POLÍTICAS INSTITUCIONALES

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Comfamiliar RISARALDA

Introducción

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de Comfamiliar Risaralda con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Objetivos

Establecer las políticas que regulan la seguridad de la información en Comfamiliar Risaralda y presentar en forma clara y coherente los elementos que conforman la Política de Seguridad que deben conocer, acatar y cumplir todos los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la entidad, bajo el liderazgo del Área de Tecnologías y Sistemas de Información.

Alcance

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de Comfamiliar Risaralda y la ciudadanía en general.

Declaración de Compromiso

Comfamiliar Risaralda se compromete en velar por la implementación y cumplimiento de la Política de Seguridad de la Información, de aplicar dichas políticas y de darla a conocer a sus colaboradores y a los terceros.

Además, adquiere el compromiso de salvaguardar toda información generada, procesada, utilizada en los sistemas de información, implementando medidas preventivas para proteger las tecnologías informáticas evitando ataques y mitigando riesgos.

Marco de Actuación

Políticas de Seguridad de la Información

Comfamiliar Risaralda establece la Política de Seguridad de la Información como un conjunto de controles y procedimientos con la intención de definir las bases para gestionar de manera adecuada y efectiva la seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de la información.

Control de Desarrollo y Adquisición de Software

Comfamiliar Risaralda garantiza que tanto el software adquirido y desarrollado internamente (inhouse), como por terceras partes, cumpla con los requisitos de seguridad y calidad establecidos, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información de la entidad.

El documento **"Control de desarrollo y adquisición de software"** describe los lineamientos definidos por la entidad para la protección de la información de manera adecuada, y para su elaboración se tomó como referente la norma ISO/IEC 27001:2013 y la guía MINTIC de adquisición, desarrollo y mantenimiento de sistemas de información.

Control de Catálogo de Sistemas de Información

Comfamiliar Risaralda está comprometida con el registro y la recopilación descriptiva y estructurada de los sistemas de información mediante este control, el cual permite tener un inventario actualizado de todos los módulos, aplicativos o software que posee la Institución. Este control busca orientar a la dirección de tecnologías y sistemas de información, en la estructuración y documentación del catálogo de sistemas de información, para su elaboración se tomó como referente "Guía para la construcción del catálogo de sistemas de información - MINTIC".

Conforme se establece en el documento **"Control de Catálogo de Sistemas de Información".**

Metodología Para el Desarrollo de Sistemas de Información

Considerando la metodología de referencia para el desarrollo de sistemas de información, y la metodología de referencia del estándar internacional ISO/IEC 25000, la entidad deberá contar con

metodologías de referencia que definan los componentes principales de un proceso de desarrollo de software y que oriente los proyectos de construcción o evolución de los sistemas de información que se desarrollen.

Mediante el "control de metodología para el desarrollo de sistemas de información" se establece que, dados los requerimientos de la Superintendencia, no será obligatoriamente necesaria la inclusión de todos los procesos establecidos en la norma ISO/IEC 25000.

Control de Cambios

Se define un control de cambios en los sistemas de información de la entidad, tomando como referencia y siguiendo los lineamientos planteados en la norma ISO/IEC 27001:2013, el cual permite establecer un procedimiento que de una manera sencilla y organizada, administra y controla los cambios realizados en los sistemas de información de la entidad, asegurando que se mantenga la confidencialidad, la integridad y la disponibilidad de los Sistemas de Información, previniendo interrupciones de servicio por cambios realizados no planificados, minimizando errores que puedan presentarse en los sistemas y mejorando el funcionamiento de estos.

Mediante el documento **"Control de cambios" y el anexo "Anexo Control de cambios"** se especifica la información necesaria y la plantilla para realizar el proceso de cambios de los Sistemas de información de la entidad.

Control de Derechos Patrimoniales

Comfamiliar Risaralda busca mediante este control proveer la información necesaria para adoptar buenas prácticas administrativas que permitan garantizar el derecho de autor y protección de derechos patrimoniales de los sistemas de información de la entidad.

En el documento **"Control de derechos patrimoniales"** se especifican las normativas y las buenas prácticas administrativas que la entidad deberá cumplir y acatar, para garantizar y respetar el derecho de autor.

Control de Auditoría

El sistema de Control Interno de Comfamiliar Risaralda busca proveer seguridad razonable en el logro de sus objetivos estratégicos, operacionales, en el reporte de la información y en el cumplimiento normativo,

mediante la gestión oportuna de sus riesgos y la efectividad de sus controles. Este Control Interno de auditoría ha tomado en consideración los lineamientos definidos por Comfamiliar Risaralda, concebida para agregar valor y mejorar las operaciones de la organización. Ayudando a la Entidad a cumplir sus objetivos, proporcionando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de Gestión de Riesgo, Control y Gobierno.

En el documento **"Control de Auditoría"** se define el marco de actuación de la entidad para lograr el cumplimiento del compromiso establecido por la entidad.

Control de Acceso Físico y a Medios

Se considera esencial, mantener la seguridad de la información de la organización protegida de accesos inadecuados y otras amenazas a las que se pueda enfrentar, para esto, Comfamiliar Risaralda se compromete mediante el documento de **"Control de acceso físico y a medios"** a seguir la normativa ISO 27001 de la seguridad física y del entorno, que pretende evitar accesos no autorizados, daños e interferencias que puedan afectar a la seguridad de la información, para así garantizar su confidencialidad, integridad y disponibilidad.

Control de Acceso

Es necesario establecer normas que garanticen un adecuado control de acceso a los sistemas de información de Comfamiliar Risaralda, para asegurar la confidencialidad, integridad y disponibilidad de la información y su correcto uso.

También se incluirán procesos y acciones para garantizar la seguridad de las redes y sus servicios, logrando que el acceso a la información se dé únicamente por el personal autorizado y evitando que existan vulnerabilidades.

En el documento **"Control de acceso"** se especifican las buenas prácticas que llevará a cabo la entidad para una óptima integridad de la información.

Control de Acceso Remoto

El control de acceso remoto establece las condiciones, restricciones, procedimientos y mecanismos

operativos necesarios para permitir el acceso remoto, garantizando que cuando se accede remotamente a los sistemas de información de Comfamiliar Risaralda, la seguridad de la información no se vea afectada.

En el documento **"Control de Acceso remoto"** se encuentran las condiciones, restricciones, procedimientos y mecanismos operativos para cumplir con un adecuado acceso remoto a los sistemas de información.

Control de Gestión de Activos

Comfamiliar Risaralda considera esencial el conocimiento preciso de los activos de información que posee como parte importante de la administración y control de riesgos, para esto, se tomarán como referencia la guía para la clasificación y gestión de activos de información proporcionada por la MINTIC, Y el control A.8 Gestión de activos, de la ISO 27001, para su correcto uso e implementación en la entidad.

Este control permite implementar una metodología para la identificación y clasificación de los activos de información de la entidad, protegiendo la información frente a la posible materialización de riesgos.

En el documento **"Control de gestión de activos"** se determinan los lineamientos para la realización del registro de activos de información de la entidad.

Control de Gestión de Software

Comfamiliar Risaralda considera este control como instructivo para el inventario de Software autorizado y no autorizado de la entidad. Permitiendo mantener un control sobre la instalación de software, protegiendo los sistemas de información frente a la posible materialización de riesgos.

El documento "Control de gestión de software" establece las medidas que toma la entidad para la gestión de software.

Procedimiento Para Configuración Segura

Para un procedimiento de configuración segura se considera esencial poseer un modelo lógico de infraestructura de la organización; mediante la identificación y control de los distintos elementos que componen el ecosistema de TI de la entidad, para establecer una configuración base segura de los sistemas de información, mediante el documento de **"Procedimiento para configuración segura"** que proporciona directrices para una configuración base a nivel computadores, servidores y redes.

Control de Monitoreo y Gestión de Logs

Un control de monitoreo y gestión de logs determina los eventos más significativos de los sistemas de información de la entidad, los cuales deben ser registrados con el fin de realizar un monitoreo permanente de estos. Permitiendo establecer un proceso de monitorización que permita la detección de posibles intrusos o ataques, errores o situaciones peligrosas las cuales puedan afectar la Integridad, disponibilidad y confidencialidad de la información.

El documento **"Control de monitoreo y gestión de logs"** proporciona la información correspondiente al procedimiento de registros de logs y auditoría, permitiendo a la entidad tener evidencia de estos.

Control Sobre Correo Electrónico y Acceso Web

Comfamiliar Risaralda mediante el documento **"Control de correo electrónico y acceso web"** permiten establecer la metodología que se debe implementar para proteger la información contra software malicioso que puede ser transmitido a través del navegador y del correo electrónico a los sistemas de información de la entidad.

Plan de Recuperación de Datos

Comfamiliar Risaralda está comprometido con la protección y con garantizar el correcto respaldo, almacenamiento y recuperación de la información crítica almacenada en la entidad. Mediante el documento **"Plan de recuperación de datos"** se definen los procedimientos de copia de seguridad, respaldo y recuperación de datos e información que se implementan en la entidad.

Control de Flujo de Información

El control de flujo de información de Comfamiliar Risaralda describe los procedimientos empleados para la protección y defensa del flujo de información de la entidad, mediante el uso de mecanismos de defensa perimetral, con el fin de evitar el acceso no autorizado a la información.

Mediante el documento **"Control de flujo de información"** se describen los mecanismos que implementa la entidad para asegurar la correcta transmisión y flujo de información.

Procedimiento Para la Remediación de Vulnerabilidades

Comfamiliar Risaralda define un procedimiento para la remediación de vulnerabilidades técnicas que se puedan presentar en los sistemas, permitiendo detectar a tiempo dichas vulnerabilidades para evitar posibles ataques que puedan llegar a comprometer la seguridad de la información de la entidad.

Se definen una serie de roles y responsabilidades en el documento **"Procedimiento para la remediación de vulnerabilidades"** y además se define el proceso de gestión de vulnerabilidades de Comfamiliar Risaralda.

Control de Amenazas y Defensa Perimetral

Comfamiliar Risaralda considera el documento **"Control flujo de información"** como un control del flujo de transmisión de información de la entidad, en el cual se describen los procedimientos empleados para la protección y defensa de estos, mediante el uso de mecanismos de defensa perimetral.

Test de Penetración

Comfamiliar Risaralda considera esencial el análisis y registro de las intervenciones adelantadas para mitigar el riesgo aplicando pruebas de Ethical hacking para probar la seguridad de sus sistemas, así como herramientas para el monitoreo de tráfico de red, usuarios remotos y contraseñas de administración para monitorear y registrar posibles vulnerabilidades.

En el documento **"Test de penetración"** se indica la metodología que se debe implementar para realizar test de penetración a los sistemas de información de Comfamiliar Risaralda, con el fin de detectar los problemas de seguridad presentes y de esta manera evitar la pérdida y robo de datos de la entidad.

Capacitación en Ciberseguridad

Teniendo presente la integridad, disponibilidad y confidencialidad de la información, Comfamiliar Risaralda identifica las necesidades y las prioridades que tenga la entidad respecto al tema de entrenamiento y sensibilización de su personal, implementando un modelo centralizado para la administración del programa de entrenamiento y sensibilización resaltadas en el documento **"Capacitación en ciberseguridad".**

Control de Criptografía

Comfamiliar Risaralda hace uso de controles criptográficos para el intercambio de información garantizando la integridad, disponibilidad y confidencialidad de esta misma. Las técnicas criptográficas que se usan dentro de la entidad para la protección de la información están establecidas en el documento **"Control de criptografía".**

Control de Seguridad de las Comunicaciones

El control de seguridad de las comunicaciones le permite a Comfamiliar Risaralda asegurar y proteger la información en redes y comunicaciones mediante una serie de parámetros que están descritos en el documento **"Control de seguridad de las comunicaciones".**

Estos parámetros permiten regular y controlar el acceso a las redes de datos por medio de claves de acceso a los sistemas de información de la entidad.

Control de Relación de Proveedores

Mediante el control de relación de proveedores de Comfamiliar Risaralda se define la relación que tiene la entidad con sus proveedores de servicios, con el fin de asegurar la protección de la información a la cual estos tienen acceso, manteniendo un nivel acordado de seguridad y privacidad.

Las directrices que deben cumplir los proveedores de la entidad en relación al tratamiento de la información se establecen en el documento **"Control de Relación de Proveedores".**

Control de Gestión de Incidentes

El control de gestión de incidentes de Comfamiliar Risaralda establece una serie de lineamientos definidos a través de una oportuna identificación, gestión y respuesta a incidentes con el fin de mitigar el impacto que pueda llegar a afectar la seguridad de la información de la entidad.

El procedimiento para una correcta gestión de incidentes se describe paso a paso en el documento **"Control de Gestión de incidentes".**

Control de Escritorio Limpio y Pantalla Segura

Todos los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con Comfamiliar Risaralda debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicaciones de Comfamiliar deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los usuarios de los sistemas de información y comunicaciones de la entidad deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.

Al imprimir documentos con información pública reservada y/o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

Normatividad Aplicable

· **Ley 1581 del 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
· **Constitución Política de Colombia:** Artículo 15.
· **Ley 1712 de 2014:** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la información Pública Nacional y se dictan otras disposiciones.
· **Decreto 235 de 2010:** Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
· **Decreto 886 de 2014:** Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
· **ISO/IEC 27001:2005:** Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

Responsables de Gestión

UNIDAD DE SISTEMAS: Departamento dentro de la organización que vela por los procesos relacionados con utilización y manejo de computadoras, sistemas de información, redes informáticas, procesamiento de datos e información, y la comunicación en sí, a través de medios electrónicos.

Documentos Relacionados

Procedimientos y controles mencionados en el Marco de Actuación.

Conceptos (Glosario)

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, archivos, edificios, personas) que tenga valor para la organización.

ALCANCE: ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si incluye una parte de la organización.

AMENAZA: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

AMENAZA INFORMÁTICA: es la aparición de una situación potencial o actual donde una persona tiene la capacidad de generar una agresión cibernética contra la población, el territorio.

ANÁLISIS DE RIESGOS: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

AUDITORÍA: proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permiten emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

CIBERSEGURIDAD: capacidad de la entidad para minimizar el nivel del riesgo al que están expuestos los sistemas de información, ante amenazas o incidentes de naturaleza cibernética.

CIFRAR: transcribir en letras o símbolos, de acuerdo con una clave; un mensaje o texto cuyo contenido se quiera proteger.

CONFIDENCIALIDAD: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONFIABILIDAD: capacidad de un producto de realizar su función de la manera prevista, de otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes, por un periodo de tiempo especificado y bajo condiciones indicadas.

CONTROL: comprenden políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

DISPONIBILIDAD: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

EVENTO: suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

GESTIÓN DE CLAVES: controles que se realizan mediante la gestión de claves criptográficas.

GESTIÓN DE RIESGOS: proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

IMPACTO: resultado de un incidente y coste para la entidad, que puede o no ser medido en términos estrictamente financieros, pérdida de reputación, implicaciones legales, etc.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la seguridad de la información.

INFORMACIÓN: conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

INFORMACIÓN PÚBLICA: es toda información que un sujeto obligado genere, obtenga, adquiera, o control en su calidad de tal.

INTEGRIDAD: propiedad de salvaguardar la exactitud y complejidad de la información.

INVENTARIO DE ACTIVOS: lista de todos aquellos recursos (físicos, de información software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO 27001: estándar para sistemas de gestión de la seguridad de la información adoptado por IS transcribiendo la segunda parte de BS 7799. Primera publicación en 2005, segunda publicación en 2013.

PLAN DE CONTINUIDAD DEL NEGOCIO: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

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.

POLÍTICA DE SEGURIDAD: definición en la cual se establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

PROCESO: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

PROPIETARIO DE ACTIVOS DE INFORMACIÓN: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

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 consideraciones.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

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, basando en un enfoque de gestión y de mejora a un individuo o entidad.

TRATAMIENTO DE RIESGOS: a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

VULNERABILIDAD: debilidad de un activo o control que pueda ser explotado por una o más amenazas.