1. GENERALIDADES

La Caja de Compensación Familiar de Cundinamarca - COMFACUNDI, reconoce la importancia de identificar y preservar todos aquellos activos de la información, entendiendo estos como los recursos del Sistema de Gestión de Seguridad de la Información (SGSI) necesarios para que la organización funcione y consiga los objetivos que se ha propuesto la alta dirección. Que busca entre otras evitar la destrucción, divulgación, alteración y utilización no autorizada de toda información relacionada con afiliados, colaboradores, pacientes, proveedores, contratistas, sistemas de información, bases de conocimiento, manuales y archivos físicos; comprometiéndonos a desarrollar, implementar y fortalecer un mejoramiento continuo del Modelo de Seguridad y Protección de la Información (MSPI).

Para el presente documento de Política de Seguridad de la Información de COMFACUNDI, se toman como base los requisitos legales en materia de seguridad de la información, la Política de Gobierno Digital, controles y requisitos identificados en el Modelo de Seguridad y Privacidad de la información de MINTIC y el estándar ISO/IEC 27001.

2. ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- **Confidencialidad:** los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- **Integridad:** el contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Disponibilidad:** los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Para ello es necesario considerar aspectos tales como:

- **Autenticidad:** los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- **Posibilidad de Auditoría:** se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.
- **Protección a la duplicación:** los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- **No repudio:** los autores, propietarios y custodios de los activos de información se pueden identificar plenamente. Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.
- **Legalidad:** los activos de información cumplen los parámetros legales, normativos y estatutarios de la organización.
- **Confiabilidad de la Información:** es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad de los datos o información propiedad de la Corporación.

- **Propiedad de la información:** la información pertenece a COMFACUNDI a menos que en una relación contractual se establezca lo contrario.
- **Continuidad de la gestión de la información:** los activos de la información son capaces de mantener la operación que permita la gestión y operación de seguridad del negocio.

3. ALCANCE

Esta política es de aplicación al Consejo Directivo, Director Administrativo, los Subdirectores, los recursos, a la totalidad de los procesos internos o externos vinculados contractualmente con la organización o acuerdos con terceros y en general a todos los colaboradores de COMFACUNDI, cualquiera sea su situación contractual, el proceso o área a la cual pertenezca o al nivel de funciones que desempeñe.

4. OBJETIVOS

- Fortalecer continuamente la función corporativa mediante la implementación, difusión y mejoramiento continuo del Modelo de Seguridad y Protección de la Información (MSPI).
- Brindar mecanismos de aseguramiento que permitan preservar adecuadamente el cumplimiento del marco legal, confidencialidad, integridad y disponibilidad de la información bajo responsabilidad de COMFACUNDI.
- Mitigar los incidentes de seguridad y privacidad de la Información, seguridad digital y continuidad de COMFACUNDI.
- Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y Continuidad de COMFACUNDI.
- Establecer los lineamientos necesarios para el manejo de la información y los recursos de COMFACUNDI.
- Dar cumplimiento a los requerimientos establecidos en el marco legal de la Ley general de Protección de Datos Personales.

5. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Cada líder de proceso o área bajo supervisión del Comité de Seguridad de la Información debe elaborar y mantener un inventario de los activos de información que poseen (recibida, procesada y producida). Las características del inventario, donde se incorpore la clasificación, valorización, ubicación y acceso de la información, las especifica el Oficial de Seguridad de la Información, correspondiendo al proceso de Tecnología brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

6. LINEAMIENTOS PARA LA GESTIÓN DEL RECURSO HUMANO

La política de Seguridad de la Información pretende asegurar que los colaboradores, contratistas y pasantes de COMFACUNDI, comprendan sus responsabilidades frente a la seguridad de la información con el fin de reducir el riesgo de pérdida, hurto, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información. Por ende, se establecen los siguientes lineamientos:

6.1 Lineamientos Sobre la Vinculación y Desvinculación de Colaboradores

La gestión de la seguridad de los recursos humanos se efectuará a través del proceso de Talento Humano.

La selección de los colaboradores vinculados a COMFACUNDI debe cumplir con los requisitos establecidos en el procedimiento PR-TH-001 Aprobación, Elección y Vinculación de Talentos, el cual debe incluir la verificación de antecedentes disciplinarios, fiscales y de policía, además de la verificación de experiencias laborales y validación de títulos académicos.

Para la vinculación de los colaboradores se deberá realizar la visita domiciliaría.

6.2 Lineamientos Sobre la Gestión de Contratistas Frente a la Seguridad de la Información

Para los contratos de prestación de servicios, el supervisor administrativo del contrato es el responsable de realizar la solicitud de cuentas de usuario a las plataformas, sistemas o herramientas que requiera el contratista mediante la mesa de servicio, para lo cual debe proporcionar los datos del contratista y del contrato.

Si el contrato establece que la Caja debe proporcionar el equipo de cómputo, el supervisor administrativo del contrato debe realizar el suministro de dicho equipo con la previa validación por parte del proceso de Tecnología que serán los responsables de entregar las características técnicas mínimas necesarias, para el normal desempeño de las funciones del contratista.

El equipo de cómputo proporcionado al contratista debe quedar a cargo del supervisor administrativo del contrato.

Para los contratos con personas jurídicas, en el caso de requerirse, el supervisor administrativo debe realizar la solicitud de la cuenta de usuario proporcionando los datos del contrato y de las personas que tendrán a cargo dichas cuentas de usuario.

Los contratistas, deben dar cumplimento al MA-JU-001 Manual de Contratación.

Al momento de terminar el plazo de ejecución del contrato, el supervisor administrativo del mismo debe solicitar la eliminación de la cuenta(s) de usuario(s) asociada(s) al contrato.

Si se asignó equipo de cómputo al contratista, el supervisor administrativo debe realizar la devolución del bien.

Los contratistas deben aceptar dentro de sus obligaciones la cláusula de confidencialidad sobre la información a la que tengan acceso y aceptar el cumplimiento de las políticas de seguridad de la información corporativas, las políticas de operación corporativas y los procedimientos del sistema integrado de gestión.

6.3 Control de Acceso Colaboradores, Contratistas, Pasantes y Visitantes

Los colaboradores, contratistas y pasantes deben portar el carné que los identifica como tales en un lugar visible, mientras se encuentren en las instalaciones de COMFACUNDI.

Si el colaborador, contratista o pasante porta un carné institucional que no le corresponde, será considerado como suplantación de identidad y deberá notificarse al proceso de Talento Humano.

Los colaboradores, contratistas y pasantes de la organización deben registrar el ingreso y la salida de las instalaciones y de acuerdo a los mecanismos establecidos por el proceso de Talento Humano cuando estos apliquen, deberá quedar registro de al menos información de nombre, número de documento, hora de entrada y hora de salida.

COMFACUNDI actuará como responsable del tratamiento de sus datos personales y hará uso de los mismos únicamente para las finalidades para las cuales se encuentra facultada, según lo establece la PO-SC-02 Política de Protección de Datos Personales de la organización.

Los contratistas que realicen actividades en las instalaciones de COMFACUNDI de forma regular en razón a la prestación de servicios, deben utilizar prendas distintivas que faciliten su identificación. Tal es el caso de las empresas de vigilancia, aseo y adecuación de infraestructura física.

6.4 Control de acceso a las instalaciones de la organización

El personal de vigilancia debe observar que los colaboradores, pasantes, contratistas y visitantes no se encuentren en estado de ebriedad, bajo el efecto de sustancias alucinógenas, armado o en cualquier estado dudoso que pueda afectar la seguridad de la organización e informar cualquier novedad a los procesos de Apoyo Logístico o Talento Humano.

El personal de vigilancia debe estar debidamente uniformado.

Si alguna persona llega a una dependencia restringida sin que previamente haya sido autorizado su ingreso y registrado el mismo en la recepción del edificio, de manera inmediata se debe informar dicha situación al personal de seguridad.

Cuando en desarrollo de eventos corporativos se deba autorizar el ingreso masivo de personal al edificio, es indispensable que el colaborador del proceso o área responsable de la organización del evento debe remitir el listado del personal que asistirá, indicando nombres y apellidos y número de identificación y con mínimo 4 horas de anticipación al inicio del mismo. Con esta información, el personal de recepción autorizará el acceso directo del visitante para que se registre en debida forma.

El personal de vigilancia debe registrar la entrada o salida los equipos de cómputo, portátiles y demás equipos electrónicos en el libro de registro de elementos ubicado en la recepción. COMFACUNDI no se responsabiliza por los equipos de cómputo, portátiles, equipos electrónicos y otros objetos personales que ingresen a la entidad. Por lo tanto, la custodia y cuidado de estos elementos es de total responsabilidad de su propietario, por lo cual es responsabilidad de la empresa de vigilancia informar esto al propietario del bien que se ingresa a las instalaciones de la organización.

El personal de vigilancia debe asegurar que ningún visitante salga de las instalaciones de la entidad con activos de la entidad, sin el debido formulario de autorización que otorga el proceso de Apoyo Logístico.

6.5 Circulación interna de colaboradores, contratistas, pasantes y visitantes.

Todo colaborador, contratista y pasante deberá portar su carné de identificación de manera visible.

El proceso de Talento Humano es responsable de solicitar, actualizar y retirar los carnés de los colaboradores y pasantes.

Los supervisores de contratos son los responsables de solicitar y devolver los carnés al proceso de Talento Humano de los contratistas a su cargo.

El primer carné que se entregue no tendrá costo para el colaborador, contratista o pasante.

En caso de pérdida del carné, el responsable debe reportar la pérdida del documento en la página de la Policía Nacional - opción Constancia por pérdida de documentos y notificar al proceso de Talento Humano a la mayor brevedad posible.

El colaborador, contratista o pasante deberá cubrir el costo de la reposición de su carné por motivo de pérdida.

Al momento de presentarse un contratista para prestar un servicio externo en las instalaciones de COMFACUNDI, el colaborador, contratista o pasante que autoriza el ingreso debe realizar el acompañamiento constante hasta que finalice el o los servicios prestados.

Todo ingreso de colaboradores, contratistas y pasantes en horario no hábil debe ser autorizado previamente por el proceso de Apoyo Logístico.

6.6 Seguridad para el Trabajo en Casa

En el marco de la Ley 2088 de 2021, por la cual "SE REGULA EL TRABAJO EN CASA Y SE DICTAN OTRAS DISPOSICIONES", y en la cual se define al trabajo en casa como "la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones.

Este no se limita al trabajo que puede ser realizado mediante tecnologías de la información y las comunicaciones, medios informáticos o análogos, sino que se extiende a cualquier tipo de trabajo o labor que no requiera la presencia física del trabajador o funcionario en las instalaciones de la empresa o entidad".

En el marco de lo anterior se dan los siguientes lineamientos frente a la seguridad de la información y el trabajo en casa:

Es responsabilidad del colaborador, acatar las políticas de seguridad de la información establecidas por COMFACUNDI.

Es responsabilidad del colaborador cumplir con los controles técnicos que defina el proceso de Tecnología para garantizar la seguridad en las actividades de trabajo en casa incluido:

- Utilizar únicamente los equipos autorizados por COMFACUNDI para tener acceso a los sistemas de información e infraestructura tecnológica organizacional.
- Asegurar su acceso a Internet local con contraseña fuerte siguiendo los lineamientos de seguridad corporativas o conectarse a la red local organizacional únicamente mediante conexión de red privada virtual autorizada para tal fin.
- Limitar el uso de familiares, amigos o desconocidos a los equipos de cómputo utilizados para las actividades de trabajo en casa. Para el caso de los recursos entregados por COMFACUNDI, se prohíbe compartir los mismos con terceros.
- Reportar a la mesa de servicio, cualquier comportamiento sospechoso o inusual que se detecte cuando se realicen actividades de trabajo en casa.
- Conocer y estar alerta a los tipos de amenazas informáticas socializadas por COMFACUNDI para evitar ser víctima de estafas o software malicioso.

- En caso de utilizar equipos de propiedad personal para las actividades de trabajo en casa, debe cumplir con los lineamientos de seguridad que determine proceso de tecnología para este tipo de dispositivos.

- Se recomienda el cifrado de disco completo, que garantiza que incluso si el dispositivo cae en las manos equivocadas, no se puede acceder a los datos de la organización.

- Cerrar la sesión cuando no se esté usando la computadora, tanto en casa como en lugares públicos.

- Se debe aplicar contraseñas seguras en el arranque, establecer tiempos para la suspensión del equipo según el tiempo de inactividad y no son permitidas las notas con contraseñas pegadas al equipo.

- Se prohíbe el uso de dispositivos externos, como los de almacenamiento USB, así como dispositivos periféricos que no estén autorizados.
- Se encuentra prohibido descargar, almacenar o guardar bases de datos personales en cualquier dispositivo. En aquellos casos donde se requiera el tratamiento de bases de datos personales, debe hacerse única y exclusivamente a través de la nube asignada por la organización para tal fin. El proceso de Tecnología prestará apoyo necesario para este proceso de acuerdo a solicitud en la mesa de servicio.

7. LINEAMIENTOS DE SEGURIDAD FÍSICA Y AMBIENTAL

Dos elementos relevantes en esta política son los asociados a la seguridad física y ambiental de la organización, que buscan prevenir el acceso físico no autorizado, el daño e interferencia a la información, instalación de procesamiento y almacenamiento de la información corporativa, entre ellos:

7.1 Áreas Seguras

Se consideran áreas seguras los sitios donde se gestiona la información sensible de la entidad cuyo acceso debe ser controlado. Para ello se implementan mecanismos de seguridad física y control de acceso, por ejemplo, el centro de cómputo "Datacenter", centro principal de cableado, el área de archivo documental. Los lineamientos para estas áreas son:

- Solo personal autorizado puede acceder a las áreas consideradas como seguras, siendo responsabilidad del coordinador del área segura designar el encargado de gestionar los accesos.

- El proceso de Apoyo Logístico es la responsable de establecer y divulgar los lineamientos de seguridad física y seguridad de los colaboradores, pasantes, contratistas y visitantes que laboren o visiten la caja.

- El proceso de Tecnología y el proceso de Talento Humano son los responsables de dar cumplimiento a las normas de Seguridad y Salud en el Trabajo para el centro de datos.

- El acceso al centro de cómputo de la organización está a cargo del proceso de Tecnología, el cual es responsable de enrolar, asignar tarjetas de acceso y dar los permisos de acceso según el caso, con el fin de garantizar la seguridad de los activos.

- La solicitud de ingreso al centro de cómputo debe realizarse al Administrador de Infraestructura y Redes o al Administrador de Redes y Comunicaciones o el Jefe de Tecnología, que deberán llevar registro físico de la autorización en la que se especifique como mínimo motivo, fecha, hora del ingreso y salida.

- El acceso y mantenimiento de los centros de cableado es responsabilidad del proceso de Apoyo Logístico.

- El proceso de Tecnología debe proveer en cada vigencia los elementos físicos necesarios que garanticen la correcta operación de la plataforma tecnológica ubicada en el centro de cómputo.

- El proceso de Tecnología debe disponer en todo momento para el centro de cómputo de un sistema de control de temperatura, un sistema de detección y extintor de incendios, un sistema de alimentación eléctrica ininterrumpida (UPS) y un sistema de vigilancia, así como mantener bajo llave su acceso.

- El proceso de Apoyo Logístico es el responsable de gestionar el procedimiento ante incidentes asociados a la detección de incendio y cumplimiento de normas de seguridad industrial del centro de cómputo. Así mismo, son responsables de las actividades de evacuación del centro de cómputo y área de control de operaciones.

- Los procesos de Tecnología y Talento Humano son responsables de dar cumplimiento a las normas de Seguridad y Salud en el Trabajo para el centro de cómputo.

- En el centro de cómputo, está prohibido realizar actividades que generen polvo, suciedad o partículas ya que pueden causar un mal funcionamiento de los equipos y generar falsas alarmas de incendio, dando como resultado el daño parcial o total de la infraestructura tecnológica y activos de información de la entidad.

- No está permitido el ingreso al centro de cómputo y centros de cableado de líquidos, alimentos y material inflamable. Las áreas deben permanecer ordenadas, limpias y sin elementos que no correspondan con la operación del área.

- Es responsabilidad de las personas autorizadas para el ingreso y mantenimiento del centro de cómputo y los centros de cableado mantener organizado los cables de voz, de datos (peinado).

- La limpieza y aseo del centro de datos y de los centros de cableado está a cargo del proceso de Apoyo Logístico y debe efectuarse en presencia de un colaborador o contratista autorizado por parte del proceso de Tecnología.

- El personal de limpieza debe ser capacitado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza.

- Así mismo, está prohibido el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

- La autorización de ejecución de cambios en el centro de cómputo es responsabilidad del proceso de Tecnología.

- Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cuando se finalice la actividad.

- Mientras no se encuentren personas dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

- El centro de cómputo contará con pisos elaborados con materiales no combustibles, sistema de refrigeración por aire acondicionado, unidad de potencia ininterrumpida UPS, que proporcione respaldo al centro de datos en caso de falla en el fluido eléctrico, alarmas de detección de humo y extintor de fuego con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales, cableado de la red protegido de interferencias mediante canaletas u otros mecanismos que impidan acceso o interferencia no autorizada, cables de potencia separados de los cables de comunicaciones, siguiendo las normas técnicas, puertas siempre cerradas.

- Las llaves de los centros de cableado están a cargo de los encargados de su administración, quienes deben garantizar el registro de ingreso y salida del personal que acceda a estas áreas.

- La grabación de vídeo en las instalaciones del centro de cómputo con destino a terceras partes debe estar autorizada por el Comité de Seguridad de la Información.

- Todo cambio dentro del centro de cómputo se debe tramitar a través del procedimiento PR-SI-004 Gestión del Cambio establecido por la organización.

7.2 Almacén y Archivo

El acceso al almacén estará autorizado por el Jefe de Apoyo Logístico, el cual coordinará el debido acompañamiento para garantizar la seguridad de los activos.

El Jefe de Apoyo Logístico, garantizará las condiciones de seguridad física y ambiental de las áreas de almacenamiento de activos. Así mismo, contará con equipos de almacenaje adecuados que permitan la fácil ubicación, correcta custodia y minimicen los riesgos de accidente y daño.

El Profesional de archivo o quien haga sus veces, debe garantizar las condiciones de seguridad física y ambiental del área de archivo, tales como ventilación, iluminación, temperatura y humedad. Contará al igual con equipos de almacenaje adecuados para los diferentes tipos de formatos que maneja la Caja (papel, microfilm, cintas, rollos, fotografías, disquetes, CD, DVD, memorias extraíbles).

El acceso las áreas de gestión de correspondencia está restringido, sólo se permite el acceso al personal designado por el proceso de Apoyo Logístico.

8. LINEAMIENTOS DE CIFRADO DE INFORMACIÓN

Con las siguientes acciones COMFACUNDI, busca asegurar el uso apropiado y eficaz del cifrado de información para preservar la confidencialidad e integridad de la información de la organización:

COMFACUNDI en cabeza de los responsables de la información y con el apoyo del proceso de Tecnología vela por que toda información digital, etiquetada como altamente sensible y clasificada sea cifrada cuando se transmita o almacene, minimizando al máximo posible los riesgos asociados a la preservación, confidencialidad e integridad de la misma.

El proceso de Tecnología define, implementa y comunica los estándares para la aplicación de controles criptográficos o cifrado.

El proceso de Tecnología vela por que los desarrolladores internos y externos que diseñan desarrollan y/o implementan sistemas de información, aplicaciones y/o portales donde se maneje información digital reservada o confidencial, cuente con mecanismos de cifrado de datos.

Para los sistemas de información, aplicaciones y/o portales ya desarrollados que no cuentan con mecanismos de cifrado de datos, se debe hacer el análisis de impacto y el plan para su implementación. Si no es posible su implementación, se debe llevar el riesgo al Comité de Seguridad de Información para su respectivo análisis.

Todo sistema de información o servicio tecnológico debe incluir parámetros de seguridad basados en usuarios, perfiles y roles, para ser aplicados en la autorización y autenticación de necesidades.

Para las soluciones WEB consideradas como servicios misionales o críticos el acceso debe hacerse utilizando conexión segura.

Se utilizarán controles criptográficos o cifrados en los siguientes casos:

a) Para la protección de claves de acceso a sistemas, datos y servicios.
b) Para la transmisión de información clasificada, fuera del ámbito de COMFACUNDI.
c) Para el resguardo de información, cuando así se determine a partir de la evaluación de riesgos realizada por el administrador del activo de información, o por el área responsable de la Seguridad de la Información.

Se debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

Los sistemas de información o aplicativos que requieran realizar transmisión de información reservada o restringida, deberán implementar mecanismos para el cifrado de datos.

Se debe contar con un manual para el manejo de las claves de cifrado y para la aplicación de controles criptográficos.

Los desarrolladores de aplicativos informáticos (internos o externos) deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

De igual manera deben asegurarse de que los controles criptográficos de los sistemas desarrollados cumplen con los procedimientos y estándares adoptados por la organización.

9. LINEAMIENTOS EN LA GESTIÓN DE OPERACIONES

Los presentes lineamientos son señalados para asegurar la correcta y segura operación de la gestión de la información. Es responsabilidad de colaboradores, contratistas y pasantes su cumplimiento obligatorio, cualquier incumplimiento de los mismos será considerado como falta grave:

Los usuarios deben ser conscientes de los riesgos legales que implica la utilización de los medios electrónicos, especialmente en cuanto a la responsabilidad penal y/o civil en la que puedan incurrir por los inconvenientes, perjuicios y/o reclamaciones de cualquier tipo que llegaren a presentarse como resultado de cualquiera de las siguientes conductas:

- Enviar o reenviar información sensible sin estar legalmente autorizado para ello.
- Reenviar o copiar sin permiso mensajes “confidenciales” o protegidos por las normas sobre derechos de autor, o contra expresa prohibición del originador.
- Manejo inadecuado de Datos Personales.
- Enviar o reenviar un correo electrónico con cualquier contenido difamatorio, ofensivo, racista u obsceno.

- El uso del Internet no debe afectar el oportuno y eficiente cumplimiento de las funciones asignadas, ni la obligación de dedicar la jornada laboral a la realización de sus funciones.
- Evite suscribirse a boletines en línea, con el correo institucional, esto evita la llegada de cadenas de correo publicidad etc.

Todo correo de origen desconocido o de dudosa procedencia, debe ser eliminado, sin abrir, para evitar el contagio de algún virus o malware informático.

La utilización de estas herramientas (correo electrónico e internet debe ser racional, eficiente y segura, por lo cual deberá evitarse cualquier actividad que pueda poner en riesgo los equipos y sistemas de COMFACUNDI o que pueda afectar su correcto y adecuado funcionamiento.

Está prohibido utilizar esas herramientas (correo electrónico e internet) como medio para generar o transmitir mensajes que puedan afectar de cualquier manera la imagen, dignidad y el buen nombre de terceras personas o de COMFACUNDI.

El proceso de Tecnología configura los permisos y colocará restricciones de acceso a páginas de internet según el estándar anterior o por solicitud de algún líder de proceso, subdirector o director.

COMFACUNDI tiene el derecho de monitorear todos los aspectos relacionados con sus sistemas de cómputo, incluyendo, pero no limitándose a, grupos de conversación o chats, de noticias, revisión de material bajado de internet, monitoreo de sitios visitados en internet, revisión del correo enviado/recibido por el usuario.

El material que contenga carácter fraudulento, ilegal que vaya en contra de la moral o buena conducta, no podrá ser enviado por correo electrónico o cualquier forma de comunicación electrónica (grupos de noticias, grupos de conversación o chats) o exhibido o almacenado en los equipos de COMFACUNDI.

Está prohibido adulterar o intentar adulterar mensajes de correo.

No está permitido mensajes de correo utilizando la cuenta de correo de otra persona exceptuando la administración de calendarios compartidos cuando el jefe inmediato lo autorice.

Las listas de distribución son administradas por el responsable del proceso de Tecnología y requieren autorización del jefe inmediato.

No se puede cambiar, o disfrazar o intentar cambiar el campo de identificación de quien origina el correo.

Está prohibido enviar información confidencial o reservada de COMFACUNDI a personas, organizaciones externas, salvo en los casos expresamente previstos en la Constitución Política y en la Ley y por parte de los colaboradores autorizados internamente para ello.

No responda mensajes donde solicitan información personal o financiera para participar en sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Debe informar a través de la mesa de servicio con el fin de bloquear dicho remitente y evitar que estos mensajes lleguen a más colaboradores.

COMFACUNDI establecerá controles a internet para minimizar el riesgo, regular el tráfico y en consecuencia prestar un mejor servicio. El control de acceso a internet será medido con base a la navegación sobre grupo de páginas (por ejemplo, categorías) consideradas como no productivas para COMCACUNDI. Es decir que no sirvan de apoyo para el desempeño de las funciones de los usuarios de COMFACUNDI, que no son de interés general.

COMFACUNDI puede utilizar tecnología para identificar y bloquear sitios de internet con material considerado inadecuado bajo las regulaciones colombianas. En el evento, que el usuario encuentre este tipo de material en internet, deberá desconectarse del sitio de manera inmediata e informar al proceso de Tecnología por medio de la mesa de servicio para su solicitar su bloqueo.

El correo en cadenas es un mensaje enviado a un número de destinatarios para que estos a su vez se lo reenvíen a otro. El envío de correo masivo se refiere a aquel enviado a un gran número de receptores sin un propósito relacionado con la misión de COMFACUNDI. El usuario deberá borrar todos los correos de cadena masivos (no relacionados con la misión de COMFACUNDI) y abstenerse de enviarlos a otras personas.

COMFACUNDI, contará permanentemente con las herramientas de protección a nivel de red y de estaciones de trabajo, contra código maliciosos que será administrado por el proceso de Tecnología.

Todos los equipos corporativos que se conecten a la red LAN o la red WIFI de colaboradores de COMFACUNDI deben tener instalado el antivirus institucional actualizado.

Es responsabilidad de cada usuario, revisar que todos los medios extraíbles sean verificados con un antivirus provisto por COMFACUNDI, antes de procesarlos en los computadores personales o servidores de la organización.

Es responsabilidad del administrador del antivirus mantener en estado óptimo de funcionamiento (configuración, actualización, licenciamiento) las herramientas y procedimientos que permitan prevenir, detectar y corregir incidentes por código malicioso.

El antivirus debe ser configurado desde la consola para que diariamente realice búsqueda y detección de código malicioso y lo reporte a la consola.

Los equipos que reporten código malicioso o virus serán desconectados de la red LAN hasta tanto sea remediado y se implementen los controles de protección.

En casos de excepción, sólo se debe permitir la utilización de código ActiveX firmados por entidades de confianza.

Las copias de respaldo de los activos de información de COMFACUNDI deben reposar según lo establecido en el procedimiento PR-GT-001 Backup Bases de datos.

Deben existir al menos dos copias de la información de las bases de datos, una de las cuales deberá permanecer fuera de las instalaciones de COMFACUNDI.

La restauración de las copias de respaldo en ambientes de producción debe estar debidamente aprobadas por el responsable de la información.

Los operadores o administradores de las bases de datos periódicamente verificarán la ejecución correcta del Backup en el sistema de almacenamiento dispuesto para tal fin.

El proceso de Tecnología debe mantener un inventario actualizado de las copias de respaldo.

Es responsabilidad de cada área mantener depurada la información de las carpetas designadas para su uso en la nube, como mejor práctica para la optimización de uso de los recursos que entrega COMFACUNDI a sus usuarios.

Toda conexión a la red debe contar con un mecanismo de autenticación que valide al usuario.

Toda estación cliente que se conecte a la red LAN o WIFI de colaboradores de COMFACUNDI, debe estar debidamente autorizada, debe ser incluida en el dominio y cumplir con los mecanismos de control de seguridad como instalación de actualizaciones, herramienta de gestión y antivirus actualizado.

La conexión de terceras partes a la red LAN se hará cumpliendo con la debida autorización del proceso de Tecnología y con una aceptación por parte del tercero de cumplir con las características de seguridad y políticas definidas por COMFACUNDI.

La conexión de usuarios que realicen labores de carácter temporal se hará a la red de invitados en la cual solo tendrán acceso al servicio de internet, sin necesidad de incluirlo al dominio.

La seguridad perimetral debe tener mecanismos de control que incluya: firewall, filtro de contenido, antivirus y antispam.

Las conexiones con las redes públicas deben estar protegidas por un firewall y los mecanismos de control, que posea las reglas apropiadas para filtrar el tráfico permitido entre las redes.

La red interna de COMFACUNDI debe contar con una segmentación lógica o física que agrupe los elementos de red con al menos los siguientes segmentos: Red LAN que contiene las estaciones cliente, red de servidores y dispositivos de red.

Los Administradores de Infraestructura y Redes o el Administrador de Redes del área de tecnología son los responsables de garantizar que los medios extraíbles a cargo del centro de cómputo sean destruidos antes de darlos de baja.

Los equipos que van a ser objeto de reemplazos por daño de alguno de sus componentes se les debe retirar los medios extraíbles antes de la salida de COMFACUNDI.

El acceso a los buzones de correo electrónico debe estar controlado por contraseña y nombre de usuario.

Se encuentra prohibido descargar, almacenar o guardar bases de datos personales en cualquier dispositivo de la organización. En aquellos casos donde se requiera el tratamiento de bases de datos personales, debe hacerse única y exclusivamente a través de la nube o medio remoto asignado por la organización para tal fin. El proceso de Tecnología prestará apoyo necesario para este proceso de acuerdo a solicitud en la mesa de servicio.

10. GESTIÓN DE COMUNICACIONES

Se encuentran enfocadas a generar las políticas de intercambio de información y gestión de la seguridad en las redes.

Los accesos de conexión remota son exclusivamente para propósitos laborales y su solicitud debe sustentarse con el diligenciamiento del formato de solicitud de usuarios claves.

El acceso remoto de usuarios a la red LAN de COMFACUNDI se permitirá por medio del servicio de conexión remota y VPN, siempre y cuando cuenten con tecnología de cifrado.

La activación de conexión remota de usuarios internos o externos deber ser debidamente solicitada, justificada y aprobada a través de un procedimiento de solicitud de usuarios y claves.

Si las áreas requieren conexiones remotas o VPN deben ser solicitadas al proceso de Tecnología a través de la mesa de servicio.

Las conexiones de acceso Remoto o VPN deben estar monitoreadas.

Se deberá igualmente seguir todos los lineamientos establecidos en la Política Manejo Correo electrónico PO-GT-004.

11. LINEAMIENTOS PARA LA ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

A través de lineamientos generales para el desarrollo seguro, mantenimiento y adquisición de software al interior de COMFACUNDI se definen los controles de seguridad de la siguiente manera:

11.1 Establecimiento de los Requisitos Seguridad de los Sistemas de Información

El proceso de Tecnología es responsable de dar cumplimiento a los estándares de seguridad establecidos con los líderes funcionales de los sistemas de información y aplicaciones.

Para los sistemas de información, aplicaciones y portales que manejen datos confidenciales o reservados, los líderes procesos y el proceso de Tecnología deben velar por el cumplimiento de los controles de seguridad que garanticen la preservación de la confidencialidad e integridad de la información.

El proceso de Tecnología establece los lineamientos de seguridad de la infraestructura tecnología, que garantice el cumplimiento de los controles y la salvaguarda de la información de manera segura.

El proceso de Tecnología primará la adopción de enfoques de seguridad para diseño de sistemas, en aquellos procesos de desarrollo contratados con terceros y sobre todo en los catalogados como críticos.

Los Administradores o líderes técnicos de los sistemas de información, aplicaciones y portales de la entidad deben asegurar que desde los sistemas de información, aplicaciones y portales no se permita la modificación de parámetros a nivel de software base o sistema operativo. Así mismo, se debe garantizar que no se visualicen en pantalla ni se almacene en base de datos las contraseñas con cadenas de conexión e información en texto plano.

Está prohibida la manipulación de información directamente desde la base de datos. Si en algún momento se requiere realizar ajustes directamente en la base de datos, deberá dejarse el registro en el sistema de mesa de servicio con la aprobación del propietario del activo de información, Jefe de Tecnología y visto bueno del proceso de Control Interno.

Los Administradores o líderes técnicos de los sistemas de información, aplicaciones y portales de la entidad deben asegurar que la información establecida como reservada, cuente con mecanismos de seguridad necesarios que eviten su alteración o borrado por personal no autorizado.

Los desarrolladores internos o externos deben asegurarse de que los controles criptográficos o de cifrado, de los sistemas de información desarrollados para COMFACUNDI, cumplan con los lineamientos o directrices establecidos por el proceso de Tecnología.

El proceso de Tecnología es la responsable de mantener licenciado el software institucional necesario para el desarrollo y puesta en producción de los sistemas de información, aplicaciones y portales.

El proceso de Tecnología debe asegurarse que los sistemas de información adquiridos o desarrollados por contratistas cuenten con un adecuado licenciamiento y se debe especificar las condiciones de uso del software y los derechos de propiedad patrimoniales. Una vez recibido por la entidad se debe dejar registro en para que ingrese al inventario de activos de la información.

11.2 Desarrollo seguro, pruebas y soporte

COMFACUNDI vela porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad y buenas prácticas para desarrollo seguro y pruebas de aceptación de los Sistemas de Información, Aplicaciones y Portales desarrollados. Así mismo, se asegura que el software desarrollado o adquirido cuente con el nivel de soporte requerido por la organización.

El proceso de Tecnología es responsable de:

- Establecer la metodología 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.
- Velar porque el contratista disponga de una herramienta para el control de versiones que permita a los desarrolladores llevar el control de versiones del software desarrollado.
- Asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- Asegurar la infraestructura tecnológica necesaria para la puesta en producción de los sistemas de información, aplicaciones y portales, ya sean nuevos o ajuste a los existentes.
- Ofrecer soporte especializado a los sistemas de información, aplicaciones y portales a través del sistema de mesa de servicio.
- Realizar monitoreo periódico del soporte especializado a los sistemas de información, aplicaciones y portales.

Los Administradores o líderes técnicos de los sistemas de información, aplicaciones y portales de COMFACUNDI son responsables de:

- Velar por que los desarrolladores internos y externos implementen los lineamientos de seguridad, de tal forma que se controle el acceso no autorizado a éstos.
- Considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Mantener actualizada la documentación (desarrollo interno o externo) de acuerdo a la lista de chequeo de la documentación de los sistemas de información, donde se establecen los documentos mínimos exigidos dependiendo de su clasificación.
- Garantizar que el desarrollo se realice con herramientas y software debidamente licenciado.
- Asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de controles adicionales como captcha o el ingreso de parámetros adicionales de verificación como por ejemplo doble autenticación.
- Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, que pudiera ser almacenada en cookies y complementos, entre otros.
- Prevenir la revelación de la estructura de directorios o estructuras relacionales en las bases de datos de los sistemas de información desarrollados o adquiridos.
- Remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

- Evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- 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.
- Proteger el código fuente de los aplicativos desarrollados ya sean propios o contratados, de tal forma que no pueda ser descargado ni modificado por los usuarios.
- Asegurar que no se permita que los aplicativos desarrollados ya sean propios o contratados, ejecuten comandos directamente en el sistema operativo.
- Definir el servicio y los acuerdos de niveles de servicio para la atención de incidencias y peticiones a nivel técnico.
- Proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de COMFACUNDI; dicho soporte debe contemplar tiempos de respuesta aceptables para la organización.
- Garantizar que los sistemas de información, aplicaciones y portales sean compatibles con los protocolos IPv4 e IPv6. Solicitar al proceso de Tecnología, la autorización para la utilización de software libre, software gratuito o software licenciado y que esté no se hubiese contemplado desde el inicio de las especificaciones. De no ser así, incurre en falta grave y puede ser rechazado el producto o servicio ofrecido, dando a lugar al incumplimiento en las obligaciones del contrato.

Los líderes funcionales y propietarios de los sistemas de información, aplicaciones y portales de COMFACUNDI son responsables de:

- Definir los requerimientos funcionales de los sistemas de información.
- Una vez aprobados los requerimientos funcionales, cualquier ajuste se debe realizar por control de cambios para el análisis respectivo, para su aprobación o rechazo. En caso de ser rechazado el ajuste se debe anexar la debida justificación.
- Realizar las pruebas funcionales para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción.
- Definir el servicio y los acuerdos de nivel operacional para la atención de incidencias y peticiones a nivel funcional.

12. LINEAMIENTOS PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

COMFACUNDI adopta los siguientes lineamientos para que la gestión de la seguridad de la información se encuentre alineada e incluida dentro de los planes de continuidad del negocio y la estrategia de recuperación ante desastre a nivel organizacional:

- El proceso de Planeación y Proyectos coordinará el establecimiento y revisión anual del Plan de Continuidad del Negocio organizacional, mediante la identificación de los eventos que constituyen una emergencia o desastre, elaborando conjuntamente con los líderes responsables de los diferentes procesos COMFACUNDI, los planes de contingencia que permitirán mitigar los efectos adversos de un evento y disminuyendo los riesgos de afectación de las operaciones.
- Los subdirectores y líderes de procesos junto con los responsables de los activos de información deben garantizar la aprobación, pruebas y revisión periódica de los planes de contingencia de los servicios a cargo. Así como evaluar los riesgos e impactos de la pérdida de continuidad.
- El Plan de Recuperación de Desastres (DRP) de TI es responsabilidad de del área de tecnología, quien deberá formularlo, probarlo, implementarlo, actualizarlo y gestionarlo.

12.1 El Comité de Seguridad de la Información debe:

- Identificar y evaluar las situaciones que serán consideradas como emergencia o desastre para COMFACUNDI y autorizar la activación de planes de manejo de emergencias o continuidad de negocio.
- Establecer los lineamientos de respuesta ante incidentes de seguridad y desastres.
- Evaluar y hacer seguimiento a los resultados de las pruebas periódicas del plan de recuperación ante desastres o continuidad de negocio.
- Elaborar el plan de recuperación ante desastres de TI (DRP), para el centro de cómputo de la entidad y un plan de contingencia para cada sistema informático, servidores, sistemas operativos y dispositivos de red.
- Participar en las pruebas de recuperación ante desastres planificadas y efectuadas, notificando los resultados obtenidos al Comité de Seguridad de la Información.
- Formular las mejoras a los planes de contingencia y recuperación ante desastres de acuerdo con los resultados de las pruebas efectuadas.
- Liderar la aplicación del plan de recuperación ante desastres y apoyar dentro de su competencia a las áreas en la ejecución de sus planes de contingencia.

12.2 Responsabilidad de todos los procesos o áreas:

- Participar en la elaboración del plan de continuidad, para los servicios y productos a su cargo.
- Elaborar el plan de contingencia del servicio correspondiente al proceso.
- Participar en las pruebas de continuidad de servicios planificadas y efectuadas, y notificar los resultados.
- Formular las mejoras a los planes de continuidad de acuerdo con los resultados de las pruebas efectuadas.

- Liderar la aplicación del plan de continuidad a su cargo y apoyar, dentro de su competencia, a las dependencias en la ejecución de sus planes de contingencia.

12.3 Responsabilidades del oficial de seguridad de la información:

- Apoyar la realización de los análisis de impacto al negocio y el análisis de riesgos y de continuidad.
- Proponer estrategias de recuperación, en caso de activarse el plan de contingencia o continuidad del negocio.
- Definir los controles de seguridad de la información que se deben adoptar en caso de ser necesario activar el plan de continuidad o recuperación ante desastres.

13. LINEAMIENTOS PARA LA GESTIÓN DE VULNERABILIDAD TÉCNICA

El objetivo de estos lineamientos es prevenir la ocurrencia de eventos e incidentes de seguridad de la información generadas por el aprovechamiento de vulnerabilidades técnicas por parte de atacantes, las cuales se definen a continuación:

- El Oficial de Seguridad de la Información, realiza un análisis de vulnerabilidades periódica de los servicios y análisis de riesgos de los activos de información. Como resultado del análisis, se establece un plan de tratamiento de riesgo acorde con los recursos técnicos y financieros con los que se cuente, a fin de cerrar las brechas de seguridad encontradas.
- El Oficial de Seguridad de la Información es el encargado de dar lineamientos y recomendaciones para la mitigación de las vulnerabilidades.
- El Oficial de Seguridad de la Información y el Jefe de Tecnología, establecen la prioridad en la ejecución de los controles dentro de la declaración de aplicabilidad y los responsables de su ejecución.
- El Comité de Seguridad de la Información establece el procedimiento y los protocolos para la gestión de incidentes de seguridad, el cual debe seguirse cuando se considere que un incidente es causado por una falla de seguridad.

14. LINEAMIENTOS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de gestionar adecuadamente los eventos e incidentes que puedan afectar la confidencialidad, integridad o disponibilidad de los activos de información, COMFACUNDI adopta, implementa, mantiene y mejora una guía de gestión de incidentes de seguridad de la información y protección de datos personales, la cual se complementa con los siguientes lineamientos:

- Todos los colaboradores, contratistas o pasantes deben reportar sin demoras injustificables a los responsables de sus procesos o áreas o al proceso de Tecnología cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de cualquier activo de información.

- El reporte de los eventos o incidentes de seguridad de la información se realiza de acuerdo con la guía de gestión de incidentes de seguridad de la información y protección de datos personales en la mesa de servicio del proceso de Tecnología.
- La evaluación de los diferentes eventos e incidentes de seguridad de la información es realizada por la mesa de servicio del proceso de Tecnología. Los eventos de seguridad de la información que sean calificados como incidentes de seguridad de la información se administran mediante la guía gestión de incidentes de seguridad de la información.
- COMFACUNDI evaluará como incidentes de seguridad de la información eventos asociados al incumplimiento de las políticas de seguridad de la información, los que correspondan a delitos informáticos calificados como tales por la normatividad vigente y los eventos que materialicen riesgos de seguridad digital y eventos asociados a la Protección de Datos Personales.
- La guía de gestión de incidentes de seguridad de la información define las acciones específicas para el reporte de eventos, incidentes o debilidades en seguridad de la información, evaluación y respuesta ante incidentes de seguridad de la información, aprendizaje y recolección de evidencias asociadas a los incidentes de seguridad de la información.

14.1 Acerca de la gestión de seguridad de la información

- La Política de Seguridad de la Información se desarrolla y actualiza en cada vigencia de acuerdo con los riesgos, los requerimientos corporativos y la normatividad colombiana, atendiendo las nuevas necesidades y la situación de la organización.
- El Oficial de Seguridad de la Información, realiza los análisis de impacto a la organización y los análisis de riesgos de continuidad para posteriormente proponer posibles estrategias de recuperación, en caso de activarse el plan de contingencia o continuidad del negocio, con las consideraciones de seguridad de la información que sean pertinentes tener en cuenta.
- El proceso de Tecnología y el Oficial de Seguridad de la Información, serán los encargados de elaborar el plan de recuperación ante desastres de TI (DRP), para el centro de cómputo de la entidad y un plan de contingencia para cada sistema informático, servidores, sistemas operativos y dispositivos de red.
- El proceso de Tecnología y el Oficial de Seguridad de la Información coordinan las pruebas de recuperación ante desastres planificadas y efectuadas, notificando los resultados obtenidos al Comité de Seguridad de la Información.

13.2 Reporte y tratamiento de incidentes de seguridad

- COMFACUNDI promoverá entre los colaboradores, contratistas y pasantes el reporte de incidentes relacionados con la seguridad de la información y los medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.
- COMFACUNDI asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y

solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

- El Director Administrativo o en su ausencia el Subdirector Organizacional y Financiero son los únicos autorizados para reportar incidentes de seguridad ante las autoridades o delegar este reporte en otro colaborador; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas sobre incidentes de seguridad de la información.
- Los propietarios de los activos de información deben informar a través de la mesa de servicio, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

El proceso de Planeación y Proyectos, a través de su jefe es responsable en conjunto con el Oficial de Seguridad de la Información de:

- Establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- Evaluar todos los incidentes de seguridad de acuerdo con las circunstancias particulares y escalar al proceso de Tecnología y al Comité de Seguridad de la Información, aquello que considere pertinente.
- Designar un colaborador o contratista calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su recurrencia.
- Crear bases de conocimiento para los incidentes de seguridad presentados con las respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros. Lo anterior con el apoyo del proceso de Tecnología.
- Convocar una vez materializado el incidente, al Comité de Seguridad de la información para tomar las medidas a que haya lugar y generar un plan de mejoramiento para evitar nuevamente su ocurrencia.

15. LINEAMIENTOS PARA EL CONTROL DE ACCESOS INFORMÁTICOS

15.1 Control de acceso a la red

El proceso de Tecnología es la responsable de implementar los protocolos de seguridad e infraestructura de red local, que permitan acceder a los recursos de manera segura.

Con el propósito de proteger los equipos de cómputo, equipos de comunicaciones y demás dispositivos tecnológicos de COMFACUNDI, no se permite la conexión a la infraestructura de red local de la organización a los equipos de cómputo y de comunicaciones propiedad de terceros sin previa autorización del Director Administrativo, Subdirector, Jefe, Coordinador o Supervisor Administrativo de contrato, mediante la solicitud realizada por medio de la mesa de servicio.

Los colaboradores, contratistas y pasantes pueden acceder a la infraestructura de la red local de COMFACUNDI a través de conexión LAN y WIFI, utilizando el equipo de escritorio o portátil asignado por la caja, el usuario asignado y clave.

Se pueden conectar a los recursos de conexión remota – VPN los colaboradores y contratistas previamente autorizados por el Director Administrativo, Subdirector, jefe, coordinador o supervisor administrativo del contrato, la solicitud se debe realizar a través de la de mesa de servicio del área de tecnología.

15.2 Control de acceso al sistema operativo

El proceso de Tecnología debe asegurar que los usuarios y perfiles de usuario que traen por defecto los sistemas operativos de la infraestructura tecnológica y bases de datos sean asegurados al ingresar a la infraestructura de COMFACUNDI y revisados periódicamente.

El proceso de Tecnología debe asegurar que los usuarios y perfiles de usuario que traen por defecto los sistemas operativos y software instalado en los computadores de escritorio, equipos portátiles, impresoras y demás dispositivos adquiridos por la entidad sean asegurados antes de entrar en uso.

Dichos elementos deben entregarse sin permisos de acceso al sistema operativo.

El proceso de Tecnología debe asegurar que desde los sistemas de información, aplicaciones y portales no se acceda directamente a los sistemas operativos.

El proceso de Tecnología debe realizar monitoreo periódico del software instalado en los equipos de cómputo conectados a la red de COMFACUNDI.

15.3 Control de acceso a aplicaciones e información

Las áreas propietarias de los sistemas de información, aplicaciones y portales de COMFACUNDI con el apoyo del proceso de Tecnología son responsables de mantener actualizados los privilegios de acceso a los sistemas de información de sus usuarios.

El proceso de Tecnología es responsable de garantizar la seguridad de la plataforma tecnológica donde se encuentran alojados los sistemas de información, aplicaciones y portales de COMFACUNDI

Los Subdirectores y/o Jefes de proceso o área designan al colaborador que es responsable del manejo funcional del cada sistema de información, aplicación y portal de COMFACUNDI

El Jefe de Tecnología es el encargado de designar el colaborador y/o contratistas responsables de atender los requerimientos realizados por un área funcional para un determinado sistema de información, aplicación o portal de COMFACUNDI.

Para aquellos sistemas que permitan la opción de caducidad contraseñas, las mismas deberán ser configuradas para un tiempo no superior a seis (6) meses.

15.4 Gestión de Contraseñas

Las contraseñas o claves de acceso a los activos de información son personales e intransferibles.

Toda acción realizada con el usuario y contraseñas asignadas es responsabilidad del colaborador, contratista, pasante o tercero al que se le ha asignado.

Las contraseñas no deben ser divulgadas o compartidas entre usuarios.

Cualquier daño o alteración de la información es responsabilidad del usuario que la realizó.

No se debe prestar el usuario asignado ni la contraseña, ya que, en caso de haber alguna violación de seguridad, la responsabilidad recae sobre la persona a cargo de dicho usuario.

Las contraseñas se deben construir de acuerdo con las guías e instrucciones que emita el proceso de Tecnología.

15.5 Lineamientos para una contraseña segura

Utilizar al menos ocho (8) caracteres para crear la clave, la cual debe incluir como mínimo mayúsculas, minúsculas y números.

Se recomienda utilizar caracteres que alternan aleatoriamente mayúsculas y minúsculas.

Se recomienda elegir una contraseña que pueda recordarse fácilmente y que pueda digitarse rápidamente (preferiblemente sin que sea necesario mirar el teclado).

Evitar utilizar la misma contraseña siempre en todos los sistemas o servicios de información.

No se debe utilizar información personal en la contraseña (nombre del usuario, nombre de familiares, apellidos, apodos, fecha de nacimiento, número de documento, número de teléfono, nombre de mascotas, actores preferidos).

Evitar utilizar secuencias básicas de teclado. Por ejemplo: “qwerty”, “asdf” o las típicas en numeración: “1234” o “98765”.

No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).

No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar las claves de acceso en documentos de texto o en el celular sin el debido aseguramiento por cifrado.

No enviar la contraseña por correo electrónico o mensajes de texto

16. LINEAMIENTOS PARA EL CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Con la identificación de estos lineamientos se pretende evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad de la información, por lo tanto:

- Para la elaboración de las políticas del Sistema de Gestión de Seguridad de la Información de COMFACUNDI, se tomarán como base los requisitos legales en materia de seguridad de la información, la política de gobierno digital controles y requisitos identificados en el Modelo de Seguridad y Privacidad de la información de MINTIC y estándar ISO/IEC 27001.
- Las políticas incluidas se constituyen como parte fundamental del Sistema de Gestión de Seguridad de COMFACUNDI y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos. Esto debe quedar incluido en los términos contractuales.
- La seguridad de la información es una prioridad para COMFACUNDI y, por lo tanto, es responsabilidad de todos los colaboradores, contratistas y pasantes cumplir con lo establecido en la Política de Seguridad de la Información, de tal forma que no se realicen actividades que se encuentren en contra de la esencia y el espíritu de cada una de estas políticas.
- Las actualizaciones sobre la Política del Sistema de Gestión de Seguridad de la Información se publicarán en el Sistema Integrado Gestión.
- De conformidad con sus obligaciones en materia de protección de datos personales, la entidad ha adoptado la Política de Tratamiento de Datos Personales.

Los servicios informáticos por contratistas y proveedores deben realizarse de una forma controlada, segura y organizada definida a través de acuerdos de niveles de servicio (ANS).

Los contratistas y proveedores deben cumplir con las normas de seguridad y controles definidos por COMFACUNDI.

Los contratistas y proveedores están obligados a cumplir los Acuerdos de Nivel de Servicio (ANS).

Los contratistas y proveedores deben incluir la evaluación de riesgos asociada al cambio, la cual debe ser revisada y aceptada por el interventor o supervisor técnico del contrato.

Los terceros que tengan acceso a los activos de información tecnológicos deben cumplir con el Manual de seguridad de la Información y el Manual de Protección de Datos Personales.

17. ROLES Y RESPONSABILIDADES

Por lo cual se asegura que cada actividad establecida dentro de la etapa de planeación, implementación y gestión del Modelo de Seguridad y Protección de la Información tenga un responsable claro y de igual forma que cada uno de los miembros del equipo responsable

de la ejecución entiendan claramente sus roles y responsabilidades. Lo anterior tiene como objetivo minimizar el riesgo a que se presenten imprecisiones en referencia a las responsabilidades que cada rol tiene.

Es de resaltar que el Consejo Directivo y la Dirección Administrativa se comprometen a velar por el cumplimiento de la presente política y tomar las acciones necesarias en caso del incumplimiento parcial o total de la misma.

17.1 Jefe de Tecnología

Responsabilidades:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias de la planeación, implementación y gestión del MSPI, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.
- Alinear los objetivos operacionales de seguridad de la información hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la corporación.
- Gestionar el equipo de trabajo encargado de la implementación y aplicación del MSPI, definiendo roles, responsabilidades, entregables y tiempos.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos de su implementación dentro del MSPI para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- Monitorear el estado de la planeación e implementación del MSPI en términos de calidad de los productos, tiempo y costos.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Asegurar la calidad de los entregables y de la implementación del MSPI en su totalidad.
- Mantenimiento de esta política y brindar consejo y guía para su aplicación, así como también participar activamente en la investigación de cualquier indicio de desviación en el cumplimiento de sus objetivos.

17.2 Grupo de Trabajo de Tecnología

Sus responsabilidades son:

- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo de la planeación, implementación, gestión y operación del MSPI.
- Ayudar al Jefe de Tecnología, en la gestión de proveedores de seguridad en TI e infraestructura tecnológica.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el Jefe de Tecnología.
- Las que considere el Jefe de Tecnología o el comité de seguridad de la organización.

17.2.1 Equipo de trabajo del SIG

Responsabilidades:

- Dar apoyo para la correcta integración y articulación del Sistema de Gestión de Seguridad de información (SGSI) en el Sistema Integrado de Gestión (SIG).
- Articular la metodología de gestión de riesgos a nivel institucional con los riesgos de la información y protección de datos personales a nivel de procesos.
- Recomendar lineamientos y criterios para mitigar riesgos.
- Participar en el análisis de los requerimientos de los usuarios y criterios para mitigar riesgos.
- Publicar las matrices de riesgos, campañas de promoción de cultura de gestión del riesgo y de avances y resultados en la gestión, en conjunto con el equipo de gestores del Sistema Integrado de Gestión.

17.2.2 Líderes de Proceso o Áreas y Proceso de Talento Humano

Son los responsables de:

- Solicitar la creación, modificación o cancelación de cuentas de usuario, como también de perfiles de cuentas a la mesa de servicios del proceso de Tecnología.
- Conjuntamente con el área responsable de TI, el proceso de Talento Humano se encargará de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.
- Los líderes de proceso o área serán responsables de la identificación, clasificación y valoración de activos de información que es recibida, procesada y producida. Las características del inventario, como su clasificación, ubicación y acceso las especifica el área responsable de TI a través del oficial de seguridad de la información, así mismo deberá brindar con ayuda del proceso de tecnología, las herramientas que permitan la administración del inventario y facilitar los recursos que aseguren su disponibilidad y confidencialidad.
- De igual manera los líderes de proceso o área son los responsables de definir qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es gestionado, para lo cual el área de TI proporcionará las herramientas necesarias.

17.2.3 Oficial de Seguridad de la Información

Sus responsabilidades son:

- Identificar la brecha entre el MSPI y la situación de COMFACUNDI.
- Generar el cronograma de la implementación del Modelo de Seguridad y Privacidad de la Información.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo.

- Planear, coordinar y administrar los procesos de seguridad informática en COMFACUNDI.
- Brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de COMFACUNDI.
- Asegurar el buen funcionamiento del proceso de Seguridad Informática de COMFACUNDI.
- Ser el punto de referencia para todos los procesos de seguridad y ser capaz de guiar y aconsejar a los usuarios de COMFACUNDI sobre cómo desarrollar procedimientos para la protección de los recursos de software y hardware.
- Guiar al cuerpo directivo y a la administración de COMFACUNDI ante incidentes de seguridad mediante un Plan de Respuesta a Incidentes, con el fin de atender rápidamente este tipo de eventualidades.
- Proponer y coordinar la realización de un análisis de riesgos formal en seguridad de la información que abarque toda la organización.
- Planear y diseñar soluciones de seguridad informática de acuerdo con los requerimientos y necesidades que se presenten en los diferentes proyectos, verificar el cumplimiento de la norma y de los estándares internacionales.
- Emitir conceptos técnicos, con el objeto de aconsejar y orientar la toma de decisiones en relación con la seguridad de los proyectos informáticos y demás requerimientos.
- Apoyar a COMFACUNDI en la definición de procesos, procedimientos, lineamientos asociados al componente de Gestión de Seguridad de la Información (SGSI).
- Apoyar a COMFACUNDI en la actualización de la presente política, activos de información e identificación de los riesgos en materia de tecnologías de informática y comunicaciones con el fin de velar por la disponibilidad, seguridad, integridad y respaldo de la información que la corporación utiliza y procesa para su funcionamiento y toma de decisiones.
- Apoyar a COMFACUNDI en las actividades relacionadas con la implementación de las estrategias de ciberseguridad y la normativa de protección de datos personales de la Superintendencia de Industria y Comercio.
- Apoyar la aplicación del Modelo de Seguridad y Privacidad de la Información (MSPI) en el componente de Gestión de Seguridad de la Información (SGSI) de la corporación, alineado con la norma ISO/IEC 27001:2013.
- Apoyar las actividades de divulgación y promoción de la importancia del componente de Gestión de Seguridad de la Información (SGSI) y los temas relacionados en la normativa aplicable.

17.2.4 Oficial de Protección de Datos Personales.

- Velar por la implementación y seguimiento efectivo de las políticas y procedimientos adoptados para el cumplimiento de la Ley y la implementación de buenas prácticas de gestión de datos personales dentro de COMFACUNDI.
- Promover una cultura de protección de datos dentro de COMFACUNDI.

- Mantener el inventario de las bases de datos personales de COMFACUNDI.
- Registrar las bases de datos en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio.
- Servir de enlace y coordinador con los demás procesos o áreas de COMFACUNDI para asegurar la implementación transversal del Programa Integral de Gestión de Datos Personales.
- Diseñar un programa de entrenamiento de los colaboradores.
- Integrar las políticas de protección de datos dentro de las actividades de los demás procesos o áreas.
- Obtener las declaraciones de conformidad de la SIC cuando sea requerido.

17.2.5 Administradores del Área Responsable de TIC

El rol de Administrador de Soluciones y TI (Sistemas de Información, aplicativos y portales), Administrador de Infraestructura, redes y plataforma tecnológica tienen las siguientes responsabilidades:

- Apoyar la recolección de evidencia de los incidentes informáticos relacionados con la infraestructura tecnológica.
- Identificación de riesgos de los activos de información de su competencia, de acuerdo con el procedimiento de Gestión de Riesgos y los lineamientos vigentes para la Gestión de Riesgos de COMFACUNDI.

17.3 Proceso de Control Interno

- El proceso de Control Interno es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información.
- Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

17.4 Comité de Seguridad de la Información y Ciberseguridad

COMFACUNDI garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación del Comité de Seguridad de la Información, el cual será integrado por los líderes de los siguientes procesos o áreas:

- Director Administrativo
- Jefe de Tecnología
- Jefe de Planeación
- Jefe de Control Interno
- Subdirectores
- Jefe Jurídico

- Oficial de Seguridad de la Información
- Oficial de Protección de Datos Personales

El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

Este Comité tiene como objeto asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en COMFACUNDI, así como de la aplicación de la presente política.

Sus miembros serán responsables de elaborar su reglamento interno de trabajo.

18. VIGENCIA

La presente Política entrará en vigencia a partir de su aprobación y podrá ser modificada en cualquier momento de acuerdo a los procedimientos previstos para tal fin.

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
01	26/Abr/2018	Emisión (Aprobada con Acta #486 del Consejo Directivo el 26 de abril del 2018).
02	26/Feb/2019	Se incluyo el ítem “Se establezcan políticas encaminadas al buen uso del correo electrónico y acceso a internet”. Política aprobada con Acta #497 del Consejo Directivo el 25 de febrero del 2019.
03	26/Oct/2021	Se actualiza política de seguridad de la información y ciberseguridad dando alcance a la planeación, implementación y gestión del Modelo de Seguridad y Protección de la Información. Se actualiza el código de la política con las iniciales del proceso tecnología (TE). Se actualiza el nombre del cargo del responsable de la documentación de la política (Profesional Especializado en Seguridad de la Información, ciberseguridad e Infraestructura). Aprobada con Acta #533 del Consejo Directivo el 26 de octubre del 2021.

DOCUMENTÓ	REVISÓ	APROBÓ
Firma:	**Firma:**	**Firma:**
Nombre: Jorge Asdrúbal Tamayo	**Nombre:** José Gildardo Téllez	**Nombre:** Víctor Julio Berrios
Cargo: Profesional Especializado en Seguridad de la Información, ciberseguridad e Infraestructura	**Cargo:** Jefe de Tecnología	**Cargo:** Director Administrativo
Fecha: 28/Jun/2021	**Fecha:** 28/Jun/2021	**Fecha:** 26/oct/2021