CAJA DE COMPENSACION FAMILIAR DE SUCRE

COMFASUCRE

POLÍTICAS

DE

SEGURIDAD DE LA INFORMACIÓN

División de Sistemas Y Tecnologías

V: 1.0

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Este documento es un conjunto de políticas de seguridad de la información de cumplimiento obligatorio por parte de todos los empleados, contratistas, proveedores y estudiantes en pasantía o práctica en COMFASUCRE.

Las presentes políticas sirven para desarrollar procedimientos más detallados y guías de acción para solucionar y enfrentar posibles violaciones a la seguridad.

Estas políticas sirven también para evitar sanciones legales, ya que reglamentan controles sobre contingencias, negligencia o violación de la seguridad informática u otros efectos adversos que pudieran afectar los intereses propios de la Corporación o de terceros.

2. OBJETIVOS DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1. OBJETIVO GENERAL

Preservar la seguridad de la información de COMFASUCRE, protegiéndola desde su ingreso, durante su procesamiento y en su salida del sistema de cómputo.

2.2. OBJETIVOS ESPECÍFICOS

Proporcionar la guía y apoyo de la División de Sistemas que garanticen:

- ✓ El establecimiento suficiente y necesario de estándares operativos para la administración segura del hardware y el procesamiento confiable de la información.
- ✓ La prevención de cambios irregulares o incorrectos en el software aplicativo, por los programadores.
- ✓ Las debidas limitaciones de acceso de la División de Sistemas a la información de los usuarios.
- ✓ El establecimiento de los planes de contingencia que se requieran en COMFASUCRE.

2.3. Dar cumplimiento formal a lo dispuesto por la SSF en la circular externa 023 de noviembre de 2010, específicamente en lo relacionado con los siguientes numerales:

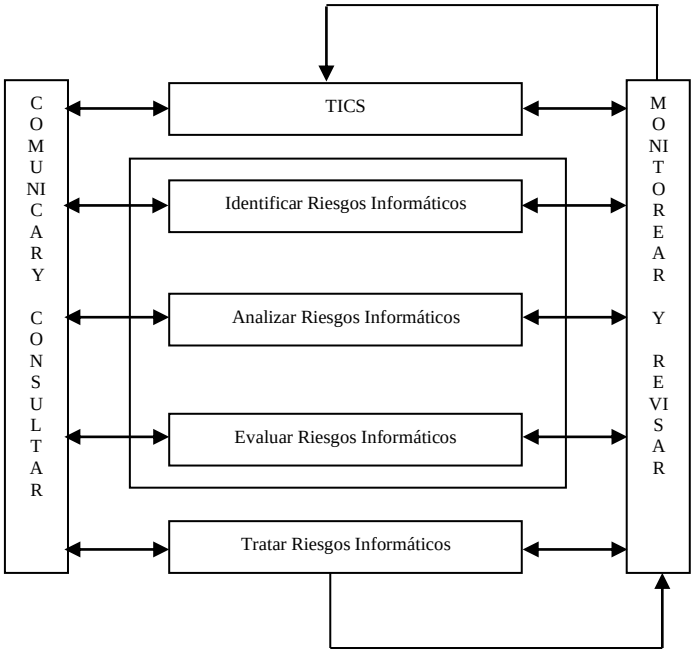
2.3.1. Numeral de la circular externa 023 No. 2.3 Objetivos del SCISF referentes a gestionar de forma efectiva los riesgos.

En el caso de la División de Sistemas, las presentes políticas tienen como objetivo primordial el gestionar los riesgos de informática que puedan vulnerar la seguridad de la información de COMFASUCRE, en sus diversas manifestaciones, así:

- Gestión de riesgos sobre la integridad de la información.
- Gestión de riesgos sobre la confidencialidad de la información.
- Gestión de riesgos sobre la disponibilidad de la información.

Como parte de la implantación de este objetivo de control interno informático las presentes políticas se apoyan en la siguiente normatividad.

5254 – Gestión del Riesgo (Véase siguiente diagrama de la visión general del proceso de gestión del riesgo informático).



Esta Norma guía el establecimiento e implementación del sistema de administración de riesgos. Involucra el contexto de la Corporación y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso, de los riesgos.

SERIE DE NORMAS TÉCNICAS COLOMBIANAS NTC ISO/IEC 27000 – SGSI - Facilita la implementación de estándares de seguridad de la información y los sistemas computarizados de la Corporación.

2.3.2. Reglamentar el uso eficiente y seguro de las TICs que la Caja entrega a los usuarios de Sistemas.

2.3.2.1. Inventario de Tics.

2.3.2.1.1. Hardware.

Descripción	**Cantidad**
IBM System x3200	2
IBM System x3650	1
Clone	1
HP Proliant ML115	1
HP Proliant ML 310E	2
PCs de escritorio	185
PCs portátiles	22
Impresoras laser	56
Impresoras de matriz de puntos	10
KVM	2
Switches	4

2.3.2.1.2. Software.

2.3.2.1.2.1. Programas.

Descripción	Cantidad
Subsidio	1
Contabilidad	3
Presupuesto	1
Suministros	1
Quejas y Reclamos	1
Crédito y Cartera	1
Estadísticas	1
Fonede	1
Vivienda	1
Archivo Central	1
Nomina	1
Activos Fijos	1

2.3.2.1.2.2. Sistemas operativos

Descripción	Cantidad
Centos 5.6	4
Windows 2008	1
Windows Server 2012	
SCO System V	1

2.3.2.1.2.3. Bases de datos.

Descripción	Cantidad
Informix IDS 11.1	1

2.3.2.1.2.4. Antivirus.

Descripción	Cantidad
Kaspersky Open Space	150

2.3.2.1.2.5. Desarrollo

Descripción	Cantidad
Hydra Studio 4.2	1

2.3.2.1.3. Telecomunicaciones

Descripción	Cantidad
Switches 3COM	1
Swiches Allied Telesyn	1
Switches CISCO	24

3. ALCANCE

La presente Directiva es de aplicación para todo el personal de COMFASUCRE en la sede administrativa de Sincelejo y en las sedes municipales o regionales que se establezcan cuando dispongan de TICs, así mismo aplica para reglamentar la interacción con proveedores, contratistas y clientes internos o externos de la División de Sistemas.

4. BASE LEGAL – COLOMBIA

Constitución Política de Colombia. ART. 61.- El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

LEY No. 23 DE 1982 “Sobre derechos de autor”. ART 1.- Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de fonogramas y a los organismos de radiodifusión, en sus derechos conexos a los del autor.

DECISIÓN ANDINA 351 DE 1993 (Acuerdo de Cartagena). ART. 1.- Las disposiciones de la presente Decisión tienen por finalidad reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino.

LEY 44 DE 1993 “Por la cual se modifica y adiciona la ley 23 de 1982 y se modifica la ley 29 de 1944”. Contempla disposiciones relacionadas con el Registro Nacional del Derecho de Autor y las Sociedades de Gestión Colectiva de Gestión Colectiva de Derechos de Autor y Derechos Conexos.

LEY 599 DE 2000 (CÓDIGO PENAL COLOMBIANO), TÍTULO VIII De los delitos contra los derechos de autor: ART. 270.- Violación a los derechos morales de autor. Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a doscientos (200) salarios mínimos legales mensuales vigentes quien:

Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.

Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

DECRETO 1360 DE 1989 “Por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor”.

DECRETO 460 DE 1995. Estipula procedimientos y requisitos de inscripción en el Registro Nacional del Derecho de Autor y reglamenta el depósito legal.

DECRETO 162 DE 1996 “Por el cual se reglamenta la Decisión Andina 351 de 1993 y la Ley 44 de 1993, en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos“.

Ley 1273 de enero 5 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”.

4.10 Ley 603 de julio 27 de 2000. Por la cual se modifica el artículo 47 de la Ley 222 de 1995. ART 20.- Las autoridades tributarias colombianas podrán verificar el estado de cumplimiento de las normas sobre derechos de autor por parte de las sociedades para impedir que, a través de su violación, también se evadan tributos.

5. MARCO DE ESTÁNDARES NORMATIVOS.

SERIE DE NORMAS TÉCNICAS COLOMBIANAS NTC ISO/IEC 27000 – SGSI. Facilita la implementación de estándares de seguridad de la información y los sistemas computarizados de la Corporación.

NORMA TÉCNICA COLOMBIANA NTC 5420 – Ingeniería del Software – Calidad del Producto de Software (SW).

Parte 1: Modelo de Calidad.
Parte 2: Métricas Externas.
Parte 3: Métricas Internas.
Parte 4: Métricas de Calidad de Uso.

La parte 1 define el modelo de calidad interna y externa del producto de SW, que plantea seis (6) características cuando el SW es parte de un sistema informático y plantea la calidad de su uso, mediante cuatro (4) características, que son el efecto combinado para el usuario de las 6 características de calidad del producto de SW. Ej. de usos del modelo de calidad son: Validar la complejidad de una definición de requisitos, identificar los requisitos del SW, identificar los objetivos para el diseño del SW, identificar los objetivos para las pruebas del SW, identificar los requisitos para el aseguramiento de la calidad, identificar los criterios de aceptación de un productos de SW determinado.

Normas técnicas colombianas referentes a seguridad y calidad del ciclo de vida del producto de software, así:

NTC 5415-4 TECNOLOGÍA DE LA INFORMACIÓN, EVALUACIÓN DEL PRODUCTO DE SOFTWARE. PARTE 4: PROCEDIMIENTOS PARA COMPRADORES.

OBJETO Y CAMPO DE APLICACIÓN

Esta parte de la NTC 5415 contiene los requisitos, recomendaciones y directrices para la medición, la valoración y la evaluación sistemática de la calidad de productos de software durante la compra de productos de software, productos personalizados, o modificaciones de los productos existentes. Utiliza el modelo de calidad del software descrito en la NTC 5420-1; amplía el procedimiento general para la evaluación de la calidad del software descrito en la NTC 4243. Puede ser utilizado conjuntamente con las normas ISO/IEC 12119, NTC 5415-2, NTC 5415-3 y NTC 5415-6 (proyecto de norma). Las fases del proceso de evaluación son similares entre esta parte de la NTC 5415 y la NTC 5115-5, pero el contexto de uso es bastante diferente. En el caso de que los compradores requieran la comprobación de los paquetes de software por parte de terceros contra sus requisitos de calidad, se puede aplicar la norma ISO/IEC 12119.

NOTA La norma ISO/IEC 12119 fue reemplazada por la norma ISO/IEC 25051:2006

El proceso de evaluación descrito en esta parte de la NTC 5415 también contribuye a responder a los objetivos de decidir la aceptación de un producto único, o a seleccionar un producto de entre productos alternativos. El proceso de evaluación puede ser adaptado a la naturaleza y a los niveles de integridad de la aplicación. También es lo suficientemente flexible para acomodarse al mayor abanico de formas y usos de productos de manera que sean efectivos en cuanto al costo.

Esta parte de la NTC 5415 está dirigida, aunque no limitada, a gerentes de proyectos, ingenieros de sistemas, equipos de mantenimiento de ingeniería del software y usuarios finales que planean adquirir productos de software, así como a proveedores que facilitan dichos productos.

Los productos de software objeto del proceso de evaluación en esta parte de la NTC 5415 pueden ser integrados como componentes dentro de un sistema más grande o pueden ser utilizados autónomamente. Se clasifican como:

- **A.** Productos de software comerciales.
- **B.** Productos existentes, desarrollados o comprados para otras aplicaciones, o para una amplia gama de aplicaciones comunes.
- **C.** Productos de software personalizados o modificaciones de productos de software existentes.

NTC 4243 - Tecnología de la información. Proceso del Ciclo de Vida del Software. Esta norma establece un marco común para los procesos del ciclo de vida del software, con terminología bien definida que puede ser usada como referencia por la industria del software. Contiene procesos, actividades y tareas que se deben aplicar durante la adquisición de un sistema que contenga software.

NTC 4244 - Tecnología de la información. Evaluación del producto de software. Características de calidad y directrices para su uso. Esta norma define seis características que describen la calidad del software. Estas características ofrecen una línea de base para posterior refinamiento y descripción de la calidad del software.

NTC 3560 - Sistemas de procesamiento de la información. Procedimientos y desarrollo. Guía para la adquisición de sistemas de computación. Esta norma establece recomendaciones para tener en cuenta en la adquisición de sistemas de computación.

NTC 4242 - Tecnología de la información. Vocabulario. Desarrollo del sistema. Esta norma facilita la comunicación internacional referente al procesamiento de la información. Presenta términos y definiciones de conceptos seleccionados, relevantes al campo del procesamiento de información e identifica las relaciones entre las entradas.

6. DEFINICIONES

Los siguientes conceptos o definiciones se aplican a la información empresa, o escrita en documentos físicos, o aquella registrada en medios digitales electrónicos de **COMFASUCRE**, o de sus bases de datos con registros de empresas y trabajadores afiliados, proveedores, empleados, clientes, usuarios y beneficiarios de los servicios sociales.

NTC: Norma técnica colombiana.

Usuario *final*: Es aquel funcionario que, por necesidades de su cargo, se le asignan recursos de cómputo, convirtiéndose así en un usuario del proceso de Sistemas y Tecnología.

Hardware: Son los equipos de cómputo, por ejemplo, Microcomputador o PC, impresora, módem, terminal portátil.

Firewall: Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de

dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Software: Son los programas que se ejecutan en los Microcomputadores.

Sistema Operativo: Programa central que administra el computador, sobre el que corren los demás programas.

Estación de trabajo: Es un ordenador que facilita a los usuarios el acceso a los servidores y periféricos de la red. A diferencia de un ordenador aislado, tiene una tarjeta de red y está físicamente conectada por medio de cables u otros medios no guiados con los servidores.

Sistemas de información: Dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios.

Criterios de Seguridad de la información:

Integridad: Capacidad para producir y mantener la información recibida o generada como resultado de cumplir las funciones del cargo, que sea precisa, coherente con las normas internas y externas, autorizada y completa.

Confidencialidad: Capacidad para producir y mantener la información recibida o generada como resultado de cumplir las funciones del cargo, debidamente protegida de accesos, modificaciones, consultas o borrado no autorizado.

Disponibilidad: Capacidad para producir y mantener la información recibida o generada como resultado de cumplir las funciones del cargo, disponible en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Criterios de Calidad de la información:

Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.

Confiabilidad: La información debe ser la apropiada para la administración de Comfasucre y el cumplimiento de sus obligaciones.

Vulnerabilidad informática: Ausencia o deficiencia que permite violar las medidas de seguridad informáticas para poder acceder a un canal de distribución o a un sistema específico de forma no autorizada y emplearlo en beneficio propio o como origen de ataques por parte de terceros.

Cifrado fuerte: Técnicas de codificación para protección de la información que utilizan algoritmos de robustez reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES y/o AES.

Sistema de Acceso Remoto (RAS): Para efectos de la presente circular, RAS hace referencia a la conexión realizada por un tercero a los sistemas de información de la Corporación utilizando enlaces dedicados o conmutados.

Operaciones: Son las acciones a través de las cuales se desarrollan, ejecutan o materializan los productos o servicios que presta COMFASCURE a sus afiliados, clientes o usuarios Ej. Consulta de estado de aportes, cambios de clave de usuario, actualización de datos, etc.

Cuando la operación implique o conlleve movimiento de dinero se denominará transacción. Ej. Banca Electrónica.

Cliente: Es toda persona natural o jurídica con la cual la Corporación establece y mantiene una relación contractual o legal para el suministro de cualquier producto o servicio propio de su actividad.

Usuario: Aquella persona natural o jurídica a la que, sin ser cliente, la Corporación le presta un servicio.

Producto: Operaciones legalmente autorizadas que pueden adelantar COMFASCURE mediante la celebración de un contrato o acuerdo escrito Ej. Pignoración del subsidio familiar monetario, crédito social, libranza para empleados.

Servicio: Es toda aquella interacción de COMFASUCRE con sus afiliados, clientes y usuarios para el desarrollo de su objeto social.

Dispositivo: Mecanismo, máquina o aparato dispuesto para producir una función determinada.

Contabilización: Capacidad para garantizar que la información recibida o generada sobre hechos económicos procesados como resultado de cumplir las funciones del cargo, queda registrada y acumulada contablemente en las cuentas aplicables y dentro del periodo contable correcto.

Eficacia: Capacidad de alcanzar o lograr las metas y/o resultados propuestos del cargo para los objetivos planteados.

Eficiencia: Capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.

Autocontrol: Capacidad de todos y cada uno de los funcionarios de la Corporación, independientemente de su nivel jerárquico para evaluar y controlar su PROPIO trabajo, detectar desviaciones y efectuar correctivos en el ejercicio y cumplimiento de sus funciones, así como para mejorar sus tareas y responsabilidades.

Autorregulación: Capacidad de la Caja de Compensación Familiar para desarrollar en su interior, aplicando métodos, normas y procedimientos que permitan el desarrollo, implementación del SCISF, dentro del marco de las disposiciones legales aplicables.

Autogestión: Capacidad de la Corporación para interpretar, coordinar, ejecutar y evaluar de manera eficiente y eficaz su funcionamiento.

Hurto / Fraude: Actos de corrupción o delincuenciales que de forma intencionada defraudan y se apropian de activos de la Corporación. En este tipo de eventos pueden verse implicados empleados o personas externas a la Corporación. Ejemplos:

Colusión: Pacto ilícito de varias personas para cometer un daño contra la Corporación.

Falsificación de dinero, cheques, títulos valores o documentos: Falsear o adulterar el papel, texto o números de contenido, forma, o firmas de billetes, cheques, títulos valores y otros documentos comerciales originales, con fines contrarios a la Ley.

Fraude en Contrato: Cuando el encargado de suscribir o vigilar la ejecución de contratos donde participa la Corporación, se confabula con intereses opuestos a los de la Corporación.

Fraude (Definición General): Acción contraria a la verdad y a la rectitud que perjudica a la persona contra quien se comete.

Fraude en cuentas por cobrar: Acto del deudor de la cuenta, generalmente simulado y rescindible, que deja al acreedor sin medio de cobrar lo que se le debe.

Fraude en Cuentas por pagar: Acto malicioso en contra de la Corporación para beneficiar inapropiadamente al acreedor de una cuenta por pagar, incluyendo proveedores, acreedores, contratistas, empleados con supuestos pagos laborales por pagar, entre otros.

Malversación de Fondos: Cuando empleados de la Corporación sustraen o facilitan que terceros sustraigan caudales económicos u otros activos, cuando tienen custodia o administración sobre los mismos.

Sanciones: Sanciones por incumplimiento de leyes o normas oficiales, en cualquier contexto, sea: laboral, comercial, tributario, cambiario, civil, penal, entre otros.

Pérdida de Imagen y Credibilidad Pública: Pérdida de reputación de la Corporación, desprestigio público, mala imagen, publicidad negativa, cierta o no, con respecto de la Corporación y sus prácticas de gestión humana, o sobre la administración de las compras, o debido a una percepción negativa en la calidad de los productos o servicios prestados de la Corporación, o por sospechas de mal manejo, no transparente, de sus activos, de forma que se cause pérdida de clientes y disminución de ingresos, especialmente cuando los productos o servicios también son ofrecidos por empresas competidoras.

Daño o Destrucción de Activos: Pérdidas por daños o perjuicios de activos físicos.

Fallas Tecnológicas: Pérdidas por incidentes de fallas tecnológicas en el hardware, software, people ware (personal de sistemas o usuarios, que interactúa con la tecnología informática) y las telecomunicaciones.

Errores en la Ejecución y Administración de Procesos: Pérdidas por errores u omisiones en la ejecución y administración de los procesos. Incluye: Falta de planeación, falta de metas, falta de control, decisiones erróneas, desempeño deficiente, ineficiencia e ineficacia en los procesos, errores humanos (involuntarios) en la ejecución de los mismos.

Exceso de Egresos: Pérdida cuando la Caja gasta más dinero del presupuestado, o por errores consistentes en pagos de mayor valor, por cualquier concepto, pagos dobles o compras sin la debida evaluación costo-beneficio.

Pérdida de Ingresos: Dejar de ganar, perder clientes, falta de recuperación de cuentas por cobrar, principalmente.

Factores de Riesgo: Son las fuentes generadoras de eventos adversos y perjudiciales para la Corporación. Ejemplos: Recurso humano, procesos,

tecnología, infraestructura y acontecimientos externos. La Corporación clasifica los factores de riesgo en internos y externos, así:

Factores Internos:

Talento Humano: Personas vinculadas directa o indirectamente para que ejecuten los procesos de la Corporación. Ejemplos: Proveedores / Ejecutores de Procesos / Clientes de los procesos.

- **Vinculación directa:** Por contrato de trabajo según la legislación laboral vigente.
- Vinculación indirecta: Para personas que prestan servicios externos, diferente a los que se originan en un contrato de trabajo.
- **Procesos:** Conjunto de actividades interrelacionadas para transformar entradas en productos o servicios con un valor agregado, a fin de satisfacer determinadas necesidades de los clientes del proceso.
- **Tecnología:** Conjunto de dispositivos, metodologías y procedimientos para automatizar procesos de la Corporación. Incluye: hardware, software y telecomunicaciones.
- **Infraestructura:** Conjunto de elementos que se necesitan para el funcionamiento de una Corporación. Ejemplos: edificios, instalaciones de trabajo, muebles y enseres, bodegas y transporte, principalmente.
- **Factores Externos:** Eventos relacionados con la naturaleza u ocasionados por terceros, cuyas causas escapan al control de la Corporación.

Impacto del Riesgo: Pérdidas económicas por la ocurrencia de un determinado evento de riesgo, incluyendo los gastos derivados de su tratamiento.

Perfil de Riesgo: Resultado consolidado de acumular riesgos residuales ocurridos o a los que está expuesta la Corporación durante un periodo de tiempo en años.

Plan de Contingencias, Recuperación y Continuidad de Operaciones: Conjunto de procedimientos, sistemas y recursos necesarios para enfrentar contingencias, recuperar la funcionalidad de los procesos (manuales y sistematizados) y normalizar la continuidad de la operación de los mismos, cuando se presente una interrupción prolongada (según cada sistema) durante un lapso mayor al máximo tolerable. Las causas pueden ser: fallas humanas,

fenómenos de la naturaleza, fallas tecnológicas, daño o destrucción de las instalaciones físicas, entre otras causas.

Probabilidad Anual del Riesgo: Resultado de dividir la cantidad de años en que ha ocurrido un determinado evento de riesgo por el número de años en que se ha medido su posible ocurrencia.

Riesgo en relaciones con empleadores, trabajadores afiliados, clientes, usuarios y beneficiarios: Fallas negligentes o involuntarias de las obligaciones de la Corporación ante empleadores y trabajadores afiliados, agregando clientes, usuarios y beneficiarios de los servicios sociales que presta la Corporación. Dichas fallas impiden satisfacer una obligación o compromiso frente a aquellos.

Riesgo en las Relaciones Laborales: Actos incompatibles con la legislación laboral, o con los acuerdos internos de trabajo.

Riesgo Inherente: Nivel de riesgo propio de la actividad u objeto social de la Corporación, incluyendo sus áreas de servicios y de Administración, sin considerar el efecto de los controles.

Riesgo Legal: Posibilidad de pérdidas para la Corporación en caso de ser sancionada u obligada a indemnizar por incumplimiento de normas, regulaciones y obligaciones contractuales. El riesgo legal surge además por errores en los contratos y transacciones, o por actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones de la Corporación.

Riesgo Operativo: Posibilidad de pérdidas para la Corporación por errores o irregularidades de sus empleados, procesos, tecnología, infraestructura o por acontecimientos externos. Esta definición incluye el riesgo legal y el riesgo reputacional.

Riesgo Reputacional: Posibilidad de pérdidas por desprestigio público, mala imagen, publicidad negativa, cierta o no, respecto de la Caja y sus prácticas organizacionales, administrativas, de manera que pueda producirse pérdida de afiliados, clientes o usuarios de servicios o disminución de sus ingresos.

Riesgo Residual: Nivel del riesgo después de la acción de los controles.

Requisitos de Seguridad de Sistemas: Se refiere a las condiciones de seguridad identificadas y acordadas entre la División de Sistemas, los usuarios, los proveedores de hardware, software o comunicaciones y/o los programadores de aplicativos, previamente a la adquisición, desarrollo y/o implementación de los sistemas de información. La adecuada especificación, diseño, desarrollo, pruebas e implementación de los sistemas informáticos que sustentan los

procesos de COMFASUCRE son cruciales y obligatorios para mantener la seguridad. Todos los requisitos de seguridad deben identificarse en la fase de recolección de términos de referencia de un proyecto y deben ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

Seguridad de las aplicaciones del sistema: Capacidad para mantener la integridad, confidencialidad y disponibilidad de la información con base en controles eficaces y suficientes en las entradas, procesos y salidas de las aplicaciones. Estos controles deben incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.

Cuando se trate de proteger activos informáticos sensitivos, valiosos o críticos deben requerirse controles adicionales, determinados en función de los requisitos de seguridad y la estimación del riesgo.

Validación de los datos de entrada: Se refiere a los controles sobre los datos de entrada a las aplicaciones de usuario final para garantizar que son correctos y apropiados de acuerdo con el formato, límites de valores por transacciones, integridad del input, periodo contable adecuado y totales de control de exactitud y valuación de transacciones.

Control del proceso interno: Son chequeos de validación en las aplicaciones para la detección de una posible corrupción en la información debida a errores de procesamiento o de acciones deliberadas.

Autenticación de mensajes, operaciones y transacciones: Son controles para asegurar la autenticidad y la protección de la integridad del contenido de los mensajes, operaciones y transacciones en los aplicativos.

Validación de los datos de salida: Son los controles aplicados sobre los datos de salida de las aplicaciones para garantizar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.

Seguridad de los ficheros, archivos o tablas del sistema: Conjunto de controles para restringir el acceso a los sistemas de ficheros, archivos, tablas, índices y código fuente de los programas. Los proyectos TIC's y las actividades de soporte deben ser dirigidos de un modo seguro. Se busca evitar la exposición de los datos sensibles en entornos de desarrollo y prueba.

Control del software en explotación: Son procedimientos para controlar la instalación de software en sistemas que se encuentran operativos.

Protección de los datos de prueba del sistema: Se trata de las actividades de control o medidas para seleccionar, proteger y controlar cuidadosamente los datos utilizados en las pruebas de los aplicativos en desarrollo o mantenimiento.

Control de acceso a la librería de programas fuente: Son el conjunto de restricciones al acceso hacia el código fuente de los programas.

Seguridad en los procesos de desarrollo y soporte: Son los controles que estrictamente se aplican en los entornos de desarrollo de proyectos y de soporte. El Jefe de la división de Sistemas es responsable seguridad del proyecto o del entorno de soporte, aún en los casos donde se hayan contratado terceros. En este caso el Jefe de División Sistemas debe solicitar pólizas de cumplimiento y otras garantías a los proveedores externos, quienes deben garantizar que todas las actividades de cambio en los sistemas, son revisadas para verificar que no comprometen su seguridad o del entorno operativo.

Procedimientos de control de cambios: Consiste en la aplicación de procedimientos formales de control de cambios.

Revisión técnica de los cambios en el sistema operativo: Revisiones y pruebas sobre las aplicaciones críticas cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Corporación.

Restricciones en los cambios a los paquetes de software: Son el conjunto de medidas tomadas por la división de Sistemas para disminuir en lo posible la cantidad de modificaciones realizadas por programadores internos sobre los paquetes de software desarrollados por programadores externos, restringiéndose a lo imprescindible, en cuyo caso todos los cambios deben ser estrictamente controlados.

Controles sobre el desarrollo externalizado del software: Metodologías prácticas para supervisar y monitorizar el desarrollo del software contratado por la Corporación.

Gestión de las vulnerabilidades técnicas: Se refiere a implementar métodos efectivos, sistemáticos y cíclicos, con la toma de medidas que confirmen la efectividad para identificar, registrar, priorizar y atender eventos de seguridad técnica en los equipos computacionales o en su utilización. Se deben considerar sistemas operativos, así como todas las aplicaciones que se encuentren en uso.

Control de las vulnerabilidades técnicas: Se debe obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la Corporación ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados.

- **Control de Accesos:**

Requisitos de negocio para el control de accesos: Son las regulaciones para el control de los accesos donde se toman en cuenta las reglas para la distribución de la información entre los directivos, los empleados de cargos medios y básicos, o cuando se involucran terceros. Lo anterior, con base en criterios razonables para el uso de la información, dentro de cada área y cargo de la Corporación, de acuerdo con la naturaleza de las actividades y procesos que realizan.

Política de control de accesos: Reglas que definen el nivel de acceso a la información (por módulos, tablas y opciones de acceso) con base en las necesidades de seguridad y de objeto social de la Corporación.

Gestión de acceso de usuario: Son los procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información que presta la División de Sistemas a sus clientes internos o externos. Este tipo de procedimientos cubren todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos usuarios hasta su inactivación, cuando ya no sea necesario su acceso a los sistemas y servicios de información. Se presta especial atención, a la necesidad de controlar la asignación de permisos de acceso con privilegios especiales que pasan por encima y anulan la eficacia de los controles del sistema.

Equipo informático desatendido por el usuario: Se refiere a los controles automatizados a través del sistema operativo que permiten garantizar que los equipos desatendidos o encendidos pero inactivos disponen de la protección apropiada ante el riesgo de acceso no autorizado.

Escritorios y monitores limpios de información: Son directrices establecidas para garantizar que los usuarios se habitúan a mantener sus pantallas libres de información sensible al igual que sus escritorios, para disminuir la posibilidad que personas no autorizadas puedan leerla, reproducirla, modificarla o borrarla.

Control de acceso en red: Trata sobre el conjunto de controles de acceso y procesamiento en los servicios informáticos internos y externos, conectados en red. El acceso de los usuarios a redes y servicios en red se aplican para garantizar que existen interfaces adecuadas entre la red de COMFASUCRE, Internet y las redes públicas o privadas de otras organizaciones. Así mismo, que los mecanismos de autenticación funcionan adecuadamente y se aplican a los usuarios y a los equipos interconectados, mediante rutinas de autenticación de los nodos de la red.

Segregación en las redes: Se refiere a la separación lógica o virtual que la División de Sistemas realiza para los grupos de usuarios, servicios y sistemas de información en las redes.

Control de conexión a las redes: Corresponde a las medidas de control aplicables a las redes compartidas, especialmente cuando se extienden más allá de los límites de COMFASUCRE, la División de Sistemas restringe las competencias de los usuarios para conectarse en red, según la política de control de accesos y la necesidad de uso de las aplicaciones de negocio.

Control de encaminamiento en la red: Hace referencia a los controles de enrutamiento en las redes para asegurar que las conexiones de los computadores y flujos de información no incumplen la política de control de accesos a las aplicaciones de la Corporación.

Control de acceso al sistema operativo: Está conformado por el conjunto de controles automatizados y políticas de seguridad que la División de Sistemas utiliza para restringir el acceso y uso de las opciones del sistema operativo, de manera que la Corporación tenga la capacidad de autenticar los usuarios autorizados; registrar los intentos de autenticación correctos y fallidos del sistema (mediante LOGs o AUDIT TRAILs); registrar el uso de privilegios especiales del sistema; emitir alarmas cuando se violen las políticas de seguridad del sistema; restringir los horarios de conexión de los usuarios cuando sea necesario.

Identificación y Control de Uso de Programas Utilitarios del Sistema: Se refiere a los controles que se establecen para identificar, restringir y controlar el uso de programas de utilidad del sistema tales como editores, compiladores, comandos para la manipulación de archivos y directorios, programas para gestión de perfiles de acceso, utilitarios para generar y restaurar copias de respaldo, o para optimizar, limpiar, formatear, o reorganizar el espacio de los discos, programas de desintaladores, principalmente, programas para acceder y controlar de manera remota computadores de la red corporativa. Todos esos tipos de utilitarios podrían eludir los controles convencionales del sistema y de las aplicaciones.

Desconexión automática de terminales: Se refiere a las rutinas automáticas que se encargan de desconectar las sesiones tras un determinado periodo de inactividad.

Limitación del tiempo de conexión: Es el tiempo de conexión máximo permitido para determinados usuarios con accesos a activos de información sensibles, valiosos o críticos, de forma que se proporcione un nivel de seguridad adicional a las aplicaciones de alto riesgo en determinados horarios. Ej. En el medio día, en horas nocturnas, fines de semana y festivos.

Inventario de activos informáticos intangibles: Consiste en que la División de Sistemas relaciona, identifica, clasifica y define los controles de salvaguarda para cada activo de información de acuerdo con su grado de sensibilidad o exposición a los riesgos de pérdida, destrucción, acceso no autorizado y valor para COMFASUCRE.

En desarrollo de los criterios de seguridad y calidad, **COMFASUCRE** deberá cumplir, como mínimo, con los siguientes requerimientos:

Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios para prestar sus servicios y manejar su información y la de terceros bajo su custodia, en condiciones de seguridad y calidad.

Gestionar la seguridad de la información, para lo cual tomará como referencia los estándares referidos anteriormente en el marco legal y en el marco normativo.

Disponer de controles de seguridad para el manejo y envío de información riesgosa sobre la Corporación y trabajadores afiliados, clientes y usuarios de los servicios sociales tales como certificaciones, estados de cuenta de deudores, notificaciones, tarjetas débito para pago de subsidio familiar monetario y chequeras, entre otros.
Se haga en condiciones de seguridad. Cuando la información que la Corporación remite a sus clientes sea de carácter confidencial y se envíe como parte de, o adjunta a un correo electrónico, ésta deberá estar cifrada.

Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la Corporación.

Velar por que la información enviada a los clientes esté libre de software malicioso.

Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las Corporaciones deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las Corporaciones deberá ser única y personalizada.

Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.

Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.

Disponer de los mecanismos necesarios para que los clientes tengan la posibilidad de personalizar las condiciones bajo las cuales se les prestará servicios por los diferentes canales, dejando constancia de ello. En desarrollo de lo anterior, la Corporación deberá permitir que el cliente, por lo menos, inscriba las cuentas a las cuales realizará transferencias o pagos, defina montos, número de operaciones y canales. En cualquier caso, los montos máximos deberán ser definidos por la Corporación. Así mismo, deberá permitir que el cliente registre las direcciones IP, los números de los teléfonos fijos y móviles desde los cuales operará. La Corporación podrá determinar los procedimientos que permitan identificar y, de ser necesario, bloquear las transacciones provenientes de direcciones IP o números fijos o móviles considerados como inseguros.

Ofrecer, cuando el cliente así lo exija, la posibilidad de manejar una contraseña diferente para cada uno de los canales.

Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo solo lo pueda realizar personal debidamente autorizado.

Establecer procedimientos para el bloqueo de canales o de medios, cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos.

Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes y definir procedimientos para la confirmación de las operaciones que no correspondan a sus hábitos.

Realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales y medios de servicio al cliente y al usuario. En desarrollo de lo anterior, las entidades deberán establecer los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios.

Definir los procedimientos y medidas que se deberán ejecutar cuando se encuentre evidencia de la alteración de los dispositivos usados en los canales de distribución de servicios financieros.

Sincronizar todos los relojes de los sistemas de información de la Corporación involucrados en los canales de distribución. Se deberá tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio.

Tener en operación solo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad.

Contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar y corregir las fallas oportunamente.

Incluir en el informe de gestión a que se refiere el artículo 47 de la ley 222 de 1995 y sus modificaciones, un análisis sobre el cumplimiento de las obligaciones enumeradas en la presente Circular.

Considerar en sus políticas y procedimiento relativos a los canales y medios de distribución de productos y servicios, la atención a personas con discapacidades físicas, con el fin de que no se vea menoscabada la seguridad de su información.

7. POLITICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

7.1. Responsabilidad de Elaboración y Actualización de las Políticas de Seguridad Informática:

Siendo la División de Sistemas de COMFASUCRE la encargada de diseñar y desarrollar procedimientos de Tecnología de Información será responsable de la emisión y/o actualización de la presente Directiva y de todas aquellas disposiciones necesarias para regular el uso y control de los sistemas computarizados aplicables a COMFASUCRE.

7.2. Cumplimiento de las Políticas de Seguridad de la Información

El cabal cumplimiento de las Políticas de Seguridad de la Información de la Corporación por parte de los trabajadores es obligatorio. La supervisión de tal cumplimiento es responsabilidad de la División de Sistemas.

7.3. Examen y pruebas de conformidad por parte de profesionales independientes.

Profesionales independientes deben comprobar por lo menos cada año la conformidad técnica de las medidas de seguridad implementadas por la División de Sistemas, mediante el examen de controles y pruebas de intrusión, pruebas de validación, de controles de acceso, procesamiento y razonabilidad de la información procesada en diversos sistemas de la Corporación.

7.4. Controles de auditoría de sistemas

El área de auditoría interna debe planear y ejecutar cada año la realización de pruebas de auditoría informática para evaluar el sistema de gestión de riesgos informáticos y los controles administrativos y técnicos de la División de Sistemas, así como los controles de sistemas de las áreas usuarias.

Debe dejarse evidencia de la planeación y la ejecución de las auditorías de sistemas en papeles de trabajo de conformidad con las normas profesionales que regulan el ejercicio de la Auditoría Interna.

8. POLÍTICAS SOBRE LA ESTRUCTURA ORGÁNICA DE CARGOS RESPONSABLES DE LA SEGURIDAD DE LA INFORMACIÓN

8.1. Comité Directivo de Seguridad de la Información

El Comité Directivo de Seguridad de la Información está conformado por el Director Administrativo, Jefes de División y Jefes de Oficina, se encarga de promover las iniciativas de seguridad de la información dentro de la Corporación, así como de obtener los recursos necesarios para poner en funcionamiento dichas actividades.

8.2. Dirección Administrativa

De acuerdo con el estándar NTC ISO/IEC 27001, la Dirección Administrativa de la Corporación asigna una alta prioridad a la Seguridad de la Información en todas las actividades e iniciativas actuales y futuras.

8.3. Jefe de División de Sistemas

Elabora los manuales de procesos, políticas y procedimientos sobre seguridad de la información y los hace reglamentar formalmente a través de la oficina de Gestión de Calidad.

Garantiza el cumplimiento de todos los estándares de seguridad informática que dependen de su área.

8.4. Jefe de Divisiones y de Oficina, Usuarios de los Sistemas

Garantizan el cumplimiento de todos los estándares de seguridad informática que dependen de su área.

8.5. Gestión de Riesgos

Garantiza que el jefe de la División de Sistemas mantenga una copia actualizada bimensualmente de los mapas de riesgos que podrían vulnerar la seguridad de la Información, tanto en esa división, como en todas las demás áreas de usuarios.

8.6. Auditoría Interna

Realiza pruebas de auditoría tendientes a verificar el funcionamiento de los controles de seguridad informática en la División de Sistemas y en todas las áreas de usuarios de la Corporación.

8.7. Jefe Oficina Gestión de Calidad

Se encarga de formalizar, integrar y divulgar dentro del S.G.C. los estándares de seguridad informática producidos por la División de Sistemas.

8.8. Asesoría especializada en Seguridad de la Información

La Corporación buscará asesoría especializada sobre Seguridad de la Información de consultores internos o externos.

Se mantendrá un registro actualizado de todas las organizaciones relevantes que pudieran intervenir en casos de incidentes de seguridad, incluyendo los contactos responsables de coordinar dichos aspectos en tales organizaciones.

8.9. Revisión independiente de la seguridad de la información

Revisión periódica del documento de Políticas de Seguridad de la Información

El documento de Políticas de Seguridad de la Información será evaluado periódicamente por personas independientes o especialistas externos para garantizar que las prácticas organizacionales reflejan apropiadamente la política y que ésta es factible y eficaz.

9. POLITICAS DE SEGURIDAD PARA PROTECCIÓN DE ACTIVOS INFORMÁTICOS

Los activos informáticos abarcan dos categorías, así:

Activos Informáticos Tangibles: Corresponden al hardware.
Activos Informáticos Intangibles: Corresponden al software, manuales y bases de datos.

9.1. Clasificación de la información de la Corporación o de Terceros manejada Internamente:

Información Pública:
A la cual tienen acceso todas las personas que trabajan o que se relacionan directa o indirectamente con la Corporación. No implica control de acceso. Ejemplo: Publicada en la Página de Internet (WEBSITE), carteleras de la Corporación, Folletos, Informe de Gestión Corporativo Anual, etc.

Información Privada:
Es aquella a la cual pueden acceder y usar el personal de empleados de la Corporación, pero no así personas externa o ajena a la misma.

Información Confidencial:
Archivos o tablas cuyo acceso está permitido solo para algunas pocas áreas o usuarios de la Corporación o de sus contratistas (Ej. Revisor Fiscal, Asesor de Riesgos).

Información Secreta:
Aquella a la que pueden acceder uno o pocos directivos de COMFASUCRE.

Ejemplos de activos informáticos intangibles:
Programas fuentes, bases de datos de nómina, bases de datos de Corporaciones, nóminas de Corporaciones afiliadas, composición familiar de los trabajadores afiliados, archivos de cartera, saldos y movimientos de efectivo en caja y bancos, datos de proveedores y contratos, principalmente.

9.2. Responsabilidad sobre los activos.

Cada activo importante o valioso de información debe tener un propietario designado formalmente que es responsable de establecer la seguridad de dicho activo y garantizar que se mantenga su adecuada protección.

9.3. Defensa contra delitos informáticos.

Los riesgos de los sistemas e información de la Corporación deben reducirse al mínimo fomentando la concientización y vigilancia del personal, e instalando sistemas y dispositivos de protección apropiados.

9.4. Mantenimiento del Inventario de Activos de Información.

La División de Sistemas debe contar con un inventario formal, clasificado y actualizado de todos los activos de información. La clasificación de dichos activos debe realizarse en función de su importancia, criticidad, exposición a riesgos, integridad y disponibilidad para la Corporación.

9.5. Datos de beneficiarios, clientes y terceros.

Se debe clasificar la información de contacto de beneficiarios, clientes y terceros como altamente confidencial y protegerla en consecuencia.

9.6. Manejo de Información Financiera.

La información financiera debe clasificarse como altamente confidencial y se deben tomar las medidas de seguridad necesarias (técnicas y administrativas) que protejan tal información de accesos no autorizados.

9.7. Etiquetado de información.

Toda activo de información debe tener una etiqueta claramente visible a fin que los usuarios conozcan quien es el propietario y cuál es el nivel de clasificación designado.

9.8. Uso de nombres de archivos.

Los nombres de archivos de datos de la Corporación deben tener un significado reconocible por sus usuarios.

9.9. Grabación periódica de datos por usuarios.

A fin de prevenir daños o pérdida debido a malos funcionamientos del sistema o fallas de energía, los usuarios de sistemas de información que crean o modifican archivos de datos, deben grabar su trabajo de manera periódica usando las mejores prácticas.

10. POLITICAS DE SEGURIDAD PARA LA ADMINISTRACIÓN DEL HARDWARE Y DEL PROCESAMIENTO DE LA INFORMACIÓN

10.1. Especificación de los requisitos para los nuevos equipos

Las requisiciones de compras significativas de nuevos equipos deben contar con un Expediente Técnico que detalle la especificación de los requerimientos del usuario, los requisitos de Seguridad de la Información, la prioridad, el cumplimiento de estándares técnicos y funcionales, y la relación con los objetivos a corto y largo plazos de la Corporación.

10.2. Instalación de nuevos equipos

Todas las nuevas instalaciones de equipos, y sus respectivos requisitos de Seguridad de la Información, deben planificarse formalmente y notificarse a los interesados con la debida anticipación.

10.3. Prueba de equipos y sistemas

Todo equipo debe probarse exhaustivamente y pasar por un proceso de aceptación formal de usuarios antes de ser transferido al entorno de producción.

10.4. Gestión y uso de documentación de hardware

La documentación de hardware debe estar siempre actualizada y fácilmente accesible para el personal autorizado de soporte o mantenimiento.

11. POLÍTICAS DE PREVENCIÓN DEL RIESGO DE CAMBIOS IRREGULARES O INCORRECTOS EN EL SOFTWARE APLICATIVO

11.1. Desarrollo y Mantenimiento de Software Aplicativo.

En todos los proyectos de desarrollo o mantenimiento de software aplicativo, sea por analistas y programadores internos o externos, el Jefe de la División de Sistemas debe garantizar la aplicación razonable de los siguientes estándares:

NTC 3585 - Sistemas de procesamiento de la información. Auditoria. Programa de aseguramiento de calidad para el software previamente desarrollado utilizado en aplicaciones no criticas. Esta norma contiene definiciones, responsabilidades, requisitos de administración y elementos del programa de aseguramiento de calidad.

NTC 4243 - Tecnología de la información. Proceso del Ciclo de Vida del Software. Esta norma establece un marco común para los procesos del ciclo de vida del software, con terminología bien definida que puede ser usada como referencia por la industria del software. Contiene procesos, actividades y tareas que se deben aplicar durante la adquisición de un sistema que contenga software.

NTC 4244 - Tecnología de la información. Evaluación del producto de software. Características de calidad y directrices para su uso. Esta norma define seis características que describen la calidad del software. Estas características ofrecen una línea de base para posterior refinamiento y descripción de la calidad del software.

NORMA TÉCNICA COLOMBIANA NTC 5420 – Ingeniería del Software – Calidad del Producto de Software (SW) – **Parte 1**: Modelo de Calidad, **Parte 2**: Métricas Externas, **Parte 3**: Métricas Internas y **Parte 4**: Métricas de Calidad de Uso.

11.2. Compra de Software Aplicativo Comercial

Igualmente se deben aplicar los siguientes estándares para adquisición de software comercial, cuando sea necesario y razonable, de acuerdo con el criterio profesional del Jefe de la División de Sistemas:

NTC 3560 - Sistemas de procesamiento de la información. Procedimientos y desarrollo. Guía para la adquisición de sistemas de computación. Esta norma establece recomendaciones para tener en cuenta en la adquisición de sistemas de computación.

NTC 5415-4 TECNOLOGÍA DE LA INFORMACIÓN. EVALUACIÓN DEL PRODUCTO DE SOFTWARE. PARTE 4: PROCEDIMIENTOS PARA COMPRADORES.
POLITICAS DE SEGURIDAD DE LAS APLICACIONES DEL SISTEMA
Validación de los datos de entrada

Como parte del proceso de diseño, desarrollo y/o implementación de todo software en la Corporación debe realizarse, de manera obligatoria, el control de datos de entrada, considerando, como mínimo, los procedimientos de consistencia de datos, correspondencia a las autorizaciones y privilegios de usuario, y procedimientos de manejo de errores.

11.3. Control del proceso interno

Todo sistema en producción debe contemplar el control de los datos en proceso. Dichos controles deberán ser diseñados conjuntamente con el dueño del sistema. Como mínimo se debe considerar controles externos de integridad de datos así como momentos de ejecución de programas.

11.4. Validación de los datos de salida

Como parte del proceso de diseño, desarrollo y/o implementación de todo software en la Corporación debe existir, de manera obligatoria, un procedimiento para controlar los datos de salida, considerando, como mínimo, procedimientos de consistencia de datos de salida, correspondencia a las autorizaciones y privilegios de usuario, y procedimientos de manejo de errores.

11.5. Uso de los controles criptográficos

La Corporación debe evaluar constantemente, mediante un análisis de riesgos, qué información requiere ser protegida con medidas criptográficas.

11.6. Uso de técnicas de encriptación

Las técnicas de encriptación a ser usadas en la Corporación deben considerar las regulaciones y restricciones nacionales e internacionales. Antes de la transmisión, se deben coordinar los procedimientos que utilizarán el emisor y el receptor.

11.7. Firmas digitales

La conveniencia y viabilidad, así como los casos en los que se puede usar firmas digitales debe analizarse conjuntamente entre la parte técnica y legal de la Corporación, teniendo en cuenta toda la legislación relativa que describe las condiciones en las que una firma digital tiene validez legal.

11.8. Seguridad de los archivos del sistema

La operación y administración de sistemas de la Corporación debe llevarse a cabo siguiendo procedimientos diseñados y documentados detalladamente

(REFERENCIAR O ELABORAR) según las mejores prácticas debidamente aprobadas por los dueños de los sistemas.

11.9. Seguridad de bibliotecas de programas en producción

Las bibliotecas de programas que están en producción deben tener controles que impidan el acceso de personas no autorizadas, el cual se debe otorgar estrictamente por necesidad de uso. Los procedimientos de modificación deben estar formalmente autorizados por el usuario dueño del sistema y prever el control dual.

11.10. Uso de datos para pruebas

Todo sistema de información debe tener un juego de datos de prueba que sea consistente y no contenga datos reales o confidenciales. Si no se puede evitar el uso de uso de datos reales confidenciales, éstos deben ser despersonalizados antes de ser usados.

11.11. Gestión de bibliotecas de programas fuente

Las bibliotecas de programas fuente deben tener controles que impidan el acceso de personas no autorizadas y manejarse con un adecuado control de versiones. Los procedimientos de uso de los programas fuente deben estar definidos formalmente de acuerdo a la metodología de desarrollo de sistemas de la Corporación.

11.12. Procedimientos de control de cambios

Todo cambio a sistemas de información debe realizarse mediante procedimientos formales de control de cambios, y debe autorizarse y probarse exhaustivamente en un ambiente de la prueba antes de pasarlo al ambiente de producción.

11.13. Control de versiones

Se deben aplicar procedimientos del control de versiones a todos los programas de software y procedimientos pertenecientes a la Corporación.

11.14. Actualizaciones de software recomendadas por el proveedor

Solo de se debe actualizar el software a una nueva versión si se han evaluado adecuadamente las ventajas previstas, la necesidad de dicha actualización, las implicaciones de beneficio-costo y los riesgos.

11.15. Reparaciones de emergencia al software

En el caso que se requiera realizar reparaciones de emergencia al software aplicativo, será la gerencia quien tome la decisión al respecto, después de evaluar la necesidad e implicancias de dicha operación. En cualquier caso, la reparación

deberá hacerse estrictamente de acuerdo a procedimientos acordados de control de cambios.

11.16. Revisión técnica de mejoras (upgrades) de software al sistema operativo

Toda decisión de instalar mejoras a sistemas operativos debe considerar los riesgos asociados y tener la adecuada planificación mediante el establecimiento de un proyecto formal que también considere el manejo de contingencias.

11.17. Restricciones en los cambios a los paquetes de software

No se deben realizar modificaciones a los paquetes de software a menos que sea estrictamente necesario, en cuyo caso se deberá guardar el software original (sin cambios) y probar y documentar los cambios realizados.

11.18. Desarrollo externo del software

Todo desarrollo externo de software debe hacerse por empresas debidamente certificadas en dicha actividad y determinar los derechos de propiedad intelectual. Se debe tener acuerdos para manejar los posibles fallos del contratista.

12. POLÍTICAS DE CONTROL DE ACCESO LÓGICO A LA INFORMACIÓN DE LOS USUARIOS.

12.1. Asignación de identificador de usuario a nuevos empleados

Se debe aplicar el procedimiento actual (referenciarlo) de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información de la Corporación.

12.2. Privilegios de acceso

La asignación de privilegios de acceso en los sistemas de la Corporación debe controlarse mediante un proceso formal de autorización, en el cual debe participar el usuario Jefe del área usuaria del sistema y éste debe corresponder con el perfil funcional del cargo.

12.3. Uso de contraseñas alfanuméricas de usuarios o de números PIN (Personnal Identification Number)

Las contraseñas otorgadas a los trabajadores son privadas y altamente confidenciales. La violación a dicha confidencialidad dará lugar a una acción disciplinaria.

12.4. Consideraciones para el manejo de clave de accesos:

Debe evitarse el uso de contraseñas triviales o fáciles de adivinar, como nombres, números de la placas de vehículos, fechas del nacimiento, o similares; la

contraseña no debe almacenarse en teclas de función programables, debe ser cambiada si llega a ser conocida por personas no autorizadas, entre otras.

El Sistema le solicitará automáticamente al usuario que cambie su clave de acceso cada 90 días.

La longitud mínima de clave de acceso debe ser igual o mayor a 5 caracteres alfanuméricos.

Al escoger una clave de acceso, el usuario debe evitar asociaciones obvias, como nombres de familiares y/o mascotas, números telefónicos, fechas importantes, número de código de empleado, marca de su auto, dirección, etc.

Debe evitarse anotar la clave de acceso en medios visibles.

El sistema bloqueará automáticamente las cuentas de usuarios que presenten 3 intentos fallidos consecutivos.

Para volverlas a activar se deberá contactar a la División de Sistemas.

12.5. Inicio y fin de sesión

Los sistemas deben considerar el manejo de sesiones con los usuarios, las cuales se cerrarán después de un tiempo de inactividad en su utilización (time-out).

12.6. Protección de computadoras desatendidas

Todos los usuarios de computadoras personales y laptops deben asegurarse que sus pantallas queden protegidas y no muestren información cuando estén desatendidas.

Cuando un usuario con acceso al sistema o a los recursos de red se ausente por motivo de vacaciones, enfermedad o permiso, por un periodo mayor a 5 días, el jefe del área correspondiente deberá comunicarlo Jefe de la División de Sistemas, dentro de las 24 horas siguientes de ocurrido el hecho, vía correo electrónico, para que se pueda realizar el bloqueo de su clave de acceso, la cual será restituida a su retorno.

Para el caso de cese o ingreso de un nuevo personal a la Corporación, también se deberá comunicar dentro de las 24 horas siguientes con la finalidad de desactivar o activar un usuario.

12.7. Manejo de renuncias de personal

En el caso de renuncias o ceses de personal, el jefe del área implicada debe coordinar con el Jefe de la División de Sistemas, si los derechos de acceso del personal saliente constituyen un riesgo alto para la Corporación y en tal caso deben inactivarse el identificador de usuario correspondiente.

12.8. Gestión de seguridad de redes

El acceso a los recursos de la red de la Corporación debe controlarse estrictamente de acuerdo con la Lista de Control de Accesos aprobada, la cual debe estar actualizada permanentemente.

12.9. Establecimiento de rutas forzosas

La red debe estar configurada y equipada de tal manera que se puedan establecer rutas forzosas desde las estaciones de trabajo hacia los servidores de la Corporación.

12.10. Autenticación de nodos de la red

Las conexiones remotas a sistemas informáticos se deberán autenticar con la finalidad de reducir la amenaza de accesos no autorizados a las aplicaciones.

12.11. Control de acceso al sistema operativo

El acceso a comandos del sistema operativo debe restringirse para que solamente las personas administrativas de la división de sistemas que puedan ejecutar dichos comandos. Las funciones de administración de dichos sistemas deben requerir aprobación específica.

12.12. Aislamiento de sistemas sensibles o altamente confidenciales

Los controles de acceso para sistemas de información altamente confidenciales deben ser fijados en concordancia con la clasificación de los activos de información a ser protegidos.

12.13. Seguimiento de accesos y usos del sistema

Se debe advertir a todos los empleados que en caso de incidentes de seguridad, es necesario registrar y conservar evidencias o pistas para uso del Jefe División de Sistemas.

12.14. Monitoreo de accesos y uso del sistema

Todas las transacciones registradas con la clave de acceso serán de exclusiva responsabilidad de cada usuario en particular y podrán ser objeto de seguimiento al ser registradas automáticamente en los archivos LOG's.

Se debe registrar y supervisar el acceso a los sistemas para identificar su posible mala utilización. Se debe monitorear regularmente el uso de los sistemas de información, registrando e investigando todos los eventos inesperados. Tales registros también deben auditarse periódicamente de tal manera que sus resultados, sumados al historial de errores fortalezcan la investigación.

12.15. Sincronización de relojes

Los relojes del sistema se deben sincronizar regularmente, especialmente cuando hay diferentes plataformas de procesamiento.

12.16. Uso de equipos portátiles de cómputo

Las personas que usan computadoras portátiles fuera de la Corporación deben conocer los riesgos de Seguridad de Información referidos a equipos portátiles e implementar las protecciones apropiadas para reducir al mínimo dichos riesgos.

12.17. Respaldo de datos (backup) de equipos portátiles de cómputo

La información y datos almacenados en computadoras portátiles se deben respaldar regularmente (backup). Es responsabilidad del usuario asegurarse de que éste se realice de manera periódica.

12.18. Viajes de trabajo

Los empleados que viajan por asuntos de la Corporación son responsables de la seguridad de la información en su poder.

12.19. Seguridad en los accesos de terceras personas

La División de Sistemas debe mantener un registro de los tipos de accesos de terceros a los recursos de información de la Corporación, así como los motivos por los cuales se les puede otorgar dicho acceso.

Sólo se permitirá el acceso de terceros a información de la Corporación cuando dicha información esté aislada y que el riesgo de posibles accesos no autorizados esté debidamente controlado.

Los acuerdos que permiten el acceso de terceros a recursos de tratamiento de información de la Corporación deberán estar basados en contratos formales que incluyan todos los requisitos de seguridad acordes con las políticas y normas de seguridad de la Corporación.

12.20. Difusión de las políticas a contratistas y trabajadores temporales

Se entregará formalmente un resumen de las Políticas de Seguridad de la Información a todo contratista y/o trabajador temporal antes del inicio de sus servicios.

12.21. Brechas de confidencialidad de terceros

Las violaciones de confidencialidad de terceros deben ser reportadas al Oficial de Seguridad de la Información tan pronto como sea posible.

13. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA DEFINICIÓN DE CARGOS

13.1. Inclusión de cláusulas en el contrato de trabajo

El contrato de trabajo debe incluir cláusulas de cumplimiento de la Seguridad de la Información y en los cargos riesgosos debe especificar la obligatoriedad de cumplir la Ley 1273 de enero de 2009, así como las sanciones administrativas o procesales que la Corporación podría ejecutar.

13.2. Responsabilidad de los empleados sobre datos confidenciales

Todos los trabajadores que tengan acceso a información clasificada como confidencial deben firmar cláusulas de protección de la confidencialidad de dicha información, durante y después de terminada la relación contractual con la Corporación, hasta un plazo prudencial.

13.3. Contratación de nuevo personal

Debe existir un mecanismo de verificación de identificación, referencias de nuevos trabajadores que vayan a desempeñar cargos de usuario con acceso o función de procesamiento que resulte riesgosa para la seguridad del sistema, el cual corresponderá al nivel de las responsabilidades que se le asignarán. En los casos de responsabilidades financieras, se hará una verificación del historial crediticio y certificación del pasado judicial.

13.4. Acuerdos de confidencialidad

En los casos donde la información esté clasificada como confidencial, se deben generar y suscribir “Acuerdos de confidencialidad” por los trabajadores o terceros que tengan acceso a dicha información. Artículo 58 numeral 2º.del C.S. del Trabajo y como un apéndice del contrato de trabajo.

13.5. Declaraciones a medios de comunicación

Sólo personas expresamente autorizadas pueden dirigirse a medios de difusión sobre temas referidos a la Corporación.

13.6. Conocimiento de obligaciones laborales sobre seguridad de la información

Las responsabilidades formales, funcionales y legales de los trabajadores en el uso de los sistemas de información de la Corporación y de los datos computarizados que se procesan en éstos deben ser descritas explícitamente dentro del Contrato de Trabajo, o mediante acuerdo de ética y seguridad para el manejo de recursos de informática, que sea parte integral del contrato laboral.

La Oficina de Gestión Humana debe garantizar que todos los empleados estén completamente enterados de dichas responsabilidades.

13.7. Respeto de la privacidad en el trabajo

La Corporación respeta la privacidad del trabajador en su lugar de trabajo; sin embargo, éste no limitará el derecho de la Corporación a tener acceso a la información creada y almacenada en los equipos de la Corporación.

13.8. Propiedad Intelectual sobre la Información generada por los Empleados en el desempeño de sus funciones laborales

Está legalmente aceptado que toda producción informática e intelectual de los trabajadores durante el desempeño de sus funciones es propiedad de la Corporación y como tal debe respetarse y protegerse de accesos no autorizados, cuando sea aplicable y está prohibida su comercialización, cesión o divulgación no autorizada.

Ejemplos: Manuales de políticas, procedimientos, software desarrollado internamente, metodologías de trabajo internas, entre otros.

14. POLÍTICAS SOBRE PLANES DE CONTINGENCIA

La División de Sistemas es responsable de elaborar o contratar la elaboración de un plan de contingencias, recuperación y continuidad de Sistemas.

Para la elaboración de dicho plan se debe contar con la participación de todos los jefes de áreas usuarias.

El plan de contingencias, recuperación y continuidad de Sistemas, una vez elaborado, debe ser sometido a pruebas, revisiones, simulacros y ajustes por lo menos cada dos años o antes si se presentan cambios de fondo en las tecnologías informáticas o en el personal de la división de sistemas o de usuarios clave para su ejecución.

Para la estructura de contenidos del plan de contingencias, recuperación y continuidad de los sistemas, se deben tener en cuenta los siguientes factores:

- Daño o destrucción de Instalaciones Físicas.
- Daño o destrucción de Equipos (se abre una fila para cada tipo de equipo que influya en la continuidad del procesamiento).
- Interrupción del fluido eléctrico.
- Bloqueo de las telecomunicaciones por diversas causas (abrir filas ej. Internet, enrutadores, daño en la red interna, en switches, etc).
- Daño, corrupción o pérdida de integridad en las bases de datos en línea.
- Daño o destrucción de backups.
- Ausentismo no planeado o no disponibilidad de usuarios para el procesamiento.

- Virus Informático.
- Acceso de hackers y adulteración de información.
- Escenario N

15. POLITICAS SOBRE CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

15.1. Capacitación en Seguridad de la Información a trabajadores

Como primera medida fundamental en la administración de la seguridad informática, se debe priorizar la capacitación y actualización continuada al Jefe de la División de Sistemas, quien es responsable de su divulgación al interior de la Corporación.

La capacitación en Seguridad de la Información se debe impartir de manera individual, obligatoria y actualizada a todos los trabajadores, cuando sea necesario.

Se debe concientizar en temas de seguridad de la información al personal permanente de la Corporación mediante información actualizada sobre amenazas existentes y las medidas de seguridad apropiadas.

15.2. Capacitación en Seguridad de la Información a personal nuevo

El personal nuevo debe recibir capacitación básica en Seguridad de la Información como parte del proceso de inducción.

15.3. Capacitación en Seguridad de la Información al personal técnico

La capacitación del personal técnico en Seguridad de la Información deberá estar actualizada y acorde con la responsabilidad de configurar y mantener las protecciones requeridas por la Corporación.

15.4. Respuesta ante incidentes y malos funcionamientos de la seguridad

Investigación de causas e impacto de incidentes

Los incidentes de Seguridad de la Información deben ser investigados apropiadamente por personal debidamente capacitado.

15.5. Reporte de incidentes de seguridad

Los incidentes, sospechas de incidentes y brechas de seguridad de la información deben reportarse al Jefe División de Sistemas lo más rápidamente posible para agilizar las actividades de identificación de daños, reparación y recuperación, así como facilitar la recolección de evidencias.

Sólo se deben comunicar los incidentes de Seguridad de la Información a autoridades externas siempre que sea necesario debido a requisitos legales o regulatorios y con previa autorización del Director Administrativo.

15.6. Reporte de debilidades, excepciones o deficiencias de seguridad

Deben notificarse al Jefe División de Sistemas lo más rápidamente posible.

15.7. Revisión del registro de incidentes de Seguridad de la Información

Se debe crear y mantener un registro de incidentes, sospechas de incidentes, brechas y amenazas a la seguridad de la información y las acciones correctivas identificadas. El registro debe estudiarse regularmente para tomar medidas de reducción del riesgo y frecuencia de los incidentes de la seguridad de la información en la Corporación.

15.8. Proceso disciplinario

Cualquier incidente de seguridad originado por un incumplimiento de dichas políticas, dará lugar a una acción disciplinaria o administrativa o legal, según la gravedad del caso.

16. POLITICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO INFORMÁTICO:

Estas políticas se deben tener en cuenta para la configuración de las instalaciones y de la tecnología de edificio inteligente, en la nueva sede de la Caja, especialmente en aquellas áreas que deben ser protegidas, como: Dirección Administrativa, División de Sistemas, Centro de Procesamiento de la Información, Tesorería, área de archivo físico, entre otras.

16.1. Seguridad de ambientes de cómputo

Los ambientes que contengan servidores, consolas administrativas del sistema, puestos de trabajo del Jefe de la División de Sistemas, o de analistas, programadores, DBA (Data Base Administrador), equipos activos de comunicaciones, equipos de seguridad perimetral, equipos de copias de respaldo, principalmente, deben protegerse contra cualquier intrusión física de personas ajenas a su manejo.

16.2. Control de Acceso a los Repositorios de Datos Off-Line / On-Line

Los medios de almacenamiento de datos o información de respaldo o de bases de datos productivas deben tener controles especiales de acceso para reducir el riesgo de pérdida, sustracción, daño o destrucción.

16.3. Protección de acceso físico

Se debe controlar el acceso físico a ambientes de alta seguridad mediante técnicas de identificación y autenticación.

Se debe tener un sistema de control que monitoree todos los intentos de acceso. Se debe informar al personal con autorización de ingreso a tales áreas sobre los riesgos de seguridad inherentes.

16.4. Seguridad de oficinas, despachos y recursos

Las oficinas, los muebles y enseres deben estar configuradas en materiales no inflamables, para minimizar los daños por incendio, o similarmente por inundación, explosión, disturbio y otras formas de desastres naturales o provocados, así como amenazas que procedan de lugares colindantes.

16.5. Seguridad de oficinas

Se deben instalar sistemas de detección de intrusos y probarse regularmente para cubrir todas las puertas externas y las ventanas accesibles. Las ventanas y puertas deben permanecer cerradas cuando la oficina esté vacía, y las alarmas deben estar activadas.

16.6. Almacenamiento seguro

El material y equipo con información sensible o valiosa deben almacenarse con seguridad y según el nivel de clasificación de la información almacenada.

16.7. Desconfiar de extraños en los locales de la Corporación

Todos los trabajadores deben conocer la necesidad de desconfiar de extraños en los ambientes de la Corporación.

16.8. Acceso de terceros a las áreas seguras

El personal de terceros sólo podrá acceder a áreas seguras cuando sea aprobado expresamente y su acceso se supervisará. No se permitirá la presencia de equipos de fotografía, vídeo, audio u otras formas de registro salvo autorización especial.

16.9. Áreas de acceso público, entrega y recepción

Las áreas de acceso público, entrega y recepción deben tener controles apropiados y, de ser posible, aislarse de los recursos de tratamiento de información para evitar accesos no autorizados.

17. POLITICAS SOBRE INSTALACIÓN Y PROTECCIÓN DE EQUIPOS

17.1. Preparación de ambientes para cómputo

Los lugares elegidos para instalar computadoras y almacenar datos deben protegerse convenientemente contra intrusión física, hurto, incendio, inundación, temperatura y humedad excesiva, y otros peligros.

17.2. Suministro continuo de energía eléctrica a equipos críticos

Se debe instalar fuentes de alimentación continua (UPS) donde sea necesario para asegurar la continuidad del servicio durante interrupciones del suministro eléctrico.

17.3. Gestión y mantenimiento de generadores de reserva

Se deben usar generadores de reserva (plantas eléctricas) cuando sea necesario para asegurar la continuidad del servicio durante interrupciones del suministro eléctrico.

17.4. Seguridad del cableado

Instalación y mantenimiento de cableado de red

El cableado de red debe ser instalado y mantenido por profesionales calificados. Cualquier punto de red que no esté en uso debe ser sellado y su estado registrado.

17.5. Seguridad del cableado

La seguridad del cableado de red debe ser revisada cada vez que se hagan mejoras, cambios de equipo o de ambientes.

17.6. Mantenimiento de equipos

Todo equipo de la Corporación debe tener mantenimiento apropiado a cargo de profesionales calificados, lo cual debe reflejarse en un documento formal.

17.7. Limpieza de equipos

Deben implementarse procedimientos de limpieza de equipos que no comprometan la seguridad de la información, ni la integridad de los equipos. Los materiales y personal de limpieza deben estar aprobados para dicha función.

17.8. Seguros de equipos

Todo equipo de tratamiento de la información de propiedad de la Corporación debe tener cobertura de seguro contra robo, daño o pérdida. Los equipos portátiles deben tener un seguro que cubra viajes nacionales y al exterior.

17.9. Ficha técnica de cada computador

La división de sistemas debe tener un inventario de cada computador donde se indique sus características técnicas, modelo, configuración y usuario asignado.

La ficha técnica debe usarse como lista de chequeo al momento de entregar y recibir equipos en mantenimiento, para identificar cambios no autorizados o sustracción de los componentes del hardware, instalación o eliminación de software, de forma no autorizada.

17.10. Traslado de equipos

Todo movimiento de equipos entre locales de la Corporación debe ser estrictamente controlado por el personal responsable de dichos activos.

17.11. Desecho de equipo obsoleto

Solo personal autorizado puede disponer de equipos de propiedad de la Corporación para su desecho, siempre y cuando se hayan controlado los riesgos de seguridad asociados a la información contenida en dicho equipo.

17.12. Escritorios y monitores limpios de información

Cuando los usuarios se ausenten de su equipo deben dejar sus pantallas libres de información sensible o con protector de pantalla con contraseña, al igual que sus escritorios, para disminuir la posibilidad que personas no autorizadas la lean, reproduzcan, modifiquen o borren.

17.13. Impresión de documentos confidenciales

Se debe asegurar que una persona autorizada reciba la impresión de documentos confidenciales que se envían a una impresora de red, a fin de proteger la confidencialidad durante y después de la impresión.

17.14. Retiro de Equipos fuera de la Corporación

Solo se permite a personal autorizado por Servicios Generales retirar equipos de la Corporación, siendo dicho personal responsable de su seguridad.

17.15. Inventario físico de equipos

Es responsabilidad del Jefe del Departamento de Servicios Generales realizar este tipo de inventarios por lo menos una vez al año y debe reportar a la División de Sistemas y al jefe del área usuaria cualquier novedad, daño visible o pérdida de estos activos.

18. POLITICAS DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

18.1. Documentación de procedimientos operativos

Los procedimientos operativos deben especificar las instrucciones detalladas para la ejecución de cada tarea, incluyendo las actividades de administración de sistemas. Dichos procedimientos deben estar documentados formalmente.

18.2. Cronograma de Copias de Seguridad

Los cronogramas de estas operaciones automatizadas que programa el personal de apoyo técnico deben planearse y contar con la autorización del Jefe de la División de Sistemas.

18.3. Control de Cambios Operacionales

Los cambios operacionales deben probarse exhaustivamente y ser aprobados formalmente antes de ser puestos en producción.

18.4. Respuestas ante incidentes de Seguridad de la Información

El Jefe División de Sistemas debe responder rápidamente a cualquier incidente de Seguridad de la Información, coordinando la recolección de información y sugiriendo medidas a tomar donde sea necesario.

18.5. Protección contra ataques de negación de servicio (DoS)

Se deben tener listos planes de acción contra ataques de negación del servicio (DoS) los cuales deben ser mantenidos y probados periódicamente para asegurarse de su eficacia.

18.6. Análisis de incidentes de Seguridad de la Información ocasionados por fallas de sistemas

Los incidentes de seguridad de la información originados por fallas de hardware o software deben investigarse de manera apropiada por especialistas.

18.7. Confidencialidad de los incidentes de Seguridad de la Información

La información relacionada a incidentes de seguridad de la información sólo puede ser divulgada entre personas autorizadas.

18.8. Segregación de funciones

Necesidad de control dual / segregación de funciones

Dondequiera que un incidente de seguridad de la información pueda ocasionar daño material o financiero a la Corporación, debe emplearse técnicas de control dual y segregación de funciones para mejorar el control de procedimientos de seguridad.

18.9. Separación de los ambientes computacionales de desarrollo y de producción

El Jefe de la División de Sistemas debe asegurarse que existe una segregación de funciones apropiada en todas las áreas encargadas de funciones de desarrollo, operaciones y administración de sistemas.

18.10. Tercerización de operaciones

En el caso de tercerización de operaciones, se deben identificar los riesgos por anticipado e incorporar al contrato las medidas de seguridad apropiadas.

18.11. Planeamiento de capacidad y prueba de nuevos sistemas

Para las pruebas de nuevos sistemas se deben aplicar criterios de capacidad, carga máxima y prueba de stress. Debe demostrarse que sus niveles de rendimiento y resistencia cumplen o exceden las necesidades o requisitos técnicos de la Corporación.

18.12. Paralelo de sistemas

Los procedimientos de prueba de sistemas deben considerar un período de funcionamiento paralelo antes que el sistema nuevo o mejorado sea aceptado para su uso en producción. Los resultados del paralelo no deben revelar problemas o dificultades diferentes a los ya vistos durante la prueba de aceptación de usuario.

18.13. Elaboración de bases de datos

Antes de poner una base de datos en producción, se deben realizar pruebas exhaustivas de su funcionamiento, tanto a nivel lógico de su estructura, como de su eficiencia en un ambiente de producción.

18.14. Medidas y controles contra software malicioso

Todos los recursos activos de tratamiento de información: infraestructura de red, software base y de aplicación, deben configurarse y protegerse adecuadamente contra ataques físicos e intrusión.

Defensa contra virus informáticos

Todas los PCs y servidores de la Corporación deben tener instalado un software antivirus actualizado diariamente. Igualmente, se deben escanear regularmente todos los equipos.

El software antivirus debe adquirirse de un proveedor reconocido, que tenga soporte técnico adecuado.

18.15. Respuesta a incidentes de virus

Se debe desarrollar una estrategia integral y procedimientos de actuación para hacer frente a los virus informáticos, lo cual incluirá procedimientos y responsabilidades de administración, capacitación en el uso de software antivirus y recuperación después de los ataques de virus.

18.16. Descargar archivos e Información de Internet

Se debe tener mucho cuidado al descargar información y archivos de Internet a fin de evitar el ingreso de código malicioso así como la descarga de material no apropiado.

18.17. Certeza de orígenes de archivos

Los archivos electrónicos recibidos de remitentes desconocidos deben ser eliminados sin ser abiertos.

18.18. Instalación usuaria de software adicional

Está prohibido instalar software no autorizado en las computadoras de la Corporación, tales como protectores de pantalla, software demostrativo, manejadores de música, video, mensajería instantánea, juegos, protectores de pantalla, aplicativos particulares (software con licencia adquirido por el usuario para uso doméstico), aplicativos recibidos por la red (correo electrónico, internet), aplicativos entregados en calidad de prueba; salvo autorización del Jefe de la División de Sistemas, para fines de evaluación y pruebas preliminares.

18.19. Respaldo y recuperación de la información.

Es de alta prioridad generar copias de respaldo de archivos de datos (backup) de la Corporación y garantizar la capacidad de restaurarlos. El Jefe de la División de Sistemas será responsable de que la frecuencia de tales operaciones y que los procedimientos aplicados se adecuan a las necesidades de la Corporación.

18.20. Monitoreo de los logs de operaciones

Los registros de log operacional deben ser revisados periódicamente por personal calificado y las discrepancias con los procedimientos operacionales deben ser comunicadas al usuario propietario de información y al Jefe de la División de Sistemas.

18.21. Registro y reporte de fallas de equipos

Toda falla de equipos (incluyendo daños) debe anotarse en un registro especialmente designado para tal fin por el personal encargado de su mantenimiento.

18.22. Registro y reporte de fallas de software

Se debe registrar y reportar formalmente toda falla de software a los responsables de soporte de software.

18.23. Gestión de redes

Los administradores de redes deberán implantar los controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de computadoras, así como la integridad de la red y protección de los servicios conectados contra accesos no autorizados.

18.24. Uso de medios removibles de almacenamiento

Solamente el personal autorizado a instalar o a modificar el software podrá utilizar medios removibles para transferir datos de la Corporación. Cualquier otra persona requerirá autorización expresa.

18.25. Eliminación segura de documentos

Todos los documentos de naturaleza confidencial deben ser destruidos cuando ya no se requieren. El dueño del documento debe autorizar o realizar esta destrucción.

18.26. Eliminación de Software

Sólo se debe eliminar un programa de software cuando se haya decidido que dicho programa ya no es necesario y que no se necesita tener acceso a sus archivos de datos mediante dicho programa.

18.27. Uso de buenas prácticas de gestión de información

Todos los usuarios deben proteger la confidencialidad, integridad y disponibilidad de los archivos durante la creación, almacenamiento, modificación, copiado y borrado/eliminación de archivos de datos.

18.28. Comprobación de exactitud y validez de documentos

Se debe confirmar la validez e integridad de documentos, especialmente aquellos que comprometen u obligan a la Corporación.

18.29. Dependencias entre documentos y archivos

Los documentos altamente sensibles o críticos no deben depender de la disponibilidad o integridad de archivos de datos sobre los que el autor no tenga control. Los documentos e informes importantes deben ser autónomos y contener toda la información necesaria.

18.30. Fotocopiado de información confidencial

Los trabajadores deben conocer los riesgos de brechas de confidencialidad durante el fotocopiado/duplicación de documentos. Sólo se debe duplicar documentos confidenciales con la debida autorización del dueño del documento.

18.31. Eliminación de archivos temporales (tmp)

Los archivos temporales en las computadoras de usuarios deben ser eliminados con regularidad para prevenir su posible mal uso por usuarios no autorizados.

18.32. Seguridad de la documentación de sistemas

La documentación de sistemas es un requisito obligatorio para todo sistema de información de la Corporación. Dicha documentación debe mantenerse actualizada y disponible.

18.33. Envío de información a terceros

Antes de enviar información a terceros, se debe verificar que el receptor está autorizado a recibir dicha información y que las medidas adoptadas por los receptores aseguran la confidencialidad e integridad de la información que se envía.

Se prohíbe facilitar reportes impresos, documentos, acceso a computadores personales e información propia de COMFASUCRE a personas ajenas a la Corporación, sin autorización.

18.34. Transporte de documentos confidenciales

Las medidas de protección de la confidencialidad, integridad y disponibilidad en el transporte o transmisión de documentos confidenciales serán establecidas por los dueños de dichos documentos, quienes deberán asegurarse que tales medidas son las apropiadas.

18.35. Desarrollo y mantenimiento de sitios Web

Solamente personal debidamente calificado y autorizado participará en el desarrollo y mantenimiento de sitios Web de la Corporación.

18.36. Seguridad en el Envío de correo electrónico.

Se debe utilizar el correo electrónico solamente para fines relacionados con la Corporación. Antes de adjuntar archivos a un mensaje de e-mail se debe verificar que la clasificación de información de dicho archivo permite su envío al destinatario previsto y también. Previamente se debe escanear y verificar que no exista virus u otro código malicioso.

18.37. Seguridad en la Recepción de correo erróneo

Los mensajes de correo electrónico no solicitado deben ser tratados con precaución y no ser respondidos.

18.38. Recepción de correo no solicitado

Se debe verificar la identidad y la autenticidad del remitente de cualquier mensaje de correo electrónico no solicitado antes de abrirlo.

18.39. Uso de correos electrónicos

- Está prohibido usar el correo electrónico para las labores ajenas a la Corporación.
- Se debe evitar el uso de lenguaje obsceno y/o abusivo.
- Si se reciben mensajes de cadenas recomendando que los distribuya a sus amigos, NO lo haga. Elimínelos sin abrirlos.
- Está prohibido el envío y distribución de mensajes desde el correo electrónico corporativo no relacionados con el desarrollo de las actividades de la Corporación. Cada empleado con acceso a Internet podrá utilizar su correo electrónico personal de forma razonable.
- Se deberá tener en consideración que los mensajes enviados por el correo electrónico tendrán plena validez para todos los efectos, es decir serán considerados como documentos oficiales. Se deberá revisar los mensajes antes de enviarlos, verificando el destinatario y/o las listas de distribución, para asegurarse que todos los receptores del correo requieren conocer la información.

18.40. Uso de equipos de fax y fax-módems

Sólo se puede enviar información confidencial por fax cuando no estén disponibles métodos más seguros de transmisión. El dueño de la información y el recipiente previsto debe estar avisado y autorizar las transmisiones por anticipado.

Se debe comprobar cuidadosamente las direcciones de email y números de fax antes de enviar información, especialmente en los casos de información confidencial. La misma precaución debe aplicarse cuando existe la posibilidad que se divulguen las direcciones de E-mail u otra información de contacto.

18.41. Seguridad de sistemas públicamente disponibles

Se deben establecer controles en los sistemas públicamente disponibles de captura de información con la finalidad que la información confidencial se proteja

durante su recojo y almacenamiento, y que el acceso a dicho sistema no permita accesos no autorizados a otras redes a las que está conectado el sistema.

18.42. Transmisión e intercambio de información de banca virtual u otra confidencial

Solamente se puede transmitir datos o información de banca virtual u otro tipo de información confidencial cuando la seguridad de los datos puede garantizarse razonablemente usando técnicas de encriptación.

18.43. Control de distribución de información

Los datos e información deben protegerse mediante controles técnicos y administrativos a fin de asegurarse que están disponibles solo para personas autorizadas.

18.44. Estándares de control de acceso

Los estándares de control de acceso de los sistemas de información deben establecerse de manera que prevengan ingresos de usuarios no autorizados y a la vez proporcionen acceso inmediato según los requerimientos de la Corporación.

18.45. Estructura de carpetas y datos para usuarios

Las estructuras de carpetas de datos de la red compartidos por los usuarios deben ser definidas por el Jefe de la División de Sistemas y los usuarios deben seguir dicha estructura. Las restricciones de acceso se deben aplicar para evitar o prevenir el acceso no autorizado.

18.46. Protección de documentos electrónicos con contraseñas

Se debe proteger la información confidencial usando, preferentemente, el control de acceso de la carpeta donde está situado el archivo correspondiente. No se recomienda el uso solamente de contraseñas para proteger documentos.

18.47. Defensa contra ataques internos intencionales

Los estándares de control de acceso y de clasificación de datos deben ser revisados y actualizados periódicamente para reducir la incidencia y la posibilidad de ataques internos.

18.48. Configuración de acceso a la Intranet . Se configuro la Intranet en COMFASUCRE y se socializo con los Jefes de División de esta Corporación.

La Intranet cuenta con los servicios de correo corporativo, tickets, certificado de Aportes, Certificado de Paz y Salvo, Gestión de Reserva de Salas y Aulas, Gestión de Encuestas.

18.49. Configuración de acceso a Internet

El personal encargado de configurar el acceso a Internet debe asegurarse que la red de la Corporación tenga la debida protección. Como mínimo se debe instalar un firewall debidamente configurado.

18.50. Acceso a información sobre proyectos de la Corporación

Solamente personas autorizadas pueden tener acceso a datos confidenciales sobre proyectos de propiedad de la Corporación o administrados por sus ejecutivos.

18.51. Documentación de sistemas

Todos los sistemas deben tener documentación completa y actualizada. Ningún sistema debe pasar a producción si no tiene la documentación de soporte disponible.

18.52. Análisis y especificación de los requisitos de seguridad

Todo desarrollo de software, dentro o fuera de la Corporación, debe contar con un sustento técnico-económico, un presupuesto adecuado, una justificación basada en requerimientos de usuario previamente descritos, analizados y aprobados al nivel adecuado por el Jefe de la División de Sistemas y del área usuaria. Así mismo debe existir un compromiso de disponer de los recursos necesarios para solventar el proyecto de inicio a fin.
La aprobación final del proyecto debe ser por parte de la Dirección Administrativa.

18.53. Desarrollo y mantenimiento de software

Las especificaciones técnicas y funcionales para el desarrollo y mantenimiento de un software deben contemplar formalmente los requerimientos de seguridad, incluyendo los controles técnicos de acceso, la asignación restringida de privilegios y otros requisitos que resulten convenientes para dicha aplicación.

18.54. Interfaces de software aplicativo

El desarrollo de interfaces de sistemas es una tarea altamente especializada y por lo tanto sólo debe ser realizada por profesionales con la debida calificación y experiencia comprobada en el tema. Debe considerar sobremanera los aspectos de seguridad de los sistemas que son conectados y de las plataformas que intervienen.

18.55. Reporte de eventos y debilidades de la Seguridad de la Información

La División de Sistemas debe establecer un procedimiento formal de reporte de eventos o incidentes de riesgos sobre la seguridad de la información que indique las respuestas y las acciones que deben ser tomadas.

18.56. Procedimiento del reporte

Los procedimientos de reporte del cual deben tener conocimiento los empleados, contratistas y terceros, deben incluir: procesos de retroalimentación que aseguren que los eventos sean notificados; formulario de reporte, el cual apoya la acción del reporte y ayuda al encargado del reporte a recordar las acciones necesarias cuando se produce un evento.

18.57. Evidencias del evento de riesgo

Es indispensable recolectar evidencias después de la ocurrencia de eventos de riesgo sobre la seguridad de la información.

18.58. Integridad de material de evidencia

La integridad de todo material de evidencia debe ser protegida. Las copias deben ser supervisadas por personal confiable y se debe registrar la información de cuando y donde fue ejecutado el proceso de copia, quien realizo dicha actividad, y que herramientas y programas se utilizaron.

18.59. Probar debilidades

Se deben probar técnicamente las debilidades del sistema (*Ethical Hacking*) sin producir mal uso, ni ocasionar daños al mismo o al servicio de información, ni incurrir en responsabilidades legales para quien realiza la prueba.

La gestión de la continuidad del negocio debe incorporarse en los procesos y estructura de la Corporación, asignando la responsabilidad de coordinación de este proceso a la División de Sistemas.

El proceso de continuidad del negocio debe incluir la identificación y priorización de los procesos críticos y el impacto de las interrupciones. Los planes y procesos de continuidad así definidos deben probarse y actualizarse periódicamente.

18.60. Iniciativa para el Plan de Continuidad del Negocio

La Dirección Administrativa o en su ausencia el Jefe de la División de Sistemas debe tener la iniciativa para iniciar la ejecución del Plan de Continuidad del Negocio.

18.61. Plan de recuperación de desastres

Los usuarios dueños de cada sistema de información deben asegurarse que disponen de planes de recuperación de desastres, documentados, probados y en funcionamiento.

18.62. Continuidad del negocio y análisis de impactos

Los usuarios dueños de los sistemas de información, conjuntamente con los responsables técnicos de su manejo y identificarán los eventos de riesgo potencialmente causantes de interrupciones a procesos y/o servicios.

18.63. Minimización de impacto de ataques informáticos

Se deben elaborar planes para minimizar los daños por posibles ataques informáticos, los que deberán ser mantenidos y probados periódicamente para asegurar su eficacia y que los tiempos de recuperación sean razonables.

18.64. Activación de los Planes de Continuidad

Cada plan de continuidad del negocio debería especificar claramente las condiciones para su activación, los procedimientos de emergencia a llevar a cabo, los procedimientos de respaldo que permitirán operar, los procedimientos de reanudación en condiciones de normalidad así como las personas responsables de ejecutar cada etapa del plan.

18.65. Mantenimiento y concientización

Todo plan de continuidad debe tener un calendario de mantenimiento de pruebas del plan, así como prever actividades de concientización y capacitación diseñadas para asegurar que los procesos sean eficaces

18.66. Prueba del Plan de Continuidad del Negocio

El Plan de Continuidad del Negocio debe ser probado periódicamente para asegurarse que cada uno de los responsables de las diferentes acciones entienda correctamente la ejecución del Plan.

18.67. Mantenimiento y reevaluación del Plan de Continuidad del Negocio

El Plan de Continuidad del Negocio debe ser continuamente actualizado para reflejar los cambios en los recursos, procesos y servicios de la Corporación.

19. POLITICAS DE SEGURIDAD DEL *INPUT* A LOS APLICATIVOS

Todos los aplicativos deben satisfacer las siguientes normas técnicas para el ingreso de datos:

19.1. Validación y corrección o impedimento automático del INPUT cuando no corresponda al tipo, formato y longitud del dato de entrada.
19.2. Los campos de fecha deben ser en formato mm/dd/aaaa.
19.3. Los campos numéricos deben ser en el formato 999,999.99
19.4. Los campos de llave primaria deben ser únicos e irrepetibles.
19.5. Los valores de entrada sensitivos (salarios, tarifas y cantidad de horas extras al mes, valor de comprobantes de pago, entre otros) deben controlarse mediante limites en rangos de razonabilidad.
19.6. Todas las pantallas de captura de INPUT deben incluir un control de campos obligatorios.
19.7. Todas las pantallas de captura de comprobantes de contabilidad deben incluir controles de balance débitos y créditos
19.8. Dígitos de verificación (Para códigos, NIT, etc).

20. POLITICAS DE SEGURIDAD EN LA IDENTIFICACIÓN DE TRANSACCIONES RECHAZADAS Y EN SUSPENSO

Con el concurso de la División de Sistemas, los usuarios son deben verificar que los programas con procesamientos en lote (*batch*) disponen de controles para confirmar si todas las transacciones de cada batch fueron adecuada y totalmente procesadas, sin que queden partidas rechazadas o en suspenso por identificar.

21. SEGURIDAD DE PROCESAMIENTO DE LA INFORMACIÓN

Con el concurso de la División de Sistemas, todos los líderes de cada área o sección usuarios deben asegurarse que antes de la instalación de nuevos programas o de sus actualizaciones, se validen las normas y demás estándares de calidad inherentes al ciclo de vida del producto de software contemplados en la NTC 4244, específicamente en cuanto a las siguientes seis características:

21.1. Funcionalidad
21.2. Confiabilidad
21.3. Facilidad de uso
21.4. Eficiencia
21.5. Mantenibilidad
21.6. Portabilidad

22. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN OUTPUT

Se adoptarán los textos de las normas citadas en la circular externa 023 de la SSF de Nov. 2010, como sigue:

22.1. Políticas y Procedimientos Contables:

a. Validaciones de calidad de la información, revisando que las transacciones u operaciones sean veraces y están adecuadamente calculadas y valoradas aplicando principios de medición y reconocimiento.
b. Supervisión de los sistemas de información.
c. Controles Generales.
d. Autorización y control de documentos.

22.2. Controles sobre los Sistemas de Información Contable:

Las operaciones del proceso contable dependen del sistema de información, por lo tanto es necesario adoptar controles que garanticen la exactitud y validez de la información, los cuales se pueden clasificar en controles generales y en controles de operación para prevenir errores que se introduzcan en el SCISF, así como detectarlos y corregirlos una vez involucrados para facilitar el control de los datos introducidos.

22.3. Normas de Control Interno para la Gestión de la Tecnología:

La tecnología es imprescindible para el cumplimiento de los objetivos y la prestación de servicios de las Cajas de Compensación Familiar en condiciones de seguridad, calidad y efectividad, para ello es necesario velar que el diseño del SCISF para la gestión de la tecnología responde a las políticas, necesidades y expectativas de la Caja, así como a las exigencias normativas, siendo necesario establecer igualmente mecanismos de evaluación y mejoramiento continuo para lograr los objetivos institucionales; contando con estándares, políticas, directrices y procedimientos debidamente aprobados, orientados a cubrir los siguientes aspectos:

a. Plan estratégico e infraestructura de tecnología.
b. Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
c. Administración de proyectos de sistemas.
d. Administración de la calidad.
e. Adquisición de tecnología.
f. Adquisición y mantenimiento de software de aplicación.
g. Administración de cambios.
h. Administración de servicios con terceros.
i. Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
j. Continuidad de la Caja.
k. Seguridad de los sistemas.
l. Educación y entrenamiento de usuarios.
m. Administración de instalaciones.
n. Administración de operaciones de tecnología.
o. Documentación.

La información de los usuarios finales, crítica para la Corporación, debe ser protegida y respaldada por manuales que son responsabilidad de los usuarios. División de Sistemas velará por la información que se encuentra en los servidores ubicados en el Centro de Cómputo, y el usuario por la información que se encuentra en su PC.

Si los datos almacenados en estos equipos se pierden y si el usuario no dispone de las copias de respaldo apropiadas, la información podría no ser recuperada.

Los usuarios con equipos cuyo sistema operativo sea Windows 95, Windows 98, Windows 2000 – 2003 o Windows XP NO deben compartir su disco duro. Si se requiere compartir un disco duro éste debe estar protegido con una contraseña y debe realizarse esta operación de manera temporal (eliminar la unidad compartida una vez realizada la copia requerida). Se debe consultar a División de Sistemas para recibir la mejor recomendación de manejo en estos casos.

Los discos de duros no deben ser compartidos con acceso total para evitar pérdidas debido al borrado o modificación de la información contenida en este, ya sea de forma voluntaria o involuntaria.

23. POLITICAS DE CUMPLIMIENTO DE LEYES, REGULACIONES y OTRAS DISPOSICIONES LEGALES VIGENTES EN MATERIA DE INFORMÁTICA

23.1. Documentación de requisitos

Cada dueño de sistema de información será responsable de documentar de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para su sistema. Esta documentación estará disponible para uso legal y técnico del sistema.

23.2. Tratamiento o respuesta al Riesgo de Sanciones Legales por incumplimientos de Informática

El Jefe de la División de Sistemas es responsable de implantar los procedimientos apropiados de cumplimiento de las restricciones legales sobre uso de material protegido por derechos de propiedad intelectual.

La Auditoría Interna y la Revisoría Fiscal deben verificar selectiva y periódicamente el cumplimiento de las políticas de seguridad informática incluidas en el presente documento.

23.3. Uso de software licenciado

Todo software que se utilice en la Corporación debe estar amparado en una Licencia de Usuario, cuyos términos se deben respetar estrictamente con la

finalidad de cumplir con las leyes y asegurar el soporte continuo por parte de los proveedores.

23.4. Uso de información protegida por derechos de autor (con copyright) de la Internet

Para utilizar información obtenida de la Internet o de otras fuentes electrónicas, se debe obtener previamente (no después) la autorización del propietario de los derechos de autor.

23.5. Envío electrónico de información protegida por derechos de autor (con copyright)

Para retransmitir información por Internet u otras fuentes electrónicas, se deben obtener la autorización del propietario de los derechos de autor.

23.6. Archivos de Documentos

Se deben aplicar las normas y controles técnicos y administrativos de archivística para garantizar el cumplimiento de las leyes sobre esta materia.

23.7. Conservación de información

Los registros e información creados y almacenados por sistemas de información de la Corporación deben conservarse por el tiempo que sea necesario para cumplir con los requisitos legales, sectoriales y los propios de la actividad de la Corporación.

23.8. Conservación o borrado de correo electrónico

Los mensajes de correo electrónico almacenados en sistemas de la Corporación deben conservarse por el tiempo que sea necesario para cumplir con los requisitos legales, sectoriales y los propios de la actividad de la Corporación.

El Jefe de la División de Sistemas es la encargada de guardar, almacenar y administrar todo tipo de software de uso en COMFASUCRE, (Sistemas Operativos, Aplicaciones, Instaladores, etc)

23.9. Recopilación de pruebas

La Corporación denunciará con todo el peso de la ley, a quienes incurran en delitos informáticos, de acuerdo con la Ley 1273 de enero de 2009. Se debe asegurar la recolección y protección adecuada de las respectivas evidencias.

24. SANCIONES POR INCUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

24.1. Funcionarios de COMFASUCRE

El incumplimiento de la presente Directiva, después de las investigaciones y comprobaciones pertinentes, será considerado como falta grave de acuerdo a lo dispuesto por reglamento interno de trabajo de COMFASUCRE y de conformidad con las leyes y demás regulaciones legales y contractuales vigentes.

El propietario de la clave de acceso será también responsable por la utilización de la misma por un tercero que incumpla lo especificado en la presente directiva de Seguridad de Información y se aplicará la misma sanción detallada en el numeral anterior.

24.2. Terceros

El incumplimiento de la presente Directiva acarreará responsabilidad civil y/o penal contra las personas naturales o jurídicas que presten servicios bajo cualquier modalidad de contratación.

Lo señalado en el numeral anterior será de aplicación para las personas que en razón de sus funciones y cargo, desempeñen labores en COMFASUCRE.

NOTA: Este manual es una referencia para la implementación del Sistema de Seguridad de la información.

ELABORÓ	REVISÓ	APROBÓ
DANNY BUELVAS VELILLA	**CARLOS HERNANDEZ TORRES**	**AHMED CHADID ESTRADA**
Auxiliar Administrativo	*Jefe de Oficina de Calidad*	*Jefe de División Sistemas*
ANGELICA VERGARA MARRUGO	**DIANA CAROLINA ORTEGÓN LANCHEROS**	
Asistente Calidad	*Asesora de Calidad*	