PLAN DE CONTINGENCIA Y POLÍTICAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCION

El 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 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 paralicen 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.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

• **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:

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

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
El Fuego: destrucción de equipos y archivos.	Bajo	Extintores, pólizas de seguros.
El robo común: pérdida de equipos y archivos.	Medio	Seguridad Privada, Alarma, Seguro contra todo riesgo y copias de respaldo (Back up).
El vandalismo: daño a los equipos y archivos.	Medio	Seguro contra todo riesgo, copias de respaldo.
Fallas en los equipos: daño a los archivos.	Medio	Mantenimiento, equipos de respaldo, garantía y copias de respaldo.
Equivocaciones: daño a los archivos.	Bajo	Capacitación, copias de respaldo, políticas de seguridad.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

Acción de Virus: daño a los equipos y archivos.	Medio	Actualizaciones del sistema operativo, Antivirus actualizados, copias de respaldo.
Terremotos: destrucción de equipo y archivos.	Medio	Seguro contra todo riesgo, copias de respaldo. Las sedes cumplen con las normas antisísmicas.
Accesos no autorizados: filtrado no autorizado de datos.	Bajo	Cambio de claves de acceso mínimo cada seis meses. Política de seguridad para acceso a personal competente.
Robo de datos: 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.
Fraude: 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 encontrase 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. **Responsable**: 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. **Responsable**: Ingeniero de Sistemas del IDERF.
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. **Responsable**: *Ingeniero de Sistemas del IDERF*
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. **Responsable**: *Ingeniero de Sistemas del IDERF*.
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. **Responsable**: Profesional de Gestión Administrativa.
6	Mantenimientos, revisiones preventivas y correctivas de equipos de computación y comunicación, extintores, alarmas	Equipos de computación y comunicación periféricos, sistemas eléctricos UPS, Aire acondicionado,	Contratos anuales de mantenimiento, garantías vigentes y control del mantenimiento de los equipos.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

	y sistemas contra incendio, para mantenerlos en óptimas condiciones.	Alarmas, Sistemas contra incendio, Extintores.	**Responsable**: 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. **Responsable**: 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. **Responsable**: Ingeniero de sistemas *del IDERF*.
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. **Responsable**: 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 su reemplazo inmediato en caso de falla.	Equipos de computación y comunicación de la Entidad.	Reducción del tiempo de respuesta a fallas de hardware y sistemas de información. **Responsable**: 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.	**Concepto n+1:** 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. **Responsable**: *Ingeniero de Sistemas del IDERF*.

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 el formato SI-fr-03 (Ver anexo 9.1), cuyos resultados podrán ser consultados por el jefe inmediato desde el sistema Workflow.

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.

El profesional responsable del área de sistemas debe registrar el siniestro en el libro de registro de contingencias, formato SI-fr-07 (Ver anexo 9.6), el cual puede ser consultado por el jefe inmediato desde el sistema Workflow.

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:

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

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 DEDESARROLLO	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 DE RECUPERACIÓN	Actividades por realizar para volver a contar con el Sistema de Información (actividades de Restauración).
10	TIEMPO DE RECUPERACIÓN	Tiempo estimado en horas o días, para que EL IDERFpueda 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 el formato SIfr-04 (Ver anexo 9.2), la cual puede ser consultada por el jefe inmediato desde el sistema Workflow.

4.3.2 EQUIPOS DE CÓMPUTO:

EL IDERFdebe 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.

La información anterior debe mantenerse actualizada en el formato SI-fr-10, (Ver anexo N° 9.3) por el funcionario responsable del manejo de los inventarios en el sistema de activos fijos, la cual podrá ser consultada por el jefe inmediato desde el sistema Workflow.

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.

La información anterior debe mantenerse actualizada por el área de sistemas en el formato SI-fr-05 (ver anexo 9.4), el cual debe incluir la información de todos los funcionarios y personal que labora en el área de sistemas del IDERF, la cual puede ser consultado por el jefe inmediato desde el sistema Workflow.

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

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

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)	**Período**: Anual de todos los documentos del IDERF. **Medio**: DVD o CD, Nube, Memoria USB **NOTA**: 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.	**Período**: Diaria de los documentos más importante del IDERF. **Medio**: 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.	**Período**: Semanal **Medio**: 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.	**Período**: Semanal **Medio**: 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.

La información anterior debe mantenerse actualizada por el área de sistemas en el formato Libro de Control de Backups SI-fr-06 (ver anexo 9.5), el cual puede ser consultado por el jefe inmediato desde el sistema Workflow.

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 SI-fr-11 (ver anexo 9.9) 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 IDERFdeben 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 un funcionario, supernumerario o proveedor cese de prestar sus servicios a IDERF.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

Mediante el registro del libro de bitácora de auditoría en los diferentes sistemas de información se efectúa 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 seguimiento el Área de Sistemas diligenciará el formato SI-fr-09 (Ver anexo 9.8) o el formato SI-fr-08 (Ver anexo 9.7) según sea el caso.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación en el formato SI-fr-09. 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.

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 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 los libros de bitácora 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.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

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

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

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 sensitiva, 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 la 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, 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 7x24x365, 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.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

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 sistemas 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 consiguiente 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.

5. 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 quienes 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.
Para ello el ingeniero de sistemas que atiende la solicitud deberá registrar la incidencia y la solución de la misma en el sistema Workflow, mediante el formato SI-fr-08 (Ver anexo 9.7), el cual puede ser consultado por el jefe inmediato desde el sistema Workflow.
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 y Control Interno para evaluación; 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.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

6.1 CUADRO DE ESCALAMIENTO

NIVEL	PUNTO DE ESCALAMIENTO
1	Ingeniero de sistemas del IDERF
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 SI-fr-09 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	**ATENCIÓN PRIORITARIA**: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información. **Ejemplo**: Workflow (Trámites, Radicación, Conectividad, Impresoras de radicación, Procesos Certificados de Vigencia y Antecedentes Disciplinarios, Peticiones y Reclamaciones, Etc.)
2	**ATENCIÓN NORMAL**: Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. **Ejemplo**: 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 alterno 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.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

- 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 SI-fr-08 (Ver anexo 9.7) para seguimiento y control de la solución del problema. En el formato SI-fr-08 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. 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 SI-fr-08 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.	Funcionario del área de sistemas asignado para solución y seguimiento del reporte.
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.	Todos los funcionarios usuarios de sistemas de información del IDERF.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

		Si los usuarios no presentan ninguna observación durante el período de prueba, se entiende por recibida a satisfacción la solución del problema.	
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 SI-fr-09 (Ver anexo 9.8) 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 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.	Funcionario del área de sistemas asignado para solución y seguimiento de la solicitud.
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.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

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 INTERRUPCIÓN 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
Iniciar plan de recuperación		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: 1. Evaluación del impacto de la situación del desastre en la infraestructura de los sistemas de información y/o comunicación. 2. Asignación de funciones de emergencia a los funcionarios del área de sistemas. 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. 4. Comunicación a los usuarios de la interrupción o degradación del servicio indicando el tiempo estimado de restablecimiento del servicio si se puede determinar. 5. Procedimiento de contacto y colaboración con los proveedores involucrados. 6. Se ejecuta la siguiente actividad para la puesta en marcha del plan de contingencia correspondiente. El funcionario del área de sistemas diligencia el formato SI-fr-07 (Ver anexo N° 9.6) con la información del sistema de información que presenta fallas y el periodo de caída del sistema.	Funcionario del área de sistemas asignado para la recuperación y seguimiento de la solución.
4	Ejecutar el plan de recuperación.	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. El responsable asignado ejecuta los siguientes pasos para la recuperación del sistema de acuerdo al nivel de la falla: 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. 2. Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar. 3. Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad. 4. Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información. 5. Realización del procedimiento restauración de la base de datos con la última copia de seguridad disponible (Restore). 6. Reiniciación del servicio, prueba y afinamiento del sistema de información. 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. 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. 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. 10. De acuerdo con la complejidad y especialidad del sistema de información de la Entidad, o si la actividad 4 no ha sido satisfactoria,	Funcionario del área de sistemas asignado para la recuperación y seguimiento de la solución.

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

		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 SI-fr-06 (Ver anexo 9.5) 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 SI-fr-06 (Ver anexo 9.5) como medida de control y de backups los detalles de la elaboración de la copia de seguridad.	Secretarios Seccionales y Profesionales de Gestión.
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 períodos para cada sistema de información. Verificar el libro de control de copias de seguridad con los medios físicos de respaldo.	Secretarios Seccionales Profesionales
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.		

Carrera 3 No. 14 A- 68 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
Celular: 3224154377
WEB: www.iderf.gov.co
Código Postal: 252211

9. ANEXOS

9.1 Lista de verificación plan de contingencia. (SI-fr-03)
9.2 Lista de sistemas de información activos. (SI-fr-04)
9.3 Lista de activos de equipos de sistemas. (SI-fr-10)
9.4 Lista de contratos y personal que labora en sistemas. (SI-fr-05)
9.5 Libro de control de BACKUPS. (SI-fr-06)
9.6 Libro de registro de contingencias. (SI-fr-07)
9.7 Reporte de problemas. (SI-fr-08)
9.8 Solicitud de mejora y control de cambio. (SI-fr-09)
9.9 Lista de inventario de licencias de software. (SI-fr-11).