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 a velar por la implementación y cumplimiento de la política de seguridad de la información, a través de la mejora continua, asegurando que las responsabilidades sean claramente definidas y compartidas en todos los niveles de la organización. Además de salvaguardar la infraestructura tecnológica y los activos de información generados, procesados y utilizados en los sistemas de información, frente a cualquier riesgo, incluyendo aquellos derivados del acceso por parte de terceros y del uso interno.

Así mismo se compromete a prepararse contra amenazas internas, fortaleciendo la seguridad de las instalaciones de procesamiento de datos y la infraestructura tecnológica subyacente, implementar controles de acceso robustos y garantizar que la seguridad sea una prioridad en todo el ciclo de vida del sistema de información. Adicionalmente la organización se compromete con la continuidad del negocio, manteniendo la disponibilidad de procesos comerciales para garantizar una operatividad continua ante cualquier eventualidad.

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.

- **Generalidades Seguridad de la Información**

  Comfamiliar Risaralda establece lineamientos claros para la gestión integral de la seguridad de la información, con el fin de preservar su confidencialidad, integridad y disponibilidad, garantizando el cumplimiento de las obligaciones legales, normativas y contractuales, y fortaleciendo la confianza de las partes interesadas.

  El documento **"Instructivo Generalidades Seguridad de la Información"** recopila directrices fundamentales contenidas en los instructivos: Modelo de Seguridad y Privacidad de la Información, Control de Documentos e Identificación de Requisitos. Su contenido permite a la organización estructurar las bases del Sistema de Gestión de Seguridad de la Información (SGSI), asignar responsabilidades claras, controlar la documentación institucional y establecer el marco para identificar a las partes interesadas y los requisitos aplicables. Para su elaboración se tomaron como referencia los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y la norma ISO/IEC 27001:2022.

- **Seguridad Física, Lógica y de Acceso a la Información**

  Comfamiliar Risaralda garantiza la protección integral de sus recursos tecnológicos, físicos y lógicos, mediante la implementación de medidas de control de acceso, monitoreo y resguardo de infraestructuras críticas, permitiendo asegurar la confidencialidad, integridad y disponibilidad de la información institucional.

  El documento **"Instructivo de Seguridad Física, Lógica y de Acceso a la Información"** recopila directrices fundamentales contenidas en los instructivos: Acceso Remoto, Control de Acceso, Acceso Físico y Medios y Monitoreo de Seguridad Física.

- **Uso Aceptable de Recursos Tecnológicos y Servicios de Comunicación**

  Comfamiliar Risaralda promueve el uso responsable y seguro de los recursos tecnológicos y de comunicación, asegurando que los colaboradores hagan un uso adecuado de los medios institucionales y que se apliquen controles de seguridad que prevengan incidentes que afecten la confidencialidad, integridad o disponibilidad de la información.

  El documento **"Instructivo Uso Aceptable de Recursos Tecnológicos y Servicios de Comunicación"** recopila directrices fundamentales contenidas en los instructivos: Seguridad de las Comunicaciones, Protección contra Malware y Dispositivos Finales de Usuario.

- **Gestión de Activos de Información**

  Comfamiliar Risaralda garantiza que todos los activos de información, incluyendo los sistemas, dispositivos, medios de almacenamiento, documentos y demás elementos que contienen datos relevantes para la organización, sean gestionados de forma segura, eficiente y conforme con su ciclo de vida.

  El documento **"Instructivo de Gestión de Activos de Información"** recopila directrices fundamentales contenidas en los instructivos: Catálogo de Sistemas de Información, Gestión de Activos, Disposición Final de Discos Duros, Clasificación de la Información, Disposición o Reutilización Segura de los Equipos y Eliminación de Información.

- **Desarrollo Seguro, Gestión de Software y Derechos Patrimoniales**

  Comfamiliar Risaralda establece directrices claras para garantizar que todo el ciclo de vida del software —desde su diseño, desarrollo e instalación, hasta su mantenimiento y retiro— se realice bajo criterios de seguridad, calidad y cumplimiento legal. Esto incluye tanto las soluciones desarrolladas internamente como aquellas adquiridas a terceros.

  El documento **"Desarrollo Seguro, Gestión de Software y Derechos Patrimoniales"** recopila directrices fundamentales contenidas en los instructivos: Desarrollo de Sistemas de Información y Adquisición de Software, Derechos Patrimoniales, Gestión de Software, Codificación Segura, Instalación de Software, Ciclo de Vida de Desarrollo Seguro, Pruebas de Seguridad en el Desarrollo y la Aceptación y Desarrollo Seguro.

- **Control de Cambios y Configuración Segura**

  Comfamiliar Risaralda promueve la gestión segura de su infraestructura tecnológica, asegurando que todo cambio realizado en sus sistemas de información, plataformas tecnológicas y activos críticos se lleve a cabo de forma controlada, planificada y documentada. Así mismo, establece lineamientos para mantener configuraciones seguras que minimicen la exposición a vulnerabilidades y garanticen la estabilidad operativa de los servicios institucionales.

  El documento **"Instructivo para Control de Cambios y Configuración Segura"** recopila directrices fundamentales contenidas en los instructivos: Control de Cambios y Configuración Segura.

- **Monitoreo, Auditoría y Gestión de Registros (Logs)**

  Comfamiliar Risaralda garantiza la trazabilidad, vigilancia y control de sus activos de información mediante la implementación de mecanismos sistemáticos de monitoreo, auditoría interna y gestión de registros (logs). Estas actividades permiten detectar eventos relevantes, prevenir incidentes, asegurar el cumplimiento normativo y mantener la integridad, confidencialidad y disponibilidad de la información institucional.

  El documento **"Instructivo de Monitoreo, Auditoría y Gestión de Registros (Logs)"** recopila directrices fundamentales contenidas en los instructivos: Auditoría, Monitoreo y Gestión de Logs y Actividades de Monitoreo.

- **Criptografía, Tratamiento y Protección de Datos Personales**

  Comfamiliar Risaralda garantiza la protección de los datos personales y de la información sensible bajo su custodia, mediante la adopción de prácticas seguras para su tratamiento, almacenamiento y transmisión. Esto incluye la aplicación de técnicas criptográficas, la implementación de controles para el manejo adecuado de la información personal y el uso de mecanismos como el enmascaramiento de datos, orientados a reducir la exposición no autorizada.

  El documento **"Instructivo de Criptografía, Tratamiento y Protección de Datos Personales"** recopila directrices fundamentales contenidas en los instructivos: Criptografía, Tratamiento de Datos Personales y Enmascaramiento de Datos.

- **Copias de Seguridad y Recuperación de Información**

  Comfamiliar Risaralda garantiza la disponibilidad y recuperación oportuna de su información institucional mediante la implementación de mecanismos de respaldo, restauración y protección criptográfica, alineados con las mejores prácticas de seguridad de la información.

  El documento **"Instructivo de Copias de Seguridad y Recuperación de Información"** recopila directrices fundamentales contenidas en los procedimientos: Recuperación de Datos de Restauración y Copias de Seguridad y Restauración de Copias de Seguridad.

- **Gestión de Vulnerabilidades y Aplicación de Parches**

  Comfamiliar Risaralda mantiene el compromiso de identificar y mitigar oportunamente las debilidades técnicas que puedan comprometer la seguridad de sus sistemas de información, mediante procesos estructurados de análisis, corrección y prevención.

  El presente documento, **"Instructivo para Gestión de Vulnerabilidades y Aplicación de Parches",** recopila directrices fundamentales contenidas en los instructivos: Remediación de vulnerabilidades y Test de Penetración.

- **Gestión de Incidentes de Seguridad de la Información**

  Comfamiliar Risaralda reconoce la importancia de gestionar de forma oportuna y eficiente los incidentes que puedan afectar la seguridad de la información institucional. Por ello, ha establecido lineamientos específicos para la detección, notificación, análisis, respuesta y cierre de estos eventos, incluyendo el seguimiento de causas raíz y la implementación de acciones correctivas que eviten su recurrencia.

  El documento **"Instructivo de Gestión de Incidentes de Seguridad de la Información"** recopila directrices fundamentales contenidas en los instructivos: Gestión de Incidentes, Inteligencia de Amenazas y Medidas Correctivas.

- **Continuidad del Negocio y Recuperación ante Desastres**

  Comfamiliar Risaralda reconoce la importancia de garantizar la operación ininterrumpida de sus procesos críticos y la protección de sus servicios esenciales frente a situaciones de interrupción no planificadas. A través de estrategias preventivas, planes de recuperación y medidas de preparación tecnológica, la entidad fortalece su capacidad de respuesta ante desastres y asegura la prestación continua de sus funciones misionales.

  El documento **"Instructivo de Continuidad del Negocio y Recuperación ante Desastres"** recopila directrices fundamentales contenidas en los instructivos: Continuidad de Negocio, Gestión de la Continuidad del Servicio y Preparación de las TIC para la Continuidad del Negocio.

- **Evaluación y Gestión de Proveedores**

  Comfamiliar Risaralda fortalece la seguridad de la información a lo largo de su cadena de suministro, mediante la evaluación y gestión responsable de sus proveedores y aliados estratégicos. Este proceso permite garantizar que las partes externas cumplan con los requisitos de seguridad necesarios para proteger la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

  El documento **"Instructivo para Evaluación y Gestión de Proveedores"** recopila directrices fundamentales contenidas en el instructivo: Relación de Proveedores.

- **Concientización y Capacitación en Seguridad de la Información**

  Comfamiliar Risaralda promueve una cultura organizacional orientada a la protección de la información mediante el fortalecimiento de la conciencia y las competencias del talento humano en temas de ciberseguridad y buenas prácticas de seguridad de la información.

  El documento **"Instructivo de Concientización y Capacitación en Seguridad de la Información"** recopila directrices fundamentales contenidas en el instructivo: Capacitación en Ciberseguridad.

- **Concientización y Capacitación en Seguridad de la Información**
  Comfamiliar Risaralda promueve una cultura organizacional orientada a la protección de la información mediante el fortalecimiento de la conciencia y las competencias del talento humano en temas de ciberseguridad y buenas prácticas de seguridad de la información.
  El documento **"Instructivo de Concientización y Capacitación en Seguridad de la Información"** recopila directrices fundamentales contenidas en el instructivo: Capacitación en Ciberseguridad.

- **Uso Seguro de Servicios en la Nube y Comunicación en Red**
  Comfamiliar Risaralda promueve el uso responsable, eficiente y seguro de las tecnologías de la información que permiten la conectividad y el acceso a recursos en la nube. Consciente de los riesgos asociados a la transmisión de datos y al uso de servicios externos, la entidad ha establecido controles técnicos y administrativos orientados a preservar la confidencialidad, integridad y disponibilidad de la información que circula a través de sus redes y plataformas digitales.
  El documento **"Instructivo para el Uso Seguro de Servicios en la Nube y Comunicación en Red"** recopila directrices fundamentales contenidas en los instructivos: Flujo de Información, Comunicaciones, Filtrado Web y Seguridad de la Información para uso en Nube.

- **Transferencia Segura de Información y Términos Web**
  Comfamiliar Risaralda promueve la gestión segura de la información institucional que se intercambia a través de medios electrónicos, garantizando la protección de los datos durante su transmisión, recepción y publicación en plataformas digitales.
  El instructivo **"Transferencia Segura de Información y Términos Web"** recopila directrices fundamentales contenidas en los instructivos: Seguridad de Correo Electrónico y Acceso Web, Términos y Condiciones Páginas Web y Aplicativos, Transferencia de Información y Prevención de Fuga de Datos.

- **Vigencia y Actualización**
  Esta política ha sido aprobada por la alta dirección y entra en vigor a partir de su fecha de publicación. Será obligatoria para todos los funcionarios, contratistas y terceros asociados a la organización. La política permanecerá efectiva hasta que sea modificada o reemplazada, y cualquier cambio significativo será debidamente documentado y justificado. La revisión y actualización de esta política y sus lineamientos asociados se realizarán anualmente o cuando se identifiquen nuevos riesgos o cambios en el marco legal aplicable.

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 27001:2022: 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.

Roles y Responsabilidades: La alta dirección es responsable de la aprobación y revisión de esta política, garantizando su actualización y cumplimiento. Las responsabilidades específicas relacionadas con la seguridad de la información están asignadas y comunicadas a todos los actores relevantes dentro de la organización.

Todos los líderes de proceso de Comfamiliar Risaralda asumen el compromiso activo con la seguridad de la información, garantizando su aplicación dentro de sus áreas de responsabilidad. Esto incluye promover la cultura de seguridad, velar por el cumplimiento de los controles aplicables, identificar riesgos asociados a la información gestionada en sus procesos, y asegurar que sus equipos conozcan y apliquen las disposiciones establecidas en este instructivo.

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: comprende 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 controle 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 ISO 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 activo 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.