del IDERF, para ello se deben tener en cuenta las siguientes consideraciones:

- Comunicar al área de sistemas el incidente inmediatamente vía telefónica, previa verificación en el correo electrónico si el área de sistemas envió información al respecto sobre procedimiento y tiempo estimado que durará la interrupción de la prestación del servicio del sistema de información del IDERF.
- Verificar la última radicación o la numeración del último registro o documento físico recibido y realizar la actividad y el control de forma manual o en otro sistema de información alternativo de contingencia como Word, Excel, Etc.
- Para el caso de los memorandos, se deben elaborar en Word teniendo en cuenta el último consecutivo de radicación y anexarlos al sistema Workflow una vez se restablezca el sistema.
- El área de sistemas prestará apoyo sobre cualquier procedimiento o contingencia de los sistemas de información cuando no existan formalmente.



- En caso de no tener red de Internet, servicio de electricidad, los responsables de cada oficina deben comunicarse con el proveedor del servicio público para hacer el seguimiento a la solución de la falla y obtener el tiempo estimado de la solución.
- Las planillas de asignación y traslado de correspondencia deberán realizarse en Excel, para agilizar el trámite en caso de contingencia del sistema de información, con la misma presentación del formato aprobado en el manual respectivo.
- EL IDERF prestará el soporte necesario para la generación de las Resoluciones Seccionales el día del Consejo y cierre masivo en el sistema, en caso de interrupción en la prestación del servicio de Internet, Electricidad y/o fallas técnicas de equipos y sistemas de información.
- Las UPS asignadas a los equipos de cómputo darán únicamente el tiempo necesario e indispensable para guardar la información que se esté trabajando en ese momento, permitiendo dar protección a los equipos en caso de caídas eléctricas.
- En coordinación con el Profesional de Gestión Administrativa, responsable de administración de bienes y el supervisor del contrato de mantenimiento, el área de sistemas prestará asesoría y soporte en la configuración de equipos, repuestos o periféricos para dar continuidad a la operación de la entidad en caso de suspensión de la prestación del servicio. Las autorizaciones respectivas de compras por caja menor, traslados o prestamos de equipos, repuestos o periféricos, deben ser tramitadas por escrito por el jefe de cada dependencia.

## 8. DESCRIPCIÓN DE LA ACTIVIDAD

No.	Nombre de la actividad	Descripción	Responsable
1	Inicio del Procedimiento		
2	Comunicar el problema o falla.	El funcionario usuario del sistema identifica el problema o falla del sistema de información y comunica de forma inmediata, telefónicamente o por correo electrónico al área de sistemas del IDERF los pormenores del caso. La comunicación debe especificar el sistema de información que maneja, el usuario al que se le presentó la falla, los registros afectados (radicaciones, fechas, documentos, etc.), la descripción de los pasos realizados, y toda información adicional como pantallazos necesarios para identificar el problema.	Todos los funcionarios usuarios de sistemas de información del IDERF.
4	Escalar y gestionar la solución del problema	El responsable de la etapa diligencia el formato reporte de problema para seguimiento y control de la solución del problema. En el formato se categoriza el problema de acuerdo con la prioridad y se escala al responsable de acuerdo con el nivel de servicio del numeral 6.1 Si el problema va a ser solucionado por personal externo a la entidad en el formato se registrará el responsable del área de sistemas del seguimiento de la solución.	Funcionario del área de sistemas asignado para solución y seguimiento del reporte.
5	Ejecutar pruebas	Después del diagnóstico, si se encuentra solución, se implanta la misma y se recupera la operación normal de lo contrario se escala al siguiente nivel y se verifica nuevamente el problema hasta encontrar la solución. Se realizan pruebas en el ambiente de pruebas para verificar la efectiva solución, luego se implementa en el ambiente de producción. Si no se puede volver a reproducir el problema en ambiente de pruebas o producción, se realiza seguimiento y monitoreo durante un mes hasta que se vuelva a presentar, si no vuelve a presentarse se cierra el problema y se hace reapertura si es necesario.	Funcionario del área de sistemas asignado para solución y seguimiento del reporte.



		Si la solución del problema impacta el proceso o procedimientos del sistema, requiere aprobación la cual debe quedar en un memorando instructivo. Una vez solucionado el problema se registra en el formato la descripción de la solución del problema, fecha, responsable y si la solución dada requiere que se modifiquen los manuales. Se envía comunicación de la solución y cierre del problema por email al funcionario que reportó el problema y a las partes interesadas del proceso, para verificación de la solución.	
6	Verificar solución y período de prueba.	Los funcionarios usuarios del sistema deben verificar que la solución dada sea satisfactoria durante un período no superior a dos días, de lo contrario comunicarán al área de sistemas la inconformidad para la reapertura del problema y se devuelve a la actividad 4. Si los usuarios no presentan ninguna observación durante el período de prueba, se entiende por recibida a satisfacción la solución del problema.	Todos los funcionarios usuarios de sistemas de información del IDERF.
7	Cerrar problema.	Se cierra el problema, una vez finalizado el tiempo de prueba o si existe recibo a satisfacción por parte de los usuarios del sistema sobre la solución dada. Así mismo antes del cierre se debe comunicar al responsable los cambios para la actualización de manuales si se requiere.	Funcionario del área de sistemas asignado para solución y seguimiento del reporte.
8	Fin del procedimiento.		

## 8.2 SOLICITUD DE MEJORA Y CONTROL DE CAMBIO

No.	Nombre de la actividad	Descripción	Responsable
1	Inicio del Procedimiento		
2	Comunicar solicitud de mejora.	El funcionario realiza la solicitud del requerimiento sobre la mejora o cambio del sistema de información, consecuencia de mejoras de procesos y procedimientos o actualizaciones de manuales, o por implementación de nueva reglamentación adoptada por la Entidad. Requiere mínimo una reunión con el área de sistemas para el levantamiento de información de requerimientos y el análisis de impacto que requiere el cambio de la información existente de los sistemas.	Todos los funcionarios usuarios de sistemas de información del IDERF.
3	Planificar el cambio.	Se asigna un responsable para realizar el ajuste, de acuerdo a la especialidad, un funcionario de la Entidad o un Contratista y un funcionario responsable para el seguimiento o supervisión de las actividades por realizar. Se diligencia el formato que contiene la descripción general de la solicitud de cambio o mejora, se incluyen como anexos todos los documentos necesarios sobre el requerimiento. Para algunos casos cuando el cambio del sistema es complejo o presenta un alto impacto debe realizarse un cronograma planificando todas las fases de su desarrollo e implementación. Antes de dar trámite a la solicitud esta debe haber sido aprobada mínimo por el responsable del proceso o del sistema de información, del funcionario o contratista que realizará el cambio. El funcionario será asignado de acuerdo con la especialidad según cuadro de escalamiento y tiempos de las tablas del numeral 6.1.	Funcionario del área de sistemas asignado para solución y seguimiento de la solicitud.
4	Analizar el impacto y evaluación del problema.	El responsable asignado realiza el análisis del impacto, diagnóstico y evaluación del requerimiento y estima el tiempo requerido para realizar la actividad la cual debe quedar registrada en un acta de seguimiento. Los sistemas de información son muy susceptibles a los cambios de configuración por las sofisticadas interrelaciones entre todos los procesos involucrados. Un cambio	Funcionario del área de sistemas asignado para solución y seguimiento de la solicitud.



		aparentemente menor puede desencadenar una reacción en cadena con resultados catastróficos. Es imprescindible, como mínimo, disponer siempre de un plan de contingencia (Back up) que permita la recuperación de la última configuración estable antes del cambio.	
5	Comunicar e implementar el cambio o mejora del sistema.	Si el cambio requiere ser desarrollado por un contratista externo, el funcionario asignado debe realizar seguimiento sobre el cumplimiento del término establecido y si la solución se ajusta a las especificaciones solicitadas. Se realizan pruebas en el ambiente de pruebas para verificar la efectiva solución, luego se implementa en el ambiente de producción. Requiere que los usuarios que solicitaron el cambio o mejora, sean comunicados con antelación a la implementación.	Funcionario del área de sistemas asignado para solución y seguimiento de la solicitud.
6	Verificar los cambios realizados y período de prueba.	Los funcionarios usuarios del sistema deben verificar que la actualización del sistema, de acuerdo con el cambio o mejora realizada sea satisfactoria, durante un período no superior a dos días, de lo contrario deben comunicar al área de sistemas la inconformidad la revisión y se devuelve a la actividad 4. Si los usuarios no presentan ninguna observación durante el período de prueba, se entiende por recibido a satisfacción el requerimiento. La opinión de los usuarios debe ser tomada en cuenta, como retroalimentación y debe ser revisada en caso de que se encuentren objeciones justificadas al cambio (debe tenerse en cuenta la resistencia habitual al cambio por parte de cierto tipo de usuarios)	Todos los funcionarios usuarios de sistemas de información del IDERF.
7	Cerrar la solicitud de cambio o mejora en el sistema de información	Se cierra la solicitud, una vez finalizado el período de prueba o acuse de recibo a satisfacción por parte de los usuarios del sistema sobre la solución dada. Así mismo antes del cierre debe existir comunicación al responsable de los cambios para la actualización de manuales si se requiere.	Funcionario del área de sistemas asignado para solución y seguimiento de la solicitud.
8	Fin del procedimiento		

### 8.3 PROCESO DE RECUPERACIÓN EN CASO DE INTERRUPTIÓN DEL SERVICIO

No.	Nombre de la actividad	Descripción	Responsable
1	Inicio del Procedimiento.		
2	Comunicar la falla.	Los funcionarios del IDERF tienen la responsabilidad de comunicar de forma inmediata, por cualquier medio de comunicación, al área de sistemas la interrupción parcial o total del servicio de un sistema de información y/o comunicación de la Entidad.	Todos los funcionarios usuarios de sistemas de información del IDERF



3	Iniciar plan de recuperación	<p>Los ingenieros de sistemas del IDERF o Contratistas realizan pruebas preliminares para constatar la veracidad del incidente y constatar la suspensión total o parcial del servicio del sistema de información. En principio se deben tomar en cuenta los siguientes aspectos del plan de emergencias:</p> <ol style="list-style-type: none"> <li>1. Evaluación del impacto de la situación del desastre en la infraestructura de los sistemas de información y/o comunicación.</li> <li>2. Asignación de funciones de emergencia a los funcionarios del área de sistemas.</li> <li>3. Verificación de disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos distribuidos, sistemas eléctricos, comunicación, hardware, y Backups.</li> <li>4. Comunicación a los usuarios de la interrupción o degradación del servicio indicando el tiempo estimado de restablecimiento del servicio si se puede determinar.</li> <li>5. Procedimiento de contacto y colaboración con los proveedores involucrados.</li> <li>6. Se ejecuta la siguiente actividad para la puesta en marcha del plan de contingencia correspondiente.</li> </ol> <p>El funcionario del área de sistemas diligencia el formato con la información del sistema de información que presenta fallas y el periodo de caída del sistema.</p>	Funcionario del área de sistemas asignado para la recuperación y seguimiento de la solución.
4	Ejecutar el plan de recuperación.	<p>Si el sistema se encuentra funcionado parcialmente y es posible realizar una copia de seguridad, se suspende el servicio para que los usuarios no registren más transacciones y se realiza la copia de seguridad.</p> <p>El responsable asignado ejecuta los siguientes pasos para la recuperación del sistema de acuerdo al nivel de la falla:</p> <ol style="list-style-type: none"> <li>1. Instalación y puesta a punto de un equipo de cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.</li> <li>2. Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.</li> <li>3. Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.</li> <li>4. Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información.</li> <li>5. Realización del procedimiento restauración de la base de datos con la última copia de seguridad disponible (Restore).</li> <li>6. Reiniciación del servicio, prueba y afinamiento del sistema de información.</li> <li>7. En un horario de baja demanda, se realiza la recuperación de otras aplicaciones y documentos que no influyen directamente en el funcionamiento del sistema de información recuperado.</li> <li>8. Si el equipo de cómputo no requiere cambiarse por fallas técnicas de hardware y se cuenta con una copia imagen del disco duro, únicamente es necesario restaurar la imagen del disco duro y restaurar la copia de seguridad de la información, sin realizar los pasos del 1 al 4.</li> <li>9. Para algunos sistemas de información únicamente se requiere copiar la carpeta donde se encuentra el software ejecutable y actualizar la carpeta de la base de datos con el último back up automático almacenado en el disco duro o memoria USB del usuario.</li> </ol>	Funcionario del área de sistemas asignado para la recuperación y seguimiento de la solución.



		10. De acuerdo con la complejidad y especialidad del sistema de información de la Entidad, o si la actividad 4 no ha sido satisfactoria, se debe escalar y determinar el nivel de servicio de acuerdo a los cuadros del numeral 6.1	
5	Comunicar el restablecimiento del servicio.	Una vez puesta en marcha y funcionamiento el sistema de información, se comunica a los usuarios del mismo. Se realiza un seguimiento en las primeras dos horas sobre el comportamiento y rendimiento del sistema para verificar su correcto funcionamiento. Se lleva a cabo una encuesta sobre del funcionamiento del sistema de información, como retroalimentación para el cierre del proceso.	Funcionario del área de sistemas asignado para la recuperación y seguimiento de la solución.
6	Cerrar el proceso de recuperación en caso de contingencia.	Se cierra el proceso, una vez finalizado el período de seguimiento y no exista ninguna observación por parte de los usuarios.	Funcionario del área de sistemas asignado para la recuperación y seguimiento de la solución.
7	Fin del procedimiento		

#### 8.4. PROCEDIMIENTO DE COPIA DE SEGURIDAD (BACKUP)

No.	Nombre de la actividad	Descripción	Responsable
1	Inicio del Procedimiento		
2	Elaborar copias de seguridad de sistemas de información.	Elaborar copia de seguridad en CD o DVD o BD de los sistemas de información de la Entidad. Para algunos sistemas de información se requiere que no se encuentre operando en el sistema tarea alguna al momento de realizar la copia de seguridad, por lo anterior se programará en horario no hábil. Los discos CD-DVD-BD que contendrán la copia de seguridad deben identificarse con la siguiente información: Fecha, Área, Nombre del sistema, Año, funcionario que realizó la copia de seguridad. Requiere registro en el formato de control de back ups con los detalles de la elaboración de la copia de seguridad.	Funcionario del área de sistemas asignado la elaboración de la copia de seguridad.
3	Elaborar copias de seguridad de archivos y documentos.	Los funcionarios responsables de computadores personales deben elaborar una copia de seguridad en CD o DVD o BD anual de todos los archivos y documentos y una copia diaria, si se requiere, en una memoria USB. Para automatizar la copia de archivos y documentos a la memoria USB el área de sistemas prestará soporte suministrando una aplicación que actualiza únicamente los archivos modificados a la fecha de la realización de la copia de seguridad. Los discos CD-DVD-BD que contienen la copia de seguridad deben estar debidamente identificados con la siguiente información: Fecha, Área, Contenido, Año, funcionario que realizó la copia de seguridad. - La nomenclatura de los subdirectorios se mantendrá de acuerdo a como la entregue el funcionario. Para algunos sistemas de información se requiere que no se encuentre operando en el sistema tarea alguna al momento de realizar la copia de seguridad, por lo anterior se programará en horario no hábil. Los Secretarios Seccionales y Profesionales de Gestión deben llevar el registro del Backup en el formato como medida de control y de backups los detalles de la elaboración de la copia de seguridad.	Funcionario del área de sistemas asignado la elaboración de la copia de seguridad.



4	Verificar medios	Verificar la información que se almacena, tanto en original como las copias. Así mismo se verifica el cumplimiento del procedimiento establecido de acuerdo con los periodos para cada sistema de información. Verificar el libro de control de copias de seguridad con los medios físicos de respaldo.	Secretarios Administrativa
5	Archivar y custodiar copias de seguridad	Las copias de seguridad en línea deben permanecer por lo menos una semana en el disco duro. Las copias de seguridad de gestión e históricas permanecen guardadas de acuerdo con lo establecido en la tabla de retención documental. El responsable del traslado y retiro del archivo de las copias de seguridad es el funcionario de sistemas encargado de realizar la copia de seguridad.	Funcionario del área de sistemas asignado.
6	Fin de procedimiento.		

Para llevar a feliz término este Plan, se deberá contar con el apoyo de la Dirección y la aprobación del Comité de Gestión y Desempeño de la Empresa.

Por lo anterior se presenta el Plan de Tratamiento y Riesgo de Seguridad del Instituto Deportivo y Recreativo de Fusagasugá IDERF para la vigencia, a los 27 días del mes de enero de 2023



LIC. ELVIS YONJAN CORTÉS GARCÍA.

Director



ANA LILIANA MEDINA POLANIA.

Secretaria General