CONTENIDO

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) 3

INTRODUCCIÓN 3

OBJETIVOS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN 3

DEFINICIONES 4

POLÍTICA DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN 5

MAPA DE PROCESOS 6

TÉRMINOLOGIA 7

LINEAMIENTOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN .. 9

1. CONTACTO CON LAS AUTORIDADES. 9

1.1 Identificación de los riesgos relacionados con las partes externas. 9

1.2 Consideraciones de la seguridad cuando se trata con los clientes. 10

2 RESPONSABLE DE LOS ACTIVOS 11

2.1.1 Uso aceptable de los activos 11

3. SEGURIDAD DE LOS RECURSOS HUMANOS 13

3.1 Antes de la contratación laboral 13

3.1.1 Roles y responsables. 13

3.2 Durante la vigencia del contrato laboral 13

3.2.1 Responsabilidades de la Dirección 13

3.2.2 Educación, formación y concientización sobre la seguridad de la información 14

3.3 Terminación o cambio de la contratación laboral 14

3.3.1 Devolución de los activos. 15

3.3.3 Retiro de los derechos de acceso. 15

REVISO:	APROBO
Nombre y Firma: GERMÁN BETANCOURT HURTADO	Nombre y Firma: Ehiana Galeano Reyes
Fecha: 07-Diciembre-2017	Fecha: 07-diciembre-2017

4. SEGURIDAD FISICA Y DEL ENTORNO..... 16

4.1 Áreas seguras 16

4.1.1 perímetro de seguridad física 16

4.1.2 Controles de acceso físico..... 16

4.1.3 Seguridad de oficinas, recintos e instalaciones. 17

4.1.4 Protección contra amenazas externas y ambientales. 17

4.1.5 Áreas de carga, despacho y acceso público..... 18

4.2 Seguridad de los equipos. 18

4.2.1 Ubicación y protección de los equipos. 19

4.2.2 Servicios de suministro 20

4.2.3 Seguridad de cableado 20

- *Los cables de datos están debidamente etiquetados según norma ANSI/TIA/EIA-606A*21

4.2.4 Mantenimiento de los equipos de cómputo 22

4.2.5 Seguridad de los equipos fuera de las instalaciones..... 23

4.2.6 Seguridad en la reutilización o eliminación de los equipos..... 24

4.2.7 Retiro de activos 24

5. GESTIÓN DE COMUNICACIONES Y OPERACIONES. 25

5.1 Respaldo 25

5.1.1 Respaldo de la información 25

5.2 Gestión de la seguridad de las redes 26

5.2.1 Controles de las redes 26

6. CONTROL DE ACCESO 28

6.1 Requisitos de la Corporación para el control de acceso..... 28

6.1.1 de control de acceso 28

6.2 Control de acceso al sistema operativo 29

6.2.1 Procedimientos de ingreso seguros..... 29

6.2.2 Identificación y autenticación de usuarios..... 30

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

INTRODUCCIÓN

El Manual de seguridad de la información de *la Caja de Compensación Familiar de Arauca COMFIAR,* tiene por objeto describir el sistema de gestión de la seguridad de la información que la Corporación ha establecido de acuerdo a la Norma Técnica Colombiana ISO 27001, para lograr la satisfacción de los usuarios y/o afiliados respecto al manejo de su información, garantizar el cumplimiento de los requisitos legales, los reglamentarios aplicables y la orientación misional de la corporación donde además se identifican la política y objetivos de la seguridad de la información, el alcance, la descripción e interacción de los procesos.

Es compromiso de todos los trabajadores de La Caja de Compensación Familiar de Arauca COMFIAR, aplicar este Manual como principal documento para la consolidación y mejora continua del Sistema de Gestión de la información, que le permita a la Corporación años tras año ser más competitiva. La implementación del SGSI refleja la convicción de que el Sistema de Gestión de la Información contribuya a salvaguardar la información como bien primordial para la toma de decisiones.

OBJETIVOS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

- Brindar disponibilidad, integridad, seguridad y confidencialidad de la información de los Clientes externos (usuarios y/o afiliados de la Caja de Compensación Familiar de Arauca Comfiar) y clientes internos (procesos de la Corporación), cumpliendo con los requisitos legales

- Garantizar la satisfacción de los clientes internos y externos en materia de seguridad de la información

- Asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres

DEFINICIONES

- La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

POLÍTICA DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Realizar las acciones pertinentes con el fin de garantizar la protección y manejo de la confidencialidad de la información interna de la corporación por parte de los usuarios internos y contratistas (clientes internos), a través del uso y mantenimiento adecuado de la infraestructura y activos tecnológicos dispuesta para la gestión de la información.

Basado en el enfoque de procesos adoptado por la Caja, la Sección de será el responsable de liderar y de velar por el cumplimiento de la política y directrices establecidas aprobadas por dirección en el manejo de seguridad de la información. De igual manera todos los procesos son responsables del cumplimiento de esta política.

MAPA DE PROCESOS

TÉRMINOLOGIA

Activo: Bien o elemento tangible o intangible que tiene valor para la organización

Amenaza: causa potencial de un incidente que puede producir daño a un sistema u organización

Análisis de riesgo: uso sistemático de la información para identificar las fuentes y estimar la magnitud del riesgo

Confiabilidad: propiedad de tener comportamiento y resultados previstos consistentes

Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal

Directrices: descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

Evaluación del riesgo: proceso de combinar identificación, análisis y evaluación del riesgo

Impacto: resultado de un incidente de seguridad de la información

Política: Toda intención de directriz expresada formalmente por la dirección.

Política de seguridad de la TIC: reglas, directivas y prácticas que rigen la forma en que los activos, incluyendo la información sensible, se manejan, protegen y distribuyen dentro de una organización y sus sistemas de TIC.

Proceso: es cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas.

Riesgo: potencial de una amenaza determinada aproveche las vulnerabilidades de un activo o un grupo de activos y produzca daño a la organización. Se mide en términos de la combinación de la probabilidad de un evento y sus consecuencias.
Riesgo residual: riesgo que permanece después del tratamiento del riesgo

Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Sistema de gestión de la seguridad de la información: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Vulnerabilidad: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

LINEAMIENTOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. CONTACTO CON LAS AUTORIDADES.

Contactos con las autoridades pertinentes:

Para efectos de robos, incendio, accidentes laborales y otros

ÍTEM	NOMBRE	DIRECCIÓN	TELEFONOS
1	POLICIA NACIONAL	Cra 20 con 19 Esquina	885 3300
2	BOMBEROS	Calle 23 # 16 -	119
3	DEFENSA CIVIL	Cra 21 # 19 -	885 22 92
4	HOSPITAL	Calle 15 con 16 esquina	885 20 24
5	CRUZ ROJA	KR 18 # 30-25	885 70 10

Para efectos contactos de proveedores de servicios:

Ítem	Proveedor de Servicios	Correo Electrónico	Teléfono
1	Sistemas y Soluciones Integradas E.U	sysintegradas@gmail.com	(1) 833 4545
2	Telefónica Telecom	sandra.parra@telefonica.com	018000 940099
3	Tv Satélite Arauca	prodrigu9209@gmail.com	(7) 885 0389

1.1 Identificación de los riesgos relacionados con las partes externas.

Los accesos no autorizados tales como ataques por acceso remoto (partes externas) són monitoreados y controlados permanentemente, bloqueando la dirección Ip, MAC, para evitar ataques y accesos a los sistemas de información de la corporación.

El acceso físico a oficinas, recintos de computadores y gabinetes de archivos se realiza con acompañamiento del personal de la sección de sistemas, supervisando y controlando todo tipo de soporte realizado en dichos lugares y llevando un registro en el Formato de visita asistencia técnica presencial.

Únicamente se permite el acceso lógico o remoto de partes externas cuando sea necesario y pactada por las dos partes en una fecha y horario definido previamente, puntualizando el tipo de requerimientos que amerite el soporte que se solicita.

Los soportes de proveedores de servicios como Internet, redes, telefónicos, eléctricos, circuitos cerrados de televisión, alarmas y otros que se requieran, se realizan con acompañamiento del personal de la sección de sistemas y llevando un registro en el Formato de visita asistencia técnica presencial FT-GA-26

1.2 Consideraciones de la seguridad cuando se trata con los clientes.

Todos los requisitos de seguridad identificados se abordan antes de dar acceso a los clientes a los archivos o a la información de la organización tales como:

- Protección de activos
- Descripción del producto o servicio que se va a proveer
- Requisitos y beneficios del acceso del cliente

2 RESPONSABLE DE LOS ACTIVOS

Toda la información y los activos asociados con los servicios de procesamiento de información deberán ser del responsable al cual se le ha sido asignado.

Este se le hará entrega mediante formato acta individual de recibido a satisfacción de computadores (FT-GD-10) y este se cargará en el inventario de activos en la oficina de almacén.

Los activos se asignan como herramienta de trabajo para el óptimo funcionamiento y desempeño de sus actividades laborales y/o procesos al cual pertenece y demás funciones que se encuentran en el manual de funciones.

El propietario del activo será responsable de:

- Garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifiquen adecuadamente.
- Respetar continuamente las restricciones y clasificaciones del acceso.

Los activos se pueden delegar por ejemplo a un custodio que cuide el activo diariamente, pero la responsabilidad sigue siendo del propietario.

2.1.1 Uso aceptable de los activos

Todos los empleados, contratistas, visitantes y usuarios deben dar cumplimiento a la política de seguridad de la información, para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información incluyendo:

Reglas para el uso del correo electrónico institucional y de internet.

- Toda información, documentación o trámite electrónicamente que tiene como remitente u origen el nombre de la Caja de Compensación Familiar de Arauca Comfiar, se debe realizar por la cuenta de correo institucional que se le ha sido asignado a cada usuario, si este no tiene cuenta de correo institucional, es necesario diligenciar la solicitud a los administradores de las cuentas de correos, en este caso a la sección de sistemas, por medio de su jefe inmediato ya que la información es de interés único de la corporación, y toda información electrónica de la debe quedar un registro dentro del dominio www.comfiar.com.co

- El correo electrónico institucional es únicamente para el uso de trámites, contactos y demás diligencias a fines que cumplan con el objetivo principal que es el envío y recepción de información que involucre los procesos al cual hace parte el personal que esté laborado en la corporación. No se permite el uso para el envío o recepción de información personal, ni para la administración de cuentas de páginas de redes sociales diferentes a la de corporación y de otras características.

- Los contratistas y visitantes a la Corporación, deberán pedir autorización a la sección de sistemas para poder tener acceso a los dispositivos o puntos de red o redes inalámbricas que prestan el servicio de internet, datos y demás sistemas de información el cual lo habilitará y restringirá su uso dependiendo del periodo que este vaya a durar en la entidad.

- Si un funcionario de la Corporación necesita hacer uso de un activo fuera de las instalaciones donde está ubicado o asignado, es necesario solicitar a la Oficina de Almacén, dicha autorización la cual se realizará mediante el diligenciamiento del formato comprobante de Préstamo Interno o Externo de Bienes Inmuebles. Si este activo no es previamente autorizado por la Oficina de Almacén se puede clasificar como hurto, y estará expuesto a sanciones disciplinarias administrativas, civiles, penales y de ley.

  Cuando el activo y/o información esté autorizado con el proceso anteriormente nombrado, se debe adoptar las medidas de seguridad apropiadas para la protección contra:

  - Hurto por terceros
  - El acceso por contraseña: esta debe únicamente ser conocida por el propietario del activo en la sesión habilitada para ese usuario

  De acuerdo a las reglas anteriores los empleadores, contratistas y usuarios de tercera parte serán consientes de los límites que existen para el uso de la información, así como de los recursos, por esto son responsables del uso que hagan de los recursos de procesamiento de información y de cualquier uso efectivo bajo su responsabilidad.

3. SEGURIDAD DE LOS RECURSOS HUMANOS

3.1 Antes de la contratación laboral

Asegurar que los contratistas y usuarios externos, entiendan sus responsabilidades y que estos sean apropiados y se ajusten a los roles para los que se les considera, esto para reducir el riesgo de robo, fraude o uso de las instalaciones. Para los empleados de esta Corporación lo anterior se realizará una vez se haya suscrito el vínculo contractual.

3.1.1 Roles y responsables.

Es responsabilidad de los empleados de Comfiar:

- Proteger los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizada.
- Implementar y actuar de acuerdo con las políticas de seguridad de la información de la Corporación.
- Garantizar que se asigne la responsabilidad a la persona que tome las acciones.
- Informar los eventos de seguridad, los eventos potenciales u otros riesgos de seguridad.

3.2 Durante la vigencia del contrato laboral

Asegurar que todos los empleados, contratistas y usuarios visitantes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados parar apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el error humano mediante concientización, educación y formación en los procedimientos de seguridad y el uso correcto de los servicios y de la información para minimizar los posibles riesgos de seguridad.

3.2.1 Responsabilidades de la Dirección

La Dirección Administrativa deberá exigir que los empleados, contratistas y usuarios visitantes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización y estén adecuadamente informados sobre las funciones y las responsabilidades respecto a la seguridad

de la información antes de que se les otorgue acceso a información o sistemas de información sensibles.

También se debe buscar concientización sobre la seguridad correspondiente a sus funciones y responsabilidades dentro de la organización y estén de acuerdo con los términos y las condiciones laborales, las cuales incluyen la política de seguridad de la organización y los métodos apropiados de trabajo.

Si los empleados, contratistas y usuarios visitantes no están conscientes de sus responsabilidades, pueden causar un daño considerable a la Corporación.

La Alta Dirección realizará revisiones anuales debidamente documentadas al SGSI con el fin de garantizar su eficacia y la conformidad con los requisitos de la NTC ISO 27001 y los requisitos de la organización y los aplicables a la organización.

3.2.2 Educación, formación y concientización sobre la seguridad de la información

Todos los empleados, contratistas y usuarios visitantes deberán recibir formación educada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales las cuales incluyen información sobre las amenazas conocidas, a quién contactar para obtener asesoría adicional sobre seguridad y los medios apropiados para reportar los incidentes de seguridad de la información.

3.3 Terminación o cambio de la contratación laboral

Asegurar que los empleados, los contratistas y los usuarios visitantes salgan de la organización o cambien su contrato laboral de forma ordenada.

En el momento que un empleado, contratista o usuario termine su contrato con esta entidad, se debe asegurar la completa devolución de todo el equipo y la cancelación de todos los derechos de acceso a estos, a la red, correos institucionales, a toda la información y a los aplicativos de la corporación.

Para la devolución de los equipos cargados al empleado, se debe diligenciar el formato de reintegro a almacén y corroborar con la que allí está cargada a esta persona, para que cruce esta información y recibir el visto bueno.

3.3.1 Devolución de los activos.

Todos los empleados, contratistas o usuarios externos deben devolver todos los activos pertenecientes a la organización que estén cargados a su nombre a la oficina de almacén, al finalizar su vinculación o acuerdo.

Es necesario que los empleados, contratistas o usuarios externos, tengan conocimiento de la importancia de una información para la continuidad de los procesos o de las operaciones, esta información será entregada a su jefe directo manifestándole la importancia y en qué estado se encuentra el proceso.

3.3.3 Retiro de los derechos de acceso.

A todos los empleados, contratistas o usuarios de terceras partes, una vez finalizada su vinculación con esta entidad o se encuentren en periodo de vacaciones previa notificación de la oficina de Talento Humano, se le cancelarán las contraseñas de las sesiones de ingreso al sistemas operativo, redes inalámbricas, usuario y contraseñas de los diferentes plataformas de la Corporación y demás accesos o permisos que llegare a tener, generándole un nuevo usuario, contraseña y permisos al funcionario entrante, la cual es solicitada por el jefe de sección o de división al cual corresponda o en su defecto la sección de Talento Humano.

4. SEGURIDAD FISICA Y DEL ENTORNO

4.1 Áreas seguras

- Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la Caja de Compensación Familiar de Arauca Comfiar.

- Los servidores que prestan los diferentes servicios en la corporación, están situados en la primera planta de la Sede Administrativa ubicada en la Calle 22 # 16-51.

- Están aislados de todo contacto del personal no autorizado, daño e interferencia con cualquier otra señal que afecte el perfecto funcionamiento de la corporación.

4.1.1 perímetro de seguridad física

Se utiliza un perímetro de seguridad (paredes, puertas con llaves) que protegen el área que contiene los servidores con la información de la corporación.

Recomendaciones:

- Que Los perímetros de seguridad tengan puertas de incendio que a su vez tengan alarmas visuales y de ruido según con el código local de incendios.

4.1.2 Controles de acceso físico

- En las áreas tales como cuarto de servidores y planta eléctrica sólo se permite el acceso al personal autorizado.

- El personal autorizado debe contar con conocimientos e instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia.

- El cuarto de servidores tiene acceso controlado, únicamente tiene acceso el personal de la Sección de Sistemas,

- Al personal del servicio de soporte de terceras partes se le da acceso restringido a las áreas seguras o a los servicios de procesamiento de información sensible únicamente cuando sea necesario; este acceso

debe ser autorizado y monitoreado por la Sección de Sistemas.

Recomendaciones:

- Es conveniente cambiar el esquema de acceso al cuarto que contiene los servidores de la entidad, como una puerta de acceso controlada con tarjeta o con lector biométrico, cámaras activadas con movimiento, tarjeta de control de acceso más el número de identificación personal PIN para autorizar y validar el acceso.

- Exigir a todos los empleados, contratistas, usuarios, terceros, utilización de alguna forma de identificación visible y se debería notificar inmediatamente al personal de seguridad si se encuentran visitantes sin acompañante o que no usen identificación visible.

4.1.3 Seguridad de oficinas, recintos e instalaciones.

- Se presenta como objetivo el diseño e implementación de seguridad física para oficinas, recintos e instalaciones, teniendo como base los reglamentos y las normas pertinentes a la seguridad y la salud.

- Las oficinas que no atienden al público (directamente), se les notifica por parte del personal de seguridad la solicitud de requerimiento para que éste autorice el acceso a las instalaciones, teniendo en cuenta la utilización de alguna forma de identificación visible.

4.1.4 Protección contra amenazas externas y ambientales.

- Se tienen en cuenta todas las amenazas para la seguridad que presenta las instalaciones circundantes tales como: incendios, fuga de agua, atentados terroristas, explosiones, etc.

- Los materiales combustibles o peligrosos se almacenan a una distancia prudente del área de seguridad.

- Se cuenta con el suministro de equipo apropiado contra incendios (Extintores de los siguientes tipos: polvo químico seco ABC, dióxido de carbono, Solcaflan y de agua) y están ubicados adecuadamente según estudio.

4.1.5 Áreas de carga, despacho y acceso público.

- Los puntos de acceso tales como las áreas de carga y despacho, y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se controlan y están aisladas externamente a las áreas de procesamiento de información, evitando así el acceso no autorizado.

- El personal de vigilancia privada contratado para la protección de todos los bienes de la Corporación, a manera de colaboración se encargan de guiar, asesorar a los visitantes a esta entidad, y los encargados de abrir y cerrar las puertas de acceso para la carga o descarga de los diferentes productos o activos que se utilizan en Comfiar.

4.2 Seguridad de los equipos.

- Se evita pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de Comfiar

- Todos los equipos de cómputo (computadores de escritorio, portátiles, equipos de comunicaciones, servidores) de todas las sedes de la corporación, están protegidos contra amenazas físicas y ambientales. (Seguro Multi riesgo Empresarial)

- Está prohibido ingerir alimentos, bebidas o fumar cerca de los equipos informáticos que se encuentran en operación que puedan originar directa o indirectamente su mal funcionamiento siendo el usuario responsable por el deterioro del mismo, en estos casos se informará a la oficina de la División Administrativa o Dirección Administrativa para que ésta determine las acciones a seguir o el remplazo del equipo. Se cuenta con avisos de advertencia ubicados en *cada área* específica.

- No está permitida la manipulación maliciosa de los recursos informáticos que puedan originar daños en los servidores, equipos pc , periféricos, equipos de comunicaciones, la estructura de red, las aplicaciones desarrolladas, la base de datos, el servicio de internet, el servicio de aula virtual , el servicio de correo electrónico y los servicios y/o recursos informáticos asociados.

- No está permitido imprimir trabajos personales sin autorización del Jefe de la División Administrativa, empleando los recursos del área (papel, tóner, tinta, cinta) como lo contempla el Reglamento de Trabajo.

- No se deberá usar los recursos informáticos para acceso, descarga, transmisión, distribución almacenamiento de material: obsceno, ilegal, nocivo o que contenga derecho de autor, para fines ilegales.

- No está permitido el uso de los recursos informáticos para generar ganancias económicas personales o desarrollar actividades o labores de terceros. En el caso de los ambientes de aulas y auditorio queda bajo la responsabilidad del personal encargado velar por el cumplimiento de esta política.

- En las oficinas los equipos de cómputo, el software y aplicaciones instalados en ellos, son usados únicamente por el usuario asignado o por las personas designadas como responsables de dichos equipos (activos). En las aulas y auditorios tanto docentes como alumnos pueden hacer uso de los equipos y sistemas pero bajo responsabilidad del propietario y respetando las políticas implementadas en este documento.

- No está permitido usar los equipos informáticos incluidas las impresoras de la corporación para fines que no sean académicos o propias de la labor del usuario.

- El uso de la sala de juntas como toda la parte tecnológica que allí se encuentra, es responsabilidad del usuario, contratistas, usuarios terceros que lo soliciten a la división Administrativa por medio de la plataforma de calendario de Sala de Juntas el cual se puede acceder por el portal de la intranet institucional. Dicha oficina es la encargada de realizar préstamo del sitio, y responsable de los activos correspondientes a esta sala.

- No está permitido el uso de los equipos informáticos, servicios y red de datos para propagar cualquier tipo de virus, gusano, o programa de computador cuya intención sea hostil o destructiva; esto deberá ser reportado por la Sección Sistemas al Jefe de la División Administrativa para que inicie las acciones pertinentes.

4.2.1 Ubicación y protección de los equipos.

- Los equipos están ubicados o protegidos en recintos cerrados para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado, exceptuando los equipos de afiliación en subsidio, atención aportes, y servicio al cliente, los cuales se encuentran a la vista del personal de vigilancia privada y las cámaras del circuito cerrado de televisión CCTV.

- Los equipos que requieren protección especial tales como servidores de datos, servidor CCTV, Firewall, Racks de datos, etc., están ubicados de forma tal que se minimice el riesgo de visualización de la información por personas no autorizadas durante su uso, y los sitios de almacenamiento se encuentran seguros evitando el acceso no autorizado.

4.2.2 Servicios de suministro

- Los equipos deberán estar protegidos contra fallas en el suministro de energía eléctrica y otras anomalías causadas por fallas en los servicios de este suministro como los son las UPS´s individuales para dar soporte al cierre ordenado o al funcionamiento continuo de equipos que soportan operaciones críticas para la entidad y el respaldo del Generador eléctrico (para todas las sedes de la corporación) el cual dispone el suministro adecuado de combustible para garantizar que el generador pueda funcionar por periodos prolongados

- Todos los servicios de suministros tales como electricidad, agua, alcantarillado y aire acondicionado deberán estar adecuados para los sistemas a los que dan apoyo. Estos servicios se someten a inspecciones y mantenimientos preventivos. A los equipos eléctricos se les realiza mantenimiento preventivo cada tres (3) meses, a los de agua y aires acondicionados cada seis (6) meses, esto para garantizar su adecuado funcionamiento y reducir cualquier riesgo debido a su mal funcionamiento o falla.

- El servicio de agua es suministrado por la Empresa Municipal de Servicios Públicos de Arauca EMSERPA, la cual es almacenada en un tanque subterráneo y de allí es bombeado tanque aéreo por medio de una bomba eléctrica para su distribución a la cafetería, sanitario y otros sitios que dependen de este suministro.

4.2.3 Seguridad de cableado

- El tendido de cableado de datos cumple con las normas de cableado estructurado según los organismos ANSI/TIA/EIA/IEEE, el cual nos permite interconectar equipos activos, de diferente o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc, cumpliendo el objetivo fundamental que es brindar los diferentes servicios y cubrir las necesidades de los usuarios durante la vida útil de las instalaciones sin necesidad de realizar más tendido de cables.

- El cableado de red está protegido contra intercepciones no autorizadas o daño, por medio de conductos evitando rutas a través de áreas públicas.
- *Los cables de datos están debidamente etiquetados según norma ANSI/TIA/EIA-606A*
- Antes de entrar al etiquetado es necesario saber los componentes de comunicaciones.

Componentes de Comunicaciones		
Componente	Símbolo	Ubicación
Gabinete 1	GAB1	Primer Piso
Gabinete 2	GAB2	Primer Piso
Gabinete 3	GAB3	Segundo Piso
Switch 1	SW1	Primer Piso
Switch 2	SW2	Primer Piso
Switch 3	SW3	Segundo Piso
Switch 4	SW4	Segundo Piso
Patch Panel 1	PP1	Primer Piso
Patch Panel 2	PP2	Primer Piso
Patch Panel 3	PP3	Segundo Piso
Patch Panel 4	PP4	Segundo Piso
Datos	Dxx	Todos los Pisos
Voz	Vxx	Todos los Pisos
Video	VCxx	Todos los Pisos
Face Plate	FP	Todos los Pisos

- PP3-D01-OFA: Este cable indicaría que está tendido desde la OFICINA A, y que ese cable es de DATOS con número consecutivo 01 y el otro extremo está en el PATCH PANEL 3 y detrás del Patch Panel va marcado de la siguiente manera: OFA-D01-PP3

  - OFx = Letra que representa a una oficina
  - Dx, Vx, VCx = Tipo de servicio Datos, Voz o Video y el número de la conexión (x)
  - PP3: El tipo de elemento al cual está conectado

  Los cables de energía están separados de los cables de comunicaciones para evitar interferencias.

- Las líneas de energía cumplen con el Reglamento Técnico de Instalaciones Eléctricas (RETIE) que fija las condiciones técnicas que garantizan la seguridad en los procesos de Generación, Trasmisión, Transformación, Distribución y Utilización de energía eléctrica en Colombia y asegura la calidad de las instalaciones y productos que las empresas utilizan para la correcta prestación de los servicios eléctricos.

  Cumple con los requerimientos para la instalaciones de sistemas puesta a tierra (SPT) de telecomunicaciones ANSI/TIA/EIA-607, la cual es especifica cómo se debe hacer la conexión del sistema de tierras confiable

- Los gabinetes y los protectores de voltaje son conectados a una barra de cobre (busbar) con "agujeros". Estas barras se conectan al sistema de tierras (grounding backbone) mediante un cable de cobre cubierto con material aislante (mínimo número 6 AWG, de color verde. Este backbone estará conectado a la barra principal del sistema de telecomunicaciones en la acometida del sistema de telecomunicaciones.

4.2.4 Mantenimiento de los equipos de cómputo

- Los equipos deben recibir mantenimiento adecuado para asegurar su continua funcionalidad, disponibilidad e integridad.

- El mantenimiento preventivo de los equipos de cómputo se realiza según lo programado a principio de cada año mediante el diligenciamiento del formato FT-GA-0.

- Sólo el personal de la Sección de Sistemas está autorizado para realizar

los mantenimientos de los equipos de cómputo, cuando un equipo de cómputo se encuentra en garantía el mantenimiento es realizado por el respectivo proveedor.

- Se deberá llevar un registro de todas las fallas reales o sospechosas y de todo el mantenimiento preventivo y correctivo (formato "Control de asistencia mantenimiento preventivo y correctivo a equipos de sistemas), además de las recomendaciones para los funcionarios a los cuales se tiene asignado dicho activo.

4.2.5 Seguridad de los equipos fuera de las instalaciones

Para brindar seguridad a los activos que salen de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de la Corporación, se tienen los siguientes formatos para préstamos de los activos:

- Préstamos internos ALM-001 para los funcionarios de la caja
- Préstamos externos ALM-002 afiliados que soliciten préstamos de activos
- Préstamos internos permite que los activos se saquen de la entidad (laboralmente), ya sea para otra sede o municipio

Independientemente del responsable, es necesario que almacén autorice el uso del equipo fuera de las instalaciones de la corporación, para lo cual se debe diligenciar el formato establecido para el egreso de activos ("Comprobante de egreso de bienes devolutivos", código: FT-GA-14) el cual debe ir firmado por el responsable de la oficina de almacén.

Es necesario tener en cuenta las siguientes recomendaciones para la protección del equipo por fuera de las instalaciones.

- El equipo y los medio llevados fuera de las instalaciones no se deben dejar solos en sitios públicos, los computadores portátiles se deberían llevar como equipaje de mano y camuflado, cuando sea posible, durante los viajes.

- Se deben observar en todo momento las instrucciones del fabricante para la protección del equipo.

- Cuando los activos son retirados de la Corporación por parte de los usuarios en calidad de préstamo (laboralmente), se debe notificar nuevamente a almacén el reintegro del mismo para darle el visto bueno a la entrada a través del diligenciamiento del formato "Comprobante de

ingreso de bienes devolutivos", código: FT-GA-13. Este permiso es por el periodo de trabajo en otras sedes o instituciones.

4.2.6 Seguridad en la reutilización o eliminación de los equipos.

- Se verifica todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o se asegura que se hayan sobrescrito de forma segura, antes de la eliminación.

- Todo equipo de cómputo que se vaya a dar de baja, ya sea para la venta, donación, etc, se borran todos los datos para impedir que datos infidentes (corporativos) sean recuperados por terceros.

- En la actualidad se utiliza un software Open Source que permite borrar el contenido del Disco Duro sobrescribiendo varias veces con datos aleatorios.

4.2.7 Retiro de activos

Ningún equipo, información ni software se retiran de las instalaciones de Comfiar sin autorización. Todo activo requiere autorización de retiro de las instalaciones mediante diligenciamiento del formato "Comprobante de egreso de bienes devolutivos", código: FT-GA-14, con la verificación del servicio de vigilancia aun cuando el activo se encuentre a nombre del empleado que lo desee retirar, siendo la oficina de almacén el autorizador de los retiros de activos.

- Los empleados, contratistas y usuarios externos que tienen autoridad que permite retirar activos, están claramente identificados mediante el diligenciamiento de los formatos ALM-001 y ALM-002.

- Los límites de tiempo de préstamo para el retiro de equipos para los afiliados (préstamos externos) aprobados por Dirección es máximo un día y medio y para los funcionarios de la caja (préstamos internos) tres días, si los funcionarios solicitan el préstamo para desplazamiento en otras ciudades el tiempo máximo es el tiempo que dure en dicha desplazamiento más medio día.

5. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

Asegurar la operación correcta y segura de los servicios de procesamiento de información.

5.1 Respaldo

Se mantiene la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

5.1.1 Respaldo de la información

Se realizan periódicamente copias de respaldo de la información y del software

- Se empleará un servidor de Backus local y un servidor en la nube de la información, adecuado para garantizar que la información y los diferentes softwares utilizados en la Corporación, se recuperen después de un desastre o una falla de los medios de almacenamientos originales.

Estas copias de respaldo tendrán como consideración los siguientes elementos.

- El respaldo de los datos del aplicativo interno de la Caja, se realiza diariamente de la base datos y cada viernes de las fuentes del software.
- Se Clasificó y definió los niveles necesarios para la información de respaldo. Con excepción a los funcionarios de recreación y deportes, publicidad y mercadeo, eventos y programas especiales, ningún otro funcionario tendrá derecho a realizar el respaldo de imágenes, música y videos (contenido multimedia), el restante de funcionarios solamente se les salvaguardará archivos tales como documentos (extensiones doc, docx, docm, txt, pdf, ppt, pptx, ppsx, sldx, xls, xlsx, csv) para el servidor de la vivienda correspondiente a información de la CAVIS UT también se salvaguarda archivos con extensión (.mdb, mda, mdn).

- No se debe guardar respaldo de archivos personales (información concerniente a personas físicas identificadas o identificables).

Se usará el siguiente método de copias de seguridad:

- Primero se crea una carpeta dentro del disco D la cual contenga todo el contenido a realizar el proceso de copia de seguridad según las consideraciones y clasificaciones vistas anteriormente.

- La primera copia o Backup es completo. Se crea una copia de resguardo de todas las carpetas y archivos que contenga la carpeta del disco D en la herramienta para hacer el Backup. Es ideal para crear la primera copia de todo el contenido de una unidad o bien de sus archivos de datos solamente.

- Después procedemos a realizar el Backup diferencial el cual compara el contenido de los archivos a la hora de determinar cuáles se modificaron de manera tal que solamente copia aquéllos que hayan cambiado realmente y no se deja engañar por las fechas de modificación de los mismos.

  Este método tiene como ventaja que se puede ir manteniendo diferentes versiones de los mismos archivos en cada uno de los Backup's incrementales, con lo que se podría restaurar la versión deseada.

- Esta copia de seguridad se realizará periódicamente cada viernes al medio día, aprovechando la ausencia de los funcionarios que laboran con estos activos, y por medio de un software Opensource para copias de seguridad utilizando el método antes descrito, se conecta al servidor de Backup mediante FTP y una contraseña por cada usuario.

- Ningún documento magnético que tenga información de interés institucional podrá ser difundido, distribuidos o comercializados.

5.2 Gestión de la seguridad de las redes

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

5.2.1 Controles de las redes

- Las redes se mantienen y controlan adecuadamente para protección de las amenazas, manteniendo la seguridad de los sistemas y aplicaciones que se utilizan en esta red.

- Para el soporte remoto que se brinda a los usuarios de otras sedes, este se hace con previo aviso para que los usuarios a los cuales se esté brindado dicho soporte, autoricen la conexión remota y tenga conocimiento del soporte que se está realizando.

- Para los soportes remotos hechos hacia la corporación, también es necesaria la autorización, la cual se define el tipo de soporte y el tiempo en que se llevará a cabo.

- Las redes físicas se deben cambiar en un periodo de uso de 10 años, ya que es la vida útil de dicho material para el óptimo rendimiento de la red, y se debe realizar mantenimiento cada vez que se requiera o se detecte alguna falla de conexión o si en su defecto se requiera cambio físico de la misma

6. CONTROL DE ACCESO

6.1 Requisitos de la Corporación para el control de acceso

El acceso a la información, a los servicios de procesamiento de información se debe controlar con base en los requisitos de seguridad y de la empresa.

Las reglas para el control del acceso tienen en cuenta las políticas de distribución y autorización de la información.

6.1.1 de control de acceso

Las políticas de navegación web tienen como objetivo salvaguardar la información y todo sistema de información que pueda atentar con el óptimo funcionamiento del mismo el mal uso de los recursos informáticos y servicios.

La sección de sistemas controla el acceso a Internet mediante el uso "listas negras" y "listas blancas" para bloquear o permitir el acceso a sitios determinados; aplicando una serie de reglas (Calidad de Servicio - QoS) dando prioridades a diferentes tipos de contenidos que hagan del este servicio, un servicio óptimo e ideal para el buen funcionamiento de las funciones de cada uno de los usuarios y que garanticen la seguridad y fomentan uso responsable por parte de los empleados.

Los perfiles son determinados de acuerdo el nivel jerárquico de los funcionarios de la Comfiar, clasificándose de la siguiente manera:

- **Jefes de División y asesores:** Se adoptan para este grupo la regla general de bloqueo y el contenido streaming exceptuando el acceso a YouTube, permitiendo la consulta o navegación de cualquier otro contenido y aplicaciones internas de la corporación, también se incluye a este grupo el perfil del contador.

- **Jefes de Sección y auxiliares:** Se adopta para este grupo la regla general de bloqueo y contenido streaming los cuales no tienen acceso a los sitios de redes sociales (chat, facebook, msn, entre otros), vídeo, sitios online. permitiendo la consulta o navegación de cualquier otro contenido y aplicaciones internas de la corporación

- **Administradores de redes sociales:** Es el caso de la sección de comunicaciones, y áreas como instituto de formación empresarial, que administran perfiles de redes sociales se activara el acceso a dichas redes en horarios específicos para poder alimentar y tener actualizadas

estas cuentas.

- **Especiales:** A este grupo pertenece la sección de comunicaciones, recreación y deportes ya que por sus funciones necesitan de estos contenidos online tales como YouTube, emisoras radiales, según requerimiento directo a la sección de sistemas.

6.2 Control de acceso al sistema operativo

Objetivo: evitar el acceso no autorizado a los sistemas operativos para asegurar que no se realicen cambios que interfieran en el buen funcionamiento de estos.

En las estaciones de trabajo de los funcionarios de la Corporación (PC's) están habilitados dos usuarios de sesión. La primera sesión es sistemas, la cual tiene permisos de administrador y sólo tiene ingreso los funcionarios de la Sección de Sistemas, en esta sesión se es permitido realizar cualquier tipo de instalaciones de programas o software no licenciado o corrupto.

El otro usuario con permisos de invitado "**USUARIO STANDAR**" es donde los funcionarios de la entidad tienen su información y a la vez es la sesión de trabajo la cual debe tener protección por contraseña para salvaguardar sus datos.

6.2.1 Procedimientos de ingreso seguros

- El acceso a los sistemas operativos se controla mediante un procedimiento de registro de usuarios y contraseñas de inicio seguro asignadas individualmente a los funcionarios a los cuales pertenece la estación de trabajo.

- Este procedimiento de registro en el sistema operativo está diseñado para minimizar la oportunidad de acceso no autorizado.

- El procedimiento de registro de inicio cumple con los siguientes aspectos:

  - No se suministra mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.
  - Si se presenta una condición de error al ingresar la

contraseña de un usuario, el sistema no indica que parte de los datos es correcta o no.

- No se muestra la contraseña que se introduce, los caracteres se cifran mediante puntos.

6.2.2 Identificación y autenticación de usuarios

Todos los usuarios tienen un identificador único (ID del usuario) para su uso personal, ya sea para el ingreso al módulo interno de la corporación, sistema de gestión documental, plataforma mesa de ayuda GLPI, internet, entre otros.

VERSIÓN	FECHA APROBACIÓN	PAGINA(S)	NUMERAL(ES)	CAMBIO
Versión 02	07 de diciembre de 2017	16	4.1.2	En las áreas tales como cuarto de servidores y planta eléctrica sólo se permite el acceso al personal autorizado
		19	4.2	El uso de la sala de juntas como toda la parte tecnológica que allí se encuentra, es responsabilidad del usuario, contratistas, usuarios terceros que lo soliciten a la división Administrativa por medio de la plataforma de calendario de Sala de Juntas el cual se puede acceder por el portal de la intranet institucional. Dicha oficina es la encargada de realizar préstamo del sitio, y responsable de los activos correspondientes a esta sala
		30	6.2.2	Todos los usuarios tienen un identificador único (ID del usuario) para su uso personal, ya sea para el ingreso al módulo interno de la corporación, sistema de gestión documental, plataforma mesa de ayuda GLPI, internet, entre otros