RESUMEN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN COIMPRESORES

A continuación, se definen las políticas de seguridad de la información que deben de cumplir todos los Colaboradores de COIMPRESORES como parte del compromiso con el Sistema de Gestión de Seguridad de la Información.

1 OBJETIVO DEL MANUAL

Establecer los criterios que deben seguir los colaboradores de Coimpresores con el fin de regular la seguridad de la información

2 ALCANCE DEL MANUAL

Este documento describe las políticas de seguridad de la información definidas por Coimpresores para la elaboración de este se toman como base las leyes dictadas por los entes de control y el estado colombiano, además la NTC-ISO-IEC 27001:2013 y las recomendaciones del estándar ISO 27002:2013. Este manual cubre todos los aspectos administrativos y de control que deben ser cumplidos por los Colaboradores de COIMPRESORES

3 DEFINICIONES

Ver ANEXO 1 MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se definen las políticas de seguridad de la información que deben de cumplir todos los Colaboradores de COIMPRESORES como parte del compromiso con el Sistema de Gestión de Seguridad de la Información.

4.1POLÍTICA PARA DISPOSITIVOS MÓVILES

-En Coimpresores esta permitido el ingreso de dispositivos móviles personales, aparte de los que están autorizados por ser directamente de la cooperativa, los celulares de los empleados no tienen acceso a ningún aplicativo con el cual se pueda sustraer información de la cooperativa ya que se maneja un segmento de red diferente a la red LAN

4.2 POLÍTICA DE TELETRABAJO

-Toda sesión de teletrabajo se realizará el acceso después de recibir el requerimiento con la autorización del jefe inmediato. Se instalará la respectiva VPN, las conexiones se realizan en equipos propiedad de Coimpresores que manejan una seguridad de dominio lo cual no permite la

instalación de otros programas aduanales que puedan burlar la seguridad, en la conexión con la red de la cooperativa se anula el acceso a internet del equipo local, con lo cual el desarrollo de las actividades esta garantizando que no se traslade información al equipo local

4.3 POLÍTICA DE CONTROL DE ACCESO

-En COIMPRESORES se protegen los accesos tanto físicos como lógicos con el fin de asegurar la confidencialidad, integridad y disponibilidad de los activos de información acorde con los criterios de clasificación establecidos y los lineamientos para gestionar los accesos tanto a los activos de información (físicos y lógicos) como a los activos tipo instalaciones de procesamiento de información (físicos y lógicos) y periféricos.

VER ANEXO 1 - MANUAL E INSTRUCTIVO PARA LA GESTION DE LOS USUARIOS EN EL SISTEMA SIESA ENTERPRISE

4.3.1 GESTIÓN DE ACCESO DE USUARIOS

-Todas las contraseñas asignadas deben mantenerse en secreto y no se pueden compartir con ningún colaborador, las políticas de cmabio de contraseña están configuradas en el directorio activo, para el caso de siesa el primer ingreso solicita cambio de contraseña, si un usuario ingresa una clave incorrecta el sistema siesa bloquea el acceso, la cuentas tienen una asignación dependiendo de sus funciones, cuando un funcionario sale de la cooperativa el usuario es deshabilitado inmediatamente, para el tema de vacaciones desde gestión humana se realiza la notificación para identificar que usuario remplazara las funciones de la persona que disfrutara su periodo de vacaciones.

4.3.2 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA (RESPONSABILIDAD DE LOS USUARIOS)

-Cada usuario es responsable de salvaguardar sus credenciales, no esta permitido guardar las contraseñas en medios físicos los cuales puedan ser fácilmente vulnerados, se recomienda no utilizar datos personales o familiares que sean fácilmente de identificar, las contraseñas deben ser estructuradas con las siguientes características: uso de mayúsculas, minúsculas, números, caracteres especiales y longitud entre ocho (8) y doce (12) dígitos.

4.3.3 USO DE CONTRASEÑAS

Los usuarios de la red deben de ser conscientes de sus responsabilidades en el uso de las contraseñas, no pueden ser compartidas con otro usuario, realizar el cambio de la contraseña en caso de sospechar que alguien logro identificarla, desde la parte administrativa las contraseñas ninguna tiene el check de que nuca expira, el incumplimiento de las reglas establecidas con el uso de la información

4.3.4 ELIMINACIÓN DE ACCESO LÓGICO

-Cuando un usuario es retirado o renuncia a la cooperativa, la persona encargada de recursos humanos debe aplicar el procedimiento establecido para estas situaciones, en este proceso el área de sistemas cuando recibe la notificación debe negar todos los accesos con el propósito que no pueda acceder a los aplicativos que consultaba y eran su herramienta de trabajo,

4.3.5 a partir de dicha fecha, se revoque todo permiso de acceso se verificaran accesos remotos (vpn – correo electrónico – acceso al directorio activo – puntos de impresión – ERP Siesa Enterprise).

4.3.6 REVISIÓN DE LOS DERECHOS DE ACCESO

-De igual forma, el área responsable de la administración de usuarios de COIMPRESORES deberá realizar una revisión anual de privilegios y derechos de los usuarios, a fin de identificar cambios o cancelación de estos. Cualquier cambio en las funciones de una persona que acceda a información de la entidad, deberá verse reflejado en sus privilegios de acceso.

-Los lineamientos que deberá cumplir esta actividad son:

-Revisar los derechos de acceso en intervalos regulares no mayor a un año.

-Revisar los derechos de acceso después de cualquier cambio mayor en la organización.

-Los privilegios especiales deberán ser revisados en intervalos no mayores un año.

○ Involucrar al dueño del sistema y de la información para validar los resultados de la revisión.

4.3.7REVISIÓN DE LA ENTIDAD PARA EL CONTROL DE ACCESO

-Todos los Colaboradores que laboran en COIMPRESORES, incluso terceros, deberán tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la organización.

-El acceso otorgado a terceros debe ocurrir sólo como resultado de una clara solicitud sustentable de negocios y antes debe haberse firmado un acuerdo de confidencialidad. Las cuentas de acceso a terceros deben tener especificado un tiempo de expiración.

-COIMPRESORES se reserva el derecho a suspender o cancelar las facultades de acceso a cualquier persona que represente riesgo en la confidencialidad, integridad o disponibilidad de la información.

-Cualquier intento de acceso no autorizado a los equipos, sistemas e información de COIMPRESORES será considerado un incidente grave, por lo que debe reportarse de inmediato a la Direccion de Tecnología y a la Gerencia General.

4.3.8 ACCESO REMOTO

En caso de conexiones de tipo remoto deben existir mecanismos robustos de autenticación y transmisión segura de datos. Este servicio debe ser restringido solo a usuarios autorizados, específicamente a los recursos que requieran para el cumplimiento de los requerimientos del negocio, aplicando el principio de “mínimo privilegio”.

Todas las conexiones remotas que requieren acceso a la red interna de COIMPRESORES deben pasar forzosamente por un firewall (SOPHOS XG), el cual proporciona a las redes internas un nivel de seguridad acorde a la sensibilidad de los sistemas, aplicaciones e información disponible en ella.

4.3.9 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS

Se debe restringir y controlar estrechamente el uso de los Software Utilitarios que poseen la capacidad de sobrepasar (anular o evitar) los controles de acceso a los sistemas y aplicaciones. Debe existir un procedimiento de identificación, autenticación y autorización para este tipo de Software, además se debe asegurar que:

• Exista una segregación entre los Sistemas en producción y los Software utilitarios

• Existe un límite en el uso de software utilitarios a un número mínimo y práctico de funcionarios autorizados expresamente por el Gerente o el director de Tecnología.

4.3.10. CONTROL DE ACCESO A CÓDIGO FUENTE DE PROGRAMAS

Se debe restringir el acceso al código fuente de las aplicaciones de Software.

4.4 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

-Acorde con la estrategia de COIMPRESORES y en línea con la Política General de Seguridad de la Información, se debe proteger la información Confidencial del negocio relacionado a la INFORMACION RELACIONADA CON EL CORD DEL NEGOCIO. Teniendo en cuenta los principios mencionados en el control A 10.1.1 se debe proteger la confidencialidad, autenticidad e integridad de la información

-COIMPRESORES debe determinar los algoritmos y protocolos autorizados para su uso en la organización y configurar los sistemas para permitir únicamente aquellos que no representen un riesgo.

4.5 POLÍTICA DE GESTIÓN DE LLAVES

-La administración de llaves criptográficas y certificados digitales estará a cargo de cada uno de los Colaboradores o contratistas a quienes les fueron asignados para el desempeño de sus labores sean tokens, firmas digitales o información de autenticación o validación.

-Las llaves criptográficas serán cambiadas periódicamente, de acuerdo con lo definido por el responsable o cada vez que se sospeche que han perdido su confidencialidad.

-La administración de llaves criptográficas y certificados digitales estará a cargo de acuerdo con lo definido por COIMPRESORES. Sin embargo, la administración de tokens, firmas digitales o información de autenticación o validación estarán a cargo de cada uno de los colaboradores o contratistas a quienes les fueron asignados para el desempeño de sus labores.

4.6 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

-Del escritorio se deben retirar la información que sea confidencial o delicada la cual pueda ser robada o copiada sin autorización tanto como digital y físico para los casos que aplique en las instalaciones de la cooperativa, en caso de hacer uso de hojas recicladas revisar que la información no tenga datos confidenciales, los usuarios al retirarse del equipo deben realizar el bloqueo o cierre de sesión de cada usuario , los puestos de trabajo deben permanecer limpios y ordenados, libres de comida y obstrucciones de ventilaciones, ubicaciones inadecuadas entre otros que pongan en riesgo los dispositivos.

4.7 POLÍTICA DE RESPALDO DE LA INFORMACIÓN

-Dentro de las políticas de respaldo de la información los colaboradores tienen asignados unas carpetas asignadas en el servidor en el cual son almacenados los archivos que son de suma importancia para el área o los procesos, los discos locales no se les realiza copia de seguridad porque para esto esta diseñado este procedimiento con las unidades de red, la información personal almacenada no es copiada y no se hace responsable la cooperativa por perdida de la misma, las copias de seguridad se deben verificar semestralmente para asegurar su funcionamiento y plena confiabilidad del proceso.

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

4.8 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

-Los Colaboradores de COIMPRESORES que requieran transferir externamente información de uso interno e información confidencial, deben contar con un acuerdo de confidencialidad firmado y adicionalmente, se debe contar con la autorización previa del jefe Inmediato.

Dicha información para transferir debe ser almacenada en los medios aprobados por COIMPRESORES para tal fin.

-Los Colaboradores deben seguir las indicaciones del área de tecnología el cual dará las directrices a tener en cuenta al momento de intercambiar información clasificada como de uso interno y confidencial.

-La transferencia o intercambio de información con entes de control y autoridades de supervisión, se rige por las directrices y mecanismos que dispongan dichos entes de control.

-Las herramientas de cifrado de información son definidas por el área de IT y el área de soporte.

-Las herramientas autorizadas para gestionar comunicación de equipos de trabajo y transferencia de información son las estrictamente autorizadas por COIMPRESORES.

4.9 POLÍTICA DE DESARROLLO SEGURO

-Los desarrollos que se realizan para la cooperativa cuentan con ciertos controles con los cuales se velen por la seguridad de la información, COIMPRESORES debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios, cuando sea necesario.

Se deben aprobar las migraciones entre los ambientes de pruebas y producción de los desarrollos nuevos y/o de cambios o nuevas funcionalidades, la seguridad manejada debe ser estricta y Los desarrolladores de COIMPRESORES y proveedores de software, deben asegurar que los desarrollos construidos no puedan cambiar la estructura de la base de datos desde el código fuente de dicha aplicación

4.10 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES

Coimpresores define mecanismos de control en las relaciones con los proveedores y contratistas en cuanto al intercambio de información en ambas vías cumpla con las exigencias institucionales definidas con base en las regulaciones y exigencias en la presente política, están en la obligación de realizar la notificación de cualquier incidente que afecte la confidencialidad, integridad y disponibilidad de los activos de información que ponga en riesgo la operación, cuando hay conexiones externas se deben firmar acuerdos de confidencialidad o debe incluirse una cláusula de confidencialidad al correspondiente contrato con el fin de proteger dicha información.

la prestación de sus servicios a COIMPRESORES gestionen, transformen o transmitan información de COIMPRESORES deben conocer, aceptar y cumplir las políticas de seguridad de la información definidas por el Sistema de Gestión de Seguridad de la Información. En caso de conflicto entre las políticas de seguridad de la Información de COIMPRESORES y las políticas de seguridad de los proveedores o terceros se acordarán políticas comunes de seguridad de la información y estas se formalizarán mediante un documento formal suscrito por un representante de ambas partes, que permitan cumplir los requisitos necesarios para garantizar la protección de la confidencialidad, integridad y disponibilidad de la información.

El acceso a cualquier tipo de información al finalizar los contratos los proveedores o terceros deben cumplir con la reglamentación y realizar la devolución de información o activos de propiedad de Coimpresores que estuvieron en su responsabilidad.

Los terceros son responsables del buen uso de las credenciales de acceso asignadas. Los terceros no deben utilizar ninguna estructura o característica de contraseña genérica o de fácil deducción, incluyendo entre otras las palabras de diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales, entre otros.

5 POLÍTICAS COMPLEMENTARIAS

5.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.1.1 ROLES Y RESPONSABILIDADES

Toda persona que acceda a la información de Coimpresores es responsable de contribuir a la seguridad de su información. El área de TI de la cooperativa asumirá el desarrollo y el cumplimiento de las políticas de seguridad de la información, en caso de necesitarse se realizarán asesoría a quien maneje la información y se notificara sobre este proceso

5.1.2 SEPARACIÓN DE FUNCIONES

Todo aquel con permisos de acceder a la información de Coimpresores deberá tener claramente definido sus responsabilidades para evitar el abuso de derechos y privilegios de acceso. Siempre los aplicativos deberán contar con un super usuario que monitorea la información y los logs con transacciones que realizan los otros usuarios.

5.1.3 CONTACTO CON LAS AUTORIDADES

COIMPRESORES establece y mantiene contacto actualizado de las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes a la seguridad de la información.

5.1.4 CONTACTO CON GRUPOS DE INTERÉS

COIMPRESORES establece y mantiene contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información y expertos en seguridad de las plataformas implementadas en la organización. Lo anterior con el fin de estar al día con las últimas tendencias de protección de la información, recibir advertencias de actualizaciones, ataques, vulnerabilidades, acceder a asesoría especializada, compartir e intercambiar información acerca de seguridad de la información.

5.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

Independientemente del proyecto que Coimpresores de Colombia este planificando o ejecutando deberá integrar la seguridad de la información para tratar como parte del proyecto garantizar en cada una de sus fases y seguir las siguientes directrices

○ Incluir objetivos o requisitos de seguridad de la información en la planeación del proyecto.

○ Realizar identificación y valoración de los riesgos de seguridad de la información en la planeación y ejecución del proyecto.

○ Realizar seguimiento a los riesgos de seguridad de la información identificados y a los controles aplicados para tratar los mismos, durante las diferentes etapas del proyecto.

○ Evaluar y medir el cumplimiento de la seguridad de la información respecto a sus objetivos o requisitos definidos.

5.1.6 SEGURIDAD DE LOS RECURSOS HUMANOS

COIMPRESORES establece controles antes, durante y después de la terminación o cambio de empleo, de tal forma que se preserven los criterios de seguridad de la información de la Compañía y de sus partes interesadas.

5.1.7ANTES DE ASUMIR EL EMPLEO

Toda vinculación laboral realizada por COIMPRESORES se rige por las leyes de Colombia y por lo dispuesto por Recursos Humanos.

5.1.8TERMINOS Y CONDICIONES DEL EMPLEO O CONTRATO

-Todos los Colaboradores, contratistas y terceros que presten sus servicios a COIMPRESORES deben tomar conciencia de la seguridad de la información.

-Todos los colaboradores deben mejorar continuamente sus competencias en seguridad de la información y para ellos COIMPRESORES establecerá en las inducciones al momento de ingresar por parte del área de tecnología la trasferencia de conocimiento.

-Tanto los contratistas como los terceros están obligados a fortalecer sus competencias para poder realizar sus actividades acordes con lo que la compañía requiera en materia de seguridad de la información.

-Todos los Colaboradores, contratistas y terceros, están en la obligación de leer periódicamente las políticas de seguridad de la información (mínimo cada 12 meses o cada vez que se informe que han sido actualizadas).

-Todo el recurso humano que tenga la responsabilidad de obedecer y/o aplicar los controles que COIMPRESORES establezca para proteger la seguridad de la información debe tomar conciencia de la importancia que tiene su contribución con la protección de la información y debe tener claro que debe implementar los controles incluso cuando no lo estén viendo o vigilando.

-Todos los Colaboradores, Contratistas y Terceros de COIMPRESORES, se deberán acoger a las políticas y procedimientos de seguridad de la información establecidos, así como la os términos de uso adecuado de los activos de información que le son entregados, previo a la entrega de éstos y teniendo en cuenta que estos términos y responsabilidades son extensibles fuera de la organización.

-Todos los Colaboradores, Contratistas y Terceros que tengan acceso a la información e infraestructura Confidencial de COIMPRESORES, deberán firmar previo a la entrega del acceso, un acuerdo DE CONFIDENCIALIDAD

5.1.9 DURANTE LA EJECUCIÓN DEL EMPLEO O CONTRATO

- COIMPRESORES a través del proceso de recursos humanos asegura que todos los Colaboradores y Contratistas que tengan definidas responsabilidades en el área de seguridad de la información sean competentes para desempeñar sus funciones y que cuentan con los programas de capacitación y entrenamiento requeridos para tal fin.

-Asimismo, todos los Colaboradores, Contratistas y Terceros con acceso a los activos de información, tendrán un proceso formal de concientización, a través del cual se socializarán las políticas de seguridad de la información y los riesgos conocidos a los que se pueden ver expuestos.

-Los procesos disciplinarios serán adelantados por Recursos Humanos

5.1.10 TERMINACIÓN O CAMBIO DE ROL

Recursos humanos deberá informar del retiro de un colaborador para realizar la inhabilitación de todos los accesos físicos y lógicos a los aplicativos adema de realizar la verificación de la entrega d ellos activos que tenga en su poder. No habrá excepciones con ningún funcionario esto con el fin de preservar la información de la empresa. Con esta rigurosidad se garantiza la entrega de la información de la cooperativa.

5.2 GESTIÓN DE ACTIVOS

COIMPRESORES mantiene y constata a través de la plataforma GLPI el estado y asignación de los activos dispuestos a cada uno de los colaboradores para el desarrollo de sus funciones si así lo amerita el rol asignado por la compañía y hace constante mantenimiento de dicha plataforma de acuerdo con los movimientos que se vayan presentando en la marcha de las actividades.

5.2.1 INVENTARIO DE ACTIVOS

El inventario tecnológico de la Cooperativa es controlado en GLPI, donde se encuentra un registro profundo de asignaciones y cambios realizados en los activos

5.2.2USO ACEPTABLE DE LOS ACTIVOS

Los activos de información de la cooperativa solamente pueden ser utilizados con fines de ejecutar las labores asignadas

Los activos de información deben de salvaguardarse según su nivel de criticidad

La información Física y digital, y cualquier bien tangible y no tangible que tenga la cooperativa y son asignados a los usuarios deben darle un uso adecuado.

Todos los colaboradores son responsables de etiquetar la información y darle un manejo adecuado siguiendo las directrices de la metodología de gestión de activos.

Los Colaboradores deben reportar los eventos que vulneren la seguridad en los activos de la información.

Los dueños o propietarios de los activos de información deben mantener actualizado el sistema de gestión de seguridad el inventario de sus activos para su clasificación correspondiente.

Los activos de información solamente pueden ser utilizados a fines de satisfacer necesidades de negocios con el objetivo de ejecutar tareas vinculadas con la organización.

5.2.3 USO DE EQUIPOS DE CÓMPUTO PERSONAL DE ESCRITORIO Y PORTÁTILES

El Área de IT es la única autoridad para dar de baja cualquier elemento de hardware propiedad de Coimpresores después de haber verificado que no hay vulnerabilidades de la información.

NO se puede realizar algún cambio de hardware y Software, estos cambios deben ser informados y gestionados por GLPI para dicha autorización.

Se prohíbe el uso de medios extraíbles para almacenamiento de información de la cooperativa.

Toda Actividad informática no autorizada que afecte la red o sistemas de información de la cooperativa tendrá procesos disciplinarios y legales si corresponde.

Es responsabilidad de todos los Colaboradores de COIMPRESORES, apagar o hibernar los equipos que no estén prestando servicio al finalizar la jornada laboral.

Los equipos de cómputo, teléfonos, servidores entre otros deben siempre ir en las tomas de color naranja o con energía regulada.

Los equipos externos deben ir en las tomas de energía no regulada y la cooperativa no se hace responsable por daños sufridos sobre estos equipos.

La seguridad física e integridad de los equipos que ingresen en la cooperativa que no son activos, son responsabilidad del usuario y no hay responsabilidad de ningún tipo por estos equipos.

5.2.4 USO DE LA INTRANET Y DE INTERNET

Solo se puede acceder a internet bajo las redes de la cooperativa, el uso de otros dispositivos que brinden acceso a internet no esta permitido

La cooperativa puede bloquear el acceso a determinadas paginas el cual afecten el desempeño o la red de la cooperativa.

El usuario debe tener presente siempre la información que reciba de sitios no seguros, para realizar la respectiva verificación y no realizar acciones hasta tener verificada la fuente.

El área de TI esta encargada de mitigar todos los riesgos en la navegación de internet, así mismo promover estas buenas practicas

En COIMPRESORES, está prohibido el uso de la infraestructura tecnológica para fines comerciales, o algún tipo de acoso, difamación o calumnia.

Esta prohibido ejecutar cualquier herramienta para realizar monitoreo de puertos o cualquier tráfico de red.

Los proveedores contratados externos realizaran monitoreo de la RED después de la respectiva autorización de la cooperativa

5.2.5 USO DEL CORREO ELECTRÓNICO

El uso del correo para utilizar por los colaboradores es el autorizado por la cooperativa con el dominio de la empresa

La cuenta de correo electrónico institucional es personal e intransferible y por ende y la responsabilidad es netamente del funcionario.

El correo electrónico institucional se debe utilizar estrictamente como comunicaciones de información competente a la compañía y no una herramienta de difusión masiva de información, no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.

Toda información compartida en el correo electrónico debe llevar un texto que prevenga sobre la posibilidad de ser información confidencial y al tratamiento permitido cuando es recibida por alguien que no es su destinatario.

Los correos electrónicos sospechosos deben tratarse con extremo cuidado, debido a los riesgos de seguridad de la información inherentes. Por lo tanto, no está permitido abrir sus archivos adjuntos y se debe reportar el evento de acuerdo con el Procedimiento de Gestión de Incidentes.

5.2.6 DEVOLUCIÓN DE ACTIVOS

La devolución de los activos se realiza de manera conjunta entre las áreas de IT y Recursos Humanos.

El proceso de retiro de activos debe tener asignado un proceso de autorización para aquellos activos que no son del custodio oficial según el inventario de activos de información.

Los equipos que han sido asignados a los colaboradores de COIMPRESORES y que están relacionados en el inventario de activos tipo Hardware, no requieren autorización.

5.2.7 CLASIFICACIÓN DE LA INFORMACIÓN

Coimpresores clasifica y etiqueta la información y sus activos asociados de acuerdo con a la metodología de gestión de los activos de información

5.2.8 GESTIÓN DE MEDIOS REMOVIBLES (UNIDADES DE ALMACENAMIENTO)

En Coimpresores no esta permitido el uso de medios removibles.

Los activos tipo instalaciones de procesamiento de información como dispositivos móviles medios removibles y computadores portátiles pueden salir de la cooperativa con previa autorización.

Los equipos portátiles están protegidos con contraseña en la BIOS para evitar modificaciones de acceso al inicio.

Los medios removibles en los que se almacene información catalogada como información de uso interno e información confidencial deben estar cifrada.

5.2.9 TRANSFERENCIA DE MEDIOS FÍSICOS

La cooperativa No realizara transporte ni transferencia de medios físicos a través de servicios de mensajería, ni tampoco está permitido el transporte a otras locaciones de los medios removibles que contienen firma, ni certificados digitales.

5.3 SEGURIDAD FÍSICA Y DEL ENTORNO

5.3.1 PERÍMETRO DE SEGURIDAD FÍSICA

Los perímetros de seguridad se deben encontrar definidos al igual que sus controles de acceso físico.

El perímetro de la oficina de Coimpresores debe contener todos los recursos necesarios para tratar la información ofreciéndole cierta solidez física.

Se debe realizar la instalación de un área de recepción manual y otros medios de acceso evitando entradas no autorizadas.

Se puede instalar Sistemas de Gestión de Seguridad de la Información adecuado a la detección de intrusos de acuerdo con los estándares regionales, nacionales o internacionales.

El ingreso a áreas restringidas se debe llevar control de acceso con hora de ingreso y salida.

Las visitas tienen acceso para propósitos muy específicos y se autorizan generando instrucciones sobre los requisitos de seguridad y procedimientos en caso de emergencias.

El control del personal autorizado a la información de la cooperativa, se pueden utilizar varios métodos como lo son tarjetas personales o registros físicos.

Se pueden exigir al personal que porte de forma visible la identificación.

Se debe garantizar el acceso a restringido de terceras partes hacia las áreas de seguridad y el acceso a manejo de información confidencial.

Se debe revisar y actualizar de forma regular los derechos de acceso a las áreas de seguridad.

5.3.2 ACCESO FÍSICO A LAS ÁREAS SEGURAS

Las áreas destinadas para el procesamiento o almacenamiento de la información confidencial y de uso interno, se consideran áreas de acceso restringido por lo cual deben contar con controles y procedimientos de acceso que protejan la información

Los controles para prevenir el acceso físico no autorizado a las instalaciones de COIMPRESORES, son descritos en el Procedimiento de Trabajo en Áreas Seguras.

El acceso de visitantes a las áreas restringidas, como son Datacenter, cuartos de control, de cableado, de comunicaciones, telefónicos etc., debe contar con un procedimiento o protocolo de acceso físico aprobado por COIMPRESORES.

El acceso a áreas seguras se deberá conceder únicamente por motivos específicos y autorizados.

Coimpresores debe asegurar que las áreas de acceso restringido como son datacenter, cuantos de control, etc. Cuenten con todos los implementos de control de acceso, protección ambiental y de regulaciones eléctricas.

Los accesos de tipo permanente deben ser asignados por el responsable de accesos a aquel personal que lo requiera

Los accesos de tipo temporal por ejemplo proveedores externos, contratistas deben solicitarse con antelación con la verificación de datos personales, además de contar con continua supervisión de un funcionario de la cooperativa y dejar el registro en la bitácora correspondiente.

5.3.3 PROTECCIÓN CONTRA AMENAZAS EXTERNAS E INTERNAS

En lo posible debe haber una protección contra fuego, inundación, terremoto, etc o desastres causados por el hombre.

Tener consideración por los daños que puedan causar los vecinos con los riesgos anteriormente mencionados.

Se deben prever las fallas de energía y otras interrupciones causadas por fallas de suministro.

5.4 SEGURIDAD DE LAS OPERACIONES

COIMPRESORES debe asegurar mediante la documentación de las operaciones su correcto funcionamiento y procesamiento.

5.4.1 POLÍTICA DE GESTIÓN DE CAMBIOS

Todos los cambios realizados en los activos de información tecnológicos y los recursos informáticos deben tener un registro cuando se realicen estos cambios autorizados

El área de TI y la cooperativa deberán garantizar que todos los cambios realizados en la plataforma quedasen formalmente documentados desde la implementación hasta el cumplimiento.

5.4.2 POLÍTICA DE GESTIÓN DE LA CAPACIDAD

La cooperativa debe asegurar que los servicios y recursos de TI se vean respaldados por una capacidad de procesamiento y almacenamiento que garantice que los clientes y usuarios puedan desempeñar de manera eficiente sus tareas

5.4.3 POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO

Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos

Toda la infraestructura de procesamiento de información de Coimpresores cuenta con barreras contra la detección de intrusos y virus que pongan en riesgo la información

Está restringida la ejecución de código móvil aplicando políticas en sistemas operativos, navegadores y control de navegación.

Todos los funcionarios, colaboradores y terceros que utilizan la información y servicios de comunicación son responsables del manejo como primera instancia del antivirus.

Se debe mantener en las ultimas actualizaciones todas las herramientas de prevención y control de la seguridad tanto del lado del cliente y de los servidores.

5.4.4 SEPARACIÓN DE LOS ENTORNOS

Para todos los sistemas que constituyan la infraestructura tecnológica que soportan los procesos críticos de negocio:

Contar con ambientes separados para desarrollo, pruebas y producción.

Definir, en el marco de la política de gestión de cambios, un procedimiento formal para la gestión de estos.

Los pasajes a producción deben estar alineados con la política y procedimiento de gestión de cambios.

Los cambios siempre deben ser probados y aceptados.

Los ambientes deben contar con los mismos sistemas o herramientas provistas por terceras partes y ser homologados al menos en ambientes de pruebas y producción para que se puedan realizar los controles pertinentes.

El ambiente de pruebas debe estar completamente identificado del ambiente real.

El personal que realizara las pruebas debe tener y realizar los procesos con cuentas diferentes a las del ambiente real para realizar las verificaciones.

5.4.5 POLÍTICA DE REGISTRO Y SEGUIMIENTO DE EVENTOS

COIMPRESORES debe elaborar, preservar y revisar los registros de actividades (logs) de los usuarios de los sistemas.

Los usuarios NO están autorizados y no tienen la opción de eliminar registros de sus actividades y debe haber siempre controles para evitar estas practicas por parte de los usuarios.

El acceso a los registros es restringido, por lo cual su consulta por usuarios se debe realizar con previa autorización.

Los eventos implicados en seguridad de la información son registrados en el GLPI

5.4.6 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

COIMPRESORES controla la instalación de software en sistemas operativos por medio de la seguridad asignada en el directorio activo.

Todo software debe contar con soporte técnico que garantice el funcionamiento eficiente y no se pueda ver afectado el funcionamiento de la cooperativa.

Se debe proporcionar la capacitación adecuada a los usuarios y al personal técnico en aspectos de operación y funcionalidad de nuevos sistemas de información antes de su puesta en marcha.

Todos los sistemas nuevos y que tengan mejoras deben contar con su respectiva documentación y no pueden salir a producción sin antes contar con este documento.

5.4.7 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

Los correctivos que requieran ser aplicados en las plataformas tecnológicas derivados de la identificación de vulnerabilidades técnicas son responsabilidad de la cooperativa en el caso que se requieran realizar cambios en las plataformas tecnológicas deben seguirse las directivas de control de cambio.

5.5 SEGURIDAD DE LAS COMUNICACIONES

COIMPRESORES debe establecer los controles necesarios para proteger la información transportada desde la red interna.

5.5.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES

Se deben establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

Coimpresores debe proporcionar a todas las personas los recursos tecnológicos de conectividad para que puedan desempeñar las funciones y actividades laborales.

5.5.1.1 RED CABLEADA

La cooperativa debe instalar y mantener con personal calificado y debidamente autorizado la red de voz y datos con el fin de garantizar la operación.

Cualquier equipo o elemento activo o pasivo de la red que no se utilice debe ser desactivado y controlado. No está autorizado la instalación a un equipo diferente a los de la cooperativa

No está permitido realizar ningún trafico de red a personal no autorizado por la cooperativa.

El cableado de energía eléctrica y de telecomunicaciones debe tener una protección contra interferencias o daños.

5.5.1.2 SEPARACIÓN DE LAS REDES

Las redes están segregadas para controlar el acceso, tener control, integridad y confidencialidad de la información

Se deben definir y seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red

Se deben establecer parámetros técnicos para la conexión seguros de la red con los servicios de red

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

Se deben separar las redes inalámbricas de las redes internas para garantizar los principios de la seguridad de la información.

5.6 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Los requerimientos de seguridad de la información deben ser identificados y acordados por los responsables de los procesos Y/O usuario del desarrollo, deben estar documentados para tener evidencia.

Los responsables de los procesos son los encargados de la adquisición de software conociendo las necesidades expresas.

Los responsables de áreas y procesos deben seleccionar las metodologías para adquisición y desarrollo software que tengan en consideración los siguientes aspectos:

Control de acceso a la información, definición, y autenticación de usuarios mecanismos de detención de intrusos, cifrado de datos, roles, perfiles que permitan controlar la seguridad de la información.

Los responsables de áreas y procesos junto con los administradores de sistemas de información deben considerar en el desarrollo y adquisición de aplicaciones los controles respectivos desde la entrada hasta la salida del procesamiento de los datos. Se deben considerar controles que permitan el seguimiento al registro de las actividades en el software. En caso de contar con contratistas extranjeros se deben verificar derechos de propiedad intelectual y confidencialidad.

Se debe realizar mantenimiento periódicamente a los sistemas para garantizar el funcionamiento.

5.7 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Cualquier colaborador, contratista, tercero puede reportar incidentes de seguridad de la información que afecten a COIMPRESORES.

Cada responsable de área o proceso debe identificar los eventos y/o incidentes de seguridad de la información a través de supervisión proactiva de los sistemas de información y tecnología de COIMPRESORES.

Cualquier dispositivo de uso personal que estén implicados en incidentes de seguridad pueden ser sometidos a cadena de custodia o protección para fines de investigación o evidencia ante procesos administrativos o legales con el propietario del dispositivo.

Para prevenir algún incidente de seguridad la cooperativa aplicara los procedimientos del sistema de gestión de seguridad para llevar a cabo las actividades pertinentes que ayuden a mitigar las posibles fallas

En caso de ser requerido por la autoridad competente o grupos especializados para el tratamiento de datos personalizados, la cooperativa puede suministrar el plan de respuesta o remediación especifico para un incidente para evaluar la efectividad.

Una persona que evidencie la materialización de un incidente de seguridad debe notificarlo al director de tecnología utilizando los canales definidos dependiendo de la criticidad del incidente y serán tratados con la debida reserva.

5.8 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

Coimpresores asegura la continuidad de la seguridad de la información en la planificación e implementación de la continuidad del servicio de facturación electrónica donde están involucrados activos, talento humano, proveedores y otros procesos críticos

La cooperativa tendrá documentado procesos, procedimientos y controles que respalden la seguridad de la información en alguna contingencia.

Para Verificar los controles de continuidad y seguridad de la información se realizarán controles regulados para verificar la efectividad.

Para asegurar la disponibilidad y la redundancia de la información la cooperativa cuenta con un plan de recuperación de desastres, con pruebas anuales para verificar la eficacia del plan.

5.9 CUMPLIMIENTO

COIMPRESORES vela por el cumplimiento de la presente política y la legislación aplicable vigente por los entes de control.

La gerencia general, la dirección de tecnología implementan los controles necesarios para dar cumplimiento y protección a los activos de información mediante los requisitos de seguridad de estos.

La cooperativa se reserva el derecho de monitorear los computadores que sean de su propiedad y estén conectados o no a la red de la compañía en caso de presentarse incidentes que afecten la seguridad de la información.

Los documentos que tengan lineamientos legales deben ser resguardados bajo medidas de seguridad adecuados para garantizar su integridad.

El líder de TI debe verificar cada año los acuerdos de licencia de hardware y software.

Los contratistas y terceras partes deben cumplir con las normas establecidas por la legislación colombiana.

La omisión por parte del personal involucrado en las obligaciones y responsabilidades definidas en esta política es considerada falta grave y por ende conlleva a la toma de medidas pertinentes por la cooperativa.

Desde el punto de vista de cumplimento normativo Coimpresores debe tener presente la ley 1581 de 2012 de protección de datos personales.

El estudio de la normatividad Publicada por organismos del estado inherente a seguridad de la información es una actividad permanente para garantizar la oportuna aplicación

El área de TI y la parte encargada de lo jurídico deben publicar y actualizar la normativa con la seguridad de la información, generar las clausulas de confidencialidad y contratos de acuerdo con los requisitos del SGSI.

Todos los procesos y operaciones de COIMPRESORES deben regirse por la legislación colombiana vigente respecto a seguridad de la información.

Programar revisiones, ANUALES, de cumplimiento de las políticas, normas y directrices.

Programar revisión cada 12 meses de las políticas de Seguridad de la Información por parte de la Gerencia General.

Generar informes que evidencien las revisiones de cumplimiento.

Generar los planes de acción con las correcciones y acciones correctivas necesarias como resultado de las revisiones de cumplimiento.

Implementar las mejoras necesarias con base en los resultados de las revisiones de cumplimiento.

5.9.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

El sistema de gestión de seguridad de la información deberá ser revisado cada 12 meses o cuando surjan actualizaciones o cambios significativos.

El objetivo de la revisión es garantizar que la seguridad de la información se implemente y está operando de acuerdo a las políticas y procedimientos establecidos.

Jesus Maria Torres
Gerente General
Coimpresores De Colombia

Versión 1.1 de Agosto 24 del 2021