MANUAL DE POLÍTICAS SEGURIDAD DE LA INFORMACIÓN

TI-MA-01

MANUAL DE POLITICAS SEGURIDAD DE LA INFORMACIÓN

Resolución N 086

23 de abril de 2022, por medio de la cual el Consejo de Administración expideel Manual de Políticas Seguridad de la Información de Febor Entidad Cooperativa, de conformidad con lo establecido en la Ley 79 de 1988 y el Artículo 48 del Estatutode Febor Entidad Cooperativa.

CREACIÓN DEL DOCUMENTO		
Elaboró: Edmer Ortegón - Jefe de Sistemas Diana Forero- Gestor Riesgos y Calidad	**Reviso:** Edmer Ortegón – Jefe de Sistemas Diana Cabrera - Dir. Riesgos y Calidad	**Aprobó:** Juan Pablo Vélez Gerente
Fecha Elaboración: 19 de julio 2019	**Fecha Revisión:** 22 de julio de 2019	**Fecha Aprobación:** 14 de agosto de 2019

CONTROL DE CAMBIOS		
Fecha	**Motivo**	**Responsables**
Aprobado: 10 de agosto de2021	Se incluyen directrices de seguridad de la información paratrabajo en casa.	**Elaboró:** Edmer Ortegón – Dir. De Informática. **Revisó:** Diana Cabrera Erazo- Dir. Riesgos y Oficial de Cumplimiento. **Aprobó**: Juan Pablo Vélez Góez- Gerente
Aprobado: 29 de septiembre de 2021	Se incluyen delitos informáticos yse organiza el documento en políticas y directrices, se incluye objetivos específicos y responsabilidades, se ajusta política general.	**Elaboró:** Edmer Ortegón– Dir. de Informática.Diana Forero - Jefe Control Interno y Calidad **Revisó:** Diana Fonseca Gómez – Dir. Riesgos **Aprobó**: Consejo de Administración. Juan Pablo Vélez Góez - Gerente
Aprobado: 23 de abril de 2022	Se amplía roles y responsabilidades	**Elaboró:** Edmer Ortegón– Dir. de Informática. **Revisó:** Diana Fonseca Gómez – Dir. Riesgos**Aprobó**: Consejo de Administración. Juan Pablo Vélez Góez - Gerente

FIRMAS DE APROBACIÓN		
Edmer Ortegón Guzmán Director de Informática	**Juan Pablo Vélez Góez** Gerente	**María Elvira Molano Tamayo** Presidente Consejo de Administración

TABLA DE CONTENIDO

INTRODUCCIÓN

Para Febor Entidad Cooperativa la información es un activo de alta importancia, ya que esta permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la entidad.

Teniendo en cuenta lo anterior, es necesario implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad de la informaciónen todas sus formas.

Este Manual recopila las políticas y normas de seguridad de la información definidas por Febor Entidad Cooperativa; las cuales constituyen los pilares para el desarrollo delSistema de Gestión de Seguridad de la Información (SGSI).

La implementación de nuevas aplicaciones, servicios de información, herramientas de hardware, software, seguridad de la información, bases de datos, conectividad y en general los empleados, terceros y la información de uso de la Cooperativa deben cumplir con las políticas y normas definidas en este documento, dado que su razón deser es la protección de la información.

1 OBJETIVO

Desarrollar la Política de Seguridad de la Información, documentando formalmente las reglas para la protección de la información de la entidad que es procesada, transportada o almacenada por medios informáticos como software, hardware, redes,entre otras.

1.1 Objetivos específicos

- Establecer directrices generales relacionadas con seguridad de la información y ciberseguridad.
- Garantizar la disponibilidad, confidencialidad, protección e integridad de la información suministrada y acopiada por Febor, con la implementación de prácticas que garanticen la preservación de la infraestructura tecnológica, las normas de calidad aplicables a la gestión segura de las tecnologías de la Información.
- Gestionar los riesgos asociados con la pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información.
- Garantizar la custodia de los datos personales en sistemas de información, bases de datos, soportes y equipos empleados en el tratamiento de los datos de la Cooperativa, teniendo en cuenta la normativa interna vigente.
- Orientar el debido cuidado y la debida diligencia en la gestión de la seguridad de la información y la ciberseguridad
- Definir un lenguaje común sobre la seguridad de la información y la ciberseguridad dentro de la Cooperativa.

2 ALCANCE

Este manual condensa las políticas de seguridad de la información y es aplicable para todos los aspectos administrativos y de control que deben ser cumplidos por todos los niveles de la organización: empleados, asociados, terceros (que incluye proveedores y contratistas), entes de control, entidades relacionadas y filiales de Febor Entidad Cooperativa; que acceden, ya sea interna o externamente, a cualquier activo de información que se almacena, procesa o transporta, utilizando hardware, software, redes y otras facilidades asociadas. Las políticas de seguridad de la información cubren los aspectos de privacidad, acceso, autenticación, mantenimiento y divulgación relacionados con cualquier activo de información.

La implementación de los lineamientos y normas consagrados en este manual, será progresiva de acuerdo a la prioridad que se establezca una vez realizado el análisis de riesgo de los activos de información. Esta prioridad será definida por La Dirección de Informática.

3 CONDICIONES GENERALES

Las políticas deben ser cumplidas por todos los que tengan acceso o hagan uso de la información de Febor Entidad Cooperativa, ya sea a través de software, hardware, redes o a través de algún otro medio.

El cumplimiento de las políticas es obligatorio y cualquier excepción debe ser informada al proceso de tecnologías de información y al área de riesgos, se debe documentar y medir el riesgo en el que incurre Febor Entidad Cooperativa. Las partes interesadas deben entender las implicaciones de las directrices y lasresponsabilidades en su estricto cumplimiento.

El incumplimiento de las políticas puede resultar en acciones disciplinarias/judiciales o pecuniarias en el caso de proveedores o contratistas, que puede llegar incluso hasta la terminación de la relación contractual y/o acciones judiciales. El desconocimiento de las políticas no exime su aplicación.

4 MARCO DE REFERENCIA

4.1 Legislación

- Ley 603 de 2000: Esta Ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
- Ley Estatutaria 1266 del 31 de diciembre de 2008: Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales.
- 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.
- Ley 1480 de 2011 Se expide el estatuto del Consumidor.
- Ley Estatutaria 1581 de 2012: Entro en vigencia la Ley 1581 el 17 de octubre de 2012 de Protección de Datos Personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.
- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013. Norma técnica de sistemas de gestión de seguridad de la información.
- Decreto 1377 De 2013: Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Ley 1952 de 2019: por medio de la cual se expide los PRINCIPIOS Y NORMAS

RECTORAS DE LA LEY DISCIPLINARIA y se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.

4.2 Normatividad Interna

- Estatuto Social Febor Entidad Cooperativa.
- Código de Buen Gobierno, Ética y Conducta.
- Reglamentos internos.
- Protección de datos personales.

5 DEFINICIONES

Acción resolutiva: Acción tomada para evitar la repetición de un incumplimiento mediante la identificación y tratamiento de las causas que la provocaron.

Activos de información: Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

Acuerdo de confidencialidad: Contrato suscrito entre las partes con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Ataque cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: Deficiencia de algún recurso informático o telemáticoque pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Buzón: También conocido como cuenta de correo, es un espacio exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a Febor Entidad Cooperativa.

Centro de cómputo: También conocido como Centro de Procesamiento de Datos, o Data Center es una instalación que se encarga del procesamiento de datos e información de manera sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras (Hardware) y programas (Software) necesariospara cumplir con dicha tarea.

Chat: Comunicación simultánea y sincronizada entre dos o más personas a través de Internet.

Confiabilidad: Grado de precisión o exactitud de la información.

Confidencialidad: Propiedad que determina que la información no se haga disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Medida o acción que modifica un riesgo para prevenir su materialización.

Control de acceso: El proceso que limita y controla el acceso a los recursosde un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas. El control de acceso puede ser definido porel sistema (mandatory access control – MAC), o definido por el usuario propietariodel objeto (discretionary access control – DAC).

Contraseña o password: Es una forma de autenticación privada, compuesta por un conjunto de números, letras y caracteres, que permiten al usuario tener acceso a un computador, a un archivo y/o a un programa.

Cuentas de correo: Son espacios de buzones para la recepción, envió y almacenamiento de mensajes de correo electrónico en internet.

Disponibilidad: Propiedad de ser accesible y utilizable sobre demanda por una entidad autorizada.

Evento de seguridad de la información: Ocurrencia identificada de unasituación de sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.

Firma digital: La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Firewall: Dispositivo tecnológico que tiene como función proteger la red internade una compañía de accesos no autorizados del exterior vía Internet.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Gobierno de seguridad de la información: Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas.

Hardware (lenguaje de marcas de hipertexto): Es un término genérico para todos los componentes físicos (que se pueden tocar) de la computadora, tales como discos, unidades de disco, monitor, teclado, ratón (mouse), impresora placas, chips y demás periféricos. Se incluyen además aquellos componentes físicos que no vemos, tales como dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, entre otros.

Hacker: Persona dedicada a realizar entradas no autorizadas a los sistemas, por medio de redes de comunicación como Internet, con el objeto de encontrar vulnerabilidades en los sistemas.

Host: Termino usado en informática para referirse a los computadores conectados a la red, que proveen y/o utilizan servicios de ella. Los usuarios debenutilizar hosts para tener acceso a la red

Incidente de seguridad: Un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizadade la información y de sus usuarios; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Información.

Integridad: Propiedad de exactitud y completitud de la información.

Internet: Es una red de computadores, inter conectados a nivel mundial en forma de tela de araña.

Malware: Código malicioso o cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.

Nivel de riesgo: Evaluación del riesgo identificando su posible materialización frente al impacto y probabilidad de ocurrencia.

Política: Son instrucciones mandatarias que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

Políticas de seguridad: Conjunto de directrices, lineamientos y reglas que permiten velar porque se resguarden los activos de información, aprobados por

el consejo de administración.

Probabilidad: Posibilidad que el riesgo se pueda materializar frente a un incidente de seguridad de la información.

Red: Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

Riesgo residual: Es el riesgo que queda después de aplicar los controles al riesgo identificado.

Seguridad informática: Características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad,integridad y disponibilidad.

Seguridad de la información: Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.

Servicios de computación en la nube: Modelo para permitir un acceso de red conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o proveedor de servicios.

Sistema de información: Se refiere a un conjunto de recursos organizadospara la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada poruna o más amenazas.

Servidor: Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

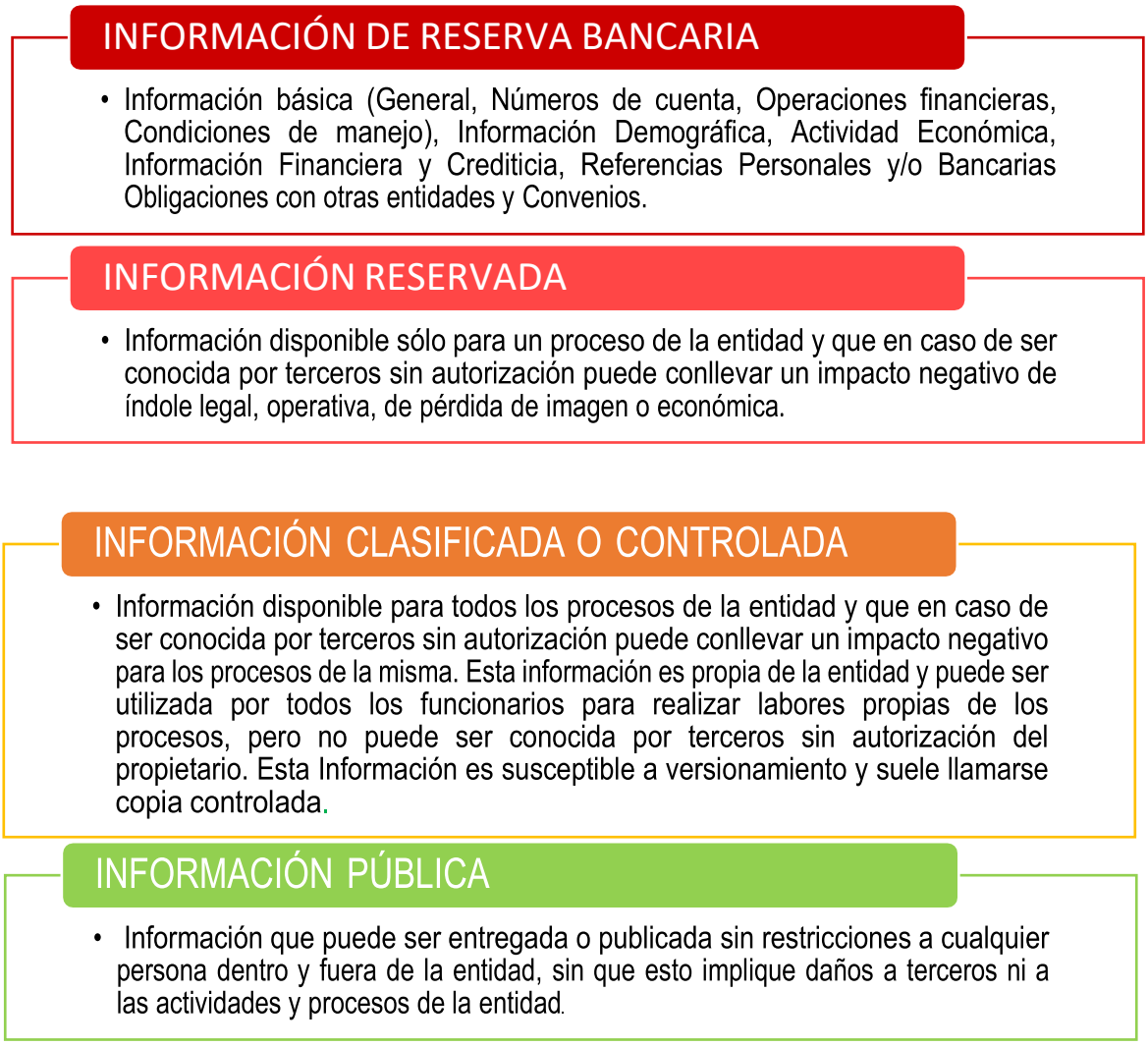
Sistema operativo: Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora, servidor o dispositivo móvil.

Terceros: Se entiende por tercero a toda persona, jurídica o natural ajena a Febor Entidad Cooperativa como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

Troyano: Es un programa con una determinada función o utilidad, pero que contiene código oculto para ejecutar acciones no esperadas por el usuario.

Virus: Software malicioso que tiene por objeto alterar el normal funcionamiento de una computadora, reemplazando así programas ejecutables, sin la autorizaciónni el conocimiento del usuario.

6 CLASIFICACIÓN DE INFORMACIÓN SEGÚN CONFIDENCIALIDAD



7 GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

Febor define y pone en marcha el sistema de seguridad de la información como un componente integral de sus prácticas de buen gobierno. El sistema de seguridad de la información proporciona la dirección estratégica a las actividades de seguridad y garantiza que se alcancen los objetivos y que se realice la debida gestión de los riesgos relacionados con seguridad de la información; igualmente establece que los recursos de información de la Cooperativa se utilicen con responsabilidad.

7.1 Estrategias de seguridad

La Cooperativa diseña los procedimientos correspondientes para la implementación de estrategias de seguridad donde se indica lo que se debe hacer en cuanto a sus etapas y métodos, los recursos financieros estarán incluidos en la programación del presupuesto anual aprobado por el Consejo de Administración y administrado por la gerencia. El recurso humano será previamente evaluado por la Dirección de TI, y se llevará a cabo la solicitud formal a la Gerencia y a la Jefatura de Talento Humano, en caso de aplicar ampliación de planta de personal deberá ser aprobado por el Consejo de Administración.

El seguimiento y reporte de resultados logrados serán incluidos en informes trimestrales presentados al Consejo de Administración.

7.2 Estructura organizacional

Febor Entidad Cooperativa crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, así como la asignación de un Administrador de Seguridad de la Información (funcionario del área de informática de la Cooperativa).

7.2.1 Roles y responsabilidades

Todo aquel que tenga acceso a la información en Febor, es responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en este documento. El proceso de tecnologías de la información, es responsable de la implementación y mantenimiento de la Seguridad de la

Información, de hacer seguimiento al cumplimiento de las políticas, en caso de requerirse prestar asesoría a todo aquel que maneje información de la entidad, coordinar las actividades de gestión de riesgos de la seguridad de la información, apoyar la identificación de controles y reportar al Gerente, el estado de la implementación y seguimiento del manual y demás documentos del sistema de gestión de la información.

7.2.2 Funciones y responsabilidades del Administrador de Seguridad de la Información

El Director de Informática es el encargado de administrar la seguridad de la información de la Cooperativa, sus principales funciones y responsabilidades son las siguientes:

- Proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como las bases de datos e información en general.
- Revisar el estado general de la seguridad de la información.
- Revisar y analizar los incidentes de seguridad de la información existentes.

- Revisar y aprobar los proyectos de seguridad de la información.
- Presentar para aprobación ante el Consejo de Administración las modificaciones o nuevas políticas de seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Identificar necesidades de evaluación de los procesos soportados por losrecursos informáticos y su plataforma tecnológica.
- Responder por el análisis, revisión y centralización de todas las acciones referidas a la gestión de seguridad de la Información de la Cooperativa y de mantener la vigencia de las políticas de acuerdo con las necesidades y requerimientos del negocio.
- Asegurar que exista una dirección y apoyo gerencial sobre los principios y las metas para soportar la administración y desarrollo de iniciativas sobre la gestiónde la seguridad de los activos de la información, a través de compromisos apropiados y de recursos adecuados, como la formulación y mantenimiento delas políticas de seguridad de la información a través de todos los funcionarios de la Cooperativa.
- Validar las políticas de seguridad de la información y procedimientos para el uso adecuado y administración de los recursos informáticos asignados a los funcionarios de la organización, asegurando que la información se encuentre protegida.
- Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes “smartphones”, tabletas), entre otros, suministrados por Febor Entidad Cooperativa y que hagan uso de los serviciosde información de la Entidad.
- Restringir opción a los usuarios para cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

7.2.3 Funciones de Talento humano

Incluir en los programas de inducción y de reinducción el tema de seguridad de la información asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos.

7.2.4 Funciones de la Dirección de Riesgos

Acompañar permanentemente al administrador de seguridad de la información en la identificación de riesgos, diseño de controles para su tratamiento.

Administrar el registro de eventos de riesgo reportado por el administrador de seguridad de la información.

Reportar a la Gerencia estado general de riesgos, la evolución del perfil de riesgo residual el informe de eventos de riesgo.

7.2.5 Funciones Jefatura de Control Interno

Sin perjuicio de las funciones asignadas en otras disposiciones al área de Control Interno y Auditoría ésta debe:

- Tener conocimiento apropiado en materia de seguridad de la información y de esta normativa en particular.
- Evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos clave del sistema de seguridad de la información, con el fin de determinar las deficiencias y sus posibles soluciones.
- Informar los resultados de la evaluación de la seguridad de la información al consejo de administración.

7.2.6 Funciones del Gerente

Sin perjuicio de las funciones asignadas en otras disposiciones al representante legal o gerente de la Cooperativa, frente al sistema de seguridad de la información le corresponde:

- Velar por el desarrollo de los objetivos estratégicos para la seguridad de la información, definidos por el Consejo de Administración.
- Velar por la implementación de la política de seguridad de la información.
- Facilitar la integración entre los diferentes dueños de procesos de negocio para lograr la implementación del modelo de seguridad de la información.
- Velar por la disponibilidad de los recursos y su uso apropiado.
- Velar por la correcta aplicación de los controles de seguridad para reducir el riesgo de seguridad de la información.
- Velar por la designación de los responsables de la implementación de la política de seguridad de la información.
- Presentar un informe periódico, como mínimo trimestral, al Consejo de Administración sobre la evolución y aspectos relevantes de la seguridad de la información incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar, seguimiento y resultados de mediciones y cumplimiento de objetivos de seguridad de la información.

7.2.7 Funciones del Consejo de Administración

El Consejo de Administración tiene determinadas las siguientes funciones:

- Definir y promover la dirección estratégica para la seguridad de la información.
- Proporcionar los recursos para la adecuada implementación de la seguridad de la información.
- Proporcionar, velar y apoyar la implementación y asignación del Sistema de Seguridad de Información.
- Autorizar, facilitar e integrar la puesta en operación del sistema de seguridad de la información, mediante la definición de mecanismos y la supervisión e integración por parte de cada líder de proceso.
- Velar por el cumplimiento de las obligaciones regulatorias en materia de seguridad de la información.
- Velar por la disponibilidad de los recursos y su uso apropiado.
- Designar los responsables de la implementación del sistema de seguridad de la información.
- Pronunciarse y hacer seguimiento a los informes trimestrales que presente el representante legal, dejando constancia en las actas de las reuniones respectivas.
- Aprobar las evaluaciones de riesgo de seguridad de la información resultantes.
- Revisar que la estrategia de seguridad de la información se encuentre alineada con los objetivos de negocio.
- Revisar y aprobar las actualizaciones al Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar su continua conveniencia, idoneidad y efectividad.
- Establecer las prioridades de los proyectos e iniciativas relacionadas con la seguridad de la información.

7.2.8 Funciones de contratistas y terceros

- Velar por el cumplimiento de las políticas de seguridad de la información dentro de su entorno laboral inmediato.
- Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de seguridad de la información.
- Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.
- Utilizar únicamente software y demás recursos tecnológicos autorizados.

7.3 Riesgos de seguridad de la información

La gestión de riesgos es un proceso encaminado a minimizar las vulnerabilidades y posibles pérdidas de información que pueden llegar a materializarse y afectar económica y reputacionalmente a la Cooperativa.

Para tal efecto, mediante matrices de riesgo se mide el perfil de riesgo de la entidad, teniendo entendimiento de las consecuencias de materialización, de tal manera que se planteen estrategias al interior del área de TI y evaluando constantemente el perfil de riesgo residual.

8 POLÍTICA INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN

Febor Entidad Cooperativa está comprometida en proteger los activos de información, enfocando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información, teniendo claro que la política será efectiva dependiendo del comportamiento de las personas y los controles establecidos en las políticas de seguridad descritas en el presente documento.

Las políticas de seguridad de la información, serán claras y en lenguaje sencillo para entendimiento de todos los integrantes de la Cooperativa, el proceso de revisión debe contemplar la aplicación de actividades de retroalimentación como soporte de conocimiento que permitan la socialización y la verificación del cumplimiento.

8.1 Directrices

- El director de Informática es responsable de que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.
- Se debe establecer un programa que permita el fomento continuo de la creación de cultura y conciencia de seguridad de la información en los funcionarios, contratistas, proveedores, personas, usuarios de los sistemas de información y telecomunicaciones.
- Todos los usuarios de los sistemas de información y telecomunicaciones, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente manual.
- El Manual de Políticas de Seguridad de la Información será revisado y actualizado (en caso de ser necesario) al menos una vez al año o cuando haya cambios relevantes en el contexto estratégico de Febor Entidad Cooperativa, con el fin de asegurar que siga siendo adecuado a la estrategia y necesidades de la entidad. Estos documentos deben ser revisados por el encargado de seguridad de la información, para presentar modificaciones o ajustes a la Gerencia.
- La aprobación de políticas está a cargo del Consejo de Administración y establecerá las instrucciones para su puesta en marcha y cumplimiento.
- Cumplidos los procesos de descripción, revisión y aprobación, la Cooperativa

dará a conocer las políticas de seguridad de la información, las cuales deberán ser publicadas a través de la intranet para conocimiento de todos los funcionarios y en otros sitios que la administración considere pertinentes.

- Sobre los recursos, el presupuesto debe contemplar la criticidad de los activos de información involucrados, y los recursos que aseguren la función de seguridad de la información, las herramientas tecnológicas que apoyen a la protección de los activos de información y el proceso de mejora continua. Así mismo, los responsables de la seguridad de la información deben contar con la competencia necesaria para gestionar los riesgos asociados, evaluar la eficacia de las acciones tomadas y garantizar la información documentada.
- La comunicación de requisitos exigidos en materia de seguridad informática debe ser comunicado a todas las áreas, incluyendo asociados y terceros, por los medios que la Cooperativa considere efectivos.
- El modelo de seguridad de la información de la Cooperativa debe incluir la información documentada considerando los siguiente:

  - ✓ Esté adecuada al propósito de la Cooperativa.
  - ✓ Incluya objetivos de seguridad de la información o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información.
  - ✓ Incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información.
  - ✓ Incluya el compromiso de mejora continua del sistema de seguridad de la información.
  - ✓ Esté disponible como información documentada.
  - ✓ Se comunique dentro de la organización vigilada.
  - ✓ Esté disponible para las partes interesadas, según sea apropiado.
  - ✓ Deben existir procedimientos, instructivos y guas técnicas.

- Es política de la Cooperativa trabajar continuamente en proteger los activos de información contra todo tipo de amenazas tanto internas como externas, deliberadas o accidentales y procurar que se cumplan con los siguientes requisitos:

  - ✓ Proteger la información de los asociados.
  - ✓ Mantener la integridad de la información creada, procesada o resguardadapor los procesos de negocio.
  - ✓ Posibilitar la confidencialidad de la información.
  - ✓ Tener disponible la información y los servicios que soportan los procesos de negocio de acuerdo a sus necesidades.
  - ✓ Cumplir las disposiciones legales, regulatorias y contractuales relacionadas con la seguridad de la información.

9 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

9.1 Política de Gestión de activo

9.1.1 Directriz de manejo de la información

Febor debe clasificar la información que posee en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia que tiene esta para el óptimo funcionamiento de la Cooperativa de igual forma se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la entidad.

Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere Febor Entidad Cooperativa, por ejemplo:

Formularios / comprobantes propios o de terceros.

- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.

Los usuarios responsables de la información de Febor Entidad Cooperativa deben identificar los riesgos a los que está expuesta la información de sus procesos, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

9.1.2 Directriz de Administración de datos personales (habeas data)

La Cooperativa a favor del cumplimiento de la normatividad vigente de habeas data establece los lineamientos para el tratamiento de datos personales por medio de la expedición de la resolución No. 21 del 31 de agosto de 2013 mediante la cual se adopta y reglamenta el cumplimiento y afirmación de la ley estatutaria 1581 de 2012.

9.1.3 Directriz de uso de los activos

La Cooperativa implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de las estaciones de trabajo, o discos virtuales de red, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sea de carácter institucional.

Febor Entidad Cooperativa mantiene un inventario actualizado de sus activos de

información, quedando bajo la responsabilidad de cada propietario de información y centralizado por el proceso de tecnologías de la información.

9.1.4 Directriz de uso de Internet

La entidad permite el acceso al servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

El proceso de tecnologías de la información implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.

Los usuarios de los activos de información de Febor Entidad Cooperativa tienen restringido el acceso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud al Director de Informática y será objeto de auditorías de seguridad mediante el módulo de seguridad web de la Entidad.

Se establecen restricciones de acceso a páginas con contenido relacionado con pornografía, juegos de azar y demás que puedan representar un riesgo de seguridad de la información.

Se prohíbe la descarga, uso, intercambio y/o instalación de programas, juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución.

9.2 Política Seguridad de los recursos humanos, proveedores o terceros y asociados

9.2.1 Directriz para antes de la contratación

Febor establece que se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y proveedores o usuarios de terceras partes con el fin de establecer cómo se desempeñara con respecto a la información y así cumplir con la política de seguridad de la información de la organización. De igual forma antes del ingreso a la entidad algunas de la parte mencionada anteriormente, se debe generar la verificación de antecedentes y de esta forma garantizar el cumplimiento de los reglamentos, la ética y las leyes pertinentes.

Como parte de su obligación contractual, los empleados, contratistas, proveedores o usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato, el cual debe establecer sus responsabilidades y las de

la organización con relación a la seguridad de la información.

9.2.2 Directriz durante la vigencia de la contratación

Febor Entidad Cooperativa exige que los empleados, contratistas, proveedores o usuarios de terceras partes apliquen la seguridad de la información según las políticas y los procedimientos establecidos por la organización. Todos los empleados de la organización y, cuando sea pertinente, los contratistas, proveedores o los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de seguridad de la información de Febor.

De igual forma se debe dar cumplimiento a la política de gestión de Incidentes de Seguridad de la Información y aplicar el procedimiento disciplinario formal establecido en el Reglamento Interno de Trabajo cuando sea el caso. Actuaciones que conllevan a la violación de la seguridad de la información establecidas por Febor Entidad Cooperativa son, entre otras:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, “documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)”.
- No guardar la información digital, producto del procesamiento de la información perteneciente a Febor Entidad Cooperativa.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Permitir que personas ajenas a Febor Entidad Cooperativa deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la Entidad.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u

ofensivo, cadenas de correos y correos masivos no autorizados.

- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Utilizar equipos electrónicos o tecnológicos desatendidos o a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el proceso de tecnologías de la información de Febor Entidad Cooperativa.
- Permitir el acceso de funcionarios a la red corporativa, sin la autorización del proceso de tecnologías de la información de Febor Entidad Cooperativa.
- Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos por Febor Entidad Cooperativa o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de Febor Entidad Cooperativa.
- No cumplir con las actividades designadas para la protección de los activos de información de Febor Entidad Cooperativa.
- Destruir o desechar de forma incorrecta la documentación institucional.
- Descuidar documentación con información pública reservada o clasificada de la Entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc., sin el debido cuidado.
- Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no pertenezca a Febor Entidad Cooperativa o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de Febor Entidad Cooperativa sin la debida autorización.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de Febor Entidad Cooperativa para beneficio personal.
- El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad de Febor Entidad Cooperativa.

- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de Febor Entidad Cooperativa sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de Febor Entidad Cooperativa.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de Febor Entidad Cooperativa.
- El que viole datos personales de las bases de datos de Febor Entidad Cooperativa.
- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por Febor Entidad Cooperativa.
- Mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de Febor Entidad Cooperativa o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de Febor Entidad Cooperativa o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por Febor Entidad Cooperativa.
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Sustraer de las instalaciones de Febor Entidad Cooperativa documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o Entidades no autorizadas.
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de Febor Entidad Cooperativa para traslado, reasignación o para disposición final.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de Febor Entidad Cooperativa o de alguno de sus funcionarios.
- Realizar cambios no autorizados en la plataforma tecnológica de Febor Entidad Cooperativa.
- Acceder, almacenar o distribuir pornografía infantil.

- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el proceso de tecnologías de la información de Febor Entidad Cooperativa.
- Copiar sin autorización los programas de Febor Entidad Cooperativa o violar los derechos de autor o acuerdos de licenciamiento.

9.2.3 Directriz para la terminación o cambio de la contratación laboral

Febor exigirá a todos los empleados, contratistas, proveedores o usuarios de terceras partes devolver todos los activos (información, equipos, documentos, etc.) pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo, de igual forma se retiraran las contraseñas y claves de acceso a los sistemas de información y documentación de la organización.

9.2.4 Directriz para usuarios que acceden a información de la Entidad local o remotamente

Los contratos celebrados por Febor Entidad Cooperativa para la atención parcial o total de los distintos canales o de los dispositivos usados en ellos, o que en desarrollo de su actividad tengan acceso a información reservada de Febor Entidad Cooperativa, o de sus clientes, deberán incluir aspectos de Seguridad de la Información.

Los contratos deben incluir, entre otras, las cláusulas señaladas a continuación, siempre y cuando tengan relación con el objeto del contrato:

- Niveles de Servicio y Operación. De acuerdo con el objeto del contrato, se deben definir los niveles de servicio y de operación para cumplir con el servicio prestado por parte del tercero.
- Acuerdos de Confidencialidad
- Propiedad de la Información.
- Restricciones sobre el software empleado.
- Normas de seguridad informática y física.
- Procedimientos y controles para la entrega, distribución y destrucción de información
- Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información.

Todo servicio prestado por los diferentes canales de la entidad debe contar con un análisis de seguridad de la información. La prestación de servicios por nuevos canales, o la modificación de los servicios por canales existentes debe incluir un análisis de seguridad de la información.

9.2.5 Directriz de sensibilización sobre Seguridad de la Información

Febor Entidad Cooperativa desarrolla un programa de sensibilización, divulgación y concientización relacionado con aspectos de Seguridad de la Información, que permita informar a todas las partes interesadas acerca de las medidas de seguridad que deberán tener en cuenta para la realización de operaciones.

La Cooperativa debe mantener un programa anual de concientización ycapacitación para todos los funcionarios y contratistas que interactúen con lainformación institucional y desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.

Todos los funcionarios y contratistas al servicio de la Cooperativa deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

9.2.6 Directriz de Tercerización u Outsourcing

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la Entidad.

Se deben establecer mecanismos de control en las relaciones contractuales, con el objeto de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de Febor Entidad Cooperativa las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por Febor Entidad Cooperativa.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a Febor Entidad Cooperativa. El resultado del análisis de riesgos será la base para el establecimiento de loscontroles y debe ser presentado a la Dirección de Informática y la Dirección de Riesgos antes iniciar el estudio de mercado y publicación del proyecto de pliegos del contrato de outsourcing en el portal de contratación.

Los funcionarios de Febor Entidad Cooperativa que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

9.3 Política Seguridad física y del entorno

9.3.1 Directriz de protección física

Febor Entidad Cooperativa establece que los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro. De igual forma, deben estar protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado; además los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.

El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegidos contra interceptaciones o daños…

9.3.2 Directriz de manejo disposición de información, medios y equipos

La Entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por Febor Entidad Cooperativa velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacenan, se procesan o se comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de su misión.

Se debe realizar la aplicación del procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario haya sido retirado de la Entidad, de acuerdo a lo definido por Febor Entidad Cooperativa.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través del proceso de tecnologías de la información, y será objeto de auditorías de seguridad mediante el módulo de prevención de pérdidas de datos de la Entidad.

9.3.3 Directriz de control de acceso a áreas seguras

Las áreas seguras (Data center, Gestión Documental, Caja y Tesorería, principalmente) deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado, de igual forma se deben diseñar y aplicar las medidas de seguridad física para oficinas, recintos e instalaciones de la cooperativa. Se deben controlar los puntos de acceso de la cooperativa para prevenir el ingreso de personas no autorizadas a las instalaciones y que se pueda dar perdida de información.

Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial que puedan afectar la seguridad de la información.

En las instalaciones del centro de datos o de los centros de cableado, no está permitido:

- Fumar.
- Introducir alimentos o bebidas.
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Los centros de cómputo deben mantener las condiciones físicas y ambientales óptimas recomendadas.

9.4 Política de gestión de comunicaciones y operaciones

9.4.1 Directriz de pantalla despejada y escritorio limpio

Se sugiere configurar todos los equipos para el bloqueo automático después de cinco (5) minutos de inactividad. De igual forma, cada usuario es responsable de bloquear la sesión de su estación de trabajo en el momento en que se retiren de la misma, de forma tal, que solo se pueda desbloquear con la contraseña de usuario. Cuando finalice la jornada laboral, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Adicionalmente todos deben conservar su escritorio físico libre de información susceptible, que pueda ser alcanzada, copiada o utilizada por terceros o personal sin autorización, cada vez que se vayan a retirar de sus puestos de trabajo.

9.4.2 Directriz de respaldo de datos o copias de seguridad

Toda la información de Febor debe almacenarse de forma segura, de acuerdo con los requerimientos de tiempo determinados y de conformidad a las normas de gestión documental de la entidad, adicionalmente se realizarán copias de respaldo de la información y pruebas de éstas, de acuerdo con el cronograma del proceso de tecnologías de información y las necesidades de la Cooperativa.

Se debe realizar seguimiento a la ejecución de las copias de respaldo y se deben registrar las fallas de las copias de seguridad programadas, con el fin de certificar su validez y correcto funcionamiento.

Las copias de respaldo se guardan únicamente con el objetivo de restaurar información cuando por situaciones como borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o equipos de cómputo, o por requisitos legales, sea necesario recuperarla.

9.4.3 Directriz de dispositivos móviles

Febor Entidad Cooperativa establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes “smart phones”, tabletas, computadores, entre otros) suministrados por la entidad o personales que usen los servicios de información de la Cooperativa, y sean utilizados dentro o fuera de la misma.

Dispositivos institucionales:

- Los dispositivos suministrados por Febor deben ser exclusivamente utilizados para brindar apoyo a las actividades de la entidad y ser sujetos a un grado equivalente de protección al de los equipos que se encuentran dentro de las instalaciones.
- Las computadoras portátiles de Febor durante los viajes se deben llevar como equipaje de mano y no se deben dejar desatendidos en ningún lugar.
- Los portátiles son vulnerables al robo, pérdida o acceso no autorizado mientras estén fuera de la Entidad, por ende, se debe dar la apropiada protección al acceso (ej. contraseñas de encendido, encriptación, etc.) con el fin de prevenir acceso no autorizado.
- Los equipos de cómputo, así como la información almacenada en los mismos, son propiedad de Febor Entidad Cooperativa, y pueden ser inspeccionados,

auditados, o utilizados de cualquier manera y en cualquier momento en que la Entidad lo considere.

- Un equipo portátil, teléfono inteligente o cualquier otro sistema de cómputo de la Entidad que contenga información sensible, no se deberá prestar a nadie y será responsabilidad exclusiva del funcionario que lo tenga asignado.
- Los dispositivos móviles institucionales deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual, tener activado la función de borrado remoto, cifrar la memoria de almacenamiento.
- Los dispositivos móviles celulares institucionales deben tener únicamente la tarjeta sim asignada por la Entidad, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados. De igual forma, estos deben permanecer encendidos y cargados durante las horas laborales o de acuerdo a la responsabilidad y requerimientos propios del cargo.
- Ante la pérdida de un equipo, ya sea por extravío o hurto, deberá informar de manera inmediata al Director de Informática a fin de continuar con las actividades de carácter administrativo por pérdida de elementos establecido por la Entidad.
- Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones. En caso de requerir instalación de aplicaciones adicionales en el dispositivo institucional se debe solicitar al proceso de tecnologías de la información.
- Los usuarios de dispositivos móviles asignados por la Entidad, deben evitar hacer uso de estos en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.

Dispositivos no institucionales de propiedad de un tercero:

- Las computadoras personales no se deben utilizar en la entidad para conectarse a Internet u otras redes diferentes a la de invitados, si no existen controles para los virus y firewall de la computadora personal, instalados y en constante funcionamiento.
- El contratista que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato deberá:
    - ✓ Tener y usar solo software legal instalado en su equipo.
    - ✓ Contar con software antivirus licenciado.
    - ✓ Elaborar el listado del software que va a utilizar y evidencia de las licencias correspondientes (tanto para el sistema operativo como para las aplicaciones), indicando el nombre del software, fabricante, versión licenciada y fecha de caducidad de la licencia.
    - ✓ Febor se reserva el derecho de monitorear y revisar cuando se

requiera, el software instalado en equipos de cómputo y servidores conectados a la red de la Entidad.

- La configuración de acceso a correo electrónico institucional en dispositivos móviles personales, se realizará únicamente con previa solicitud al proceso de tecnologías de la información.

9.4.4 Directriz de uso de correo electrónico

En Febor Entidad Cooperativa el correo electrónico es un medio formal de comunicación, todos los mensajes enviados por este medio deben enviarse mostrando el formato establecido por el proceso de comunicaciones indicando el nombre completo del funcionario, el cargo, el nombre de la entidad y que se está actuando en representación de esta. Antes de enviar un correo deberá verificarse que esté dirigido solamente a los interesados y/o a quienes deban conocer o decidir sobre el tema, evitando duplicidades y otros inconvenientes.

Está prohibido el envío de mensajes a correos externos con información objeto de protección legal por reserva bancaria. Ningún usuario está autorizado para enviar correos a cuentas externas a Febor Entidad Cooperativa con información objeto de protección legal por reserva bancaria.

No se deben transmitir o reproducir mensajes escritos y /o gráficos que no atañen directamente a asuntos propios de la entidad, de igual forma no se puede hacer uso del correo institucional para ningún tipo de solicitud personal o ajeno a las funciones de la Entidad, ejemplo: Creación de cuentas personales, solicitudes personales, como correo alterno, etc.

Si su cuenta de correo es accedida de manera ilegal por terceros no autorizados, se recomienda cambiar contraseña dando a conocer de manera inmediata a los encargados de Seguridad de la Información de la Cooperativa adjuntando la evidencia.

El correo electrónico es un medio de comunicación, no un almacén de datos, por lo tanto, en drive solo se mantendrán archivos que sean estrictamente necesarios tenerlos para la labor diaria, así mismo esta documentación no podrá usarse fuera de las instalaciones de Febor pues pueden considerarse una fuga de información.

El factor de doble autenticación es un requisito obligatorio para todas las cuentas de correo de Febor Entidad Cooperativa, por lo tanto, todas las cuentas deberán tener este factor, en caso de retiro de la cooperativa el administrador de seguridad.

9.4.5 Directriz de uso de mensajería instantánea y redes sociales

Febor Entidad Cooperativa define las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de Febor Entidad Cooperativa que sea creado a nombre personal en redes sociales como: Twitter, Facebook, YouTube LinkedIn, blogs, Instagram, etc., se considera fuera del alcance de las políticas establecidas y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por la Entidad, debe ser autorizada por los jefes y directores para ser socializadas y con un vocabulario institucional.

9.5 Política de Control de acceso

9.5.1 Directriz de confidencialidad y transferencia de la información

Febor considerará confidencial, para efectos del cumplimiento de las disposiciones legales existentes y atendiendo lo dispuesto en el Artículo 15 de la Constitución Política de Colombia, toda aquella información amparada por la reserva bancaria. Dentro de esta información se cuenta, Información Básica (general, números de cuenta, operaciones financieras, condiciones de manejo), información demográfica, actividad económica, información financiera y crediticia, referencias personales y/o bancarias obligaciones con otras entidades y convenios.

Los encargados de la información y del apoyo informático deben tener en cuenta los siguientes elementos con la intención de salvaguardar toda la información tanto física como electrónica que se encuentra en Febor:

- Si la información no está clasificada como pública, no podrá ser entregada a ninguna organización con la que no se tenga un acuerdo de confidencialidad. De igual forma el contrato de cada empleado o proveedor que tenga contacto con esa información deberá tener cláusula de confidencialidad.
- La información de dominio público será enviada o publicada por canalesoficiales como correo institucional o la página web de Febor.
- Toda la documentación impresa, escrita a mano o documento legible que contenga información pública o reservada deberá ser custodiada y salvaguardada en el archivo físico central.
- La información del sistema al igual que los documentos digitalizados que se encuentran en el sistema de gestión documental deben tener acceso restringido y deben poder ser consultados solo por personas autorizadas.
- Si se confirma o se sospecha que la información o datos confidenciales o privados, son extraviados o revelados a entidades no autorizadas, el propietario de la información o quien evidenció el hecho deberá notificar inmediatamente al encargado de la seguridad de información de la entidad, con el objeto de realizar

un control efectivo de posibles daños y tomar las acciones necesarias.

- La transferencia de información deberá realizarse protegiendo la confidencialidad e integridad de los datos y teniendo en cuenta si se puede realizar transferencia de ese tipo información y a quien se realiza.

9.5.2 Directriz de control de virus

Febor se encarga de proveer un sistema efectivo de antivirus el cual debe estar instalado en cada estación de trabajo, equipos portátiles y en los servidores; los usuarios no deben desactivar esta funcionalidad o intentar manipular la configuración en sus equipos. Es necesario y responsabilidad del usuario del equipo utilizar el software para diagnosticar la presencia de virus en la informaciónque provenga por diferentes medios como internet, USB, etc. antes de abrir o usarlos archivos. Cuando se sospeche que un equipo fue contaminado por un virus o software malicioso se debe apagar, desconectar de la red e informar al Director de Informática.

9.5.3 Directriz para la administración de cuentas y contraseñas de usuario

Febor cuenta con varios sistemas de información y aplicaciones que permiten el desarrollo exitoso de las actividades, para garantizar el correcto uso y confidencialidad de la información estos cuentan con configuración de usuario y contraseña la cual debe cumplir mínimo con los siguientes requerimientos:

- Las contraseñas no deben ser construidas con menos de ocho (8) caracteres.
- No utilizar contraseñas que sean únicamente palabras (aunque sean extranjeras), o nombres (el de usuario, personajes de ficción, miembros de la familia, mascotas, ciudades, marcas, lugares u otro relacionado).
- No utilizar contraseñas completamente numéricas con algún significado (teléfono, fechas).
- Elegir una contraseña que mezcle caracteres especiales y alfanuméricos (mayúsculas minúsculas).
- Se deben utilizar contraseñas diferentes en cada uno de los sistemas a los cuales tengan acceso, solo se podrán utilizar contraseñas similares en diferentes sistemas.

Adicionalmente, cada contraseña es de uso personal e intransferible al igual que los usuarios, está prohibido intentar ingresar cualquier aplicación por medio de la cuenta de otro funcionario. No se deben almacenar contraseñas en formato legible en archivos tipo “batch”, scripts de login automáticos, macros de software, teclas de función de terminales, entre otros. En caso de sospechar que alguien ha obtenido acceso sin autorización a una cuenta se debe modificarla en forma inmediata e informar al área de tecnología de la informática.

9.5.4 Directriz de manejo de contraseñas para administradores de tecnología

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible, se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.

Los usuarios súper-administradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en sobre sellado en el área segura donde designe la Entidad, las credenciales allí contenidas deben ser modificadas de manera mensual o cuando amerite.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal del proceso de tecnologías de la información no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Director de Informática.

Los usuarios y claves de los administradores de sistemas y/o del personal del proceso de tecnologías de la información son de uso personal e intransferible.

El personal del proceso de tecnologías de la información debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la Entidad de acuerdo al rolasignado.

Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar sólo debe tener acceso el Director de Informática.

9.5.5 Directriz de uso de puntos de red de datos (red de área local – LAN)

En Febor Entidad Cooperativa se debe asegurar la operación correcta y segura de los puntos de red.

Las direcciones internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la entidad serán restringidas, de tal forma que no sean conocidas por usuarios internos, clientes o personas ajenas a la entidad sin la previa autorización del proceso de tecnologías de la información.

Todas las conexiones a redes externas que accedan a la red interna de la Entidad pasarán a través de un punto adicional de control como: firewall, gateway, o servidor de acceso.

Los usuarios que tengan acceso a direcciones IP públicas no pueden establecer conexiones a redes de acceso a información privadas, a menos que hayan sido aprobadas por el Director de Informática, quien establecerá el medio de comunicación.

9.6 Segregación en redes

La infraestructura tecnológica de Febor Entidad Cooperativa que soporta aplicaciones debe estar separada en segmentos de red físicos y Lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La separación de estos segmentos debe ser realizada por medio de elementos de conectividad perimetrales e internos de enrutamiento y de seguridad.

9.7 Control de Acceso Remoto

La administración remota de equipos o de la infraestructura de cómputo debe dejar evidencia escrita de la justificación por las que se asigna, al igual que de la responsabilidad que tiene el funcionario a quien se otorga este permiso, la solicitud debe ser realizada por el Director o Líder de proceso, y avalada por el Director de Informática.

9.8 Política Adquisición y desarrollo de sistemas de información

9.8.1 Directriz de adquisición o desarrollo

Garantizar que la seguridad es parte integral de los sistemas de información. El desarrollo de tecnologías informáticas se debe orientar sobre herramientas basadas en tecnologías de última generación, que permitan la portabilidad y escalabilidad de las aplicaciones.

La supervisión y seguimiento a proyectos de infraestructura informática, deben incorporar como un elemento básico de la supervisión, el cumplimiento de la aplicación de políticas de seguridad tanto en el desarrollo de la solución como en el producto final que será entregado a la Entidad.

Todos los desarrollos de software deben surtir una fase de pruebas de funcionalidad en la cual se evidencien los controles establecidos en relación con la integridad de la información que será ingresada una vez se lleve a cabo su implementación.

Los desarrollos de software deben involucrar la correspondiente documentación interna y externa que permitan identificar su seguimiento hasta el nivel de rutinas y procedimientos.

9.8.2 Directriz Propiedad Intelectual

Política por la cual se establece las directrices de manejo de la propiedad intelectual en Febor.

- Asignación de derechos de propiedad intelectual a la Entidad: Mientras se tenga un contrato laboral con Febor, todos los miembros del personal le conceden a ésta los derechos exclusivos de las patentes, derechos de propiedad literaria, invenciones, procesos, procedimientos y metodologías, controversias jurídicas en las que se encuentre involucrado, archivos comerciales jurídicos, archivos de personal e información privada personal o familiar del personal, normas y/o medidas de seguridad u otra propiedad intelectual que ellos originen y/o desarrollen como parte de sus actividades en el desarrollo normal del negocio de acuerdo con el contrato de trabajo.
- Se deben incluir avisos de derechos de propiedad intelectual en todo software y su correspondiente documentación que sea propiedad de Febor.

9.8.3 Directriz de derechos de autor

Política mediante la cual Febor propende por el cumplimiento de los Derechos de Autor.

- La instalación de software o el uso de información externa en los recursos informáticos debe ser previamente autorizada y debe cumplir con los requerimientos legales que faculten su utilización. En otras palabras, Febor propende por el cumplimiento de todas las obligaciones legales, adquiriendo el material patentado de la empresa propietaria o duplicándolo bajo expresa autorización de la misma.
- Febor cuenta con la autoridad y autonomía para realizar auditorías periódicas sobre las estaciones de trabajo, previa autorización del jefe inmediato, para verificar el apropiado uso de software. Se mantendrán los registros de los hallazgos identificados
- El software que reside en los recursos informáticos de la institución sólo podrá ser el autorizado por Febor Entidad Cooperativa.
- No se podrá instalar software que no esté registrado y autorizado en los recursos informáticos de Febor Entidad Cooperativa.
- Los medios magnéticos, manuales y licencias de uso originales de los recursos informáticos adquiridos por Febor Entidad Cooperativa no deben ser reemplazados por copias.
- Febor Entidad Cooperativa debe conservar en un lugar seguro y específico para este fin, los medios, manuales y licencias originales de uso de los recursos informáticos adquiridos.

9.9 Política de gestión de los incidentes de la seguridad de la información

9.9.1 Directriz de Gestión de Incidentes de Seguridad de la Información

Se debe asegurar que los eventos o incidentes que quiebren la seguridad de la información sean comunicados y atendidos oportunamente, con el fin de tomar oportunamente las acciones correctivas.

Los integrantes de Febor deben vigilar, reportar y evaluar los incidentes de seguridad de la información, como: pérdida de confidencialidad, integridad y disponibilidad de la información.

Adicional, toda falla en el sistema, pérdida del servicio y errores de resultado de datos del negocio incompleto o inadecuado, debe ser informada oportunamente.

También se deben notificar situaciones tales como: personas ajenas a Febor y centros de cómputo, correos maliciosos, sospechas de equipos infectados, reinicio de los equipos de cómputo o enrutadores, mala utilización de recursos, uso ilegal del software, mal uso de información Corporativa, alteración de información, o cualquier violación a las políticas establecidas es este manual.

9.9.2 Directriz Administración del riesgo en seguridad de la información.

Debe realizarse regularmente un análisis de riesgos que permita identificar los recursos informáticos de mayor criticidad y orientar los esfuerzos a proteger dichos recursos, Febor Entidad Cooperativa debe contar con un proceso periódico que permita determinar el nivel de exposición al riesgo a que están sujetos los activos de Información de Febor.

Se deben contratar seguros que cubran los recursos informáticos de Febor Entidad Cooperativa que tengan cobertura específica para: el hardware, los medios de almacenamiento (Datos), el software y la documentación.

9.10 Política de Cifrado

9.10.1 Directriz de controles criptográficos

En caso de ser requerido Febor Entidad Cooperativa implementará actividades para protección de activos de información clasificada, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de cómputo de Febor sea por cualquier medio tecnológico existente,

siempre deberá estar autenticado.

9.10.2 Política de seguridad de las operaciones de TIC

Definir las reglas para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de Febor Entidad Cooperativa con el fin de robustecer la continuidad de los sistemas de TIC.

Se definirán procedimientos, registros e instructivos de trabajo debidamente documentados, los cuales serán progresivamente implementados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica.

Cada procedimiento tendrá un responsable para su definición, mantenimiento e implementación.

Para la gestión de las operaciones de la infraestructura de procesamiento de información en Febor Entidad Cooperativa, el proceso de tecnologías de la información, con el apoyo de los otros procesos, establecerá mecanismos que permitan segregar las funciones de administración (sistemas operativos, bases de datos y aplicaciones), monitoreo y operación, separando entre estos los diferentes ambientes de desarrollo, pruebas y producción.

No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información. Así mismo, en los ambientes de desarrollo y calidad si se llegaran a utilizar datos reales del ambiente de producción, se debe definir el protocolo de seguridad que permita salvaguardar la integridad de la información.

9.10.3 Directriz de respaldo y restauración de información

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la Entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitada a través de la herramienta de gestión de requerimientos establecida por la Entidad.

Semanalmente, los administradores de la plataforma de backup de Febor Entidad Cooperativa verificarán la correcta ejecución de los procesos de backup, suministrarán las cintas requeridas para cada trabajo y controlarán la vida útil de cada cinta o medio empleado.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o

destruidos de forma adecuada.

El administrador de la plataforma de backup de la Entidad, debe generar tareas de restauración aleatorias de la información y debe documentarla.

La información previamente definida y contenida en los servidores de Febor Entidad Cooperativa se respaldará de forma periódica, determinada según el procedimiento "Gestión de copias de respaldo y Backup de Información" y los medios que se consideren necesarios se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo, incendio, humedad, y mecanismos de control de acceso físico. Adicionalmente, se realizarán pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

9.10.4 Directriz para realización de copias en estaciones de trabajo de usuariofinal

Asegurar la realización de copias de información en estaciones de trabajo de usuario final.

Todos los usuarios son responsables de realizar una copia de respaldo del original de la información de valor, confidencial o crítica a su cargo. Estas copias separadas deben ser efectuadas con la periodicidad requerida de acuerdo con los cambios que se presenten en la información.

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), pueden ocasionalmente generar riesgos para la Entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal.

Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren habilitados los privilegios de escritura por puertos USB.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por Entidad.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Todos los mensajes son sujetos a análisis frente a amenazas y ataques dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la Entidad.

9.10.5 Directriz de registro y seguimiento de eventos de sistemas deinformación y comunicaciones

Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (logs) generados por los sistemas de información y comunicaciones de Febor Entidad Cooperativa.

Los funcionarios y contratistas de Febor deberán informar inmediatamente a la Dirección de Informática y Dirección de Riesgos cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.

El Administrador del Sistema de Seguridad de la Información será el encargado de realizar la investigación y seguimiento a los eventos e incidentes de seguridad reportados.

9.10.6 Directriz de control de software operacional de Febor Entidad Cooperativa.

Generar acciones que permitan preservar la integridad de los sistemas operativos pertenecientes a Febor Entidad Cooperativa.

Los responsables de la administración de las plataformas de producción estarán obligados a controlar el acceso y uso de los programas fuente, el acceso a los archivos de los sistemas y/o a las aplicaciones que operan en ellas, así como a la programación de las actualizaciones necesarias a realizar.

No se permitirá la instalación de herramientas de desarrollo, ni programas fuente en los sistemas de producción, a menos que sea autorizado por la dirección de informática.

No se permitirá el uso de versiones de software en los sistemas de producción que no sean soportadas por los fabricantes, ni versiones de prueba que no hayan sido liberadas al mercado (Beta), a menos que sea autorizado por la dirección de Informática.

9.10.7 Política de Cumplimiento

Los diferentes aspectos contemplados en este Manual, son de obligatorio cumplimiento para todos los funcionarios, personal en comisión permanente, contratistas y otros colaboradores de Febor Entidad Cooperativa. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, Febor tomará las acciones disciplinarias y legales correspondientes.

9.10.8 Directriz de cumplimiento de requisitos legales y contractuales

Febor Entidad Cooperativa respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una contínua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables para la Entidad, relacionada con la seguridad de la información.

Febor Entidad Cooperativa establecerá el procedimiento para protección de derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

El proceso de tecnologías de la información deberá garantizar que todo el software que se ejecute en los activos de información de Febor Entidad Cooperativa estén protegido por derechos de autor y requiera licencia de uso o sea software de libre distribución y uso.

El proceso de tecnologías de la información de Información realizará el procedimiento de Copias de respaldo (backups) de los registros alojados en los sistemas de información.

Las Dependencias de Febor Entidad Cooperativa que tratan con datos personales de funcionarios, proveedores, contratistas, u otras personas deben obtener la autorización para el tratamiento de datos personales que permita recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Entidad, así mismo los Jefes de las dependencias deben asegurar que tendrán acceso a los datos personales únicamente los funcionarios que tengan una necesidad laboral legitima.

9.10.9 Directriz de Revisiones de Seguridad de la Información

Garantizar la aplicabilidad de las políticas y procedimientos implementados en Febor Entidad Cooperativa. Los altos Directivos (Gerencia y Consejo de Administración), Directores, Jefes, Coordinadores, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su proceso de responsabilidad. El proceso de tecnologías de la información debe establecer el procedimiento para revisar periódicamente los sistemas de información con el herramientas automáticas y especialistas técnicos.

9.11 Política para el teletrabajo o trabajo en casa según corresponda

9.11.1 Directriz protección de los datos desde trabajo en casa o teletrabajo

Lograr que los datos que sean utilizados a través del trabajo en casa o teletrabajo reciban la protección acorde con requerimientos del Manual de Seguridad de Febor Entidad Cooperativa.

Cualquier funcionario, contratista o proveedor que requiera ingresar a los sistemas de información o aplicaciones de Febor Entidad Cooperativa de forma remota, lo deberá realizar a través de una VPN configurada y autorizada por el área de tecnología de la información, de la cual se llevara el control y la trazabilidad del ingreso por este canal.

Febor cuenta con herramientas de seguridad informática que permite la conexión de forma segura desde el trabajo remoto.

En lo posible la conexión desde casa para los funcionarios autorizados para realizar el trabajo se deberá hacer con equipos propios de Febor Entidad Cooperativa.

9.11.2 Directriz conexión segura a internet desde trabajo en Casa o teletrabajo

Garantizar una conexión segura y eficiente para una óptima labor, y además evitar ser víctimas de un malware o un virus.

Cualquier funcionario contratista o proveedor que requiera ingresar a los sistemas de información o aplicaciones de Febor Entidad Cooperativa de forma remota, lo deberá realizar a través de una conexión segura la cual debe ser de manera local, y que sea de propiedad exclusiva del funcionario evitando las conexiones de redes wifi.

Contar con una conexión a internet no menor a 50 megas de manera local y de uso personal.

9.11.3 Directriz envíos de correos desde trabajo en casa o teletrabajo

Lograr que el correo institucional sea usado en debida forma para diversas comunicaciones externas garantizando el envío seguro desde casa.

Cualquier funcionario que requiera enviar un correo electrónico a entidades externas, proveedores contratistas, deberá hacerlo a través del correo institucional, no está permitido usar correos personales para este tipo de comunicaciones.

Febor Entidad Cooperativa le ha asignado a cada colaborador una cuenta de correo electrónico que posee un proceso de doble autenticación, y que pertenece a una

plataforma de correos autorizada y con protocolos de seguridad.

El colaborador deberá contar con conexiones a internet seguras, velocidad en la trasmisión de datos y en lo posible deberá hacerlo desde los equipos asignados por Febor Entidad Cooperativa.

9.11.4 Directriz para consultar documentación desde trabajo en casa oteletrabajo

Lograr que la documentación consultada por parte del funcionario al sistema de gestión documental se realice de forma segura y a través de canales autorizados para tal fin.

Cualquier funcionario que por necesidad de su trabajo requiera consultar en línea el sistema gestión documental de Febor Entidad Cooperativa, lo deberá realizar con los mecanismos de seguridad de la información dispuestos por la Entidad, y a través de los canales autorizados.

El sistema de información de gestión documental se encuentra alojado en la nube a través del sistema Orfeo y cuenta con mecanismos y protocolos de seguridad tendientes a garantizar la seguridad en línea de esta documentación.

En la conexión desde casa para los funcionarios autorizados para realizar el trabajo se deberá hacer con equipos propios de Febor Entidad Cooperativa. Se debe utilizar la intranet institucional para acceder al sistema y realizar la consulta respectiva, es responsabilidad de cada funcionario velar por el correcto ingreso al aplicativo.

9.11.5 Directriz para intercambio de Información sensible desde trabajo enCasa o teletrabajo

Garantizar que el intercambio de información sensible se realice de forma segura desde casa.

Cualquier funcionario, que requiera intercambiar información sensible deberá hacerlo a través de la VPN configurada por Febor Entidad Cooperativa, a través del correo institucional o a través del gestor documental con el fin de garantizar la seguridad en la trasmisión de datos, en lo posible los documentos deberán estar en formato PDF con seguridad de no copiado ni de edición.

Los equipos personales suministrados por Febor cuentan con una impresora PDF configurable para este tipo de trasmisión.

9.11.6 Directriz para el buen uso de equipos institucionales para trabajo encasa o teletrabajo

Concientizar a los colaboradores en el cuidado y mantenimiento de los equipos tecnológicos entregados en dotación.

Los equipos entregados para uso institucional están configurados predeterminadamente para que la velocidad de los procesos no se vea interrumpida y pueda generar un correcto funcionamiento a las actividades diarias, para ello es importante que esta directriz sea aplicada al 100%: No deberá cambiarse la configuración predeterminada de los equipos, no se deberá instalar software alguno que no sea autorizado por el área de tecnología de la información, no se descargará videos de música, ni se accederá a música en línea mientras este laborando, ya que esto resta capacidad en la prestación del servicio de la máquina.

Contar con energía eléctrica estable o en su defecto un estabilizador de corriente, contar con la velocidad apropiada de internet, conciencia en el cuidado y uso de elementos tecnológicos a nuestro cargo.

9.12 Política de delitos informáticos

El Hurto de información incluyendo datos personales que son materia prima para la operación de la Cooperativa y que se encuentran en los diferentes medios tecnológicos, tanto digital como electrónico. Febor estipuló una secuencia de actividades en caso de llegarse a presentar algún delito informático y se encuentra documentado en **TI-PR-14 Procedimiento de Delitos Informáticos**.

10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la Entidad, para proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.

Prevenir interrupciones en las actividades de la plataforma informática de Febor Entidad Cooperativa que van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.

Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales de Febor Entidad Cooperativa podrán ser restaurados dentro de escalas de tiempo razonables.

Febor Entidad Cooperativa deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:

Identificación y asignación de prioridades a los procesos críticos asociados con tecnologías de la información de Febor Entidad Cooperativa de acuerdo con su impacto en el cumplimiento de la misión de la Entidad.

- Documentación de la estrategia de continuidad del negocio.
- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
- Plan de pruebas de la estrategia de continuidad del negocio.

La Alta Dirección de Febor Entidad Cooperativa se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.