POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

La Fundación REI Para La Rehabilitación Integral IPS determina la información como un activo de alta importancia para la entidad que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de esta, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

En el presente manual se establecen las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con Fundación REI Para La Rehabilitación Integral IPS; estas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001 y al modelo de seguridad y privacidad de la información del Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

En la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas.

1.1. Glosario.

- Interoperabilidad: capacidad de varios sistemas o componentes para intercambiar información, entender estos datos y utilizarlos. De este modo, la información es compartida y está accesible desde cualquier punto de la red asistencial en la que se requiera su consulta y se garantiza la coherencia y calidad de los datos en todo el sistema, con el consiguiente beneficio para la continuidad asistencial y la seguridad del paciente.
- Soportes lógicos: información que esté siendo utilizada mediante medios ofimáticos, correo electrónico o sistemas de información desarrollados a medida o adquiridos a un tercero.
- Soportes físicos: información que esté en papel, soportes magnéticos como USB, Disco Externos, etcétera.
- Medios ofimáticos: Son herramientas que nos permiten idear, elaborar, ceder, guardar todas las informaciones necesarias en una oficina, por ejemplo,

procesamiento de texto, base de datos, hojas de cálculo, programas de correo electrónico, suite ofimática, calculadora, agendas, entre otros programas.

1.2. Objetivo

El objetivo principal de la presente Política de alto nivel es definir los principios y las reglas básicas para la gestión de la seguridad de la información. El fin último es lograr que la Fundación REI Para La Rehabilitación Integral IPS garanticen la seguridad de la información y minimicen los riesgos de naturaleza no financiera derivados de un impacto provocado por una gestión ineficaz de la misma.

1.3. Alcance

La Política es aplicable para toda la Fundación REI Para La Rehabilitación Integral IPS, que deberá cumplir este mínimo requisito sin perjuicio de tener políticas más restrictivas y mejorar la seguridad en la medida de lo posible. El alcance de la presente Política abarca toda la información de la Fundación REI Para La Rehabilitación Integral IPS con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual. Los colaboradores tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por el comité de seguridad de la información.

Nadie está autorizado para subir imágenes ni información de las historias clínicas de los beneficiarios de la Fundación (estudiantes, pacientes, padres y madres de familia) en su red social. La prohibición se extiende tanto a empleados de la Fundación REI Para La Rehabilitación Integral IPS como para los estudiantes que se encuentran haciendo las prácticas formativas en las instalaciones de la Fundación bajo el marco del convenio docencia y servicio.

La Política deberá estar disponible en la página web corporativa www.fundacionrei.org

1.4. Adaptación y desarrollo de la Política

Esta Política de Seguridad de la información fue adaptada y desarrollada por parte de la **Fundación REI Para La Rehabilitación Integral IPS**, siguiendo las directrices de la norma ISO 27001.

2. Principios de la Política de la Información

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a la **Fundación REI Para La Rehabilitación Integral IPS**.

Además, la **Fundación REI Para La Rehabilitación Integral IPS** establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- ✓ Alcance estratégico: La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de la **Fundación REI Para La Rehabilitación Integral IPS** de forma que pueda estar coordinada e integrada con otras iniciativas estratégicas para crear un sistema totalmente coherente y eficaz.
- ✓ Seguridad integral: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.
- ✓ Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- ✓ Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- ✓ Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente dependiendo de la actualización de los sistemas de cómputo, teniendo en cuenta, el mantenimiento preventivo o correctivo de la vida útil de los equipos de cómputo se realiza semestral, dependiendo del entorno de la organización y de la naturaleza de sus activos y de la rapidez que cambien las amenazas a la seguridad, para adecuar su eficacia a la

constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.

- ✓ La confidencialidad: Esto garantiza que la información sólo sea accesible para las personas autorizadas a tener acceso.

La **Fundación REI Para La Rehabilitación Integral IPS** considera que las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos de su personal.

Puesto que la Seguridad de la Información incumbe a todo el personal de la **Fundación REI Para La Rehabilitación Integral IPS**, esta Política deberá ser conocida, comprendida y asumida por todos sus colaboradores.

3. Marco Legal.

Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 2015 de 2020. Por medio de la cual se regula la interoperabilidad de la Historia Clínica Electrónica - IHCE, a través de la cual se intercambiarán los elementos de datos clínicos relevantes, así como los documentos y expedientes clínicos del curso de vida de cada persona.

Ley 384 de 2023. Ley “Dejen de fregar”. Pendiente por aprobación.

4. Compromiso de la Dirección

La Dirección de la **Fundación REI Para La Rehabilitación Integral IPS**, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- ✓ Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- ✓ Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- ✓ Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los colaboradores de la **Fundación REI Para La Rehabilitación Integral IPS.**
- ✓ Garantizar efectividad presupuestal, para herramientas de seguridad, actualización de equipos de sistemas para hardware, software, accesorios, o consultorías.
- ✓ Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- ✓ Considerar los riesgos de seguridad de la información en la toma de decisiones.

5. Roles y responsabilidades

La **Fundación REI Para La Rehabilitación Integral IPS** se compromete a velar por la seguridad de todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, siempre garantizando el cumplimiento de las distintas normativas y leyes aplicables.

La **Fundación REI Para La Rehabilitación Integral IPS** tendrá dos figuras responsables, que definan, implementen y monitoreen las medidas de ciberseguridad y seguridad de la información, internamente será la Asistencia de Dirección Ejecutiva, esta será la figura responsable interna encargada de velar por el funcionamiento de los equipos de trabajos de la organización, externamente será SmartInfo siendo los encargados de manejar las redes sociales y creación de correos electrónicos.

Estas figuras asumirán las funciones que, con carácter general, sean atribuidas por la presente Política de Seguridad de la Información.

Será su responsabilidad desarrollar y mantener la Política, asegurándose que ésta sea adecuada y oportuna según vaya evolucionando la **Fundación REI Para La Rehabilitación Integral IPS.**

6. Gestión de la Seguridad de los Recursos Humanos

El área encargada de Talento Humano deberá realizar su gestión teniendo en cuenta los criterios de seguridad establecidos en la Política de Seguridad de la Información, siendo este un punto clave para asegurar su cumplimiento.

Se deberán salvaguardar los requisitos establecidos en la presente Política en todo momento, incluyendo en la fase previa a la contratación, fase de contratación, y fase de desistimiento de contratos de los empleados, para ello se deberá firmar un acuerdo o en su defecto una cláusula de confidencialidad y no divulgación (Ver cláusula de contratos laborales y de prestación de servicios).

6.1. Formación y concienciación

La **Fundación REI Para La Rehabilitación Integral IPS** deberá asegurar que todo el personal reciba un nivel de formación y concienciación adecuado en materia de Seguridad de la Información de acuerdo a la normativa vigente ISO 27001, especialmente en materia de confidencialidad y prevención de fugas de información, por lo que todos los equipos de cómputos y activos de la organización deben tener contraseña.

Toda clave o contraseña debe cumplir con el siguiente estándar o cumplir con los siguientes requisitos:
- Debe tener al menos un carácter en mayúscula.
- Debe tener al menos un carácter en minúscula.
- Debe tener al menos un dígito (0 a 9).
- Deben tener mínimo 8 caracteres.
- Debe tener al menos un carácter especial (*-_+?!”#$%&/)

Así mismo, los colaboradores deberán actualizarse con respecto a las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes, de manera que pueda garantizarse el cumplimiento de esta Política; además, deben obrar con diligencia con respecto a la información, asegurándose que esta no caiga en poder de colaboradores o terceros no autorizados.

6.2. Política de mesas limpias

La Política de Mesas Limpias se trata de un concepto asociado a la confidencialidad de todos aquellos documentos que puedan contener datos sensibles, considerando que dichos papeles no pueden estar a la vista de cualquier persona, como por ejemplo: la historia clínica de los pacientes.

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

- ✓ Se deberá bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueo por parte del colaborador), como de forma automatizada mediante la configuración del bloqueo de pantalla (bloqueo por tiempo de inactividad).
- ✓ Se deberá mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

6.3. Gestión de dispositivos personales

La **Fundación REI Para La Rehabilitación Integral IPS** permitirá la política conocida como **DISPOSITIVOS PERSONALES**, que permite a los colaboradores utilizar sus recursos o dispositivos móviles personales para acceder a recursos o información de la institución.

Adicionalmente, los colaboradores deberán tener en cuenta una serie de requisitos establecidos en esta Política:

- ✓ Se deberán aplicar las mismas medidas y configuraciones de seguridad a los dispositivos personales que tratan información igual que al resto de dispositivos de la **Fundación REI Para La Rehabilitación Integral IPS**.
- ✓ El colaborador será responsable de su equipo personal (Ver acápite 6.1 y 6.2).
- ✓ Los colaboradores deberán mantener actualizado el dispositivo personal donde traten información de la **Fundación REI Para La Rehabilitación Integral IPS**. Así mismo, deberán tener instaladas aplicaciones de seguridad tales como antivirus.
- ✓ Los colaboradores deberán recibir autorización de la Dirección Ejecutiva para utilizar dispositivos personales que tengan acceso a la información la **Fundación REI Para La Rehabilitación Integral IPS.**
- ✓ Cualquier incidencia que pueda afectar a la confidencialidad, integridad o disponibilidad de estos dispositivos debe ser reportado a la Asistencia de Dirección Ejecutiva la cual es responsable de la seguridad de todos los activos.

6.4. Gestión de la seguridad en el manejo del correo electrónico.

1. Los colaboradores son completamente responsables de todas las actividades realizadas con sus cuentas de correo electrónico de la Entidad.

2. La cuenta de correo electrónico es personal e intransferible. El colaborador se compromete a hacer un uso diligente de la cuenta y a mantener su contraseña en secreto. Así mismo, se compromete a notificar al responsable de la presente política (Asistencia

de Dirección Ejecutiva) de manera inmediata la pérdida de su contraseña o acceso no autorizado por parte de terceros a su cuenta.
3. El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión masiva e indiscriminada de información.

6.5. Gestión del ciclo de vida de los accesos.

A continuación, se presentan los lineamientos para que el acceso a la información y sistemas de información de la **Fundación REI Para La Rehabilitación Integral IPS** sea controlado de manera permanente, para evitar accesos no autorizados asociados con la creación, modificación y eliminación de cuentas de usuario y accesos:

- El acceso a sistemas de información y aplicaciones debe ser autorizado por la Dirección Ejecutiva.
- Todo requerimiento para creación de usuarios, solicitud de acceso a información y novedades sobre estos usuarios y accesos, deberán informarle al responsable de la presente política (Asistencia de Dirección Ejecutiva).
- El responsable de la presente política (Asistencia de Dirección Ejecutiva) debe realizar revisiones periódicas, por lo menos semestralmente, para asegurar la coherencia entre los accesos otorgados, por ejemplo, el acceso a las carpetas compartidas en Google Drive.
- Los accesos compartidos deben ser para las cuentas institucionales habilitadas por SmartInfo, salvo excepciones para utilizar correos personales, lo cual debe ser previamente estudiadas y aprobadas por parte de la Dirección Ejecutiva.

6.6. Gestión de las copias de seguridad

Se deberán realizar copias de seguridad de la información, del software y del sistema y se deberán verificar periódicamente. Para ello, se deberán realizar copias de seguridad de aplicaciones, ficheros y bases de datos con una periodicidad, al menos, mensual, salvo que en dicho período no se hubiese producido ninguna actualización. En su caso, se podrá establecer una frecuencia más alta de realización de copias de seguridad, si la información a salvaguardar es de impacto alto para la **Fundación REI Para La Rehabilitación Integral IPS**.

Las copias de seguridad deberán tener los controles de acceso adecuados, es decir, deben ser de acceso restringido.

Como norma general y siempre que sea posible, se deberá requerir que la información este almacenada en el servidor de la organización, el cual es manejado por los ingenieros de sistemas.

7. Clasificación de la información

Se deberá clasificar la información para mantener su disponibilidad, confidencialidad e integridad. La clasificación será realizada por el responsable del Sistema de Gestión de Calidad, el cual será el encargado de su actualización cuando se crea conveniente, así como de dar a conocer el modelo de clasificación a todos los colaboradores de la **Fundación REI Para La Rehabilitación Integral IPS.**

7.1. Tipos de información

La **Fundación REI Para La Rehabilitación Integral IPS** deberá clasificar la información en función del soporte en el que está siendo utilizado:

A. Soportes lógicos.
B. Soportes físicos.

7.2. Niveles de clasificación

En función de la sensibilidad de la información, la **Fundación REI Para La Rehabilitación Integral IPS** deberá catalogar la información según los siguientes niveles:

- ✓ Uso público (Actas de asamblea, información colgada en la página web)
- ✓ Difusión limitada (correos electrónicos y los documentos de trabajo de las áreas de cada Grupo o unidad).
- ✓ Información confidencial (los informes de auditoría, Actas de junta directiva, las bases de datos de donantes).
- ✓ Información reservada (La historia clínica de los pacientes).

La información de uso público es de libre circulación y acceso, siempre y cuando sean utilizados para fines lícitos.

La información clasificada como de difusión limitada solo podrá ser accedida y utilizada por las personas expresamente mencionadas en el soporte lógico o físico que se utilice.

La información confidencial solo podrá ser accedida y utilizada por las personas expresamente autorizadas por parte de la Dirección Ejecutiva. Se restringirá la circulación de la información catalogada como confidencial.

La información reservada solo podrá ser accedida y utilizada por las personas expresamente autorizadas por parte de la Dirección Ejecutiva. En el caso de las historias clínicas, podrán tener acceso los profesionales de la salud que atenderán al respectivo paciente, el mismo paciente, y en caso de ser menor de edad, podrá tener acceso su representante legal o la persona autorizada por el representante legal del menor.

7.3. Privacidad de la información

La **Fundación REI Para La Rehabilitación Integral IPS** deberá asegurar la privacidad de los datos de carácter personal con el objetivo de proteger los derechos fundamentales de las personas físicas, especialmente su derecho al honor, intimidad personal y familiar y a la propia imagen, mediante el establecimiento de medidas para regular el tratamiento de los datos.

La **Fundación** deberá cumplir con la legislación vigente en materia de protección de datos personales en función de la jurisdicción en la que esté establecida y opere (a modo ilustrativo, Ley de Protección de Datos Personales o **Ley 1581 de 2012** en Colombia).

8. Prevención de fugas de información

La fuga de información es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.

Se deberán analizar los vectores de fuga de información, dispositivos móviles y de almacenamiento externo, correos electrónicos, Malware, troyanos, spyware y keyloggers en función de las condiciones y operativa de trabajo de cada unidad de **La Fundación REI Para La Rehabilitación Integral IPS**. Para ello, se deberán identificar los activos cuya fuga supone mayor riesgo para cada unidad, basándose en la criticidad del activo y el nivel de clasificación que la información tenga. Además, se deberán identificar las posibles vías de robo, pérdida o fuga de cada uno de los activos.

La Fundación REI Para La Rehabilitación Integral IPS deberá definir procedimientos para evitar la ocurrencia de las situaciones que puedan provocar la pérdida de información, así como procedimientos de actuación en caso de que se notifique una fuga de información.

Se deberá asegurar la formación y capacitación de todos los empleados en torno a buenas prácticas para la prevención de fugas de información. Especialmente se deberán tener en cuenta, al menos, los siguientes aspectos:

- ✓ Proceso para el manejo de dispositivos de alta criticidad conocidos
- ✓ Uso adecuado de dispositivos extraíbles como USB, DISCO EXTERNO o similares
- ✓ Uso del correo electrónico
- ✓ Transmisión de información de forma oral
- ✓ Impresión de documentación
- ✓ Salida de documentación
- ✓ Uso de dispositivos móviles
- ✓ Uso de Internet

- ✓ Escritorios limpios y ordenados (véase el apartado 6.2. Política de mesas limpias)
- ✓ Equipos desatendidos o no utilizados.

9. Gestión del ciclo de vida de la identidad

La **Fundación REI Para La Rehabilitación Integral IPS** deberán definir e implementar un adecuado sistema de gestión del ciclo de vida de la identidad. La identidad es el conjunto de características que identifican de forma unívoca a toda persona con acceso físico o lógico a los sistemas de información de la **Fundación REI Para La Rehabilitación Integral IPS**. El ciclo de vida de la identidad es el proceso que sigue la identidad de un usuario desde su creación hasta su eliminación.

El ciclo de vida de la identidad se compone de las siguientes actividades:

1) Creación y asignación de la identidad
2) Revisión periódica
3) Modificación o eliminación

La gestión de este ciclo requiere definir los requisitos de seguridad y responsabilidades de cada una de las etapas, con el objetivo de centralizar y facilitar los procesos de gestión asociados a las mismas.

La gestión del ciclo de vida de la identidad deberá estar alineado con el área de Recursos Humanos con el objetivo de verificar las identidades en función de las altas y las bajas de empleados y su correspondencia en los sistemas de información.

9.1. Identidades Privilegiadas

La asignación y uso de derechos de acceso privilegiado deberá estar restringida y controlada. El acceso privilegiado es el acceso a sistemas como administrador o con un rol que ofrezca la posibilidad de modificarla configuración del sistema.

La asignación de derechos de acceso privilegiado deberá ser controlada a través de un proceso formal de autorización de acuerdo con las políticas de control de acceso. Deberán considerarse, al menos, los siguientes requisitos:

- ✓ Deberán identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso (por ejemplo, sistema operativo, sistema de gestión de base de datos o aplicación), así como los usuarios a los que estos les deberán ser asignados.
- ✓ La asignación de derechos de acceso privilegiados deberá realizarse con base en las necesidades de uso, basándose en el mínimo privilegio y necesidad de saber.
- ✓ Deberá definirse un proceso de autorización que incluya un registro de los privilegios asignados. No deberán concederse derechos de acceso privilegiado hasta que el proceso de autorización se complete.

- ✓ Deberán definirse los requisitos para la caducidad de los derechos de acceso privilegiado.
- ✓ Las competencias de los usuarios con derechos de acceso privilegiado deberán revisarse regularmente por parte del responsable de esta política (Asistencia de Dirección Ejecutiva), con el objetivo de verificar que se encuentran alineadas con sus obligaciones.
- ✓ Deberán establecerse y mantenerse procedimientos y mecanismos específicos para evitar el uso no autorizado de cuentas de usuario genéricas para la administración, conformes con las capacidades de configuración de los sistemas.
- ✓ Se deberán establecer procedimientos y mecanismos que aseguren la confidencialidad de la información secreta de autenticación para los usuarios genéricos de administración (por ejemplo, modificación frecuente de contraseña, mecanismos de compartición de la contraseña seguros, etc.).

10. Seguridad en trabajo en la nube o Cloud

La **Fundación REI Para La Rehabilitación Integral IPS** deberá mantener una política de trabajo en la nube o cloud computing que establezca las medidas de seguridad adecuadas para la confidencialidad, integridad y disponibilidad de la información. Dependiendo de tipo de modelo de servicio en la nube, se deberán aplicar diferentes medidas de seguridad:

- ✓ Infraestructura: en primer lugar, se deberá asegurar que el Proveedor monitoriza el entorno para detectar cambios no autorizados. Además, se deberán establecer fuertes niveles de autenticación y control de acceso para los administradores y las operaciones que estos realicen. Por último, las instalaciones y/o configuraciones de los elementos comunes deberán estar registrados y conectados con el objetivo de obtener la trazabilidad adecuada.
- ✓ Plataforma: de forma adicional a las medidas indicadas en el modelo de servicio de Infraestructura, el Proveedor del servicio deberá proporcionar mecanismos de seguridad correspondientes al ciclo de vida del software seguro.
- ✓ Software: El proveedor deberá establecer las medidas de seguridad que estime conveniente.

11. Seguridad en las telecomunicaciones

La arquitectura de red de la **Fundación REI Para La Rehabilitación Integral IPS** deberá contar con medidas de prevención, detección y respuesta para evitar brechas en los dominios internos y externos. Se entiende por “dominio interno” la red local compuesta por los elementos tecnológicos de la **Fundación REI Para La Rehabilitación Integral IPS** accesibles exclusivamente desde la red interna. Por otra parte, se entiende

por “dominio externo” la red accesible desde el exterior de la red de la **Fundación REI Para La Rehabilitación Integral IPS.**

Es de suma importancia la administración de seguridad de las redes que atraviesan el perímetro de la **Fundación REI Para La Rehabilitación Integral IPS**, implantando controles adicionales para los datos sensibles que circulen por las redes de comunicación públicas.

Por ello, la **Fundación REI Para La Rehabilitación Integral IPS** definirá las pautas de seguridad a seguir con relación a la transferencia de información, así como las medidas de seguridad en la utilización de equipos portátiles, servicios de Internet y correo electrónico, y de controles específicos que permitan una conexión segura a los sistemas de información de la **Fundación REI Para La Rehabilitación Integral IPS** desde fuera de sus instalaciones.

12. Seguridad en el ciclo de vida del desarrollo de sistemas

Toda la adquisición, desarrollo y mantenimiento de los sistemas deberá contar con unos requisitos mínimos de seguridad necesarios para el desarrollo de software, los sistemas y los datos acorde con las buenas prácticas del sector. Además, deberá realizarse una gestión de las pruebas, el seguimiento de los cambios, y el inventario del software.
Cada unidad de la **Fundación REI Para La Rehabilitación Integral IPS** deberá tener en cuenta la seguridad de la información en sus procesos de sistemas y datos, procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

13. Seguridad en los Proveedores

Se deberá poner especial atención en evaluar la criticidad de todos los servicios susceptibles de ser subcontratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad de negocio.

Sobre los proveedores de estos servicios se deberán cuidar los procesos de selección, requerimientos contractuales como la terminación contractual, la monitorización de los niveles de servicio, la devolución de datos y las medidas de seguridad implantadas por dicho proveedor, que deberán ser, al menos, equivalentes a las que se establecen en la presente Política.

14. Gestión de Incidentes

Todos los colaboradores de la **Fundación REI Para La Rehabilitación Integral IPS** tienen la obligación y responsabilidad de la identificación y notificación al responsable de seguridad (Asistencia de Dirección Ejecutiva) de cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información. Así mismo, la **Fundación REI Para La Rehabilitación Integral IPS** deberá implementar procedimientos para la correcta gestión de los incidentes detectados.

Se deberá definir un procedimiento de gestión de respuesta ante incidentes, en el que se defina un proceso de categorización de incidentes, análisis de impactos de negocio y escalado por parte de la función de seguridad de la información y ciberseguridad ante cualquier incidente relacionado con la seguridad de la información.

15. Cumplimiento regulatorio

La **Fundación REI Para La Rehabilitación Integral IPS** deberá comprometerse a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable.

16. Auditorías de Seguridad y gestión de vulnerabilidades

Los ingenieros de sistema deben realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo con su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.

Una vez identificadas las vulnerabilidades, la organización deberá aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

17. Gestión de Excepciones

Cualquier excepción a la presente Política de Seguridad de la Información deberá ser registrada e informada a la Dirección Ejecutiva y/o al responsable de la Seguridad de la Información (Asistencia de Dirección Ejecutiva) de la **Fundación REI Para La Rehabilitación Integral IPS**. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la fundación y, con base en la categorización de estos riesgos, estos deberán ser asumidos por el peticionario de la excepción.

18. Sanciones disciplinarias

Cualquier violación de la presente Política de Seguridad de la Información por parte de los colaboradores puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el Reglamento Interno del Trabajo de la **Fundación REI Para La Rehabilitación Integral IPS**. Es responsabilidad de todos los colaboradores de la **Fundación REI Para La Rehabilitación Integral IPS** notificar al responsable de Seguridad de la Información (Asistencia de Dirección Ejecutiva) de cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

19. Revisión de la Política

La aprobación de esta Política implica que su implementación contará con el apoyo de la Dirección para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos.

La presente Política de Seguridad de la Información, será revisada y aprobada anualmente por la Junta Directiva. No obstante, si tuvieran lugar cambios relevantes en la Fundación o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de la **Fundación REI Para La Rehabilitación Integral IPS.**

20. Vigencia.

La presente política y los documentos que de ella se generen serán efectivos a partir de la aprobación en reunión de junta directiva, socialización y publicación de la misma en la página web corporativa www.fundacionrei.org