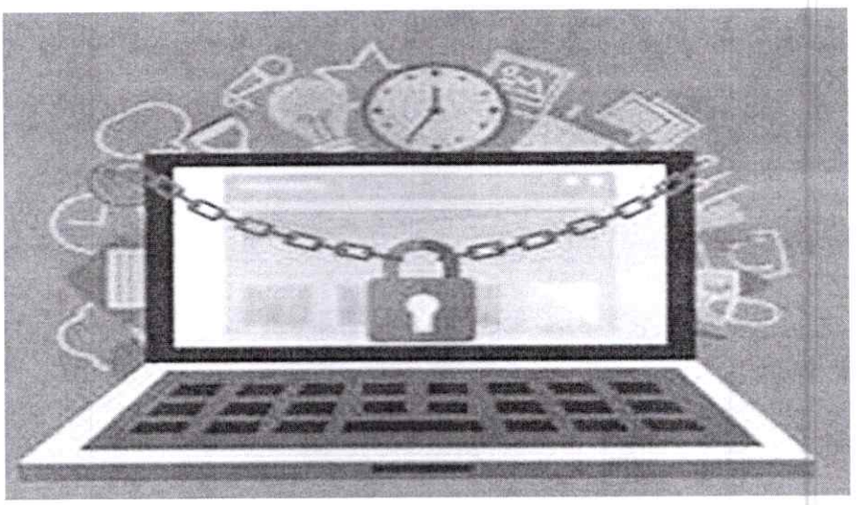
IDERF
INSTITUTO DEPORTIVO Y RECREATIVO DE FUSAGASUGÁ

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION



Daniel Alberto Parrado Díaz
Director

Vigencia 2024

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

TABLA DE CONTENIDO

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

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).

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

- **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 auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (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.

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

- **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).

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

- **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).

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

- **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,

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

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.

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

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.

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

• 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

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

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.

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

• 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

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

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.

Carrera 3 No. 14 A- 58 Coliseo Coburgo – Futsal
Teléfonos: (091) 874 8080
Celular: 3224154377
NIT: 890680338-1
E-mail: atencionalciudadano@iderf.gov.co
WEB: www.iderf.gov.co
Código Postal: 252211

• 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

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

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.

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

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 Direccion 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 Secretaria 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 Secretaria 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 Secretaria 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

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

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.

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

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 autodiagnóstico.
2. Realizar la Identificación de los Riesgos en las diferentes áreas del Instituto.
3. Realizar sensibilización del Plan.

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.

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

12. CRONOGRAMA:

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION																								
ACTIVIDAD	**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
1. Realizar autodiagnóstico.																								
2. Realizar la Identificación de los Riesgos en las diferentes áreas del Instituto.																								
3. Realizar sensibilización del Plan.																								

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

Por lo anterior se presenta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del **INSTITUTO DEPORTIVO Y RECREATIVO DE FUSAGASUGÁ IDERF** para la vigencia, a los 31 días del mes de enero de 2024

DANIEL ALBERTO PARRADO DÍAZ.
Director

ANA LILIANA MEDINA POLANIA
Secretaria General

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