PRESENTACIÓN

Director
Juan Eduardo Zuluaga Perna

Secretaria General
Ines Adriana Valencia Galeano

Auditora
Olga Piedad Peláez Castano

Gerente Productividad y Desarrollo
Héctor Andrés Abadía Garcia

Gerente de Tecnología
Carlos Andrés Duque Quintero

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Publicación Corporativa

Manizales, Septiembre de 2020
Elaborado por: Gerencia de Tecnología

CONTENIDO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Fecha de la versión:	Septiembre 7 de 2020
Creado por:	Profesional Seguridad de la Información
Aprobado por:	Gerencia de Tecnología
Nivel de confidencialidad:	Medio sólo corporativo

HISTORIAL DE CAMBIOS

Fecha	Versión	Creado por	Descripción de la modificación
	1.0	Analista de Seguridad	Descripción básica del documento
15/03/2016	1.0	Analista de Seguridad	Cambios dados por un abogado laboral.
05/05/2020	2.0	Profesional de Gestión organizacional	Revisión y concepto seguridad de la información
11/05/2020	2.0	Profesional Seguridad de la información	Cambio general al documento
11/05/2020	2.0	Profesional Auditora TIC	Revisión y Cambios políticas seguridad de la información
22/05/2020	2.0	Comité de Licencia y Seguridad de la Información	Revisión, concepto y cambios en la Política de Seguridad de la Información
06/06/2020	2.0	Auditora	Revisión y concepto seguridad de la información
14/08/2020	2.0	Profesionales Auditoría	Revisión y concepto seguridad de la información
07/09/2020	2.1	Profesional de Seguridad	Adecuación de políticas en la Organización de la seguridad de la información, Seguridad de recursos humanos, Seguridad de las operaciones y Adquisición, desarrollo y mantenimiento de sistemas

08/09/2020	2.1	Jefe de Soluciones de Tecnológicas	Revisión y Cambios políticas seguridad de la información
27/01/2021	2.1	Gerente Tecnología	Revisión y Cambios políticas seguridad de la información
27/01/2021	2.1	Jefe de Soluciones de Tecnológicas	Revisión y Cambios políticas seguridad de la información
27/01/2021	2.1	Profesional de Seguridad	Revisión y Cambios políticas seguridad de la información
28/01/2021	2.1	Abogada - Secretaría General	Revisión políticas seguridad de la información
29/01/2021	2.1	Coordinador de Gestión Organizacional	Revisión políticas seguridad de la información
23/02/2021	2.1	Jefe de Relaciones Laborales	Revisión políticas seguridad de la información
02/03/2021	2.1	Gerente Productividad y Desarrollo	Revisión políticas seguridad de la información
15/03/2021	2.2	Jefe de Soluciones de Tecnológicas	Revisión y modificación políticas seguridad de la información
15/03/2021	2.2	Profesional de Seguridad	Revisión y modificación políticas seguridad de la información

INTRODUCCIÓN

La Caja de Compensación Familiar de Caldas - Confa tiene en cuenta la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la organización, razón por la cual es necesario que se establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la cual se accede, maneja, procesa, transporta o almacena.

Este documento describe las políticas de la organización y normas de seguridad de la información. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013.

Las políticas incluidas en este documento se constituyen como parte fundamental del sistema de gestión de seguridad de la información de Confa y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos. La seguridad de la información es una prioridad para Confa y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradicen la esencia y el espíritu de cada una de estas políticas.

1.1 POLÍTICA SEGURIDAD DE LA INFORMACIÓN

La Caja de Compensación Familiar de Caldas - Confa, como institución que propende por aliviar las cargas económicas que representa el sostenimiento de la familia y que está comprometida en el mejoramiento de la calidad de vida de la población afiliada, establece que la información es vital para el desarrollo de las actividades de la organización, así como una herramienta de gran importancia para la toma de decisiones. En consecuencia, orienta sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los colaboradores, contratistas, proveedores y personas que hagan uso de la información de la organización.

1.2 OBJETIVO

El propósito de esta política es definir las directrices, principios y buenas prácticas para disminuir los riesgos a los que está expuesta la información, de manera que permita a la organización mantener el monitoreo, control, medición de las amenazas y vulnerabilidades, aplicar procedimientos que salvaguarden la confidencialidad, integridad, disponibilidad y privacidad de la misma.

1.3 ALCANCE

La política de seguridad de la información es aplicable a los Activos de Información Tecnológicos entre los cuales están los sistemas de información, bases de datos, dispositivos de telecomunicaciones, equipos de cómputo, dispositivos móviles, documentación digital, y aplica a los siguientes grupos de interés: la Asamblea General, Consejo Directivo, Director Administrativo, Revisor Fiscal, Comités de Administración, Gerencias y Coordinaciones; que componen la estructura organizacional de Confa. Así mismo aplica para los colaboradores cualquiera sea su situación contractual, proveedores o contratistas, acreedores, afiliados, pacientes, clientes, entidades públicas, organismos de vigilancia y control. Con el fin de conseguir un adecuado nivel de protección de las características del Sistema de Gestión de Calidad y seguridad de la información, aportando acciones preventivas y correctivas, siendo un punto clave para el logro del objetivo y su finalidad. Así mismo todos los colaboradores y proveedores deben dar cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección, La Gerencia de Tecnología, Comité de licenciamiento y seguridad de la información, Secretaría General, Auditoría y Gestión Humana.

1.4 Documentos de referencia

- Norma ISO/IEC 27001
- Ley 1581 de 2012 Protección de Datos Personales
- Lista de obligaciones legales, normativas y contractuales

1.5 Terminología básica sobre seguridad de la información

- **Activos de Información Tecnológicos:** Son el resultado de la construcción de un inventario y clasificación de los activos usados por Tecnología, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los colaboradores de Tecnología sobre los mismos.
- **Almacenamiento externo:** Cualquier dispositivo de hardware que no está fijo o de modo permanente dentro del equipo y que sirve para copiar, transportar y/o resguardar información. Las ventajas residen en su facilidad de transporte derivadas de su rápido acceso, larga vida útil, poco tamaño y peso.
- **Aplicaciones:** Interfaz o pantalla que se le muestra al usuario para interactuar con un sistema de información y/o base de datos.
- **Base de datos:** Banco de información que relaciona datos relativos a diversas temáticas y categorizados de distinta manera, pero que comparten entre sí algún tipo de vínculo o relación que busca ordenarlos y clasificarlos en conjunto.
- **Conexión VPN:** Conexión tecnológica privada entre el origen y el destino.
- **Confidencialidad**: Característica de la información que está disponible solo para personas o sistemas autorizados.
- **Criptografía:** Proceso tecnológico por medio del cual se oculta la información para evitar ser descubierta, interceptada, para ser modificada con fines delictivos.
- **Disponibilidad**: La capacidad de garantizar que tanto el sistema como los datos van a estar disponibles para el usuario o titular de la información en todo momento.
- **Documentación digital:** Documento en formato electrónico que puede ser tratado en computadores, servidores, dispositivos móviles, entre otros.
- **Información clasificada:** Es un tipo de información sensible que está restringida por las leyes o regulada para clases particulares de personas.
- **Integridad**: Hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros
- **Políticas de seguridad y privacidad de la información:** Es la declaración o lineamientos generales de Confa que representa la posición de la organización con respecto a la protección de la información.
- **Seguridad de la información**: Es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Servidor:** Equipo ubicado en la red, que funciona como almacenamiento de los sistemas de información y de las bases de datos, al cual se conectan los usuarios para realizar procesamiento de información.

- **Sistema de gestión de seguridad de la información(SGSI)**: Se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.
- **Token:** Es un dispositivo físico utilizado para acceder a un recurso restringido electrónicamente. El token se utiliza como complemento o en lugar de una contraseña. Actúa como una llave electrónica para acceder a algo
- **Usuarios ROOT:** Usuarios con permisos de edición, borrado, actualización.
- **Virus:** Son programas creados para infectar sistemas y otros programas creándose modificaciones y daños que hacen que estos funcionen incorrectamente.

1.6 Adaptación y estructura de la norma

Confa adapta la norma ISO 27001:2013 de acuerdo con la estructura de su organigrama, tomando, de cada una de las mejores prácticas en seguridad de la información con el objetivo de mantener la integridad, disponibilidad y confiabilidad de la información.

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

[ISO/IEC 27001:2013 A.6]

2.1 Organización Interna

Las políticas deben ser revisadas mínimo una vez cada año o cuando se produzca un cambio relevante en la operación que implique realizar ajustes o producto de los cambios en el entorno tecnológico y/o de las necesidades de la operación.

Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información, en especial las relacionadas con el comité de licenciamiento y seguridad de la información (o quien haga sus veces) y del Profesional de Seguridad de la Información.

2.2 Roles y Responsabilidades

2.2.1 Apoyo de la Alta Dirección

2.2.1.1 El Director de Confa, debe apoyar activamente la seguridad de la información dentro de la entidad, definir un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

- La Gerencia de Tecnología de Confa debe mantener dentro de sus colaboradores un funcionario o contratista con el perfil de Profesional de Seguridad de la Información, quien será el encargado de todo lo relacionado con la seguridad de la información y cuyas funciones estarán caracterizadas y definidas en la presente política.
- Se debe velar por el cumplimiento de las políticas de seguridad de la información, comprometerse para que los colaboradores de Confa, conozcan y apliquen las políticas de seguridad de la información.
- Se deben asignar responsabilidades "a las áreas y personas" asociadas a temas de la seguridad de la información.
- El Profesional de Seguridad de la Información, debe apoyar, facilitar y mantener cuando se requiera relaciones con empresas, entidades u organismos que presten asesoría especializada en seguridad de la información.
- En la administración de la seguridad de la información participan todos los colaboradores de la Caja de Compensación Familiar de Caldas - Confa.

2.2.2 Profesional de Seguridad de la Información.

2.2.2.1 El Profesional de Seguridad de la Información debe desarrollar todas las actividades de coordinación de la seguridad de la información. La Caja de Compensación Familiar de Caldas - Confa debe contar con un colaborador, funcionario o proveedor que cumpla con la función de Profesional de Seguridad de la Información que asuma las tareas y responsabilidades que conlleva este rol:

2.2.2.2 Formular, definir y actualizar políticas, normas, procedimientos y estándares definidos en el SGSI, junto con el comité de seguridad de la información.

2.2.2.3 Mantener actualizado el análisis y evaluación del riesgo sobre los Activos de Información Tecnológicos de Confa. Dentro de este propósito se debe mantener definida y actualizada una metodología e instrumentos de levantamiento de Activos de Información Tecnológicos y una política y metodología de gestión de riesgos.

2.2.2.4 Evaluar, apoyar, dar visto bueno y emitir conceptos técnicos, sobre nuevas soluciones o plataformas tecnológicas a adquirir o implementar en la organización.

2.2.2.5 Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y planes de recuperación de desastres.

2.2.2.6 Evaluar, seleccionar e implementar herramientas que faciliten la labor de seguridad de la información.

2.2.2.7 Dar los lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios.

2.2.2.8 Promover en la a Caja de Compensación Familiar de Caldas - Confa la formación, educación y el entrenamiento en seguridad de la información.

2.2.2.9 Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes.

2.2.2.10 Recibir y dar capacitación en el tema de seguridad de la información.

2.2.2.11 Realizar estudios o consultas de pruebas de seguridad en todos los ambientes informáticos de la entidad, previa autorización de Auditoría, Secretaría General, Tecnología o Gestión Humana.

2.2.2.12 Proyectar, proponer, presentar y someter a consideración del Comité, las políticas, normas, acciones o buenas prácticas necesarias para incorporar y/o aplicar en la Gestión de la Seguridad de la Información de la entidad.

2.2.2.13 Crear y revisar los acuerdos de confidencialidad con colaboradores, contratistas, proveedores y terceros.

2.2.2.14 El Profesional de Seguridad de la Información podrá convocar diferentes colaboradores para formar grupos interdisciplinarios que apoyen la definición e implementación de los diferentes temas de seguridad de la información. De igual forma será el encargado de coordinar el conocimiento y las experiencias disponibles en la entidad a fin de brindar ayuda en la toma de decisiones en materia de seguridad de la Información. Esta persona podrá obtener asesoramiento de otros organismos o entidades, con el objeto de optimizar su gestión, se habilita el contacto con todas las áreas o servicios internos.

2.2.2.15 Verificar la aceptación y aprobación de los riesgos identificados; y de sus respectivos planes de tratamiento. Evaluación de riesgos residuales.

2.2.3 Todas las gerencias, áreas y servicios de Confa

Todas las *gerencias, áreas y servicios de Confa* deben tener en cuenta y cumplir los siguientes lineamientos:

2.2.3.1 Toda adquisición e implementación de una solución o plataforma tecnológica (hardware o software), debe contar con el visto bueno, concepto técnico y acompañamiento de Tecnología y el Profesional de Seguridad de la Información, en donde se evalúen los aspectos de viabilidad técnica al momento previo de la realización de la liberación de pedido, compatibilidad, capacidad, integridad y disponibilidad, tanto desde la óptica de infraestructura de tecnología, como el de seguridad de la información.

2.2.3.2 Todo requerimiento, incidente, problema o cambio tecnológico debe ser reportado a Tecnología mediante el uso de las herramientas de comunicación de la organización.

2.2.3.3 Incluir y tener en cuenta los lineamientos y políticas de seguridad de la información en la gestión de la contratación con terceros, proveedores y contratistas.

2.2.3.4 Cumplir y apoyar el cumplimiento de todas las políticas, normas, manuales y procedimientos de seguridad de la información.

2.2.4 Gerencia de Productividad y Desarrollo

Esta dependencia debe cumplir las funciones de:

2.2.4.1 Asegurar que los colaboradores durante el proceso de selección, comprendan sus responsabilidades, los términos y las condiciones de contratación y que son idóneos en los roles para los que se contratan.

2.2.4.2 Asegurar de que los colaboradores y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan, además de dar

cumplimiento a la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

2.2.4.3. Contar con un proceso formal, el cual debe ser comunicado, para iniciar procesos disciplinarios a los colaboradores que hayan cometido una violacion a la seguridad de la información.

2.2.4.4 Incorporar un procedimiento como parte del proceso de cambio o terminación de la parte contractual de los colaboradores.

2.2.4.5 Gestionar mediante la inducción general a todos los colaboradores que ingresan a laborar en la organización de sus obligaciones respecto del cumplimiento de las políticas de seguridad de la información y de todas las normas, procedimientos y prácticas que de ella se deriven, así mismo notificar, divulgar y socializar la presente Política a todo el personal, los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad de la información de acuerdo con las necesidades y coordinadas previamente con el Profesional de Seguridad de la Información.

2.2.5 Secretaría General

2.2.5.1 Debe incluir y tener en cuenta los lineamientos y políticas de seguridad de la información en la gestión de la contratación con terceros, proveedores y contratistas.

2.2.5.2 Es responsabilidad de esta dependencia velar por el cumplimiento de la política de seguridad de la información en el desarrollo de sus funciones, con sus colaboradores contratistas, proveedores y con terceros. Así mismo, asesorar en materia legal a la Caja de Compensación Familiar de Caldas - Confa en lo que se refiere a la seguridad de la información. Para lo anterior, se definirá un Normograma en donde se identifiquen las leyes, decretos y artículos de la constitución Colombiana aplicable a la entidad en relación a la seguridad de la información.

2.2.5.3 Secretaría General debe exigir para todo contrato que requiera alguna gestión y acceso a la información de Confa con proveedores, terceros, contratistas, etc., la firma del acuerdo de confidencialidad, de igual forma los contratos que no lo requieran incluir una cláusula dentro del contrato de confidencialidad y apoyar la supervisión del cumplimiento de las políticas de seguridad de la información.

2.2.6. Gerencia de Tecnología

2.2.6.1 La Gerencia de Tecnología, debe cumplir la función de cubrir los requerimientos de seguridad de la información, definidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Caja de Compensación Familiar de Caldas - Confa.

Todo lo anterior dentro de los marcos de operación, desarrollo, gobierno, cumplimiento y de buenas prácticas que sean establecidas en la entidad.

2.2.6.2 La Gerencia de Tecnología debe dar el visto bueno, concepto técnico y acondicionamiento a todas las nuevas instalaciones de procesamiento de la información, soluciones o plataformas tecnológicas. (Hardware o software), en donde se evalúen los aspectos de viabilidad técnica, compatibilidad y capacidad.

2.2.6.3 Los nuevos recursos de procesamiento de información deben y serán autorizados por la Gerencia de Tecnología, según aplique, considerando su propósito y uso, a fin de garantizar que se cumplan todas las políticas y requerimientos de seguridad de la información, así como los lineamientos de arquitectura tecnológica.

2.2.6.4 Todas las nuevas adquisiciones e instalaciones de soluciones o plataformas tecnológicas (Hardware o software) de la Caja de Compensación Familiar de Caldas - Confa, deben contar con el visto bueno y concepto técnico de la Gerencia de Tecnología y del Profesional de Seguridad de la Información, en donde se evalúen los aspectos de viabilidad técnica (estudios, diserio, arquitectura), compatibilidad, capacidad, integridad, disponibilidad y confidencialidad.

2.2.6.5 Cuando aplique, el Administrador Funcional del Sistema de Información con el asesoramiento de los Profesionales de Tecnología, deben verificar el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas que ya están en operación o en producción en la entidad.

2.2.7 Auditoría

2.2.7.1. La Auditoría de Confa, o en su defecto quien sea propuesto por la organización debe de practicar auditorías periódicas sobre los sistemas de información y toda la plataforma tecnológica instalada y en operación (software y hardware), como

mínimo una vez al año o en caso de presentarse cambios sustanciales en los recursos tecnológicos de la entidad, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella deriven.

2.2.8 Colaboradores

Los colaboradores de Confa que hacen uso de los sistemas de información para el cumplimiento de sus actividades son responsables de conocer, dar a conocer y cumplir la política de seguridad de la Información vigente. Los colaboradores de la Caja de Compensación Familiar de Caldas - Confa, deben:

2.2.8.1 Conocer, comprender y aplicar la política de seguridad de la información de Confa en los procedimientos que apliquen a su trabajo.

2.2.8.2 Llevar a cabo su trabajo, asegurándose de que sus acciones no producen ninguna infracción de seguridad de la información

2.2.8.3 Comunicar al Profesional de Seguridad de la Información las incidencias y/o anormalidades de seguridad de la información que detecte.

2.2.8.4 Hacer uso de las mejores prácticas definidas en la entidad para todos los temas relacionados con la seguridad de la información.

2.2.8.5 Cumplir con el acuerdo de confidencialidad firmado con la entidad.

2.2.9 Responsables de Activos de Información Tecnológicos

El propietario de un activo de información, entendiéndose como tal, aquel que es el responsable de dicho activo, tendrá las siguientes responsabilidades:

2.2.9.1 Informar al Profesional de Seguridad de la Información cuando detecte cualquier incidente de seguridad de la información, para tratarlo y corregirlo mediante la aplicación de controles.

2.2.9.2 Implementar las medidas de seguridad de la información necesarias en su área o servicio para evitar fraudes, robos o interrupción en los servicios.

2.2.9.3 En los casos que aplique, asegurarse de que el personal, colaboradores, contratistas y proveedores tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

2.2.10 Administradores Funcionales de los sistemas de información de Confa

Los administradores de los diferentes sistemas de información de las diferentes plataformas de Confa, deben en forma activa implementar las políticas, normas, estándares, formatos y procedimientos, para brindar un nivel apropiado de seguridad de la información. Deberán:

2.2.10.1 Conocer y cumplir las políticas de seguridad de la información.

2.2.10.2 Dentro de sus funciones de administración de los sistemas de información, aplicar los lineamientos o políticas de seguridad de la información que le sean comunicadas y apliquen a su línea de administración.

2.2.10.3 Informar al Profesional de Seguridad de la Información cuando detecte cualquier incidente de seguridad de la información y sugerir controles o contramedidas para su tratamiento.

2.2.10.4 Documentar los aspectos de seguridad de la información aplicados dentro de su línea de gestión y su respectivo control de cambios.

2.2.11 Contratistas Proveedores y/o Terceros

Confa debe establecer para los contratistas, terceros y proveedores las mismas restricciones de acceso a la información que a un colaborador interno. Además, el acceso a la información debe limitarse a lo mínimo indispensable para cumplir con la actividad asignada o contratada. Las excepciones deben ser analizadas y aprobadas por el Administrador Funcional, Responsable del Activo de Información, el Profesional de Seguridad de la Información, el Gerente, Líder o Coordinador de la organización. Esto incluye tanto acceso físico como lógico a los Activos de Información Tecnológicos.

2.2.11.1 Los contratistas, proveedores y terceros que tengan acceso a los Activos de Información Tecnológicos, están obligados a cumplir las políticas de seguridad de la información de Confa.

2.2.11.2 Todo acceso por parte de personal externo debe ser autorizado por un responsable interno o supervisor del contrato, quien asume la responsabilidad por las acciones que pueda realizar el mismo.

2.2.11.3 El personal externo debe firmar un acuerdo de confidencialidad antes de obtener acceso a información de la entidad.

2.2.11.4 A los contratistas, proveedores y/o terceros, solo se les dará acceso a los sistemas de información de la organización, únicamente bajo un requerimiento formal y previa aprobación del dueño, Administrador Funcional o responsable del activo de información y solo cuando sea necesario.

2.2.11.5 Todas las conexiones que se originan desde redes o equipos externos hacia la Caja de Compensación Familiar de Caldas - Confa, deben limitarse únicamente a los servidores y aplicaciones necesarios.

2.2.11.6 En los contratos de procesamiento de datos externos se debe especificar los requerimientos de seguridad y acciones a tomar en caso de violacion de los contratos.

2.2.11.7 Los contratistas, proveedores y terceros deben comunicar los incidentes de seguridad de la información que detecten, al respectivo supervisor del contrato, para hacer el trámite o seguir el conducto regular.

2.2.11.8 El área de Compras y el Supervisor Administrativo deben asegurar que los contratistas o proveedores durante el proceso de selección, comprendan sus responsabilidades, los términos y las condiciones de contratación y que son idóneos en los roles para los que se contratan.

2.2.12. Cooperación Interinstitucional

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, el Profesional de Seguridad de la Información debe y podrá mantener contactos con entidades, organismos o empresas especializados en temas relativos a la seguridad de la Información, como por ejemplo:

- Ministerio de Tecnologías de Información y comunicaciones
- Alta Consejería TIC

- CSIRT de la Policía Nacional
- ColCert
- Instituto Colombiano de Normas Técnicas ICONTEC
- Empresas especializadas del sector privado
- Academia
- Registraduría
- Otros Organismos

2.2.12.1 En las actividades de asesoramiento, cuando se presente intercambio de información de seguridad, no se divulgará información confidencial perteneciente a la Caja de Compensación Familiar de Caldas - Confa a personas no autorizadas.

2.2.12.2 El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, solo se permite cuando previamente se haya firmado un Acuerdo de Confidencialidad, el cual debe ser de obligatorio cumplimiento para el personal que participe en los temas que se tratan.

2.2.13 Acuerdos de Confidencialidad

2.2.13.1 Todos los colaboradores, contratistas, proveedores y terceros, que deban realizar labores dentro de la Caja de Compensación Familiar de Caldas - Confa, ya sea por medios lógicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información.

2.2.13.2 Se debe revisar a intervalos de tiempo regulares el texto de los acuerdos de confidencialidad, avalando que reflejan las necesidades de la entidad para la protección y seguridad de la información.

3. SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

[ISO/IEC 27001:2013 A.7]

3.1 Antes de asumir el empleo

La Gerencia Productividad y Desarrollo es la encargada de realizar las siguientes actividades relacionadas a la selección de nuevos colaboradores para la organización y que son fundamentales para la seguridad de la información:

3.1.1 Verificar los antecedentes de todos los candidatos a un empleo, de acuerdo con:

- Las leyes, reglamentos y código de ética vigente en la Confa y el país
- La clasificación de la información a la cual se va a tener acceso.

3.1.2 Confirmar la información de referencias personales, familiares y comerciales, para los casos en los que el candidato vaya a tener acceso a información considerada sensible.

3.1.3 Realizar todas las verificaciones necesarias para confirmar la veracidad de la información suministrada por el candidato a ocupar un cargo antes de su vinculación definitiva.

3.1.4 Certificar que los colaboradores de Confa que en razón de su cargo deban tener acceso a información confidencial de la organización, firmen en calidad de aceptación un Acuerdo de Confidencialidad, en el cual se les informe de la existencia de las políticas de seguridad de la información y el sitio o ubicación donde reposa dicha información.

3.1.5 El área de compras, Secretaría General y/o Administrador Funcional, serán las encargadas de garantizar que los proveedores o terceros, que en razón de sus funciones deban tener acceso a información de Confa firmen en calidad de aceptación un Acuerdo de Confidencialidad y el conocimiento de las políticas de seguridad de la información.

3.2 Durante la ejecución del empleo

3.2.1 Responsabilidades de los colaboradores de Confa

3.2.1.1 Todos los colaboradores de la Caja de Compensación Familiar de Caldas - Confa, cualquiera sea su situación contractual, el área o gerencia en la cual desarrolle sus actividades y el nivel de las tareas que desempeñe debe tener asignado un perfil de uso de los recursos de red, incluyendo el hardware y software asociado. Tecnología debe mantener un directorio completo y actualizado de los usuarios asignados en la red y los Administradores Funcionales los perfiles asignados en sus sistemas de información.

3.2.1.2 La responsabilidad de custodia de cualquier archivo almacenado, usado o producido por los colaboradores, proveedores o terceros que se retiran, o cambia de cargo, recae en el líder, coordinador o gerente o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

3.2.1.3 Todo colaborador, proveedor o tercero de Confa, cualquiera sea su situación contractual, el área o gerencia en la cual desarrolle sus actividades y el nivel de las tareas que desempeñe debe conocer las políticas de seguridad de la información y en los casos dados firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de tecnología y las reglas y perfiles que autorizan el uso de la información institucional.

3.2.1.4 Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada Administrador Funcional de los Sistemas de Información, de acuerdo a los lineamientos dados por Tecnología, en cuanto a los dispositivos hardware y los elementos software.

3.2.1.5 El reglamento de trabajo debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos inadecuados de información y de los recursos de tecnología que violen las políticas de seguridad de la información o los lineamientos dados por la organización.

3.2.1.6 Productividad y Desarrollo y Tecnología se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propendan por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

3.2.1.7 Tecnología en conjunto de Productividad y Desarrollo se encargarán de crear y mantener centralizada la información relacionada con temas de seguridad de la información tales como responsabilidad en la buenas prácticas, amenazas de seguridad, entre otros.

3.2.2 Responsabilidades de Usuarios Externos

3.2.2.1 Todos los usuarios externos y personal de empresas externas o proveedores deben firmar un acuerdo de confidencialidad de la información por parte

del representante legal de la empresa y estar autorizados por el líder, coordinador o gerente y Tecnología.

3.2.2.2 El supervisor del contrato será responsable del control y vigilancia del uso adecuado de la información y los recursos asignados a los proveedores.

3.2.2.3 La creación y mantenimiento de los usuarios en la red de Confa de los proveedores debe ser por Tecnología y el supervisor del contrato.

3.2.2.4 Los usuarios proveedores deben aceptar las políticas de seguridad de la información.

3.2.2.5 La solicitud de creación y retiros de los usuarios de los proveedores en los sistemas de información deben ser asignados por el Administrador Funcional e informado a Tecnología para revocar los permisos en la red.

3.2.3 Usuarios invitados y servicios de acceso público.

3.2.3.1 El acceso de usuarios no registrados solo debe ser permitido a la redes inalámbricas libres de Confa, usadas para brindar conexión a Internet y sus actividades pueden ser monitoreadas desde Tecnología.

3.2.3.2 El acceso y uso a cualquier otro tipo de recurso de información y/o sistemas de información no es permitido a usuarios invitados o no registrados.

3.3 Terminación y cambio de empleo

La Caja de Compensación Familiar de Caldas - Confa asegurará que sus colaboradores serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura, por lo tanto, define lo siguiente:

3.3.1 El área de Relaciones Laborales debe realizar el procedimiento de desvinculación en el cual se solicite el procedimiento de inactivación de los colaboradores en los sistemas de información de Confa, el otorgamiento de licencias son solicitadas por los jefes, coordinadores, líderes inmediatos y incapacidades, vacaciones o cambio de labores de los Colaboradores de Confa llevando a cabo los procedimientos que dicha oficina haya establecido.

3.3.2 Cada gerente, líder o coordinador deben reportar de manera inmediata a Relaciones Laborales, la desvinculación o cambio de labores de los colaboradores, con el fin que se tomen las medidas pertinentes y a su vez se informe a las áreas o servicios interesados.

4. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN TECNOLÓGICOS

[ISO/IEC 27001:2013 A.8]

4.1. Responsabilidad sobre los Activos de Información Tecnológicos de Confa por parte de las Áreas

4.1.1 Confa es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los colaboradores de la organización y proveedores, contratistas o terceros, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

4.1.2 Confa es propietario de los Activos de Información Tecnológicos y los administradores de estos activos son los colaboradores, proveedores, contratistas o demás colaboradores de la organización (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware e infraestructura tecnológica de la Caja.

4.1.3 En Confa es fundamental la protección de los Activos de Información Tecnológicos, por eso cada área debe hacerse responsable de la correcta gestión, administración y otorgamiento de acceso a los mismos.

4.1.4 La vigencia de los derechos de acceso y su revocatoria deben estar estrechamente relacionadas con la terminación del contrato laboral o con el cambio de cargo.

4.1.5 En caso de pérdida o robo de cualquier herramienta tecnológica que contenga información de Confa tales como acceso a los aplicativos o sistemas de información de la organización o estén configurados con cuentas corporativas, debe ser reportada de inmediato al Profesional Seguridad de la información, el cual activará la revisión y gestión del incidente.

4.2. Uso Aceptable de los Activos de Información Tecnológicos

4.2.1 Todos los Activos de Información Tecnológicos que sean susceptibles de intercambio entre áreas, con proveedores o terceros deben ser compartidos, enviados o transmitidos por un medio de comunicación o canal seguro, en este caso el correo institucional debe ser el medio de validación formal.

4.2.2 Un colaborador de Confa puede acceder, divulgar, usar o compartir información de propiedad de Confa en la medida en que esté autorizado por escrito por parte del líder, coordinador o gerente, o sea necesario para cumplir con sus funciones asignadas de trabajo. (ver también el Capítulo 6 del Código de Buen Gobierno y Ética).

4.2.3 En caso de transferencia de archivos con entidades financieras, estos deben ser encriptados con sus respectivas llaves privadas y públicas.

4.2.4 Los colaboradores de Confa deben usar las herramientas habilitadas por la organización para hacer la conversión de formatos de archivos.

4.3. Devolución de los Activos de Información Tecnológicos

4.3.1 Todos los colaboradores, practicantes y contratistas están en la obligación de devolver los activos fijos, dispositivos móviles y de información de la organización en su poder, a la terminación de su contrato, acuerdo de servicios o solicitud hecha por el gerente, líder y/o coordinador; teniendo en cuenta que son propiedad de Confa.

4.4. Manejo de los medios de almacenamiento

4.4.1 En Confa los colaboradores, proveedores y terceros deben gestionar los medios de almacenamiento para evitar la divulgación no autorizada, modificación, eliminación de la información almacenada en los medios físicos o electrónicos y en caso de requerir la destrucción se debe solicitar el acompañamiento del Profesional de Seguridad de la Información y Auditoría

4.4.2 Cuando se imprima o se requiera información física de tipo confidencial estipulada por la ley de habeas data o Ley 1581 de 2012, debe garantizar su:

- Debida autorización por parte del líder, coordinador o gerente.
- Autorización para transferencia o préstamo del documento impreso o físico.
- Correcta protección del documento físico.
- Almacenamiento seguro de documento físico.
- Destrucción de forma segura del documento físico.

4.4.3 Los colaboradores que manejan medios de almacenamiento externo asignados a sus funciones, deben asegurar la protección de estos y de los equipos de cómputo en donde se requiera acceder a dicho medio, cumpliendo los siguientes requisitos:

- Los medios de almacenamiento asignados a los colaboradores deben ser usados únicamente en los equipos de la organización, en caso de ser requerido el uso en equipos que no sean de la organización se debe de informar al Profesional de Seguridad de la Información, para revisar la viabilidad y evitar algún riesgo en la información de la organización.
- Se debe garantizar que la información transferida o copiada desde los medios de almacenamiento será destruida de los mismos al finalizar la actividad, utilizando los procedimientos de borrado seguro de información o formateando el medio.
- En caso de pérdida o robo de un medio de almacenamiento que contenga información de Confa, debe ser reportada de inmediato al Profesional Seguridad de la información, el cual activará el proceso de Gestión de Incidentes.
- En caso de daño que implique restauración de información, debe ser reportada de inmediato al personal de Mesa de Ayuda.
- Los colaboradores de Confa deben garantizar el uso adecuado de las herramientas tecnológicas de Confa, evitando situaciones que pongan en riesgo el funcionamiento e información del activo.
- Los archivos que requieran ser enviados o transmitidos en ambos sentidos con proveedores, deben tener implementados controles criptográficos siempre y cuando la información de los activos esté clasificada como privada, con previo acuerdo de la confidencialidad de la información y siguiendo lo estipulado por la Ley 1581 del 2012.
- Tecnología debe garantizar que las estaciones de trabajo como PC’s, portátiles y dispositivos móviles que van hacer dados de baja, se formateen o se destruyan con el fin de mitigar el riesgo de recuperación de información sin la debida autorización previa, al sustraer partes como los discos duros.

5. CONTROL DE ACCESOS

[ISO/IEC 27001:2013 A.9]

5.1. Requisitos de acceso a zonas sensibles

5.1.1 Confa debe asegurar todos los centros de procesamiento de información.

5.1.2 Los Líderes, Gerentes y/o Coordinadores de las áreas de Confa o las personas encargadas de las áreas seguridad y/o responsables de los centros de cableado, tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- El acceso a las áreas donde se maneja información clasificada es limitada únicamente a personas autorizadas.
- El acceso a las áreas seguras como Tesorería, Créditos, Auditoría, Centros de Cómputo, Centros de Cableado y monitoreo de CCTV debe controlarse.
- Los colaboradores y proveedores no deben hacer uso de dispositivos como puntos de acceso inalámbricos (Access Point), routers y cables de red, que no hayan sido asignados para el cumplimiento de sus actividades.

5.2. Requisitos de las áreas para el Control de Acceso a los sistemas de información

5.2.1 En Confa cada área es responsable de gestionar las políticas y los requerimientos para brindar los accesos y privilegios de los usuarios, a las respectivas herramientas tecnológicas de la caja, con el fin de gestionar la seguridad de la información. Por eso los usuarios que dispongan de acceso a los sistemas (aplicativos) y servicios de la red son los que han sido específicamente autorizados para su uso.

5.2.2 Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de Confa, es por eso que se prohíbe el préstamo de los usuarios y contraseñas.

5.3. Gestión de acceso de usuario de Confa

5.3.1 La creación de los usuarios en la red debe ser solicitada a la Gerencia de Tecnología según el procedimiento.

5.3.2 La creación, asignación de roles y permisos en los sistemas de información debe ser solicitada al área y Administrador Funcional correspondiente.

5.3.3 Es responsabilidad del área de Relaciones Laborales reportar los retiros, renuncias, licencias e incapacidades prolongadas a los administradores funcionales y al área de Tecnología, para hacer la desactivación o revocación de accesos.

5.4. Control de acceso a sistemas y aplicaciones de Confa

5.4.1 En Confa la asignación y utilización de los derechos de acceso preferente se deberá restringir y controlar, cómo se menciona en la siguiente directriz:

- Los usuarios administradores deben ser controlados y usados únicamente por personas autorizadas y llevar una relación sobre los seguimientos realizados.
- Los usuarios administradores no deben ser compartidos con personas ajenas al proceso.

5.4.1.1 Los administradores de bases de datos, administradores de aplicaciones, administradores funcionales y usuarios con controles de acceso avanzados en los sistemas de información de Confa, seguirán los siguientes términos:

5.4.1.1.1 Propiedad de la información

5.4.1.1.1.1 La información que se encuentre almacenada en bases de datos físicas o electrónicas (estaciones de trabajo, medios de almacenamiento externo, herramientas colaborativas, servidores de versionamientos, servidores de aplicaciones, aplicaciones y bases de datos) son de propiedad de la organización y no puede ser copiada, compartida, divulgada sin autorización del coordinador, líder o gerente.

5.4.1.1.2 Creación de usuarios funcionales y bases de datos

La creación y capacitación de un usuario, administrador funcional o tercero debe ser aprobado por el líder, coordinador o gerente y su gestión a cargo del área.

Así mismo y por la privacidad de los datos, el nuevo usuario debe diligenciar y firmar el formato de confidencialidad de la información.

Los administradores funcionales de los Activos de Información Tecnológicos deben revisar periódicamente los derechos de acceso, frente a las actividades actuales del colaborador en el sistema. Cualquier desviación debe ser tratada como un incidente de seguridad. Los responsables deben dejar trazas del ejercicio de esta actividad, las que serán objeto de revisiones por parte del área de Auditoría de Confa.

Los derechos de acceso de los colaboradores y/o contratistas en los Activos de Información Tecnológicos, deben ser retirados por los administradores funcionales en el momento de la terminación de su contrato laboral o cuando la organización lo considere pertinente.

5.4.1.1.3 Uso de usuarios administradores con acceso a servidores.

- Solo el usuario root tendrá el permiso total a los servidores.
- Solo se creará un usuario para el soporte a las aplicaciones y tendrá acceso restringido por los Profesionales de Infraestructura Tecnológica.
- Para los proveedores que requieran acceso a los servidores deben de cumplir con el acuerdo de confidencialidad y dar cumplimiento a la Ley 1581 de protección de datos personales. La creación del usuario debe ser previamente aprobada por el líder del área y Gerente de Tecnología.

5.4.1.1.4 Procesos u operaciones en la plataforma tecnológica y bases de datos

Por la criticidad de los servicios de Confa, se debe tener en cuenta que para la realización de procesos u operaciones que impliquen la modificación y actualización de la información sobre las bases de datos, las aplicaciones (sistemas de información), configuraciones de hardware y software (Sistemas Operativos) de los servidores o elementos que conforman la plataforma tecnológica que soportan la operación de los servicios, deberán efectuarse en horarios en los que no haya interrupción de la operación y con previa solicitud por orden de trabajo o correo electrónico, además de contar con la aprobación de los gerentes, líderes, coordinador del servicio y/o de Tecnología.

En el caso específico de Salud se deben acordar estos tiempos con las partes, debido a que su operación es 7x24.

Para garantizar la continuidad de la operación, los procesos (desarrollos, actualizaciones, configuraciones y parametrizaciones) que se hagan en el Hardware, Software, Sistemas Operativos, bases de datos y Aplicaciones, se debe verificar en un ambiente de pruebas (que nunca se apunte a bases de datos de producción) y una vez se validen exitosamente, se debe notificar a todos los colaboradores involucrados y/o administradores funcionales en las áreas correspondientes, para migrar los cambios al servidor de producción.

Antes de realizar salida en vivo o producción, se debe verificar que todas las aplicaciones queden apuntando al ambiente de producción.

Antes de la realización de alguna migración de desarrollos, configuración o modificación de aplicaciones, sistemas operativos o modificaciones de bases de datos, se debe elaborar y validar la existencia de una copia de seguridad actualizada de la base de datos y del software (Sistema o aplicación).

Para realizar operaciones masivas (Inserción, borrado y/o actualización mediante script o archivo plano), sobre cualquier base de datos por un medio diferente a la interfaz de usuario final, se debe contar con el análisis previo, solicitud formal mediante orden de trabajo por el Administrador Funcional del sistema de información comprometido, la aprobación del líder y notificación a Auditoría mediante el flujo diseñado en la herramienta tecnológica.

Lo aplicativos que soportan la prestación de los servicios al público externo de Confa, son calificados con una criticidad máxima lo que conlleva a que toda operación que se haga en alguno de estos sistemas sea de alto impacto, lo que implica que el Profesional de Tecnología y los colaboradores que tengan acceso a estas bases de datos por una interfaz diferente a la de usuario final, debe asegurar que se cuenta con todas las condiciones suficientes para no afectar la prestación del servicio.

Con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información, se deben realizar bajo la responsabilidad de Tecnología, copias de seguridad diaria, semanal, mensual y anual de las bases de datos y de las

aplicaciones con sus respectivos archivos anexos (cuando aplique), según el Instructivo de copias de seguridad, a cargo de las personas responsables de la infraestructura tecnológica. Los Profesionales de Soluciones Tecnológicas y/o Administrador Funcional deben comunicar a Tecnología sobre la información de las bases de datos y/o aplicaciones a las que se requiera hacer dicha actividad.

Tecnología en caso tal de no tener acceso a una copia de seguridad en sitio y de necesitarla con urgencia, se debe solicitar al proveedor encargado de la custodia externa para que se lleve a las instalaciones de Confa.

Si se tiene que desarrollar cualquier proceso desde una ubicación externa a Confa sobre bases de datos o aplicaciones, se debe contar con la autorización del administrador funcional y se deben tener en cuenta que la información que se intercambia en el proceso de conexión es confidencial.

5.4.1.1.5 Soluciones de tecnología y telecomunicaciones (hardware y Software)

Los colaboradores de Confa y terceros que tienen acceso a las bases de datos y a los sistemas de información, fuera de infraestructura de la red de la organización o que usen equipos portátiles personales, deben acceder remotamente por medio de conexión VPN como mínimo requerimiento de seguridad, previa autorización del líder, coordinador o gerente.

Los terceros que se encuentren en las instalaciones y que necesiten hacer uso de las redes de Confa, no podrán tener instalado o hacer uso de ningún software analizador de tráfico y así mismo deben acatar a las políticas de Confa y las leyes y normativas Colombianas.

El ingreso para los servicios de soporte, mantenimiento y administración de los equipos como servidores, dispositivos de red y cableados debe ser controlado con las respectivas identificaciones tanto corporativas como de terceros, notificando vía correo electrónico al Profesional de Tecnología en el proceso.

Las contraseñas de usuarios root y administradores de bases de datos, servidores, dispositivos de red y aplicaciones, deben estar custodiadas por el Profesional de Seguridad de la Información mediante el formato en papel de seguridad y ubicadas en el rack de redes bajo llave.

Cualquier cambio de ubicación de elementos (rack, dispositivos de red) dentro de los cuartos de servidores o en las instalaciones de Confa, por Profesionales de Tecnología o terceros autorizados, debe ser avalado por parte del Profesional de Infraestructura Tecnológica, Jefe de Soluciones Tecnológicas o Gerente Tecnología y se deberá realizar en una ventana de mantenimiento programada.

5.4.1.1.6 Servicios tercerizados

Cualquier acceso para consultas, modificaciones, actualizaciones, suspensiones o acciones que impliquen la interrupción en el servicio de los sistemas de información tercerizados, debe ser comunicado y autorizado al administrador funcional, líder, coordinador o gerente del área y el gerente de Tecnología.

Cualquier solicitud de reunión, conferencia, videoconferencia, asistencia técnica, donde se involucre información clasificada como confidencial debe ser notificada y autorizada vía correo electrónico por el administrador funcional el líder, coordinador o gerente del área.

Cualquier solicitud de información física que involucre información clasificada como confidencial criticidad alta debe ser solicitada directamente por el dueño de la información y con la documentación que verifique su identidad.

5.5 Responsabilidades de los usuarios.

5.5.1 Es responsabilidad de los usuarios controlar, gestionar y proteger la información almacenada de forma digital en su estación de trabajo, medios de almacenamientos externos (CD/DVD, discos duros, dispositivos móviles, memorias USB, etc.), la suite colaborativa de la organización y los Activos de Información Tecnológicos que administran para el cumplimiento de sus funciones.

5.5.2 El colaborador de Confa tendrá un usuario y contraseña para acceder a los sistemas de información de la corporación, que deberán ser gestionados correctamente, siendo responsable de las acciones que se ejecuten con ellas.

5.5.3 Los colaboradores de Confa que acceden a las bases de datos y a los sistemas de información deben salvaguardar los usuarios y/o claves en medios diferentes a los físicos como agendas, libretas o papel sobre sus puestos de trabajo.

5.5.4 Los colaboradores de Confa que acceden a las bases de datos y a los sistemas de información deben guardar usuarios y/o claves en distintos formatos a los automáticos brindados por la configuración de los navegadores.

5.5.5 Los colaboradores de Confa, no deben realizar suscripciones con las cuentas corporativas a páginas de dudosa procedencia o que no cumpla con el objetivo de las funciones asignadas.

5.5.6 Los usuarios con acceso a datos sensibles (Ley 1581) de Confa, deben tener en cuenta la confidencialidad y tratamiento de ellos, no se debe divulgar información a terceros o a otros colabores que no tengan relación con ella.

6. CIFRADO/CRIPTOGRAFÍA

[ISO/IEC 27001:2013 A.10]

6.1. Controles criptográficos

6.1.1 Los tokens de seguridad deben ser mantenidos dentro del área responsable, en un sitio seguro, seco, evitando su exposición a campos magnéticos, a líquidos y a temperaturas extremas, manteniéndolos preferiblemente siempre fuera del alcance de terceros no autorizados. Se recomienda un sitio con un nivel de seguridad asociado, llave, candado, clave o caja fuerte. Evitando que sean golpeados o sometidos a esfuerzo físico.

6.1.2 Los tokens de seguridad nunca deben de salir del perímetro del área responsable, solo en caso de extrema urgencia se podrá hacer con previa autorización del líder del área. Sus usuarios no deben permitir que terceras personas observen la clave que genera el Token y no deben de aceptar ayuda de terceros para su utilización.

6.1.3 Cualquier incidente de seguridad presentado con el token, deterioro, mal funcionamiento, robo, pérdida o caducidad, deberá ser informado al Banco de inmediato y también debe ser reportado al Profesional de Seguridad de la Información.

6.1.4 Para realizar las transacciones bancarias, los tokens de seguridad deben ser extraídos de su sitio de custodia y deben ser llevados al puesto o sitio de trabajo por

sus usuarios. Se deben realizar las transacciones electrónicas sin perder de vista los Tokens y sin que el responsable pueda ausentarse del puesto de trabajo durante este proceso. En caso de que ocurra algún evento irregular con los Tokens, los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.

6.1.5 En el momento que se termina la transacción con los Tokens de seguridad estos deben ser colocados nuevamente en su lugar de custodia. Directamente por el usuario y sin ayuda de terceros, en ningún caso.

6.1.6 No puede divulgarse la información sobre el proceso de custodia a ninguna persona ajena al proceso, dentro y fuera del área de operación.

6.1.6 Los usuarios no deben abrir los Tokens, retirar su batería o placa de circuitos, toda vez que puede alterar su funcionamiento.

6.1.7 Los tokens de seguridad única y exclusivamente pueden ser usados por las personas responsables de los mismos, en cada caso el usuario.

6.1.8 Los tokens de seguridad única y exclusivamente pueden ser usados en los equipos de cómputo asignados a los usuarios responsables de los tokens.

6.1.9 No se deben realizar transacciones electrónicas en presencia de otra persona del área, ni externa a la misma, cuando se involucren los Tokens de seguridad.

6.1.10 No utilizar las claves en otro portal de los bancos que no tenga los mínimos requerimientos de seguridad, protocolo de conexión https, candado de seguridad en la parte superior de la página.

6.1.11 El usuario solo debe hacer uso de las claves en el portal de los bancos únicamente del computador asignado para tal actividad, así mismo no se debe acceder a los portales haciendo uso de un buscador como Google o a través de un link enviado o recibido vía correo electrónico.

7. LA SEGURIDAD FÍSICA Y AMBIENTAL

[ISO/IEC 27001:2013 A.11]

7.1 Áreas Seguras

7.1.1 El perímetro de las áreas que contienen información de los usuarios sensibles o clasificados como privados, deberán estar protegidas de accesos no autorizados mediante los controles de entrada adecuados y deben tener sistemas de vigilancia y monitoreo, lo que mitigue el riesgo de robo de Activos de Información Tecnológicos; además los colaboradores que se encuentre en estas áreas tendrán todo el derecho de solicitar identificación de Confa a las personas desconocidas.

7.1.2 El acceso a las áreas consideradas como sensibles por Confa o que manejan o procesan información confidencial, sólo pueden ser usados por los colaboradores y/o contratistas autorizados, salvo en caso de emergencias el líder, coordinador, director o gerente pueden autorizar ingreso a personas ajenas a dichos sitios.

7.1.3 En el ingreso a los centros de cómputo o centros de cableado, las puertas deben permanecer cerradas y aseguradas en el momento que se haga uso de los mismos.

7.1.4 Las instalaciones de centro de cómputo y de cableado deben cumplir con las mínimas normas o estándares de calidad y funcionamiento. Y su mantenimiento preventivo y correctivo debe ser llevado a cabo por las personas encargadas y capacitadas para dicha tarea.

7.1.5 Todo personal que ingrese a las áreas consideradas como sensibles por Confa o que manejan o procesan información confidencial, deberán estar debidamente identificadas y con las protecciones exigidas por el Sistema de Seguridad y Salud en el Trabajo.

7.2 Seguridad de los Equipos

7.2.1 Los equipos de cómputo deben tener un correcto mantenimiento, con el fin de garantizar y asegurar la integridad y disponibilidad de los mismos.

7.2.2 La reutilización de equipos de cómputo o de partes de equipos de cómputo debe ser controlada por Tecnología, con el fin de evitar el robo de hardware o de información privada.

7.2.3 La salida de los equipos de cómputo de las instalaciones debe ser previamente autorizada por el personal indicado y se debe tener en cuenta la seguridad de los equipos de cómputo fuera de las instalaciones.

7.2.4 Toda estación de trabajo, servidor, base de datos, aplicación, dispositivo móvil y dispositivo de red, debe contar con un usuario y contraseña segura.

7.3 Puestos de trabajo despejado y bloqueo de pantalla

7.3.1 Todos los colaboradores, proveedores y/o terceros que desarrollen actividades en las instalaciones de Confa, deben conservar su escritorio libre de información propiedad de la organización, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

7.3.2 Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se debe reutilizar papel que contenga información confidencial.

7.3.3 La información confidencial y crítica debe estar asegurada en cajas fuertes, al igual que los Activos de Información Tecnológicos como computadoras portátiles, dispositivos de almacenamiento en los que se guarde información confidencial y con los que se hacen transferencias, transacciones y/o operaciones críticas para la organización.

7.3.4 Los colaboradores de Confa deben ser responsables de la sesión en los sistemas de información y en la estación de trabajo donde haya ingresado con su usuario y contraseña asignadas para sus actividades, es decir, deben bloquear o cerrar la sesión cuando se ausentan de su puesto de trabajo ya sea en teletrabajo, trabajo en casa o en oficina, como mínimo requerimiento de seguridad para proteger la información.

7.3.5 Al finalizar sus actividades diarias, todos los colaboradores, proveedores y terceros que hagan uso de los recursos tecnológicos, deben cerrar las sesiones y apagar las estaciones de trabajo.

8. SEGURIDAD PARTE OPERATIVA

[ISO/IEC 27001:2013 A.12]

8.1 Protección contra el código Malicioso

8.1.1 Los colaboradores, proveedores y/o contratistas que accedan a los sistemas de información y a la red de datos de Confa y que sospechen de alguna infección por virus deben dejar de usar inmediatamente el equipo de cómputo y notificar a Tecnología, para la revisión y eliminación del virus.

8.1.2 Se debe escanear con el Antivirus todo tipo de documento electrónico o medio removible y eliminar cualquier virus que se encuentre en estos Activos de Información Tecnológicos; si no se puede eliminar el virus se debe notificar al Profesional de Seguridad de la Información.

8.1.3 Confa no se hace responsable de los archivos eliminados por la existencia o detección de un virus en la información recibida o existente en medios externos.

8.1.4 Las licencias de antivirus adquiridas por la Confa, sólo deben ser instaladas por los responsables de Tecnología.

8.1.5 Cualquier equipo o dispositivo móvil conectado a la red de Confa puede ser monitoreado y supervisado para la detección de código malicioso únicamente por Tecnología y al encontrar cualquier riesgo, se realizará la debida gestión del incidente de seguridad por parte de Profesional de Seguridad de la Información.

8.1.6 El único servicio de antivirus autorizado en la organización es el licenciado en Confa y gestionado por Tecnología, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso.

8.1.7 Es responsabilidad de Tecnología la ejecución de los procesos de actualización del antivirus de manera periódica y segura.

8.1.8 En algunas excepciones, Tecnología podrá realizar la ejecución de otro programa antivirus, a efectos de reforzar el control de presencia de virus o código malicioso.

8.1.9 Se deben hacer revisiones y análisis periódicos del uso de software malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo de Tecnología.

8.1.10 Se deben hacer campañas de sensibilización a todos los colaboradores, proveedores o terceros, con el fin de generar una cultura de seguridad de la información.

8.1.11 Los colaboradores, proveedores o terceros de Confa no deben abrir archivos o link adjuntos de correo electrónico recibidos de remitentes desconocidos o de dudosa procedencia, archivos contenidos en dispositivos externos, que puedan contener software malicioso.

8.1.12 Los colaboradores, proveedores o terceros no deben deshabilitar el antivirus, el firewall, los congeladores de discos y cualquier otro recurso informático que preserve la seguridad de la Información en la organización, esta labor es exclusiva del personal técnico autorizado.

8.1.13 Se recomienda el uso de las redes asignadas por Confa, redes seguras o conocidas, el uso de redes no seguras puede permitir que un atacante intercepte el tráfico de red de tu dispositivo y obtenga acceso a información personal.

8.1.14 Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio a Confa y cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el colaborador debe informar a la cuenta de correo oficial.seguridad@confa.co o a la ext 1258.

8.2. Copias de Seguridad

8.2.1 Cada uno de los colaboradores debe hacerse responsable de la generación de copias de respaldo y almacenamiento de su información que almacena en su equipo de

cómputo; Confa le brinda una herramienta de almacenamiento en la nube para realizar las copias.

8.2.2 Tecnología debe actualizar periódicamente las configuraciones de los servidores para la correcta ejecución de las copias de respaldo de las bases de datos, aplicaciones y Web Services.

8.3 Control de software en explotación

8.3.1 Se debe asegurar que en los sistemas operativos no se instalará software diferente al que servirá para el desempeño de las funciones de los colaboradores. Cualquier tipo de instalación de aplicaciones requerida por un colaborador debe ser gestionada por el Comité de Licencias.

8.3.2 Tecnología es la única responsable de monitorear las actividades de red, es por ello que ningún colaborador debe instalar programas que escanean las redes en estaciones de trabajo como en dispositivos móviles.

8.3.3 Cualquier equipo o dispositivo móvil conectado a la red de Confa puede ser monitoreado y supervisado únicamente por Tecnología y al encontrar cualquier riesgo, se realizará la debida gestión del incidente de seguridad por parte de Profesional de Seguridad de la Información.

8.3.4 Tecnología debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.

8.3.5 Para el desarrollo de contenidos de carácter laboral, se prohíbe el uso de software no licenciado en equipos personales. De lo contrarío se debe gestionar los recursos necesarios para el desarrollo de la actividad.

8.4 Registro y seguimiento

8.4.1 La Caja de Compensación Familiar de Caldas - Confa, realizará monitoreo permanente del uso que dan los colaboradores a los recursos de la plataforma tecnológica y los sistemas de información de la organización.

8.4.2 Los responsables de los servicios, definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos de la institución.

8.4.3 Los servicios, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.

8.4.4 La Gerencia de Tecnología, en conjunto con los responsables de los servicios debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada y de los sistemas de información, acorde con los eventos a auditar establecidos.

8.4.5 La Gerencia de Tecnología, y los Administradores Funcionales deben certificar la integridad y disponibilidad de los registros de auditoría generados en la plataforma tecnológica y los sistemas de información. Estos registros deben ser almacenados y sólo deben ser accedidos por personal autorizado.

8.5. Gestión de Vulnerabilidades

8.5.1 Confa, por intermedio del Profesional de Seguridad de la Información, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades (cada año), con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

8.5.2 El Profesional de Seguridad de la Información debe revisar según se requiera, la aparición de nuevas vulnerabilidades técnicas y reportarlas a los Administradores Funcionales y a los Profesionales de Tecnología involucrados, con el fin de prevenir la exposición al riesgo de estos.

8.5.3 El Profesional de Seguridad de la Información debe gestionar los planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica cada tres meses.

8.6 Consideraciones sobre auditorías de sistemas de información

8.6.1 Confa, apoyada en la Gerencia de Tecnología, en el Procedimiento de Auditoría Interna, verificará el cumplimiento de los requisitos las normas ISO aplicables, la

normatividad legal vigente y los requisitos propios de la organización cada año o según sea necesario.

8.6.2 Tecnología y/o los Administradores Funcionales deben verificar que las auditorías concluyan sin afectar la disponibilidad y los datos de los sistemas de información implementados en la institución.

8.6.3 Los Administradores Funcionales deben planificar para reducir al mínimo las interrupciones de los procesos, de acuerdo con los requisitos de auditoría y las actividades relacionadas con la verificación de los sistemas de información.

9. SEGURIDAD DE LAS TELECOMUNICACIONES

[ISO/IEC 27001:2013 A.13]

9.1. Gestión de Seguridad en las Redes de Datos de Confa

9.1.1 Tecnología debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red.

9.1.2 Tecnología debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

9.1.3 Tecnología debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos en la red de datos de Confa e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

9.1.4 Tecnología debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos.

9.1.5 Por razones de seguridad y mantenimiento de la infraestructura de red y herramientas tecnológicas, La Gerencia de Tecnología o a quien designe está autorizada dentro de la empresa para monitorear todos los equipos, dispositivos móviles, sistemas a los que los colaboradores, usuarios y proveedores se les haya permitido el acceso para el cumplimiento de sus funciones y filtrar el contenido que se transmitan en la red en cualquier momento.

9.1.6 Todos los colaboradores, proveedores o terceros que son autorizados para acceder a la red de datos y los componentes tecnológicos son responsables de todas las actividades que se ejecuten con los usuarios de acceso.

9.1.7 Los colaboradores no deben retirar los cables de red para ser usados con otros fines.

9.1.8 En las sedes de la organización, se proporciona a los colaboradores, proveedores y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por Tecnología.

9.1.9 El trabajo a través de medios remotos o VPN a la red de datos de Confa sólo se permitirá de acuerdo a la Política de trabajo en casa, establecida por la organización.

9.1.10 Para garantizar el correcto funcionamiento del fluido eléctrico y de la red corporativa, se debe hacer un adecuado uso de las conexiones de red y eléctricas. Así mismo se prohíbe la manipulación del cableado eléctrico y de red sin la debida autorización o acompañamiento de las áreas encargadas o especializadas.

9.2 Segmentación o separación de las redes

9.2.1 Confa debe establecer un esquema de segregación, separación de las redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

9.2.2 Se debe realizar solicitud para los controles de acceso a los servicios de red.

9.2.3 Tecnología debe retirar periódicamente los activos fijos que se den de baja y que tengan acceso a la red de Confa.

9.2.4 Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.

9.2.5 Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

9.2.6 Se deben separar las redes inalámbricas de acceso a visitantes de las redes internas, para garantizar los principios de la seguridad de la información.

9.3 Intercambio de Información con Terceros

9.3.1 El intercambio de información entre colaboradores, y usuarios externos debe hacerse por medio de las cuentas corporativas del correo electrónico como medio de comunicación oficial y haciendo uso de las herramientas de seguridad que este contiene.

9.3.2 Confa velará por la protección de la información, sin embargo el contenido de los archivos enviados a través del canal de internet será responsabilidad de los colaboradores.

9.3.3 Para la transmisión de información sensible, privada o confidencial, el colaborador debe hacer uso de la red inalámbrica o cableada corporativa, las cuales tienen las protecciones necesarias para dicho fin.

9.3.4 Es deber de líderes o coordinadores, informar al Oficial de Protección de Datos Personales cuando se envíen datos a un proveedor o un externo nuevo, con el fin de gestionar su inscripción en el Registro Nacional de Base de Datos.

9.4 Políticas de uso de Internet

Confa, consciente de la importancia de internet como una herramienta para el desempeño de las labores diarias, proporcionará los recursos necesarios para asegurar su disponibilidad a los colaboradores que así lo requieran para el desarrollo de sus actividades dentro de la organización.

9.4.1 Usos aceptables del servicio

9.4.1.1 Tecnología debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos.

9.4.1.2 Tecnología debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna.

9.4.1.3 Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por Tecnología o cualquier instancia de vigilancia y control, incluyendo la carga y tráfico.

9.4.1.4 Tecnología debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos.

9.4.1.5 Tecnología debe generar y proporcionar a Auditoría, Secretaría General, y Productividad y Desarrollo registros de la navegación y los accesos de los usuarios a internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de internet.

9.4.1.6 Los colaboradores, proveedores y/o contratistas a los que se les habilite el servicio de Internet deben utilizarlo exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en Confa y no debe utilizarse para ningún otro fin.

9.4.1.7 Los colaboradores, proveedores y/o contratistas autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de Confa o que afecte la seguridad de la información.

9.4.1.8 Los colaboradores, proveedores y/o contratistas que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o malintencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.

9.4.2 Usos no aceptables del servicio

9.4.2.1 Los colaboradores, proveedores y/o contratistas deben abstenerse de descargar software no autorizado desde internet, así como su instalación en las estaciones de trabajo asignados para el desempeño de sus labores, a menos que sean autorizados por Tecnología.

9.4.2.2 Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.

9.4.2.3 Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.

9.4.2.4 Todos los usuarios invitados que tengan acceso al servicio de internet, deben cumplir estrictamente con las leyes y normativas Colombianas.

9.4.2.5 No se permite el acceso a páginas con contenido restringido como pornografía, proxy's anónimos, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware o páginas catalogadas como de alto riesgo.

9.4.2.6 No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

9.5 *Uso del correo electrónico corporativo*

9.5.1 Usos aceptables del servicio del correo electrónico

9.5.1.1 Los mensajes y la información contenida en las cuentas de correo son de propiedad de Confa y pueden ser revisadas por cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.

9.5.1.2 Los colaboradores, proveedores y terceros que les sea asignada una cuenta de correo, se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones contratadas en Confa y no se debe utilizar para otros fines. Así mismo se prohíbe el uso de cuentas personales para actividades laborales.

9.5.1.3 Se debe utilizar las cuentas de correo corporativa de manera ética, razonable, eficiente, responsable, no abusiva, dando cumplimiento a las leyes y normativas Colombianas, sin generar riesgos para la operación de equipos o sistemas de información e imagen de la organización.

9.5.1.4 Los colaboradores, proveedores y terceros que son autorizados para acceder a las cuentas de correo corporativas son responsables de todas las actividades que se ejecuten con sus usuarios.

9.5.1.5 Cuando un área o gerencia, tenga información de interés institucional para divulgar, lo debe hacer a través de Comunicaciones Internas y/o Corporativas de Confa o el medio formal autorizado para realizar esta actividad.

9.5.1.6 Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por Confa y deberán conservar en todos los casos el mensaje legal corporativo.

9.5.1.7 Todos los colaboradores, proveedores y terceros serán responsables de generar las copias de seguridad de sus buzones de correo y documentos almacenados en dicha plataforma.

9.5.1.8 Todos los colaboradores, proveedores y terceros son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de Confa, con el fin de que se realicen los ajustes de permisos requeridos. Con lo anterior también es obligación del Líder, Coordinador, Supervisor de contrato, Administrador Funcional hacer seguimiento, reportar novedades del personal a cargo con el propósito de contribuir al aseguramiento de la administración de usuarios en el sistema de información

9.5.1.9 El usuario debe reportar cuando reciba correos no deseados o no solicitados, correos de dudosa procedencia o con virus al Profesional de Seguridad de la Información, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos.

9.5.1.10 Todo usuario asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el colaborador, proveedor y tercero desconfíe del remitente de un correo electrónico debe remitir la consulta al Profesional de Seguridad de la Información.

9.5.1.11 Confa se reserva el derecho de filtrar los tipos de archivo, remitentes, asuntos de correo para evitar amenazas de virus y otros programas destructivos.

9.5.2 Uso no aceptable del servicio del correo electrónico

9.5.2.1 Todos los colaboradores, proveedores y terceros no deben enviar correos masivos que no hayan sido previamente autorizados.

9.5.2.2 Envío o intercambio de mensajes que pongan en riesgo la reputación de Confa y que promuevan la discriminación social o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

9.5.2.3 Todos los colaboradores, proveedores y terceros no deben enviar mensajes que contengan amenazas o mensajes violentos.

9.5.2.4 Todos los colaboradores, proveedores y terceros no deben divulgar información de propiedad de Confa sin autorización.

9.5.2.5 Todos los colaboradores, proveedores y terceros no deben abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

9.6 Políticas de transferencia de información

9.6.1 Secretaría General debe establecer en los contratos que se constituyan con terceras partes, los Acuerdos de Confidencialidad dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de la institución que les ha sido entregada.

9.6.2 Tecnología y/o los Administradores Funcionales deben velar porque el intercambio de información con entidades externas se realice en cumplimiento las Políticas de Seguridad de la Información y los Acuerdos de Confidencialidad.

9.6.3 Colaboradores de Confa no deben revelar o intercambiar información confidencial de la institución por ningún medio, sin contar con la debida autorización.

10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

[ISO/IEC 27001:2013 A.14]

10.1 Requerimientos de seguridad de los sistemas de información

La Caja de Compensación Familiar de Caldas - Confa, asegurará que el software adquirido y desarrollado tanto al interior de la institución como por terceras partes, incluirá buenas prácticas de seguridad y calidad. Las áreas y/o servicios propietarias de sistemas de información y Tecnología, incluirán requisitos de seguridad en la definición de requerimientos y posteriormente se asegurará que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

10.1.1 La Gerencia de Tecnología debe aprobar la compra, desarrollo, implementación, mejora, etc. de los aplicativos, sistemas de información o el software requerido por los servicios.

10.1.2 Tecnología debe establecer metodologías para el desarrollo, mejoras o implementación de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro.

10.1.3 Las gerencias, áreas y/o servicios, propietarias de los sistemas de información, en acompañamiento de Tecnología, deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando los requerimientos de seguridad de la información.

10.1.4 Las gerencias, áreas, servicios y/o Administradores Funcionales propietarias de los sistemas de información deben definir qué información confidencial puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

10.1.5 Los Profesionales de Soluciones Tecnológicas deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se requiera desarrollar o implementar, de acuerdo con los requerimientos de seguridad y los controles deseados.

10.1.6 Los Profesionales de Soluciones Tecnológicas deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y conocidas y actuales en el mercado.

10.1.7 Los Profesionales de Soluciones Tecnológicas deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.

10.1.8 Los desarrollos deben cerrar las sesiones activas de las aplicaciones cuando no hagan uso de ellas o se presente inactividad.

10.1.9 Los Profesionales de Soluciones Tecnológicas deben utilizar los protocolos sugeridos por los Profesionales de Infraestructura Tecnológica en los aplicativos desarrollados y adquiridos por Confa.

10.1.10. Los Profesionales de Soluciones Tecnológicas deben realizar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros y utilizando mecanismos o herramientas de cifrado.

10.2 Seguridad en los procesos de desarrollo y de soporte

10.2.1 La Caja de Compensación Familiar de Caldas - Confa velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la institución.

10.2.2 Tecnología en conjunto con el Administrador Funcional o quien designe el servicio deben realizar las pruebas necesarias para asegurar que los sistemas de información desarrollados cumplen con los requerimientos de seguridad establecidos antes del paso a producción.

10.2.3 Tecnología en conjunto con el Administrador Funcional o quien designe el servicio deben realizar las pruebas de los sistemas de información establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción.

10.2.4 Tecnología en conjunto con el Administrador Funcional o quien designe el servicio deben realizar las pruebas por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

10.2.5 Tecnología en conjunto con el Administrador Funcional o quien designe el servicio deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y de cambios o nuevas funcionalidades.
10.2.6 Tecnología debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

10.2.7 Tecnología debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.

10.2.8 Tecnología y Secretaría General deben asegurarse que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

10.2.9 Tecnología debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de Confa.

10.2.10 Los Profesionales de Soluciones Tecnológicas deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

10.2.11 Los Profesionales de Soluciones Tecnológicas deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el aplicativo.

10.2.12 Los Profesionales de Soluciones Tecnológicas deben garantizar que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

10.2.13 Los Profesionales de Soluciones Tecnológicas deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

10.2.14 Los Profesionales de Soluciones Tecnológicas deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

10.3 Datos de prueba

10.3.1 Protección de datos de prueba

10.3.1.1 Tecnología y el Administrador Funcional debe verificar los ambientes productivos deben apuntar a las bases de datos de producción.

11. SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON PROVEEDORES

[ISO/IEC 27001:2013 A.15]

La Caja de Compensación Familiar de Caldas - Confa, establecerá mecanismos de control en sus relaciones con los proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

11.1 Los supervisores de los contratos con proveedores o terceros se asegurará de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

11.2 Los proveedores, terceros o entidades externas que requieran acceso a la información de Confa, debe cumplir con el acuerdo de confidencialidad, este documento debe ser requerimiento de cualquier proceso de contratación y cumplir con lo establecido en la ley de habeas data o ley 1581. Así mismo el administrador funcional debe reportar a quien corresponda, para que hagan sus modificaciones en el RNBD como encargado de la información.

11.3 Los acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación de las negociaciones.

11.4 Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes.

11.5 El proveedor o contratista debe reportar a Confa cualquier vulnerabilidad de seguridad en la información detectada y que ponga en riesgo la información de Confa.

11.5 Confa debe informar a los proveedores o contratistas cualquier cambio o acciones preventivas o correctivas en la seguridad de la información.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

[ISO/IEC 27001:2013 A.16]

12.1 Proceso de Gestión de Incidentes de Seguridad de la Información con mejoras constantes

12.1.1 Todos los usuarios, proveedores y colaboradores de Confa tienen la responsabilidad de reportar cualquier violación a las políticas establecidas en este documento, evento, incidente o debilidad en cuanto a la seguridad de la información que identifique o se presente.

12.1.2 Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.

12.1.3 Se debe socializar periódicamente a los colaboradores, proveedores y terceros el procedimiento de atención de incidentes de seguridad de la información de la organización.

12.1.4 Es responsabilidad de Tecnología realizar sensibilización a todos los colaboradores sobre incidentes de seguridad de la información detectados.

12.1.5 Los incidentes de seguridad, resultantes del incumplimiento de la Política de Seguridad de la Información Corporativa serán direccionados a las áreas correspondientes donde se activará el proceso disciplinario respectivo.

12.1.6 Los empleados deberán estar informados del proceso disciplinario que se llevará a cabo en caso de incumplimiento de la Política de Seguridad de la Información o alguno de los elementos que la soportan. En cualquier caso se hará un seguimiento de acuerdo con los procedimientos establecidos para el manejo de incidentes de seguridad.

13. TRABAJO EN CASA

13.1 Política de trabajo en casa

13.1.1 Solo los colaboradores, proveedores y terceros previamente autorizados por el coordinador, líder o gerente podrán utilizar los beneficios del Sistema VPN y/o permisos por IP's desde el portal seguro de aplicaciones.

13.1.2 Es responsabilidad del usuario con VPN y/o permisos por IP's desde el portal seguro de aplicaciones, asegurarse que ninguna otra persona utilice su cuenta de acceso y de hacer préstamo del usuario y la contraseña asignada para tal fin, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.

13.1.2 En caso de pérdida de una estación de trabajo con VPN instalada y configurada, el colaborador debe reportar inmediatamente al Profesional de Seguridad de la Información, con el fin de tomar las acciones necesarias.

13.1.3 El uso del sistema VPN debe ser controlado utilizando una contraseña segura, manteniéndola siempre en secreto.

13.1.4 Cuando un colaborador esté conectado a la red de Confa haciendo uso de la VPN, el sistema permitirá el acceso a las aplicaciones de acuerdo con lo solicitado por el coordinador, líder o gerente del usuario.

13.1.5 Para cada usuario de VPN solo se permite una conexión simultánea desde la red externa hacia la red de Confa.

13.1.6 Los acceso a las aplicaciones por VPN serán configuradas y administradas por Tecnología. Todos los computadores provistos por Confa conectados a las red interna de la organización mediante VPN, deberán utilizar el software antivirus actualizado, provisto por Tecnología. Para los equipos personales se recomienda por Tecnología que el usuario tenga instalado un software antivirus en sus equipos.

13.1.7 Se recomienda que los equipos personales que se conecten a las red interna de la organización mediante VPN, tengan un Sistema Operativo (Windows 8, Windows 10, etc) original y actualizado.

13.1.8 Las conexiones establecidas desde la redes externas hacia la red interna de Confa vía VPN, deben ser establecidas desde servicios de Internet conocidos y seguros. Se recomienda no realizar conexiones desde Café Internet, Wifi`s libres o de Centros Comerciales.

13.1.9 Mediante el uso de la tecnología VPN, los usuarios deben alinear sus actividades acorde con las políticas de seguridad de la información, normas, leyes y reglamentaciones Colombianas, y los lineamientos establecidos por la organización y el uso de la VPN. Así mismo los accesos y actividades realizadas por conexión VPN, pueden ser auditados cuando sea requerido por la organización.

14. SEGURIDAD Y USO DE DISPOSITIVOS MÓVILES

14.1 Política de seguridad y uso de dispositivos móviles

14.1.1 La configuración y actualización de los dispositivos móviles como smartphones, PDA's y tablets y sus respectivas aplicaciones, pertenecientes a Confa serán realizados por personal especializado del área de Tecnología.

14.1.2 El área de Tecnología configurará los accesos solicitados por las áreas a las aplicaciones de los smartphones, PDA's y tablets de Confa que procesan información crítica.

14.1.3 La organización es el dueño del dispositivo móvil y será asignado a un colaborador, el cual se hará responsable del dispositivo y de su protección física y lógica.

14.1.4 Está prohibido por parte del colaborador prestar o dejar desatendido el dispositivo móvil que contenga o acceda a información de Confa.

14.1.5 Todo colaborador, proveedor y tercero, en caso de pérdida o robo de smartphones, PDA's o tablets personales o AF de la organización y que accedan a los recursos Tecnológicos de Confa se debe reportar de inmediato vía correo electrónico al Profesional de Seguridad de la Información y/o área de Seguridad, con el fin de revocar los accesos o permisos a la red.

14.1.6 Todos los dispositivos móviles asignados a los colaboradores y/o, proveedores Confa deben tener instalado un software de antivirus.

14.1.7 Las áreas de la organización serán responsables de efectuar y salvaguardar las copias de seguridad de los equipos de cómputo móviles.

14.1.8 Se protegerá el acceso a los dispositivos móviles con una contraseña o con el dibujo de un patrón.

14.1.9 Los colaboradores no deben prestar usuarios y contraseñas que les han sido otorgados para el cumplimiento de sus funciones, además deben ser responsables de la información que almacenan en su dispositivo móvil. Los colaboradores se deben hacer responsables de las acciones que se ejecuten con estos usuarios y contraseñas.

14.1.10 Está prohibido la instalación de aplicaciones y el cambio o la manipulación de configuraciones en los dispositivos móviles asignados por Confa, salvo expresa autorización del área de Tecnología.

14.1.11 Todos los dispositivos móviles de Confa, deben tener la última o la más segura versión de las aplicaciones.

14.1.12 Los dispositivos móviles de Confa, serán solo para el uso y almacenamiento de información de tipo laboral.

14.1.13 La información de los dispositivos móviles será de propiedad de Confa, incluso luego de la remoción del acceso personal. La información crítica debe ser respaldada con copias de seguridad periódicamente.

14.1.14 Todos los dispositivos móviles que son propiedad de Confa pueden estar o ser monitoreados y ser sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

14.1.15 Los colaboradores, proveedores o terceros de Confa deben adoptar las precauciones necesarias y apropiadas para salvaguardar la confidencialidad de la información que tenga en cualquier medio (dispositivos móviles, correo, usb, discos duros, estaciones de trabajo, portátiles, etc.).

15. CUMPLIMIENTO LEGAL

[ISO/IEC 27001:2013 A.18]

15.1. Cumplimiento de los requisitos Legales y Contractuales

15.1.1 En Confa todos sus colaboradores tienen la responsabilidad de cumplir y velar por el cumplimiento de las políticas establecidas en este documento, con el objetivo de preservar la integridad, confidencialidad y disponibilidad de la información.

15.1.2 Los colaboradores tienen la responsabilidad de cumplir las normas, regulaciones o leyes Colombianas que a derechos de autor se refiere; entendiendo las restricciones de carácter legal en el uso de contenidos como software, aplicaciones, vídeos, fotografías, documentos, presentaciones, audios.

15.2. Protección de los Registros

15.2.1 Los registros y/o información de la organización deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada de conformidad con los requisitos legales, reglamentarios, contractuales y comerciales.

15.3. Revisiones de la Seguridad de la Información

15.3.1 Confa tiene como objetivo garantizar el proceso de implementación de la Seguridad de la Información alineada a los objetivos estratégicos de la organización.

Se harán una revisiones a los aspectos de Seguridad de la Información de forma periódica o por cambios significativos que se hagan necesarios.

Anexos

Normas Legales.

I. ***Ley 1273 del 5 de enero 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".*** Ésta ley, creó nuevos

tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

II. Ley 1581 de 2012