MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN COIMPRESORES

Tabla de contenido [Ocultar]

Versión 1.1 de Agosto 24 del 2021

1. OBJETIVO DEL MANUAL

Establecer los criterios y comportamientos que deben seguir todos los Colaboradores de COIMPRESORES (empleados, contratistas, terceros, entre otros) con el fin de regular la gestión de la seguridad de la información al interior de la organización y preservar la confidencialidad, integridad y disponibilidad de los activos de información.

2. ALCANCE DEL MANUAL

Este documento describe las políticas de seguridad de la información definidas por COIMPRESORES. Para la elaboración del mismo, 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 (empleados, contratistas, terceros, entre otros), para conseguir un adecuado nivel de protección de las características de seguridad y la calidad de la información relacionada.

3. DEFINICIONES

Activo de información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020).

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000, 2012).

Auditoría: Inspección formal para verificar si se está siguiendo/cumpliendo un estándar o un conjunto de guías, que sus registros son precisos o que las metas de eficiencia y efectividad se están cumpliendo (Axelos Limited, 2011).

Confidencialidad: Propiedad que determina que la información no se haga disponible ni sea revelada a individuos (ISO/IEC 27000, 2012).

Continuidad del Negocio: Procedimientos y/o procesos para asegurar la continuidad de las operaciones del negocio (ISO/IEC 27000, 2012).

Control: Medios de gestión del riesgo, incluidas las políticas, procedimientos, directrices, prácticas y estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o jurídico (ISO/IEC 27000, 2012).

Copia de seguridad: Copiar los datos para proteger los originales de pérdidas de integridad o disponibilidad (Axelos Limited, 2011).

Disponibilidad: Propiedad de ser accesible y utilizable sobre demanda por los usuarios autorizados (ISO/IEC 27000, 2012).

Evento de seguridad de la información: La ocurrencia de un estado del sistema, servicio o red que indica un posible incumplimiento de la política de seguridad de la información o un fallo de las salvaguardias, o una situación previamente desconocida que puede ser relevante para la seguridad (ISO/IEC 27000, 2012).

Gestión de accesos: Proceso responsable de permitir a los usuarios hacer uso de los servicios de TI, datos u otros activos (Axelos Limited, 2011).

Gestión de activos: Es una actividad genérica o proceso responsable del seguimiento y la notificación del valor y la propiedad de los activos a lo largo de su ciclo de vida (Axelos Limited, 2011).

Gestión de cambios: Proceso responsable del control del ciclo de vida de los cambios, permitiendo la ejecución de los cambios beneficiosos minimizando el impacto en los servicios de TI (Axelos Limited, 2011).

Incidente de seguridad: Evento único o serie de eventos de seguridad de la información inesperada o no deseado que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (ISO/IEC 27000, 2012).

Infraestructura de TI: Todo el hardware, software, redes, instalaciones etc. requeridas para desarrollar, probar, proveer, monitorizar, controlar o soportar aplicaciones y servicios de TI (Axelos Limited, 2011).

Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización (ISO/IEC 27000, 2012).

Integridad: Propiedad de exactitud y completitud de la información (ISO/IEC 27000, 2012).

Internet: El sistema único, interconectado, mundial de redes informáticas comerciales, gubernamentales, educativas y de otro tipo que comparten (a) el conjunto de protocolos especificado por Internet Architecture Board (IAB) y (b) los espacios de

nombres y direcciones administrados por Internet Corporation para Nombres y Números Asignados – ICANN (CSRC, NIST).

Monitoreo: Verificación, supervisión, observación crítica o determinación continua del estado, con el fin de identificar cambios respecto al nivel de desempeño exigido o esperado (ISO/IEC 27000, 2012). Parte interesada: Persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad (ISO/IEC 27000, 2012).

Política: Intención y dirección generales expresadas formalmente por la Dirección (ISO/IEC 27000, 2012).

Procedimiento: Manera especificada de llevar a cabo una actividad o un proceso (ISO/IEC 27000, 2012).

Prueba: Una actividad que verifica que un elemento de configuración, servicio de TI, proceso, etc. cumple con sus especificaciones o requerimientos acordados (Axelos Limited, 2011).

Revisión: Actividad emprendida para determinar la idoneidad, adecuación y efectividad de la materia para alcanzar los objetivos establecidos (ISO/IEC 27000, 2012).

Riesgo: Efecto de la incertidumbre sobre los objetivos (ISO/IEC 27000, 2012).

Servidor: Ordenador que está conectado a la red y que provee funciones de software que son usadas por otros ordenadores (Axelos Limited, 2011).

Seguridad de la información: Preservación de confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27000, 2012).

SSL – Secure Sockets Layer: En español capa de sockets seguros, mecanismo criptográfico para la seguridad en la capa de transporte.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas (ISO/IEC 27000, 2012).

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.

4.1. POLÍTICA PARA DISPOSITIVOS MÓVILES

Dando cumplimiento al numeral A.6.2.1 de la Norma NTC-ISO-IEC 27001:2013, el cual nos indica que se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. A continuación, se despliegan las políticas establecidas por COIMPRESORES para dispositivos móviles.

a. En COIMPRESORES se permite el ingreso de dispositivos móviles personales al interior de las instalaciones, sin embargo, existen unas reglas para el uso de los mismos, de modo que se minimice el riesgo de comprometer la información.

b. Existen tres tipos de dispositivos móviles que pueden ingresar a COIMPRESORES:
○ Cualquier dispositivo electrónico móvil personal [Dispositivo + Plan de datos Personal].
○ Dispositivos móviles híbridos [Dispositivo personal + Plan de datos Corporativo].
○ Dispositivos móviles corporativos [Celulares asignados por la compañía para los cuales tanto el equipo como el plan de datos es corporativo].

c. No está permitido el acceso, en ningún dispositivo móvil, a los sistemas y aplicaciones corporativas excepto al correo electrónico el cual debe ser utilizado acorde con las políticas de uso de correo electrónico.

d. Cuando se conversan temas laborales mediante dispositivos móviles, los Colaboradores deben tener precaución de no ser víctimas de escuchas intrusivas.

e. Está prohibido el uso de dispositivos móviles como medio de almacenamiento, grabación y captura de imágenes dentro de las instalaciones de COIMPRESORES.

f. No está permitido el uso de dispositivos móviles, en las redes internas de COIMPRESORES, únicamente pueden conectarse a las redes que se encuentren identificadas como "invitados".

g. La red inalámbrica de "invitados", solo debe ser usada por usuarios externos a COIMPRESORES, la cual permite el acceso a Internet con las restricciones que establece la Entidad. No se debe permitir la conexión de usuarios externos a las redes corporativas de COIMPRESORES.

h. Los dispositivos móviles con líneas y datos de COIMPRESORES no deben dejarse desatendidos.

i. En el momento de la entrega del cargo se debe tener en cuenta la asignación/entrega de equipo y/o plan de datos al personal que por sus funciones

así lo requiera y comunicarle las políticas y demás directrices que debe conocer para proteger la información.

j. Bajo ninguna circunstancia se deben prestar los dispositivos móviles a personal ajeno a COIMPRESORES.

k. No se deben utilizar las líneas ni los datos de COIMPRESORES para comunicados con contenidos obscenos, fraudulentos, comunicaciones con contenido que afecte la integridad de las personas o viole los derechos de las mismas, tampoco se deben utilizar las líneas ni los datos de COIMPRESORES para hacer bromas o acciones de burla a las personas.

l. Existe un acuerdo con los Colaboradores para que suministren su equipo para el uso de los datos y línea corporativos, en ese sentido los Colaboradores pueden realizar llamadas, enviar mensajes personales e instalar cualquier aplicación para su uso personal.

m. No se permite la descarga de software/aplicaciones fraudulentas, que no cumplan con derechos de autor o que violen las leyes nacionales como las aplicaciones de grabación de llamadas.

n. Los responsables de áreas y procesos definirán los parámetros técnicos que deben cumplir los dispositivos que serán autorizados .

o. Los responsables de áreas y procesos deben administrar los controles de seguridad de los diferentes dispositivos de modo que se preserve la seguridad de la información tanto de COIMPRESORES como aquella que se ha considerado Confidencial de las partes interesadas. Lo anterior siempre respetando el derecho fundamental a la Intimidad del propietario del dispositivo.

p. El propietario del dispositivo debe aplicar todas las medidas de seguridad razonables que estén a su alcance para preservar la seguridad de la información.

q. Todos los Colaboradores y contratistas de COIMPRESORES son responsables de reportar a la mayor brevedad posible la pérdida o hurto de los equipos y dispositivos móviles usados para Teletrabajo y que se encuentren bajo su responsabilidad.

r. Los responsables de áreas y procesos deben coordinar y gestionar la instalación de controles de seguridad en los equipos y dispositivos.

s. COIMPRESORES se reserva el derecho de monitorear y revisar el cumplimiento de la política para dispositivos móviles conectados a las redes inalámbricas de la Entidad, cuando lo estime conveniente.

t. Los colaboradores de COIMPRESORES, los proveedores o terceros responsables de la prestación de servicios a COIMPRESORES, deben cumplir con las políticas de seguridad de la información definidas por COIMPRESORES.

4.2. POLÍTICA DE TELETRABAJO

Dando cumplimiento al numeral A.6.2.2 de la Norma ISO 27001, la cual nos indica que se debe implementar una política y unas medidas de seguridad de soporte, para protegerá la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Para el Trabajo en Casa o Remoto según la circular 041 del ministerio de trabajo dictada por el estado de emergencia sanitaria por el covid19, se hace claridad que ésta hace el traslado de las funciones y los factores de riesgo a la casa, y que la diferencia radica en que se modifica el accionar de las actividades; las políticas y controles de seguridad impuestas para la ejecución del teletrabajo aplica igualmente para el término de Trabajo en Casa.

A continuación, se despliegan las políticas establecidas por COIMPRESORES para teletrabajo:

a. Teniendo en cuenta la ley 1221 del 2008 “Por la cual se establecen las normas para promover y regular el teletrabajo y se dictan otras disposiciones”, así como los demás requisitos que la modifican, se tiene establecido que en COIMPRESORES se permite el Teletrabajo de tipo MÓVIL, a continuación se puede visualizar el concepto extraído de la ley: “Móviles son aquellos teletrabajadores que no tienen un lugar de trabajo establecido y cuyas herramientas primordiales para desarrollar sus actividades profesionales son las Tecnologías de la Información y la comunicación, en dispositivos móviles”.

b. Hasta el momento, en COIMPRESORES el Teletrabajo ha sido considerado por las necesidades de la organización debido a que en algunos procesos misionales se requiere realizar turnos de soporte y monitoreo que por ser recurrentes clasifican como Teletrabajo.

c. Desde el punto de vista tecnológico y de seguridad de la información, toda sesión de teletrabajo requerida por un usuario que previamente sea autorizado se realiza a través de una VPN (Red Privad Virtual) o cualquier solución definida por el área de IT que debe proveer conexión segura con la Entidad. La VPN o solución definida por el área de IT debe solicitarse siguiendo el procedimiento establecido para ello.

d. En el caso de los Colaboradores de COIMPRESORES , que por labores de soporte técnico requieran acceso en horarios hábiles o no hábiles a la infraestructura tecnológica de la empresa, se debe solicitar, el acceso por VPN requerido, siguiendo el procedimiento establecido para ello (Procedimiento de Control de Acceso) a través de la Mesa de Ayuda GLPI de COIMPRESORES.

e. En los casos donde el acceso y procesamiento de la información de COIMPRESORES sea mediante la modalidad de teletrabajo, los responsables de estas actividades deben dar cumplimiento a las condiciones y restricciones definidas con el entorno a la seguridad de la información, tales como:

○ Tener configurado el cifrado de disco duro.
○ Toda sesión de teletrabajo debe realizarse con un equipo propietario de COIMPRESORES.

f. COIMPRESORES prohíbe cualquier otro tipo de acceso remoto y el uso de sistemas de información que no estén autorizados por el área de Tecnología.

g. Cada colaborador de COIMPRESORES, es responsable de garantizar que las condiciones eléctricas para los equipos de cómputo sean las adecuadas.

h. Siempre que se vaya a considerar a un colaborador como elegible para procesos de soporte y/o monitoreo a través del teletrabajo, debe ser autorizado por el responsable del proceso al que pertenece el colaborador y por el área de Recursos Humanos, considerando las evaluaciones de riesgos de seguridad de la información.

i. Antes de su aprobación todo acceso de teletrabajo, a través de activos tipo instalaciones de procesamiento de información, debe ser sometido a una evaluación de riesgos de seguridad de la información.

j. Todo colaborador de COIMPRESORES que realice actividades de teletrabajo debe firmar el acuerdo establecido por las partes y administrado por el área de Recursos Humanos, para realizar dichas actividades, una vez realizado dicho tramite se debe informar al área de Tecnología.

k. Para el acceso al teletrabajo se deben tener en cuenta las necesidades técnicas y tecnológicas que garanticen que el colaborador cuente con las herramientas necesarias para poder realizar su trabajo, así como las configuraciones de acceso seguro, los medios y horarios que solicite el responsable del proceso preservando siempre los principios de seguridad de la información.

l. Los accesos para el teletrabajo deben ser implementados teniendo en cuenta los controles del Sistema de Gestión de Seguridad de la Información que garanticen en todo momento la seguridad de la información.

m. Se debe autorizar el acceso únicamente a la información, instalaciones de procesamiento de información, servicios y sistemas de información necesarios para la ejecución de las actividades a cargo del colaborador que solicita el acceso al teletrabajo.

n. Preservar el Less Privileged (Principio del mínimo privilegio).

o. Cualquier dispositivo que se emplee para las actividades de teletrabajo deberá cumplir con los requisitos y controles de seguridad establecidos por COIMPRESORES.

p. Las conexiones a servicios de teletrabajo en COIMPRESORES deben permanecer cifradas, es decir que solo debe ingresar atraves de la VPN suministrada por la compañía a traves de SOPHOS.

q. La autorización de accesos para Teletrabajo se debe dar únicamente para cumplir con las funciones designadas para soporte y/o monitoreo, cualquier uso diferente, está expresamente prohibido.

r. Cualquier dispositivo que se emplee para las actividades de teletrabajo deberá cumplir con los requisitos y controles de seguridad establecidos por COIMPRESORES a través del Sistema de su previa revisión.

s. Los responsables de áreas y procesos deben coordinar y gestionar la instalación de controles de seguridad en los equipos y dispositivos móviles utilizados para Teletrabajo, según se encuentre establecido en el SGSI de COIMPRESORES.

t. El colaborador se hace responsable de darle un buen uso y manejo a los equipos de cómputo designados para desempeñar el teletrabajo.

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

Cuando se asignan y utilizan claves de usuarios, se deben respetar las siguientes reglas:

a. Todos los usuarios deben mantener sus claves en forma confidencial, como se establece en este documento.

b. Las cuentas de usuarios, contraseñas o cualquier otro mecanismo de autenticación a los sistemas de información, deben ser tratadas como información confidencial de COIMPRESORES, por lo cual no se deben divulgar, publicar ni compartir con ninguna persona.

c. Las claves utilizadas tanto para el primer acceso a los sistemas como para los subsiguientes deben ser exclusivas y seguras.

d. Las claves de primer acceso se comunican al usuario a través de su correo corporativo o a través de medios alternativos que la compañía determine como necesarios y seguros.

e. El tiempo para cambiar las claves y demás características de seguridad como extensión, tipos de caracteres etcétera se establecerán para cada activo tipo instalación de procesamiento de información que requiera credenciales para poder ser accedido para el usuario del dominio cada 2 meses y para siesa cada 3 meses.

f. El sistema de gestión de claves debe requerir que el usuario modifique la clave de primer acceso cuando ingrese al sistema por primera vez.

g. El sistema de gestión de claves debe requerir que el usuario escoja contraseñas seguras.

h. Si el usuario solicita una nueva clave, el sistema de gestión de claves debe determinar la identidad del usuario.

i. La contraseña no debe ser visible en la pantalla durante el inicio de sesión y conservar hasta 5 claves en siesa.

j. Si un usuario ingresa una clave incorrecta cinco veces consecutivas, el sistema debe bloquear la respectiva cuenta de usuario por espacio de 10 minutos .

k. Las claves creadas por el fabricante del software o hardware deben ser cambiadas durante la instalación inicial.

l. Las cuentas de usuario deben ser asignadas a las personas de acuerdo al rol desempeñado en COIMPRESORES y según las necesidades. Solo se concede acceso a la información específica al personal autorizado.

m. Toda transacción y actividad realizada con la cuenta de usuario asignada a los sistemas de información de COIMPRESORES, es responsabilidad del propietario y jefe a cargo de dicha cuenta. La trazabilidad se analiza teniendo en cuenta aquellos sistemas de información y aplicativos que así lo permitan.

n. Las contraseñas o cualquier otro método de autenticación deben mantenerse bajo reserva y ser entregadas de forma personal o a través de un medio que asegure su confidencialidad.

o. Las credenciales creadas para los diferentes sistemas de procesamiento de información deben ser deshabilitadas para los Colaboradores y proveedores cuando se interrumpan las funciones en COIMPRESORES o cuando sean trasladados a otros procesos. En este último caso se debe revisar el perfilamiento y los accesos con el fin de cumplir con el principio de LESS PRIVILEGE.

p. Los perfiles que brinden todos los privilegios deben estar controlados y autorizados por la Gerencia GENERAL .

q. Las carpetas creadas para almacenar información (file server) de los Colaboradores, deben ser administradas teniendo en cuenta la siguiente información:

○ El acceso a las carpetas debe estar limitado al proceso al cual pertenece el usuario.
○ Los permisos para crear, eliminar, ejecutar, leer y modificar se deben limitar de acuerdo al cargo desempeñado.

r. Todas las aplicaciones de COIMPRESORES tienen sus propias credenciales de autenticación, salvo algunas aplicaciones para las cuales el logueo se hace directo contra el directorio activo.

s. Semestralmente se debe revisar y actualizar la matriz de accesos y componentes de “Matriz de perfiles de usuarios Vs Aplicación”.

t. en caso de que un funcionario salga a vacaciones el área de recursos humanos debe notificar si el usuario será reemplazado por otro usuario y debe registrar los detalles de los identificadores para asignar los roles necesarios al reemplazo utilizando la herramienta que se encuentra en siesa y que será aplicado ‘’ sustitución de usuario seleccionado con la caducidad proporcionada por el área , es decir que quedara desactivado el usuario que sale a vacaciones y se activara automáticamente una vez ingrese , de igual manera a el usuario sustituto se desactivara en la misma fecha (ver manual y procedimiento de la gestion de usuarios)

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

a. Cada usuario es responsable de salvaguardar la contraseña de ingreso a los diferentes activos de información a los cuales esté autorizado.

b. No está permitido guardar o escribir las contraseñas en papeles físicos ni documentos de texto como bloc de notas, Word o notas de Windows.

c. COIMPRESORES, establece el cambio obligatorio de las contraseñas de acceso a todos los sistemas de información según la periodicidad establecida.

d. La contraseña escogida para el acceso a cada uno de los sistemas de información de COIMPRESORES debe:

○ Ser diferente para cada aplicación o sistema de información con excepción de aquellos sistemas que se autentiquen contra el directorio activo.

○ Omitir datos personales o de familiares tales como: nombres, apellidos, fechas de cumpleaños, números de identificación o alguna otra fecha importante.

○ Estructurarse teniendo en cuenta los siguientes parámetros: uso de mayúsculas, minúsculas, números, caracteres especiales y longitud entre ocho (8) y doce (12) dígitos.

○ No utilizar repetición de las claves y/o historial de contraseñas como mínimo de 5 veces.

○ Ser cambiadas periódicamente: Para ello, las contraseñas en las aplicaciones y sistemas de información controladas mediante el directorio activo de COIMPRESORES se cambia cada 45 días y este exige el cambio automático de las mismas de igual manera cada 30 dias el sistema automáticamente pedirá que se cambien las de acceso al ERP Siesa Enterprise.

4.3.3. USO DE CONTRASEÑAS

a. Todos los usuarios de los sistemas deben estar conscientes de sus responsabilidades en el uso de contraseñas, así como de las siguientes prácticas para protegerlas:

○ La contraseña es información confidencial y queda prohibido compartirla con otras personas.

○ La contraseña no deberá ser escrita en ningún papel a menos que sea resguardado adecuadamente.

○ Las cuentas de usuarios nunca deben estar marcadas con “Password Never Expires”

○ Cambiar la contraseña después de sospechar que alguien más la conoce.

b. El campo de contraseña debe estar parametrizado teniendo en cuenta los siguientes aspectos por cada tipo de activo tipo instalación de procesamiento de información y tipo SW:

○La longitud mínima.
○ Tiempo para el cambio.
○ Opción de cambio de contraseña.
○ Caracteres alfanuméricos simbólicos que debe contener la contraseña.
○ Repetición de las claves.
○ Se deben cambiar las claves en el primer ingreso al sistema.
○ Las claves no deben ser almacenadas en un sistema de registro automatizado.

c. La persona que use indebidamente su contraseña será considerada como falta disciplinaria haciéndose acreedor a las sanciones correspondientes. Ver documento ANEXO 1 en su numeral de políticas aplicadas para los usuarios del sistema siesa Enterprise

4.3.4. ELIMINACIÓN DE ACCESO LÓGICO

a. Cuando un usuario se retira definitivamente de la empresa, el área de Recursos Humanos deberá aplicar el procedimiento establecido para que sean retirados todos los accesos antes de que la persona se retire de la empresa. Esto con el fin de que no pueda acceder a los activos tipo instalaciones de procesamiento de información en forma remota ni presencial y deberá informar con anticipación al área de tecnología para aplicar las configuraciones correspondientes.

b. El área de tecnología ante la solicitud de baja deberá deshabilitar y suspender todos aquellos accesos otorgados, confirmando con el área de recursos humanos el nombre completo de usuario, nombre del usuario, email, la fecha de baja del empleado, con el objeto de que, 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).

4.3.5. 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).Para llevar a cabo la eliminación de accesos físicos es la siguiente:

a. El colaborador que deja voluntariamente a COIMPRESORES deberá informar a su jefe inmediato y a Recursos Humanos. En el caso de que el colaborador sea despedido, el encargado debe notificar la baja del colaborador a Gestión Humana y al jefe de Tecnología de inmediato.

b. El proceso de Recursos Humanos solicita al colaborador la credencial que se le proporciona para el acceso a las instalaciones.

c. El personal de Recursos Humanos se encargará de notificar al personal de Sistemas acerca de las personas que dejan de laborar en la empresa ya sean internas

o externas, con el fin de restringir su acceso a los sistemas tecnológicos físicos de la empresa .

4.3.6. REVISIÓN DE LOS DERECHOS DE ACCESO

a. 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.

b. 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.

4.3.7. REVISIÓN DE LA ENTIDAD PARA EL CONTROL DE ACCESO

a. 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.

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

c. 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.

d. 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 Tecnologia.

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

a. 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

b. 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

a. 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.

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

c. La administración de llaves criptográficas y certificados digitales estará a cargo de acuerdo a 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 LIMPIO Y PANTALLA LIMPIA

Todas las personas que trabajan en COIMPRESORES están obligadas a cumplir con las siguientes normas de seguridad:

a. Retirar de escritorios o lugares visibles la información confidencial que haya sido utilizada, sin importar el medio en que se encuentre (papel, discos, medios magnéticos) y resguardarse en lugares con acceso controlado.

b. No dejar documentos con información de Uso Interno o Confidencial sobre impresoras, copiadoras. Por lo tanto los dispositivos de impresión y digitalización deben permanecer limpios de documentos.

c. No utilizar información impresa que sea confidencial o de uso reservado para reciclaje.

d. Mantener la pantalla de su computador limpia y libre de documentación para evitar el espionaje de información confidencial a través de este medio.

e. No se deben tener fotos, carteleras y/o información personal sobre los escritorios de la compañía a menos que estos cumplan con los lineamientos corporativos.

f. Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, etiquetados como confidenciales, deben ser retirados del escritorio o de otros lugares para evitar el acceso no autorizado a los mismos. Este tipo de documentos y soportes deben ser archivados de forma segura.

g. Si la persona autorizada no se encuentra en su puesto de trabajo, se debe retirar toda la información Confidencial del escritorio, y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

h. Todos los usuarios de equipos de cómputo deberán cerrar las sesiones de los sistemas y activar el protector de pantalla con contraseña cuando el equipo vaya a ser desatendido. Cada terminal debe de tener como tiempo máximo de inactividad cinco (5) minutos después de lo cual se bloqueará automáticamente el escritorio pidiendo nuevamente la contraseña y usuario de acceso.

i. Los puestos de trabajo deben permanecer limpios y ordenados a fin de reducir el daño causado en equipos de cómputo por prácticas inadecuadas (consumo de alimentos y/o bebidas, obstrucción de ventilación, ubicación inadecuada, entre otros).

j. El colaborador debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reacomodo de cables.

k. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser coordinados y notificados por parte del jefe del área encargada al área de TECNOLOGIA.

4.7. POLÍTICA DE RESPALDO DE LA INFORMACIÓN

a. COIMPRESORES, debe realizar copias de respaldo de la información y pruebas de estas, de acuerdo con el Procedimiento de backup locales.

b. Toda la información de tipo institucional que utilicen los Colaboradores de COIMPRESORES, debe ser almacenada en los repositorios de las unidades asignadas en el servidor de archivos autorizados para este fin.

c. Los discos duros de los equipos de cómputo de escritorio y portátiles no deben contener información institucional, ya que a éstos no se les realiza copias de respaldo, para tal fon son utilizadas las unidades de disco de los servidores de archivos a las cuales se les realiza el repaldo.

d. COIMPRESORES no es responsable del respaldo de la información personal almacenada en los equipos de cómputo de escritorio o portátiles en caso de pérdida.

e. Se debe conservar el registro de la ejecución de las copias de respaldo realizadas a los servidores de producción (archivos, sistemas operativos, bases de datos, aplicaciones, unidades de almacenamiento presentadas a los servidores) empleando el software IPERUIS BACKUP destinado para tal fin.

f. Se debe realizar seguimiento a la ejecución de las copias de respaldo, registrando las fallas presentadas, con el fin de asegurar el correcto funcionamiento de las mismas en caso de restauración.

g. Las copias de respaldo se deben probar semestralmente, con el fin de asegurar que se puede depender de ellas en caso de contingencia.

h. Las restauraciones de copias de respaldo solicitadas se deben realizar de acuerdo al Procedimiento de backup locales y se podrán documentar como pruebas.

i. La restauración de la información respaldada se debe realizar en medios de prueba dedicados, no sobrescribiendo el medio original, para evitar que en caso de que el

proceso de elaboración de copias de respaldo o de restauración falle, cause daño o pérdida de datos.

j. 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.

k. Los Colaboradores son los responsables de almacenar la información que requiera copias de respaldo en el destino o recurso asignado por el área de IT, o solicitar formalmente la ejecución de copias de seguridad de la información almacenadas por fuera de estas.

4.8. POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

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

b. 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.

c. 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.

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

e. 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

Las siguientes políticas aplican como requisitos que deben cumplir el personal interno o externo para requerimientos de desarrollo realizados por COIMPRESORES.

a. 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.

b. COIMPRESORES debe contar con sistemas de ambiente de pruebas en el ERP para administrar los cambios de los desarrollos y no poner en riesgo el ambiente real.

c. COIMPRESORES debe asegurarse que los desarrollos contratados externamente o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

d. COIMPRESORES o el tercero encargado del desarrollo debe usar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

e. COIMPRESORES en conjunto con las áreas pertinentes, deben aprobar las migraciones entre los ambientes de desarrollo y pruebas de los desarrollos nuevos y/o de cambios o nuevas funcionalidades.

f. Se deben aprobar las migraciones entre los ambientes de pruebas y producción de los desarrollos nuevos y/o de cambios o nuevas funcionalidades.

g. COIMPRESORES, debe garantizar que la información entregada a los desarrolladores en el ambiente de desarrollo, será enmascarada y no revelará información confidencial de los ambientes de producción.

h. Los desarrolladores de COIMPRESORES y proveedores de software deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

i. Los desarrolladores de COIMPRESORES y proveedores de software deben asegurar que los desarrollos construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

j. 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.

k. Se deben suministrar opciones de desconexión o cierre de sesión de los aplicativos, que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

l. Se deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

m. Se debe garantizar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.

n. Se deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos sólo tengan privilegios de lectura.

o. Se debe proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

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

COIMPRESORES define mecanismos de control en las relaciones con sus proveedores o contratistas, con el fin de asegurar el acceso por parte de ellos a la información y a los servicios tecnológicos suministrados para el desarrollo y cumplimiento de sus actividades.

a. Los proveedores, contratistas o terceros vinculados a COIMPRESORES deben garantizar que el intercambio de información desde y hacia COIMPRESORES cumpla con las exigencias institucionales definidas con base en las leyes y regulaciones vigentes, así como también las disposiciones de la presente política.

b. Los proveedores o contratistas deberán informar inmediatamente de cualquier incidente que afecte la confidencialidad, integridad y disponibilidad de los activos de información que ponga en riesgo la operación de COIMPRESORES.

c. Los proveedores y contratistas vinculados COIMPRESORES que tengan acceso a la información de Uso Interno o Confidencial de la misma, deben firmar un acuerdo de confidencialidad o debe incluirse una cláusula de confidencialidad al correspondiente contrato con el fin de proteger dicha información.

d. En el contrato de servicios se debe incluir una cláusula de confidencialidad y niveles de servicios en seguridad de la información, que detalle sus compromisos en el cuidado de la misma y las medidas a las que estaría sujeto el Proveedor o Contratista en caso de incumplirlos. El cumplimiento de los acuerdos mencionados anteriormente debe ser verificado periódicamente teniendo en cuenta los Acuerdos de Nivel de Servicio -ANS pertinentes a seguridad de la información.

e. Los proveedores o terceros que en 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.

f. Para el acceso a cualquier tipo de información o sistema de información, los proveedores y terceros que presten sus servicios a COIMPRESORES deberán suscribir acuerdos de confidencialidad y de transferencia de información con el fin de reducir los riesgos de divulgación de información con carácter de uso interno y/o confidencial.

g. Los Proveedores y terceros solo deben tener acceso a la información, sistemas de información o instalaciones que son indispensables para el cumplimiento de sus objetos contractuales.

h. Al finalizar sus contratos los proveedores o terceros que presten sus servicios a COIMPRESORES deben efectuar la devolución de información o activos de información propiedad de COIMPRESORES que estuvieron bajo su responsabilidad y procurar la destrucción o borrado seguro de información de uso interno y/o confidencial conocida en razón de su actividad.

i. Los proveedores y terceros deben cumplir con la reglamentación en materia de derechos de autor y propiedad intelectual, incluido pero no limitado al uso de información y software.

j. Los proveedores y terceros no están autorizados para utilizar los recursos de información y tecnología de COIMPRESORES para propósitos diferentes a los necesarios para el cumplimiento del objeto contractual suscrito.

k. No está autorizada la utilización de equipos informáticos dentro de las redes de comunicaciones de COIMPRESORES que no cumplan con los controles de seguridad especificados por COIMPRESORES para preservar la seguridad de la información.

l. No está autorizada la ejecución de cambios sobre la infraestructura de información, comunicaciones o cualquier otro activo tipo instalación de procesamiento de información sin contar con la autorización formal y expresa del responsable del área, proceso y/o administrador del activo tipo instalación de procesamiento de información.

m. No está autorizada la modificación o desactivación de los controles de seguridad instalados en los componentes de información y tecnología de COIMPRESORES sin

contar con autorización del responsable del área, proceso y/o administrador del activo tipo instalación de procesamiento de información.

n. Las claves de acceso a los sistemas de información de COIMPRESORES son personales e intransferibles, cada tercero debe responder por las actividades que se lleven a cabo con sus datos de identificación.

o. Todo proveedor y/o tercero que tenga acceso a los activos de información y preste servicios a COIMPRESORES debe contar con políticas, normas y/o estándares de Seguridad de la Información al interior de su organización; las cuales deben desarrollarse y mantenerse actualizadas acorde con los riesgos a los que se ve enfrentada su organización.

p. Los accesos a los sistemas de información y equipos de cómputo requeridos por terceros, deben ser solicitados de manera formal únicamente por el líder del área o proceso quienes se encargaran de su aprobación.

q. Los mensajes y la información contenida en los buzones de correo asignados a terceros, son propiedad de COIMPRESORES y cada usuario, como responsable de su buzón, debe dar uso en relación al negocio.

r. Todos los mensajes enviados desde correos electrónicos asignados a terceros, deben respetar el estándar de formato e imagen corporativa definido por COIMPRESORES y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

s. Con respecto a los buzones de correo electrónico asignados a terceros, no están permitidos las siguientes actividades:

○ Enviar cadenas de correo con contenido que no obedezca a las actividades contratadas,

○ Utilizar la dirección de correo corporativo como usuario de cualquier red social.

○ Enviar masivamente mensajes publicitarios corporativos, si un tercero debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la empresa y/o servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

t. Cualquier tercero que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de COIMPRESORES, sea por Internet o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

u. Los terceros que requiera tener acceso a los sistemas de información de COIMPRESORES deben estar debidamente autorizados y deben acceder a dichos

sistemas haciendo uso como mínimo de un usuario y contraseña asignado por la organización.

v. Los terceros son responsables del buen uso de las credenciales de acceso asignadas.

w. 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.

x. Los terceros están en el deber de informar a COIMPRESORES cualquier fuga, pérdida o alteración de información de propiedad de COIMPRESORES, sus clientes y/o usuarios y la correspondiente medida de mitigación. y. Toda violación de estas políticas se deberá notificar inmediatamente, de modo que se pueda resolver en el menor tiempo posible. Con esto se busca asegurar que todos comprendan y respeten las políticas, con el fin de reducir al mínimo el riesgo, protegiendo a usuarios, Colaboradores, clientes, terceros, así como a la Compañía.

5. POLÍTICAS COMPLEMENTARIAS

5.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.1.1. ROLES Y RESPONSABILIDADES

a. Todo el que acceda a la información de COIMPRESORES, es responsable de contribuir a la seguridad de su información, entre ellos están: Colaboradores, contratistas, proveedores, clientes y visitantes.

b. El área de TI de COIMPRESORES asumirá la responsabilidad por el desarrollo e implementación de la seguridad de la información, comprobará el cumplimiento de las políticas, en caso de requerirse, prestará asesoría a todo aquel que maneje información de COIMPRESORES, coordinará las actividades de la gestión de riesgos de la seguridad de la información, apoyará la identificación de controles y además, pondrá en contexto al Comité Estratégico en lo que se refiere a seguridad de la información.

c. En la documentación (manuales, procedimientos e instructivos) del SGSI están definidas las responsabilidades específicas de los colaboradores y contratistas que están directamente relacionados con la seguridad de la información.

5.1.2. SEPARACIÓN DE FUNCIONES

a. Todo aquel con permisos para acceder a la información de COIMPRESORES, deberá tener claramente definidos sus deberes, con el fin de reducir el uso no autorizado, abuso de derechos y privilegios de acceso.

b. Los sistemas deben contar con un súper administrador o root, con el fin de monitorear las tareas desarrolladas por el administrador y demás usuarios.

c. Todos los sistemas de información de la organización y aplicativos deberán implementar reglas de acceso, de tal forma que haya segregación de funciones entre quien administre, mantenga y audite o tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

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

a. Independientemente del proyecto que COIMPRESORES esté planificando y ejecutando, deberá integrar la seguridad de la información, para tratar como parte del proyecto los riesgos de seguridad de la información implícitos en el mismo, independientemente de su naturaleza. Así mismo, la seguridad de la información será parte de todas las fases de la metodología del proyecto aplicada. Por lo tanto, es responsabilidad de los Líderes que se sigan 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.

5.1.7. ANTES DE ASUMIR EL EMPLEO

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

5.1.8. TERMINOS Y CONDICIONES DEL EMPLEO O CONTRATO

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

b. 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.

c. 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.

d. 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).

e. 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.

f. 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.

g. 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

a. 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.

b. 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.

c. Los procesos disciplinarios serán adelantados por Recursos Humanos.

5.1.10. TERMINACIÓN O CAMBIO DE ROL

a. Recursos Humanos es responsable de informar oportunamente al jefe del colaborador y al encargado del retiro de los accesos en todas las instalaciones de procesamiento de información, el trámite de devolución de activos de información y eliminación de los accesos físicos y lógicos. En caso de que un Colaborador tenga un cambio de funciones, se deberá asegurar la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de conocimiento y la posterior entrega de los mismos de acuerdo a su nuevo rol.

b. Sin excepción, tanto para antes de la ejecución del empleo, como durante y después del cambio y/o terminación se deben seguir los procedimientos y demás lineamientos establecidos por Recursos Humanos y por la Gerencia General para preservar la seguridad de la información.

c. Cuando un Colaborador, Contratista y/o Tercero se retire de COIMPRESORES se debe reportar el retiro y tener en cuenta la rigurosidad necesaria para poder evidenciar la entrega de todos los activos de información y dejar el compromiso de borrado de esta información de los activos tipo instalaciones de procesamiento de información que pertenecen al colaborador, contratista y/o tercero.

d. Todos los Colaboradores, contratistas y/o terceros están en la obligación de preservar la confidencialidad sobre la información de COIMPRESORES, de manera

vitalicia y nunca se deben realizar comentarios y/o referencias que vayan en detrimento de la reputación de la compañía.

5.2. GESTIÓN DE ACTIVOS

COIMPRESORES ha establecido políticas para gestionar la seguridad en la gestión de activos como lineamientos generales de los cuales se deben derivar los procedimientos de gestión de activos para garantizar la seguridad de la información en la gestión de los mismos.

A continuación, se despliegan las políticas establecidas por COIMPRESORES para el dominio Y Seguridad en la Gestión de Activos:

5.2.1. INVENTARIO 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 a los movimientos que se vayan presentando en la marcha de las actividades.

5.2.2. USO ACEPTABLE DE LOS ACTIVOS

a. Los activos de información de COIMPRESORES solamente pueden ser utilizados a fines de satisfacer necesidades de la Entidad, con el objetivo de ejecutar tareas vinculadas a las labores asignadas.

b. Los activos de información de COIMPRESORES deben estar salvaguardados según su nivel de criticidad.

c. Los activos de información tales como: información (física y digital), software, servicios y hardware propiedad de COIMPRESORES, son proporcionados a los Colaboradores, para el desarrollo de sus actividades laborales en la Entidad. Es responsabilidad del propietario y custodio de los activos de información, dar uso adecuado a los mismos.

d. Todos los Colaboradores son responsables de etiquetar la información, y darle un manejo adecuado, siguiendo las directrices de la Metodología de Gestión de Activos de Información.

e. Los Colaboradores de COIMPRESORES, deben reportar los eventos de seguridad de la información identificados en los activos de información, de acuerdo con el Procedimiento de Gestión de Incidentes establecido por la Entidad.

f. Los dueños o propietarios de los activos de información deben mantener y actualizar (1 vez cada 12 meses o cada vez que se produzca un cambio en el sistema de gestión de seguridad de la información y/o en la entidad) el inventario de sus activos de información e instalaciones de procesamiento de información, indicando para cada uno su clasificación correspondiente.

g. 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

a. El área de IT, es la encargada de dar de baja cualquier elemento de hardware propiedad de COIMPRESORES, de acuerdo con los criterios y protocolos de seguridad previamente definidos, con el fin de garantizar que se han eliminado los riesgos de confidencialidad de la información.

b. Debe respetarse y no modificarse la configuración de hardware y software establecido por el área de IT. Si se presenta algún requerimiento de cambio de configuración se debe informar a través de las herramientas de gestión de mesa de ayuda GLPI, con previa autorización del Jefe Inmediato.

c. Se prohíbe el uso de medios extraíbles (USB, celulares, discos externos, CD, DVD, entre otros) para almacenamiento de información institucional, con excepción de aquellos Colaboradores que, por sus funciones, sean autorizados, de forma temporal o permanente.

d. Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte tanto las redes corporativas como los sistemas de información de COIMPRESORES, está prohibida y dará lugar a los procesos disciplinarios o legales según corresponda.

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

f. Los equipos de cómputo de escritorio, servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados (toma de color naranja) a excepción de las impresoras que pueden conectarse a las tomas blancas.

g. La conexión eléctrica de equipos de cómputo personales debe hacerse a través de los puntos eléctricos no regulados. COIMPRESORES no se responsabiliza por daños que puedan sufrir estos dispositivos.

h. La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de COIMPRESORES y que no son propiedad de la Entidad, son responsabilidad única y exclusiva de sus propietarios. COIMPRESORES, no es responsable por estos equipos en ningún caso.

5.2.4. USO DE LA INTRANET Y DE INTERNET

a. Sólo se puede acceder a la Internet a través de la red local de la organización, con la infraestructura y protección de cortafuegos adecuadas. El acceso directo a Internet mediante módems, Internet móvil, red inalámbrica externa u otros dispositivos no está permitido en COIMPRESORES. El servicio de la intranet y de Internet es exclusivo para el desarrollo de sus funciones.

b. COIMPRESORES puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los empleados de la organización. Si es necesario a algunas páginas Web bloqueadas, el usuario puede elevar una petición escrita a la Dirección solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción.

c. El usuario debe considerar como no confiable la información recibida a través de sitios web no seguros. Ese tipo de información puede ser utilizado con fines comerciales solamente después de haber verificado su autenticidad y veracidad.

d. El área de IT debe implementar las herramientas tecnológicas y los controles necesarios para mitigar los riesgos de la navegación en internet. Asimismo, debe promover entre los “usuarios internos”, el uso responsable del servicio de navegación en Internet, mediante actividades de sensibilización desarrolladas con el apoyo de las áreas encargadas.

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

f. Está prohibido, ejecutar cualquier herramienta para realizar el monitoreo de puertos o análisis de tráfico de red, por personas diferentes al área de TI o proveedores externos contratados y autorizados por la empresa para ejecutar dicha labor.

g. Está prohibido conectar módems o cualquier dispositivo móvil (en modo Access Point) para acceder a internet, dentro de la red de COIMPRESORES.

h. El área de IT y/o proveedores externos contratados y autorizados por COIMPRESORES, pueden monitorear la infraestructura (Software y Hardware) con el fin de preservar la seguridad informática de la empresa.

5.2.5. USO DEL CORREO ELECTRÓNICO

a. COIMPRESORES provee a todos los Colaboradores un correo electrónico institucional en el dominio coimpresores.com para el ejercicio de sus labores.

b. La cuenta de correo electrónico institucional es personal e intransferible y, por ende, los Colaboradores son completamente responsables de todas las actividades realizadas con sus credenciales de acceso y el buzón asociado al correo de COIMPRESORES.

c. El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de COIMPRESORES, es decir, que debe ser usado para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo asignadas.

d. Teniendo en cuenta que el correo electrónico institucional es una herramienta para el intercambio de información necesaria para el cumplimiento de las funciones propias de cada cargo 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.

e. Toda información enviada o publicada a través del correo o el sitio web de COIMPRESORES, 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.

f. 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

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

b. 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.

c. 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, etiqueta y maneja la información y sus activos asociados de acuerdo a la Metodología de Gestión de Activos de Información.

5.2.8. GESTIÓN DE MEDIOS REMOVIBLES (UNIDADES DE ALMACENAMIENTO)

a. En COIMPRESORES no se permite el uso de medios removibles excepto los medios que contienen firma y/o certificados digitales,

b. Los activos tipo instalaciones de procesamiento de información como dispositivos móviles, medios removibles y computadores pueden ser llevados fuera de las instalaciones solamente con autorización.

c. Las unidades de medios removibles de las estaciones de trabajo y equipos de cómputo portátiles pertenecientes a COIMPRESORES, están bloqueadas para booteo, desde la BIOS (hace referencia a la utilidad que se ejecuta al momento de encender el equipo de cómputo) y el acceso a esta funcionalidad requiere contraseña.

d. 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

Para el alcance del sistema de Gestión de Seguridad de la Información, COIMPREOSORES no realiza transporte, ni transferencia de medios físicos a través de servicios de mensajería y de compañías de seguridad, 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

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

b. El perímetro de la oficina de COIMPRESORES debe contener todos los recursos necesarios para tratar la información ofreciéndole cierta solidez física. Todos los muros externos de la zona deben ser sólidos y todas las puertas exteriores deben ser protegidas contra accesos que no estén autorizados por la organización, por ejemplo, se pueden utilizar mecanismos de control, alarmas, rejas, cierres, etc. Las puertas y las ventanas tienen que estar cerradas con llave cuando se encuentren desatendidas.

c. Se tiene que realizar la instalación de un área de recepción manual y otros medios de control de acceso físico a las instalaciones. El acceso se puede restringir sólo al personal que esté autorizado.

d. Las barreras físicas se pueden extender, si fuera necesario, desde el suelo real al techo real evitando que se realicen entradas no autorizadas.

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

f. Las visitas de las áreas seguras se deben supervisar, a menos que el acceso haya sido aprobado de forma previa y se tiene que realizar un registro de la fecha de entrada y salida.

Las visitas solo tienen acceso para propósitos muy específicos y se autorizan proporcionalmente generando instrucciones sobre todos los requisitos de seguridad del área y los procedimientos ante emergencias.

g. Se puede controlar al personal autorizado el acceso a la información confidencial de la organización. Se pueden utilizar diferentes controles de autenticación, por ejemplo, tarjetas personales, etc. Tiene que quedar un registro de entradas y salidas.

h. Se pueden exigir a todo el personal de la organización que porte la identificación de forma visible y deben saber que puede ser solicitada a las personas extrañas que no estén acompañadas y a cualquiera que no lleve la identificación visible.

i. Se tiene que garantizar el acceso restringido de terceras personas hacia las áreas de seguridad o los recursos de los procesos de información confidencial. El acceso debe ser autorizado y monitorizado por la persona responsable.

j. 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

Todas las áreas destinadas al procesamiento o almacenamiento de información confidencial y de uso interno, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido . En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

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

b. 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,

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

d. COIMPRESORES debe asegurar que las áreas de acceso restringido como son Datacenter, cuartos de control, de cableado, de comunicaciones, telefónicos etc., cuenten con el equipamiento mínimo requerido para asegurar el cumplimiento de los requisitos y prevención de amenazas externas, a nivel ambiental, físico y de energía necesarios para soportar su operación. Independientemente de la ubicación física.

e. Los accesos de tipo permanente deben ser asignados por el responsable de accesos a aquel personal que así lo requiera en base a requisitos basados en su función dentro de COIMPRESORES.

f. Los accesos de tipo temporal, por ejemplo, para el caso de proveedores externos y contratistas, deben ser solicitados al responsable de accesos y autorizados por el responsable de seguridad de la información y se debe proveer al menos la siguiente información: nombre, apellido, documento de identidad, empresa, fecha de inicio de acceso temporal, fecha fin de acceso temporal, motivo. Los visitantes temporales que requieran acceso a áreas seguras o centros de datos deberán permanecer acompañados de personal con permisos de acceso y portar una identificación visible. En el caso del centro de datos, se debe registrar la visita en una **bitácora de ingresos** a éste que deberá contener al menos la siguiente información: fecha, nombre, apellido, cédula de identidad, empresa, hora de entrada, hora de salida, nombre y apellido del empleado que lo acompaña.

5.3.3. PROTECCIÓN CONTRA AMENAZAS EXTERNAS E INTERNAS

a. Se debiera asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

b. Se debería prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

c. 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

a. Establecer, coordinar, controlar y documentar los cambios realizados en los activos de información tecnológicos y los recursos informáticos, asegurando que los cambios efectuados sobre la plataforma tecnológica hayan sido debidamente autorizados por las áreas correspondientes.

b. COIMPRESORES y el área de TI, deben garantizar que todo cambio realizado sobre la plataforma tecnológica quedará formalmente documentado desde su solicitud hasta su implantación cumpliendo con el procedimiento correspondiente.

5.4.2. POLÍTICA DE GESTIÓN DE LA CAPACIDAD

COIMPRESORES debe asegurar que los servicios y recursos de TI se vean respaldados por una capacidad de procesamiento y almacenamiento suficiente y correctamente dimensionada, que garantice que los clientes y usuarios de los servicios puedan desempeñar de una manera eficiente sus tareas.

5.4.3. POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO

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

b. Toda la infraestructura de procesamiento de información de COIMPRESORES cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos (SOPHOS ANTIVIRUS).

c. Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de COIMPRESORES.

d. Se debe restringir la ejecución de código móvil, aplicando políticas a nivel de sistemas operativos, navegadores y servicio de control de navegación.

e. Todos los Funcionarios, Colaboradores y Terceros que hacen uso de los servicios de tecnología de la información y comunicaciones de COIMPRESORES son responsables del manejo del antivirus para analizar, verificar y (si es posible eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

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

5.4.4. SEPARACIÓN DE LOS ENTORNOS

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

a. Contar con ambientes separados para desarrollo, pruebas y producción.

b. Definir, en el marco de la política de gestión de cambios, un procedimiento formal para la gestión de los mismos.

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

d. Los cambios siempre deben ser probados y aceptados.

e. Los ambientes deben contar con los mismos sistemas o herramientas provistas por terceras partes y ser homólogos al menos en ambiente de pruebas y producción, para que se puedan realizar los controles pertinentes antes de cualquier instalación, actualización y aplicación de cambios.

f. El ambiente de pruebas debe estar adecuadamente identificado de forma tal de diferenciarlo del ambiente de producción.

g. El personal que realiza las pruebas debe utilizar cuentas de usuario diferentes a las que posee en producción para la realización de éstas.

5.4.5. POLÍTICA DE REGISTRO Y SEGUIMIENTO DE EVENTOS

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

b. Los colaboradores no están facultados para modificar, borrar o desactivar registros (logs) de sus actividades propias, ni de los usuarios de los sistemas de información y telecomunicaciones, de igual forma se deben realizar las configuraciones de seguridad necesarias para evitar la eliminación o cambios no autorizados a los registros de información.

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

d. COIMPRESORES, deben implementar la sincronización de relojes de los sistemas de información a un único servidor NTP (Nertwork Time Protocol – protocolo de tiempo en la red).(CAMBIAR)

e. Los eventos que se presentan en COIMPRESORES, cuya implicación pueda afectar la seguridad de la información, son registrados en la herramienta de Gestión de Incidentes GLPI para ser evaluado y asignar a los especialistas a resolver..

5.4.6. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

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

b. Todo software debe contar con un soporte técnico para garantizar su funcionamiento de manera eficiente con una solución disponible y en un tiempo aceptable, de tal manera que no afecte la operación de COIMPRESORES.

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

d. Todos los sistemas nuevos y mejorados deben estar completamente soportados por una documentación suficientemente amplia y actualizada, y no deben ser puestos en el ambiente de producción sin contar con la documentación disponible.

5.4.7. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

a. COIMPRESORES debe generar y ejecutar por lo menos una vez al año un plan de análisis de vulnerabilidades y/o hacking ético para sus plataformas críticas, cuya viabilidad técnica y de administración lo permita.

b. Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de COIMPRESORES. Cuando se requiera realizar un cambio en las plataformas tecnológicas a fin de corregir dichas vulnerabilidades, se debe seguir las directrices del Procedimiento de Gestión de Cambios.

5.5. SEGURIDAD DE LAS COMUNICACIONES

5.5.1. GESTIÓN DE LA SEGURIDAD DE LAS REDES

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

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

b. COIMPRESORES debe proporcionar a los funcionarios, Colaboradores y Terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados.

5.5.1.1. RED CABLEADA

a. En COIMPRESORES se deben instalar y mantener, con personal calificado y debidamente autorizado, la red de voz y datos, con el fin de garantizar la operación, seguridad e integridad de esta.

b. Cualquier equipo o elemento activo o pasivo de la red que no se utilice debe ser desactivado y controlado. No está autorizada la instalación de ningún equipo de red, diferente a los equipos que pertenecen a COIMPRESORES.

c. No está permitido realizar seguimiento o monitoreo de puertos o tráfico de red, por parte de personas diferentes a las autorizadas por COIMPRESORES.

d. El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.

5.5.1.2. SEPARACIÓN DE LAS REDES

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

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

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

d. Se deben establecer mecanismos de autenticación seguros para el acceso a la Red.

e. 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

a. Los requerimientos de seguridad de la información deben ser identificados y acordados por los responsables de los procesos y/o el usuario antes del desarrollo o la adquisición de los sistemas de información. Estos requisitos analizados deben documentarse para generar evidencia.

b. Los responsables de los procesos junto con los administradores de sistemas de información son los encargados de la adquisición de software o del desarrollo de este, teniendo en cuenta las necesidades expresas.

c. Los responsables de áreas y procesos junto con los administradores de sistemas de información deben seleccionar metodologías para adquisición y desarrollo de software que consideren mínimo los siguientes aspectos de seguridad y control:

Control de acceso a la información, definición y autenticación de usuarios, mecanismos de detección de intrusos, definición de mecanismos de cifrado de datos, administración de la información, gestión de roles y perfiles entre otros aspectos que permitan controlar la seguridad de la información.

d. 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 para la validación de datos de entrada, procesamiento, almacenamiento, hasta la salida de dichos datos, se deben considerar los controles apropiados que permitan el seguimiento de auditoría y el registro de actividades en el software. Así mismo deberá considerar en dicho desarrollo la gestión adecuada de derechos de autor, propiedad intelectual, confidencialidad y normas especiales aplicables al desarrollo de software y a nivel internacional cuando se trate de contratistas extranjeros.

e. Se debe realizar mantenimiento periódicamente a los sistemas de información con el fin de garantizar el correcto funcionamiento de los mismos.

5.7. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

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

b. 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.

c. Cualquier incidente de seguridad de la información se debe registrar y se debe realizar tratamiento del mismo empleando la herramienta de mesa de ayuda dispuesta por COIMPRESORES.

d. Cualquier dispositivo de uso personal como teléfonos inteligentes, computadores portátiles, tabletas, u otros dispositivos de cómputo que estén implicados en incidentes de seguridad de la información de COIMPRESORES pueden ser sometidos a cadena de custodia o protección para fines de investigación o evidencia ante procesos administrativos o legales, previa coordinación del procedimiento con el propietario del equipo.

e. Para prevenir la ocurrencia de incidentes de seguridad de la información COIMPRESORES aplicará los procedimientos de su sistema de gestión de seguridad de la información para llevar a cabo actividades de prevención de incidentes, supervisión y filtrado de anomalías que puedan afectar a la seguridad de la información, instalaciones de procesamiento de información y/o periféricos.

f. En caso de ser requerido por autoridad competente o grupos especializados en el tratamiento de incidentes de seguridad de la información, COIMPRESORES puede suministrar el plan de respuesta o remediación específico para un incidente para que se evalúe su efectividad, solicitar apoyo, demostrar debida diligencia u otros propósitos definidos por COIMPRESORES.

g. Un colaborador, cliente, contratista y/o tercero que evidencie la materialización de un incidente de seguridad dentro de los escenarios mencionados en el cuadro anterior, debe notificarlo directamente al Director de Tecnología utilizando los canales definidos para el reporte en el procedimiento vigente de gestión de incidentes o al grupo de IT de COIMPRESORES debido a su criticidad, el cual es un canal en el que se podrá reportar cualquier evento relacionado dentro de las anteriores categorías y que pueda ser generado debido a un incidente de seguridad de la información. Estos eventos serán tratados con la debida reserva y confidencialidad notificando solamente al personal involucrado en la gestión para solventar el incidente.

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

a. COIMPRESORES asegura la continuidad de la seguridad de la información en la planificación e implementación de la continuidad del servicio de facturación electrónica, donde tiene en cuenta recursos tecnológicos, activos de información, talento humano, proveedores y procesos críticos que respaldan la Facturación Electrónica.

b. Asimismo, COIMPRESORES establecerá, documentará, implementará y mantendrá procesos, procedimientos y controles que propendan por un nivel de continuidad requerido para la seguridad de la información durante una situación de contingencia.

c. Con el fin de asegurar si los controles de continuidad de la seguridad de la información son válidos, COIMPRESORES verifica a intervalos regulares estos controles establecidos e implementados.

d. Para asegurar la disponibilidad y redundancia de las instalaciones de procesamiento de información que soporta, COIMPRESORES establece e implementa un Plan de Recuperación de Desastres. Así mismo, realizará pruebas anuales a este plan, con el fin de verificar que los controles tecnológicos implementados son válidos y eficaces durante situaciones adversas.

5.9. CUMPLIMIENTO

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

b. La Gerencia General, la Direccion de tecnología mediante la identificación de requisitos de seguridad de la información que sean de cumplimiento obligatorio y emitidos por entes gubernamentales o privados y cualquier disposición colombiana vigente, definen e implementan los controles necesarios para dar cumplimiento y protección a los activos de información.

c. COIMPRESORES 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 propia, siempre con el seguimiento del debido proceso y el derecho a la intimidad de sus empleados, contratistas y/o terceros.

d. Aquellos documentos que estén bajo lineamientos legales o regulatorios deben ser resguardados bajo las medidas de seguridad adecuadas para garantizar su integridad y en general el cumplimiento con las disposiciones legales y regulatorias.

e. El responsable de TI debe revisar anualmente los acuerdos de licencias de hardware y software instalado a fin de verificar el cumplimiento de estos por parte de COIMPRESORES.

f. Los contratistas y terceras partes deben cumplir con las disposiciones establecidas por la Legislación Colombiana vigente asociados a la protección de datos personales, propiedad intelectual y seguridad de la información.
g. 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 implementación de las medidas pertinentes por parte de COIMPRESORES.

h. Desde el punto de vista de cumplimiento normativo COIMPRESORES debe tener presente la Ley 1581 de 2012 de Protección de Datos Personales, así como los requisitos, normas y regulaciones como ISO 27001:2013, además de las políticas definidas por la cooperativa.

i. El estudio de la normatividad publicada por organismos del estado inherente a Seguridad de la Información es una actividad permanente en conjunto con el área

Jurídica, con el fin de garantizar su aplicación adecuada y oportuna para COIMPRESORES.

j. El área Jurídica y el responsable de TI deben publicar y actualizar la normatividad con inherencia para la Seguridad de la Información, generar los acuerdos de confidencialidad, cláusulas y contratos que estén acordes con el cumplimiento de los requisitos del SGSI.

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

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

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

n. Generar informes que evidencien las revisiones de cumplimiento.

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

p. 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 que comprende políticas, procesos, procedimientos, formatos, controles, etc, deberá ser revisado como mínimo cada 12 meses o cuando surjan actualizaciones de mejoramiento o cambios significativos.

El objetivo de la revisión es garantizar que la seguridad de la información se implemente y opere de acuerdo con las políticas y los procedimientos organizacionales, y se deberá tener como precedente los riesgos asociados, los controles del riesgo, métricas asociadas.

Jesus Maria Torres
Gerente General
Coimpresores De Colombia