CONTENIDO

1. INTRODUCCIÓN

La Caja de Compensación Familiar del Valle del Cauca Comfenalco Valle Delagente, identifica la información como componente indispensable para el logro de sus objetivos estratégicos, razón por la cual es necesario la creación de un marco regulatorio que asegure que la información está protegida de manera adecuada, independiente de la forma en que esta sea tratada.

Este documento describe las políticas y lineamientos definidos por la Corporación para la protección de la información de manera adecuada y para su elaboración se tomó como referente la norma ISO/IEC 27001:2013.

La seguridad de la información es un tema relevante para la Corporación, siendo responsabilidad de todos los colaboradores cumplir sus disposiciones y velar porque no se realicen actividades que vayan en contra de estas políticas.

2. OBJETIVOS

- Establecer las directrices generales que propendan por la Seguridad de la Información de Comfenalco Valle Delagente, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de procurar el cumplimento de la confidencialidad, integridad y disponibilidad.
- Mantener la Política de Seguridad de la información actualizada, a efectos de asegurar su vigencia y nivel de eficacia.
- Comprometer a todo el personal de la Corporación con el proceso de Seguridad de la Información, agilizando la adopción y aplicación de los controles con dinamismo y armonía.
- Convertir a los trabajadores de Comfenalco Valle Delagente en gestores de la seguridad de la información.

3. ALCANCE

El alcance de esta política se aplica a toda la Corporación, a los recursos informáticos, a la totalidad de los procesos y las personas que interactúan con los sistemas de información, ya sean internos o externos vinculados a Comfenalco Valle Delagente.

4. TÉRMINOS Y DEFINICIONES

Activo de información: Elementos de hardware, software de procesamiento, almacenamiento y comunicaciones, bases de datos, documentos físicos, procesos procedimientos y recursos humanos asociados con el manejo de los datos y la información misional que maneja la Corporación.

Acuerdo de Confidencialidad: Es un documento en los que los colaboradores de la Corporación o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Corporación, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Amenaza: Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Autenticidad: Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.

Aviso de IDS sobre Buffer overflow: Es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada.

Cadena de Custodia: Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.

Capacity Planning: Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de cableado: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para

prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: Es la propiedad de prevenir la divulgación de la información a personas o sistemas no autorizados.

Contención: Evitar que el incidente siga ocasionando daños.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo, Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: Es la propiedad que se refiere a que la información esté a disposición de quienes necesiten acceder a ella.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Erradicación: Eliminar la causa del incidente y todo rastro de los daños.
Evento de seguridad: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2018]

Gestión de Incidentes: Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de la Corporación, minimizando su impacto en el negocio y la probabilidad que se repita.

Guías de clasificación de la información: Directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

Hacking Ético: Es el conjunto de actividades para ingresar a las redes de datos y voz de la Corporación con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o

redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Hash: Función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.

IDS: Software de detección de intrusos.

Impacto: Consecuencias que produce un incidente de seguridad sobre la organización.
Incidente de seguridad: Cualquier situación o evento que comprometa la operación o cualquier activo de información. Así mismo a cualquier sospecha de violación a las políticas de seguridad de la información de Comfenalco Valle Delagente.

Integridad: Es la propiedad de preservar la información libre de modificaciones que no fueron autorizadas.

Inventario de activos de información: Es una lista ordenada y documentada de los activos de información pertenecientes a la Corporación.

KDB: Una base de conocimiento es un tipo de base de datos para la gestión del conocimiento. Provee los medios para la recolección, organización y recuperación computarizada de conocimiento.

Licencia de Software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Log's: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.

Medio Removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de Usuario: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad Intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la Información: Es la unidad organizacional o proceso donde se crean los activos de información.

Recuperación: Volver el entorno afectado a su estado natural.

Recursos Tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Corporación.

Registros de Auditoría: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el Activo de Información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
SGSDP: Sistema de Gestión de Seguridad de Datos Personales.

Sniffer: Software que captura los paquetes que viajan por la red para obtener información de la red o del usuario.

Software Malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Validación: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

Vulnerabilidad: Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

Vulneración de Bases de Datos Personales: Se entenderá como incidencia toda vulneración a las bases de datos personales (entiéndase, servidores físicos, dispositivos de computo o archivadores físicos) de la Corporación que se realice sin autorización legal, contractual u organizacional.

5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

5.1 DIRECTRICES ESTABLECIDAS POR LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

5.1.1 Política de Seguridad de la Información

Propender por la conservación de la confidencialidad, la integridad y la disponibilidad de la información de la Corporación, así como de los sistemas implicados en su tratamiento, para lograr la alineación con los objetivos estratégicos y aumentar la confianza de nuestros grupos de interés, mediante la implementación de los requisitos propios de nuestra actividad, además de los legales y reglamentarios que sean de aplicación y tomando como referencia la norma ISO/IEC 27001:2013 y sus anexos, además de tener en cuenta la mejora continua en los procesos involucrados en la seguridad de la información.

5.1.2 Revisión de las Políticas para la Seguridad de la Información

El Area de Gobierno de Infomación tendrá la potestad de modificar la Política Global o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente a la aplicabilidad de las mismas.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Corporación estableció un Sistema de Gestión de Seguridad de Datos Personales, el cual esta definido por roles y responsabilidades para la administración, operación y gestión de la seguridad de la información.

6.1 ORGANIZACIÓN INTERNA

6.1.1 Roles y Responsabilidades para la Seguridad de la Información

La Jefatura de Gobierno de Información es responsable de revisar y proponer a las directivas para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejoras en pro de la seguridad de la información. Es responsabilidad de dicha Jefatura definir las estrategias de capacitación en materia de seguridad de la información al interior de Comfenalco Valle Delagente.

La Gerencia de Tecnologia de Informacion es responsable de implementar los controles tecnologicos definidos en pro de la seguridad de la información.

La Gerencia Administrativa proporcionará los mecanismos para propender por notificar a todo el personal que se vincula contractualmente con Comfenalco Valle Delagente, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan como recomendación de la Jefatura de Gobierno de Información.

La Gerencia Jurídica propenderá porque en todos los contratos que suscriba la Corporación quede consignada la cláusula de confidencialidad y la obligatoriedad tanto de trabajadores como de proveedores de dar cumplimiento a las políticas de seguridad de la información y tratamiento de datos personales.

La Jefatura de Auditoría Interna es responsable de programar que se realicen 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.

La Jefatura Logística es responsable de informar e implementar las medidas de seguridad física y del entorno de Comfenalco Valle Delagente.

6.2 DISPOSITIVOS MÓVILES

6.2.1 Política para dispositivos móviles

La Corporación proveerá las condiciones necesarias para el manejo de dispositivos móviles (Corporativos y personales) que hagan uso de los servicios de la Corporación, como también velará porque se haga uso responsable de los equipos y servicios proporcionados.

Normas dirigidas a: Tecnología de Información

- Investigar y probar las opciones de protección de los dispositivos móviles Corporativos y personales que hagan uso de los servicios provistos por la Corporación.
- Establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles corporativos que serán entregados a los colaboradores. Se deben configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- Activar la opción de cifrado de los dispositivos o su medio de almacenamiento, para que en caso de pérdida o robo no se comprometa la confidencialidad e integridad de la de los mismos.
- Realizar el borrado remoto del perfil corporativo contenido en los dispositivos móviles cuando se presente perdida, robo del dispositivo móvil o por el retiro de personal de la Corporación.
- Instalar el software antivirus que usa la Corporación en los dispositivos móviles que estén autorizados para el uso de los servicios provistos por la Corporación.

Normas dirigidas a: Todos los usuarios

- Los dispositivos móviles deberán contar con una clave de acceso, así como realizar los cambios periódicos que solicite el equipo.
- Evitar al máximo sostener conversaciones de información confidencial o privada de los Titulares por vía telefónica en lugares de alta concurrencia de público
- El teléfono móvil siempre debe estar bajo la custodia del responsable y no se deben dejar desatendidos.
- Las acciones que se generen con los dispositivos móviles, son únicamente responsabilidad del colaborador o contratista asignado.
- Informar la pérdida o el robo del dispositivo tan rápido como sea posible a la línea de atención de TI o por medio de SIRES, para proceder con el borrado del perfil Corporativo y evitar la pérdida de los datos.

- Está prohibido almacenar datos personales en dispositivos móviles de la Corporación.

7. SEGURIDAD DEL RECURSO HUMANO.

Para la Corporación el factor humano es clave en la obtención de los objetivos misionales, por eso busca contar con personal capacitado cuyas competencias y cualidades cumplan con los requisitos exigidos por la Corporación para cada puesto de trabajo.

7.1 ANTES DE ASUMIR EL EMPLEO

7.1.1 Selección

Normas dirigidas a: Gerencia Administrativa

- El área de Seleccion de Personal debe validar la veracidad de la información suministrada por el candidato antes de su vinculación.
- El área de Compensación y Beneficios debe garantizar que los colaboradores de la Corporación firmen las cláusulas de confidencialidad, de protección de datos personales y seguridad de la información al inicio del vínculo laboral.

7.1.2 Términos y condiciones del empleo

Normas dirigidas a: Gerencia Administrativa y Gerencia Jurídica

- En todos los acuerdos contractuales con empleados y contratistas, quedara establecida una cláusula de confidencialidad y no divulgación, en lo que respecta al tratamiento de la información de Comfenalco Valle Delagente.

7.2 DURANTE LA EJECUCIÓN DEL EMPLEO

7.2.1 Responsabilidades de la Dirección

Normas dirigidas a: Dirección

- La dirección exigirá a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y lineamientos establecidos por la Corporación.

7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.

Normas dirigidas a: GI

- Todos los colaboradores de Comfenalco Valle Delagente y cuando sea necesario, los contratistas que presten servicios en Comfenalco Valle Delagente, recibirán una inducción sobre las políticas y lineamientos de seguridad de la información, además de los procedimientos que apliquen para tal fin en sus labores o actividades desarrolladas en la Corporación.

7.2.3 Proceso disciplinario

Normas dirigidas a: Todos los usuarios

- La finalidad de las políticas de seguridad de la información es crear una cultura de seguridad de la información entre los colaboradores y terceros que interactúan con la Corporación, de acuerdo a esto es necesario que las violaciones a las políticas de seguridad de la información sean clasificadas, con el fin de aplicar medidas disciplinarias y mitigar posibles afectaciones contra la seguridad de la información, estas medidas pueden ser de orden administrativas, disciplinarias o penales, de acuerdo a la violación de seguridad presentada.

7.3 TERMINACIÓN Y CAMBIO DE EMPLEO.

7.3.1 Responsabilidades en la terminación o cambio de empleo

Normas dirigidas a: Compensación y Beneficios

- El área de Compensación y Beneficios deberá reportar al responsable de TI y al Oficial de Seguridad de la Información, los cambios de cargo y/o área, para que se realice el proceso de remover los accesos anteriores.
- El área de Compensación y Beneficios deberá reportar al responsable de TI y al Oficial de Seguridad de la Información, las novedades de vacaciones y/o licencias que requieran la ausencia del trabajador por más de quince (15) días.
- Cuando un trabajador termine su vinculación laboral, el área de Compensación y Beneficios reportará al responsable de TI y al Oficial de Seguridad de la Información, esta novedad, en lo posible, el mismo día que se conozca el hecho.

Normas dirigidas a: Tecnología de Información

- El área de tecnología de información bloqueará todos los accesos de un colaborador a los sistemas de información, en la fecha que indique el área de Compensación y Beneficios como de terminación de su contrato de trabajo.

- El área de tecnología de información bloqueará todos los accesos de un colaborador a los sistemas de información, durante la fecha que indique el área de Compensación y Beneficios como de inicio y fin de novedades y/o licencias superiores a quince (15) días.

8. GESTIÓN DE ACTIVOS.

La Corporación, como propietaria de la información que maneja, tanto física como digital en sus sistemas de información ya sea almacenada, procesada o transmitida, asignara responsabilidades a los líderes de las diferentes áreas sobre sus activos de información, asegurando el cumplimiento sobre su uso adecuado.

Ofrecerá una metodología de gestión e identificación de activos de información, que le permita a la Corporación administrarlos de acuerdo con las directrices otorgadas. Así mismo, evitar problemas de seguridad con la utilización, dentro y fuera de la Corporación, de medios removibles y equipos móviles que contengan información

crítica para la Corporación.

8.1 RESPONSABILIDAD POR LOS ACTIVOS

8.1.1 Inventario de activos

Normas dirigidas a: Dirección

- La Corporación debe contar con un inventario actualizado de activos de información y otros activos asociados con la información.

8.1.2 Propiedad de los activos

Normas dirigidas a: Los propietarios de activos de información

- Las Direcciones, Gerencias, Jefaturas y Coordinaciones, deben actuar como propietarias de la información física y electrónica de la Corporación, ejerciendo las siguientes actividades:
  - ✓ Aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
  - ✓ Asegurar que los activos están inventariados.
  - ✓ Asegurar que los activos están clasificados y protegidos apropiadamente.
  - ✓ Realizar revisiones periódicas de los accesos otorgados a activos críticos de acuerdo a las políticas de control de acceso.
  - ✓ Asegurarse del manejo apropiado cuando un activo va a ser eliminado o destruido.

Normas dirigidas a: Tecnología de Información

- La Gerencia de Tecnología de Información es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la Corporación y, en consecuencia, debe asegurar su apropiada operación y administración.
- La Gerencia de Tecnología de Información en conjunto con el Comité de Control de Cambios, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Corporación.
- La Gerencia de Tecnología de Información debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- La Gerencia de Tecnología de Información es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los colaboradores y de hacer entrega de las mismas.

8.1.3 Uso aceptable de los activos

Normas dirigidas a: Todos los usuarios

- Todos los colaboradores y contratistas deberán ser responsables del uso que hacen de cualquier activo de información o de cualquier recurso de procesamiento de la información, el cual deberá ser conforme a los requisitos de seguridad de la información

de la Corporación y con el único fin de llevar a cabo las labores de la Corporación, por consiguiente, no podrán ser utilizados para fines personales o ajenos a este.

8.1.4 Devolución de Activos

Normas dirigidas a: Tecnología de Información

- La Gerencia de Tecnología de Información es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los colaboradores que se retiran o cambian de labores, cuando les es formalmente solicitado.

Normas dirigidas a: Todos los usuarios

- Todos los colaboradores de Comfenalco Valle Delagente y terceros deberán devolver todos los activos fijos que se encuentren a su cargo al terminar su empleo, contrato o acuerdo.

8.2 CLASIFICACIÓN DE LA INFORMACIÓN

- La clasificación de la información constituye un elemento importante en la gestión de riesgos, ya que determina las necesidades, prioridades y el grado de protección necesario para cada tipo de información.
- La Corporación ha adoptado una estructura de clasificación de la información en cinco (5) categorías que se detallan en el punto siguiente. Esta estructura define el nivel adecuado de protección para una determinada categoría e informa a los responsables de cualquier medida especial o tratamiento requerido para su protección.
- Toda Información utilizada en la Corporación, debe ser clasificada en una de las siguientes cinco (5) categorías:
  - ✓ **Publica:** La información Pública es aquella que puede ser divulgada a personas y empresas internas y externas a la Corporación.
  - ✓ **De uso Interno:** La información de Uso Interno es aquella que solo puede ser usada al Interior de la Corporación.
  - ✓ **Privada:** La información Privada es aquella cuyo uso es restringido y solo puede ser utilizada por los colaboradores que hacen parte de un proceso, proyecto o sistema de información.
  - ✓ **Confidencial:** La información Confidencial es aquella cuyo uso es restringido y a la que solo tienen acceso algunos colaboradores que, por su cargo o funciones, hacen uso de la misma.
  - ✓ **Sensible:** Los datos sensibles son aquellos que pueden afectar la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, se entiende que este tipo de información también debe ser información confidencial.

Normas de uso de la Información según su Categoría.

- **Información Pública:** Este tipo de información puede ser divulgada y publicada a personas o empresas internas o externas a la Corporación cuando sea requerida.
- **información De uso Interno:** Este tipo de información solo puede ser divulgada a personas internas (Colaboradores) de la Corporación, que requieran la misma para la ejecución de sus actividades. No está permitido la divulgación de este tipo de información a personas o empresas externas a la Corporación.
- **Información Privada:** Este tipo de información solo puede ser divulgada a personas internas (Colaboradores) de la Corporación, que requieran la misma y con autorización del dueño o administrador de la información.
- **Información Confidencial:** Este tipo de información no puede ser divulgada a personas internas (Colaboradores) y externas a la Corporación sin la debida autorización del líder del proceso.
- **Información Sensible:** Este tipo de información solo puede ser divulgada a personas internas y externas a la Corporación, que sean autorizadas por el encargado del tratamiento de los datos.

8.2.1 Clasificación de la información

Normas dirigidas a: Dirección

- La Corporación debe contar con la información clasificada en función de los requisitos legales, valor criticidad y susceptibilidad..

Normas dirigidas a: GI

- Debe definir los niveles de clasificación de la información para la Corporación.

- **Normas dirigidas a: Tecnología de Información**

- Debe proveer los métodos de cifrado de la información y la administración del software utilizado para tal fin.
- Debe efectuar la eliminación segura de la información en la plataforma tecnológica, ya sea por dada de baja o cambio de usuario.

Normas dirigidas a: Los propietarios de activos de información

- Los propietarios de los activos de información deben clasificar su información de acuerdo con las 5 categorías establecidas.
- Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

Normas dirigidas a: Todos los usuarios

- Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Corporación.
- La información física y digital de la Corporación debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales, este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; así mismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Todos los usuarios deben asegurarse que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desarrollo de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento.

8.3 MANEJO DE MEDIOS

8.3.1 Gestión de medios removibles

Normas dirigidas a: Los propietarios de activos de información

- Todos los dispositivos de almacenamiento removibles, deben ser rotulados y controlados mediante un registro de auditoría especial para cada dispositivo. Este registro debe contener el nombre del trabajador responsable del dispositivo, entradas, salidas y las actividades de procesamiento de información que realice con éste, especificando su tipología (pública, de uso interno, privada, confidencial, sensible).

Normas dirigidas a: Logística

- El área de activos fijos, debe tener control sobre la vida útil de los dispositivos.

Normas dirigidas a: Todos los usuarios

- Está prohibido almacenar bases de datos que manejen datos personales en dispositivos de almacenamiento removibles a menos que esté autorizado por el área de GI.
- Todos los colaboradores de Comfenalco Valle Delagente que porten información que contenga información confidencial o sensible en dispositivos de almacenamiento removibles, deben proteger el acceso lógico a la información mediante mecanismos de control de acceso (contraseña, bloqueo) y cifrado, manteniéndolo siempre en un lugar seguro y vigilado.

- No utilizar dispositivos removibles de almacenamiento que provengan de lugares ajenos a la Corporación o que hayan sido conectados en equipos que no garantizan la integridad y la confidencialidad de los datos contenidos.
- Todos los dispositivos removibles que almacenen información confidencial o sensible, deben ser guardados en ambientes protegidos y seguros, de acuerdo con las especificaciones del fabricante.
- Se debe realizar copia de respaldo de la información contenida en medios removibles, para mitigar el riesgo de daño o pérdida de los mismos.

8.3.2 Disposición de los medios

Normas dirigidas a: Todos los usuarios

- Se aplicará el procedimiento Gestión de Residuos y/o Similares para la dada de baja de activos de información y para la reutilización el procedimiento Borrado Seguro de Información.

9. CONTROL DE ACCESO

El área de Tecnología de información como responsable de las redes de datos y los recursos tecnológicos debe propender por implementar medidas de seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, con el fin de impedir accesos no autorizados a los sistemas de información, bases de datos y servicios de red, controlar la conexión entre la red de la Corporación y otras redes públicas, revisar las actividades que llevan a cabo los usuarios en los sistemas y asignar responsabilidades frente al uso de contraseñas y equipos.

9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO

9.1.1 Política de control de acceso

Normas dirigidas a: GI

- Revisar los accesos a la red y sistemas de información solicitados por los Líderes de Área para la asignación de privilegios de usuarios.
- Realizar la revisión de los derechos de acceso y uso de la información, de conformidad con los cambios informados por el área de Compensación y Beneficios referentes a ascensos y retiros.
- Monitorear el comportamiento de los accesos concedidos a los usuarios y reportar al Responsable de Tecnología de Información los que no han sido utilizados en un período mayor a tres (3) meses, para que se realice su inactivación.
- Capacitar y concientizar a los usuarios sobre el uso apropiado de los sistemas de información, redes, contraseñas y estaciones de trabajo.

Normas dirigidas a: Tecnología de información

- Debe llevar los registros asociados a la gestión de acceso a las redes y recursos tecnológicos de la Corporación en formato físico y digital según aplique.
- Gestionar el acceso a todos los sistemas, bases de datos y sistemas multiusuario con los que cuenta la Corporación, junto con las solicitudes y aprobaciones de acceso a Internet y la definición de pautas y procedimientos para su utilización por parte de los usuarios.
- Implementar mecanismos para la activación y desactivación de derechos de acceso a las redes y sistemas de información.

Normas dirigidas a: Compensación y beneficios

- Reportar al área de Tecnología y GI, los cambios en cargos y áreas en la Corporación, para llevar el registro actualizado de dichos cambios.
- Reportar inmediatamente al área de Tecnología y GI, el retiro de colaboradores para deshabilitar los accesos concedidos.

Normas dirigidas a: Auditoria interna

- Auditar los perfiles de usuarios, roles, responsabilidades, privilegios y verificar el cumplimiento continuo de la política de control de acceso y revisar el proceso de mejoramiento continuo de las medidas implementadas para el control de acceso de usuarios.

Normas dirigidas a: Líderes de Área

- Dar autorización de creación de perfiles, suministro de accesos y privilegios para los colaboradores que usan los servicios de red.
- Toda solicitud de acceso a los sistemas de información y servicios de red de la Corporación, debe ser radicada para su visto bueno al área de GI.

Normas dirigidas a: Todos los usuarios

- Todos los usuarios de los servicios de información, son responsables del manejo de sus datos de autenticación para el uso y acceso a los recursos informáticos de la Corporación.
- Los usuarios deben mantener en secreto su información de autenticación a los sistemas.
- Los usuarios son responsables de todas las actividades realizadas con su identificador ID en la red.
- Los usuarios deben hacer un uso correcto de la información a la cual tienen acceso.
- Los usuarios deben hacer uso de los datos e información contenidos en los recursos informáticos de la empresa, única y exclusivamente para fines administrativos u operativos y en razón a las funciones asignadas.

9.1.2 Acceso a redes y a servicios en red

Normas dirigidas a: Tecnología de información

- Se deben implementar medidas de seguridad en los accesos de usuarios a la red y los servicios asociados a ella, por medio de técnicas de autenticación, autorización y filtrado de tráfico con el fin de impedir accesos no autorizados a las redes privadas y públicas según sea el caso, con el fin de no comprometer la seguridad de los servicios de la red de la Corporación.
- Identificar las redes y los servicios asociados a ellas, a los cuales se deba permitir el acceso.
- Crear normas y procedimientos de autorización para poder determinar a cuáles redes y servicios de red se le va a dar acceso a los usuarios según sus funciones.
- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Implementar controles especiales para garantizar la confidencialidad e integridad de los datos que viajan a través de redes públicas, y para proteger los sistemas conectados.
- Implementar controles especiales para mantener la disponibilidad de los servicios de red y máquinas conectadas.
- Supervisar que cada uno de los controles se aplique a la infraestructura pertinente de procesamiento de información.
- Se deben deshabilitar todos los servicios que no se vayan a usar en la operación.

9.2 GESTIÓN DE ACCESO DE USUARIOS

9.2.1 Registro y cancelación del registro de usuarios

Normas dirigidas a: Todos los usuarios

- Todos los colaboradores al finalizar el vínculo laboral, deberán diligenciar el paz y salvo correspondiente en el área de Tecnología de Información para la desactivación de los permisos concedidos en los sistemas de información de la Corporación.

9.2.2 Suministro de acceso de usuarios

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información deberá establecer un procedimiento para la asignación de accesos a los sistemas de información y recursos de red de la Corporación.

- El área de Tecnología de información debe establecer ambientes separados para desarrollo, pruebas y producción, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad en producción.

- El área de tecnología de información debe controlar que los desarrolladores no tengan acceso a los ambientes de producción.

Normas dirigidas a: Los propietarios de activos de información

- Los propietarios de los activos de información deben autorizar los accesos a sus aplicativos o sistemas de información, de acuerdo con los perfiles establecidos, y acogiendo el procedimiento establecido para la gestión de accesos.

- Los propietarios de los activos de información deben realizar monitoreo periódico de los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios.

Normas dirigidas a: GI

- El área de GI será la encargada de dar el visto bueno a las solicitudes de los propietarios de la información para la asignación de permisos.

9.2.3 Gestión de derechos de acceso privilegiado

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información debe asignar los privilegios para la administración de los recursos tecnológicos de la Corporación solo a los colaboradores encargados de realizar dichas funciones.
- El área de Tecnología de información debe asignar cuentas personalizadas con altos privilegios para cada funcionario administrador de los recursos tecnológicos, servicios de red y sistema de información.
- El área de Tecnología de información debe garantizar que los usuarios que traen por defecto los sistemas operativos, el firmware, las bases de datos y los dispositivos de red sean inhabilitados o renombrados y las contraseñas que traen por defecto sean modificadas.
- Los administradores de los recursos tecnológicos deben deshabilitar los servicios o funcionalidades no utilizados de los sistemas operativos, y recursos de red. Se debe configurar el conjunto mínimo de funcionalidades requeridas.

9.2.4 Gestión de información secreta para la autenticación de usuarios.

Normas dirigidas a: Compensación y Beneficios

- La Corporación incluirá en los contratos de trabajo de los colaboradores una cláusula de confidencialidad de credenciales de acceso con el fin de proteger la integridad y confidencialidad de la información.

9.2.5 Revisión de los derechos de acceso de usuarios.

Normas dirigidas a: GI

- El área de GI se encargará de realizar la revisión de los derechos de acceso y uso de la información, de conformidad con los cambios informados por el área de Compensación y Beneficios referentes a ascensos y retiros.

9.3 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

9.3.1 Procedimiento de ingreso (Log-On) seguro

Normas dirigidas a: Tecnología de información

- Al momento de la asignación de usuarios, verificar que el cargo, rol, área de trabajo y dependencia correspondan a la solicitud.
- Propender por que en los sistemas operativos y en las aplicaciones, no se muestre ningún tipo identificador o mensaje de ayuda que facilite a un usuario no autorizado acceder a los sistemas, hasta que se haya completado el proceso de autenticación.
- Todas las contraseñas de servicios, servidores o elementos de comunicación deben de ser cambiadas inmediatamente se ponga en ambiente productivo y por ninguna razón deben de quedar con las contraseñas por defecto o asignadas por terceros.
- Las contraseñas de los usuarios administradores, servidores de aplicaciones, bases de datos y cuentas administradoras de aplicaciones deben ser cambiadas máximo, cada 4 meses.
- Limitar a diez (10) el número de intentos de autenticación fallidos.
- Llevar un registro de los intentos fallidos realizados por los usuarios.
- Establecer el cifrado de la transmisión de contraseñas para que no vayan en texto abierto a través de la red y pueda ser capturada por un programa espía.
- Se deben configurar los sistemas operativos y las aplicaciones para que las sesiones se inactiven después del time out de quince (15) minutos, especialmente en las áreas de atención al público o externas que estén por fuera del perímetro de seguridad de la Corporación.

Normas dirigidas a: Todos los usuarios

- El usuario, en el primer inicio de sesión, debe cambiar la contraseña inicial asignada por el Administrador de perfiles, según se lo indiquen, en cada uno de los sistemas.
- El usuario no debe mostrar la contraseña al momento de ser digitada para la autenticación.
- Debe guardar secreto de las credenciales y no apuntarlas en documentos o dispositivos que sean de fácil acceso a terceros.
- Verificar que el puesto de trabajo no tenga indicios de manipulación por parte de otro personal.
- Verificar que las conexiones del cableado eléctrico, de comunicaciones y periféricos, estén bien conectados y no se les haya cambiado de enchufe o puerto y que adicionalmente no tengan ningún dispositivo entre ellos y el computador o equipo del sistema de información.
- Ubicarse en su estación de trabajo de manera cómoda, pero observando que nadie pueda espiar sus credenciales de acceso a su espalda o de lado.
- Abstenerse de compartir las credenciales con otros usuarios bajo cualquier circunstancia, excepto en los casos que se necesite replicar un determinado caso con el personal de TI.
- Evitar el uso de dispositivos o memorias USB, aún si están permitidas.
- Notificar inmediatamente al equipo de respuesta a incidentes de seguridad CSIRT cualquier indicio de que sus credenciales hayan sido comprometidas o usadas por otros usuarios.

9.3.3 Sistema de gestión de contraseñas

Normas dirigidas a: Tecnología de información

- Todos los sistemas de información de Comfenalco Valle Delagente, propenderá por tener las siguientes características mínimas en su autenticación.
  - ✓ Imponer el uso de contraseñas individuales para determinar responsabilidades.
  - ✓ Permitir que los trabajadores puedan cambiar sus propias contraseñas.
  - ✓ Imponer una selección de contraseñas de calidad con las siguientes características:
  - Una longitud mínima de 8 caracteres.
  - Contener números, letras y caracteres especiales.
  - Reutilizar una contraseña, después de 15 contraseñas cambiadas.
  - Cambiar la contraseña como minimo cada 45 días.
  - ✓ Obligar a los trabajadores a cambiar las contraseñas en el primer ingreso al sistema cualquiera que este sea.

9.3.4 Uso de programas utilitarios privilegiados

Normas dirigidas a: Todos los usuarios

- Ningún trabajador deberá tener permisos para la instalación de software adicional en los equipos, cualquier instalación adicional deberá realizarse con el respectivo reporte de servicio por el aplicativo SIRES.
- No se permite el uso de herramientas, programas o técnicas que vulneren los controles que se han establecido.
- Los sistemas de seguridad como antivirus, prevención de perdida de datos instalados en los equipos de cómputo de Comfenalco Valle Delagente, no deben de ser deshabilitados, interferidos o burlados de ninguna manera.

9.3.5 Control de acceso a códigos fuente de programas

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información debe establecer las medidas de seguridad para que solo el personal autorizado tenga acceso a los códigos fuentes y que no sean modificados sin autorización.

10. CRIPTOGRAFÍA

La Corporación velará porque la información que se encuentre clasificada como confidencial y sensible, será cifrada al momento de almacenarse y transmitirse.

10.1 CONTROLES CRIPTOGRÁFICOS

10.1.1 Política sobre el uso de controles criptográficos.

Normas dirigidas a: Tecnología de información

- Se deben utilizar técnicas de cifrado para garantizar la integridad, confidencialidad y no repudio de la información crítica o sensible y en especial datos personales (Datos de menores, historias clínicas, imágenes, entre otras).
- Se deben definir los algoritmos de cifrado que se van a utilizar en cada uno de los procesos de la Corporación, teniendo en cuenta el nivel de riesgo y criticidad de la información.
- Sólo se deben usar algoritmos de cifrados definidos por estándares internacionales, de tal manera que sean fiables y genere confianza en el uso de los sistemas de información y comunicaciones.
- Las contraseñas de acceso a los sistemas de información, datos y servicios de la Corporación, deben ser protegidas por medio de técnicas de cifrado.
- En caso de transmisión de información crítica o sensible por medio de redes públicas, se deben usar controles criptográficos.
- Los servicios de no repudio se deben utilizar solo cuando sea necesario, por ejemplo, en un caso de disputa por algún incidente, evento o acción que comprometa a la Corporación a sanciones por mal manejo de datos personales.
- En las páginas web que se implementen formularios de captura de información personal, se deben adquirir certificados digitales de una Autoridad Certificadora confiable, con el fin de que la información no circule por la red en texto plano y, por tanto, susceptible de ser conocida o manipulada por terceros.
- Cuando existan relaciones contractuales con proveedores de servicios de hosting, se les debe exigir la implementación de certificados digitales en sus plataformas.

Normas dirigidas a: Líderes de Área

- Los líderes de área son los encargados de asignar los roles y determinar la criticidad de la información que necesita ser cifrada, siguiendo las recomendaciones del área de Tecnología de Información en cuanto a los algoritmos de cifrado, su implementación en los sistemas de información y la capacitación a los usuarios a los que se les ha asignado roles en los que tienen a su cargo información crítica o sensible.

10.1.2 Gestión de llaves.

Normas dirigidas a: Tecnología de información

- La criticidad de la información personal que se va a cifrar.
- Los recursos técnicos y la capacidad de cómputo de los equipos que hacen parte de los sistemas de información (estaciones de trabajo, servidores, etc.).
- Se debe tener en cuenta la velocidad de cifrado, uso de memoria, el rango de aplicaciones en el que se puede usar el protocolo de cifrado, el costo y la seguridad.
- El algoritmo de cifrado que se va a utilizar y los mecanismos de implementación. Observando que algunos algoritmos han perdido vigencia y han entrado en desuso. Se debe plantear el uso de combinaciones de algoritmos.
- Se debe establecer un servidor de claves donde se generen y al cual solo tenga acceso la persona determinada por el área de Tecnología de Información.

- Se deben utilizar herramientas generadoras de números o cadenas de caracteres pseudoaleatorios, de manera que sean impredecibles y computacionalmente imposibles de descifrar.
- En el caso en el que una autoridad certificadora sea vulnerada o se descifre un algoritmo de cifrado, la Corporación debe estar preparada para reemplazar todos sus certificados y llaves de cifrado en el menor tiempo posible.
- Es necesario crear un registro de versiones de llaves de cifrado.
- El almacenamiento de las claves debe hacerse de forma segura, cifrándolas y protegiendo el sistema de almacenamiento con contraseña. El único usuario que puede acceder a este sistema es el Responsable del área de Tecnología de Información o quien este delegue.
- Si se hace uso de un sistema de gestión de llaves, se deben seguir las recomendaciones de seguridad que indique el fabricante.
- Para distribuir las llaves se debe tener en cuenta si se usa:
  - ✓ Infraestructura de clave pública,
  - ✓ Gestión de certificados y llaves corporativas,
  - ✓ Gestión grupal de llaves en transferencia, entre otras.
- Debido a que implica una gestión compleja de muchas llaves, existen problemas relacionados con la posibilidad de romper los algoritmos de cifrado, se debe asegurar que los datos son descifrados solo por aquellos que realmente tienen los privilegios para hacerlo. Es necesario que las llaves y los sistemas de cifrado sean compatibles o tengan soporte en varias bases de datos, aplicaciones y estándares.
- La destrucción de las llaves de cifrado implica que se debe eliminar el sistema de creación de las llaves, es decir, las aplicaciones de software, las copias de las llaves y el borrado seguro de los dispositivos donde estaban almacenadas o si es necesario la destrucción física de los dispositivos de almacenamiento, la revocación de privilegios a los usuarios mientras se establece el nuevo esquema de llaves de cifrado y la revisión del registro de versiones de las claves.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

La Corporación velará por la implantación de mecanismos de seguridad física que garanticen el perímetro de las instalaciones en todas sus sedes, también propenderá por controlar las amenazas físicas externas e internas y las condiciones medioambientales.

11.1 ÁREAS SEGURAS

11.1.1 Controles de acceso físico.

Normas dirigidas a: Tecnología de información y Mantenimiento

- Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones.
- Solo el personal de TI autorizado y el personal que maneja la telefonía tendrán acceso a los centros de cableado.

Normas dirigidas a: Seguridad

- El área de Seguridad es el encargado de suministrar las llaves de acceso a los centros de cableado o la gestión de accesos y llevar un libro de registro físico de quien ingresa a estos centros si no hay registro digital.

Normas dirigidas a: Líderes de Área

- Cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información o de procesamiento de datos críticas para Comfenalco Valle Delagente, deberá ser protegida por una barrera como una pared, una puerta con control de acceso o un escritorio o recepción atendido por un funcionario de Comfenalco Valle Delagente

11.1.2 Seguridad de oficinas, recintos e instalaciones

Normas dirigidas a: Líderes de Área

- Se deben implementar controles de acceso que impidan el ingreso a público en las instalaciones de áreas que manejan actividades o información confidencial.

11.1.3 Protección contra amenazas externas y ambientales

Normas dirigidas a: Tecnología de información

- Los servidores que contengan información y servicios informáticos de Comfenalco Valle Delagente deben ser mantenidos en un ambiente seguro y protegido por los menos con:
  - ✓ Controles de acceso y seguridad física.
  - ✓ Detección de incendio y sistemas de extinción de conflagraciones.
  - ✓ Controles de humedad y temperatura.
  - ✓ Bajo riesgo de inundación.
  - ✓ Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).
  - ✓ Cámara para monitoreo al centro de cómputo principal.

11.2 EQUIPOS

11.2.1 Ubicación y protección de los equipos

Normas dirigidas a: Todos los usuarios

- Los colaboradores de la Corporación que tienen asignado estaciones de cómputo no podrán comer, consumir líquidos y fumar en los puestos de trabajo.
- Todos los equipos de cómputo deben estar conectados a tomas de energía regulada.
- Todos los equipos portátiles de la Corporación debes estar protegidos con guaya de seguridad en los puestos de trabajo.
- Está prohibido almacenar bases de datos que manejen datos personales en equipos portátiles o computadores de escritorio, a menos que esté autorizado por el área de GI.

11.2.2 Servicios de suministro

Normas dirigidas a: Mantenimiento

- Se debe propender por garantizar el suministro de energía en los equipos de cómputo de la Corporación cuando se presenten fallas de energía.

11.2.3 Seguridad del cableado

Normas dirigidas a: Mantenimiento

- La instalación y mantenimiento del cableado eléctrico y de comunicaciones de la Corporación, debe ser realizado por personal calificado con el fin de garantizar su integridad y correcto funcionamiento.
- Establecer un cronograma de revisión de cableados y estructuras de manera periódica.
- Verificar que se cumplen con los requerimientos especificados en los reglamentos técnicos para instalaciones nuevas o remodelaciones (cableado certificado).
- Realizar una revisión de las responsabilidades contractuales con terceros que presten servicios de suministro de energía y comunicaciones y verificar que cumplen con los reglamentos técnicos.
- La auditoría a los sistemas de cableado debe incluir registro documental del estado del cableado, tiempo de instalación, periodo de mantenimientos y verificación de cumplimiento con el reglamento técnico.
- Se deben revisar los procedimientos y políticas respecto al suministro ininterrumpido de energía eléctrica, para determinar si los sistemas de suministros requieren de instalaciones o configuraciones especiales diferentes a las ya establecidas.
- Adicionalmente, el Ministerio de Minas y Energía y la comisión de regulación de comunicaciones han establecido los siguientes reglamentos técnicos que aplican al cableado eléctrico y de comunicaciones:

  - ✓ Cableado Eléctrico
    - Reglamento técnico de instalaciones eléctricas RETIE 2013.
    - Resolución No. 9 0708 de agosto 30 de 2013: Anexo general de RETIE.
    - Resolución No. 9 0795 de julio 25 de 2014: Corrección RETIE.
    - Resolución No. 4 0492 de abril 24 de 2015: Corrección RETIE.

  - ✓ Cableado de Comunicaciones:
    - Reglamento técnico para redes internas de telecomunicaciones RITEL 2013 (Resolución No. 4262 del 15 de julio de 2013).
    - Resolución 4423 del 21 de febrero de 2014, modifica el RITEL 2013.
    - Resolución 4639 del 26 de noviembre de 2014, modifica el RITEL 2013.
    - Resolución 4741 del 22 de mayo de 2015, modifica el RITEL 2013.
    - Resolución 4786 del 08 de septiembre de 2015, suspende el RITEL 2013.

NOTA: Dado que la Resolución CRC No. 4786 del 08 de Septiembre de 2015, no deroga el contenido de la Resolución CRC No. 4262 del 15 de Julio de 2013, “por la cual se expidió el Reglamento técnico para redes internas de telecomunicaciones RITEL”, sino que se suspenden sus efectos hasta el día siete (7) de septiembre de 2017, se recomienda que la Corporación aplique las reglas establecidas en la referida norma jurídica como referente técnico –y no obligatorio por el tiempo de su suspensión-, por cuanto ofrece lineamientos técnicos generales respecto de este tipo de estructuras de cableado.

Normas dirigidas a: Tecnología de información

- En el caso de que existan sistemas de administración remota o por entorno web de los sistemas de suministro, se debe establecer la segregación de redes, y asignar o revocar privilegios de acceso y credenciales a dicho segmento de la red.
- Los puntos de red que están libres deben ser deshabilitados y su estado debe ser informado al área encargada.

11.2.4 Mantenimiento de equipos

Normas dirigidas a: Tecnología de información

- El área de TI debe propender por que los equipos críticos de la infraestructura de servicios de TI estén cubiertos por mantenimiento y soporte adecuados de hardware y/o software.
- Se debe realizar las tareas de mantenimiento preventivo a todos los equipos de cómputo, servidores y elementos de comunicaciones, de acuerdo con los intervalos de servicio y especificaciones definidos por el área de TI.
- Sólo el personal autorizado por TI, podrá realizar mantenimiento y llevar a cabo reparaciones en los equipos de la infraestructura de Comfenalco Valle Delagente.

11.2.5 Retiro de activos

Normas dirigidas a: Líderes de Área

- Los líderes de área serán los encargados de autorizar el retiro de activos de información de las instalaciones de la Corporación.

11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Normas dirigidas a: Líderes de Área

- Todo equipo de cómputo o elemento que contenga información sensible de Comfenalco Valle Delagente, que sea destinado para labores fuera del ámbito de la Corporación, deberá ser autorizado por el jefe del área responsable de dicho equipo.

11.2.7 Disposición segura o reutilización de equipos

Normas dirigidas a: Tecnología de información

- Se deben de adoptar mecanismos de eliminación segura de datos, de todos los equipos que contengan información sensible de Comfenalco Valle Delagente.

Normas dirigidas a: Gestión ambiental

- El área de gestión ambiental se encargará de la eliminación segura de todos los elementos que hayan sido dado de baja, que intervengan en el procesamiento de datos y que contengan información sensible de la Corporación.

11.2.8 Equipos de usuarios desatendidos

Normas dirigidas a: Tecnología de información

- El área de TI asignará una política para que los equipos desatendidos (sin actividad) sean protegidos por un protector de pantalla después de 15 minutos de inactividad.

Normas dirigidas a: Todos los usuarios

- Cierre de las aplicaciones (Log-Off) cuando ya no los necesiten.
- Asegurar los computadores y dispositivos móviles contra uso no autorizado mediante bloqueo de pantalla, bloqueo de teclas o un control equivalente cuando no estén en uso.

11.2.9 Política de escritorio limpio y pantalla limpia

Normas dirigidas a: Todos los usuarios

- Todos los escritorios de los trabajadores deben de permanecer limpios de documentos en papel y dispositivos de almacenamiento removibles y pantallas limpias, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.
- El consumo de alimentos cerca al equipo de cómputo no está permitido.
- Todos los Trabajadores deberán crear una carpeta en mis documentos de nombre “Comfenalco” donde se guardará la información pertinente a sus actividades laborales, la cual será tenida en cuenta en el momento de daños, reinstalación o cambio de máquina. Cualquier información o documento por fuera de esta ruta será ignorado al momento de una copia de información por actualización de equipo, reparación o actualización.

12. SEGURIDAD DE LAS OPERACIONES.

El área de Tecnología de información es la encargada de la operación y administración de los recursos tecnológicos de la Corporación, manteniendo la documentación actualizada de los procesos para la ejecución de actividades, asegurando que los cambios efectuados sobre los recursos tecnológicos sean adecuadamente controlados y autorizados. Así mismo velara por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la integridad, confidencialidad y disponibilidad de la información.

12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

12.1.1 Procedimientos de operación documentados

Normas dirigidas a: Tecnología de información

- Se destinará un sitio organizado para que se mantengan los procedimientos operativos de infraestructura y comunicaciones.

12.1.2 Gestión de cambios

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información 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.
- El área de Tecnología de información debe contar con un control de versiones para administrar los cambios en los sistemas de información de la Corporación.
- El área de Tecnología de información debe asegurarse que los sistemas de información suministrados por terceros, cuenten con un acuerdo de licenciamiento sobre su uso y derechos de propiedad intelectual.

12.1.3 Gestión de capacidad

Normas dirigidas a: Tecnología de información

- Se debe realizar una planeación de la capacidad de todos componentes de infraestructura y/o comunicaciones que interfiera el procesamiento, transferencia y almacenamiento de información por lo menos 1 vez al año o en caso de que una nueva implementación no planeada lo requiera.

12.1.4 Separación de los ambientes de desarrollo, pruebas y producción

Normas dirigidas a: Tecnología de información

- Los sistemas de información sensibles para la Corporación, deberán propender por estar en un ambiente dedicado y aislado siempre que sea posible.
- Los ambientes de desarrollo, pruebas y producción, deben existir en lo posible para todos los componentes de lo aplicativos de Comfenalco Valle Delagente.

12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

12.2.1 Controles contra códigos maliciosos

Normas dirigidas a: Tecnología de información

- Los códigos móviles serán ejecutados única y exclusivamente por el personal de infraestructura de TI, solo para labores administrativas y en casos específicos.
- Todos los equipos de cómputo de Comfenalco Valle Delagente deben de contar el software antivirus establecido por el área de TI de Comfenalco Valle Delagente.
- El área de TI publicara el listado de software autorizado en la Corporación.

12.3 COPIAS DE RESPALDO

12.3.1 Respaldo de la información

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información debe adoptar procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información.
- El área de Tecnología de información debe realizar pruebas de recuperación periódicas, con el fin de comprobar su integridad y uso en caso de ser necesario.

12.4 REGISTRO (LOGGING) Y SEGUIMIENTO

12.4.1 Registro de eventos

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información, en conjunto con el área de Riesgos, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de la Corporación.
- El área de Tecnología de información, a través de sus colaboradores, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- El área de Tecnología de información debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de la Corporación. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.
- Todas las actividades realizadas por el administrador y operador de las aplicaciones deben quedar registrados en los registros de auditoria (logs).
- Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.
- Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros.
- Los desarrolladores deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoria que brinden información adicional a la estrictamente requerida.

Normas dirigidas a: Auditoria interna

- El área de Auditoria interna debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

12.4.2 Sincronización de relojes

Normas dirigidas a: Tecnología de información

- Todos los sistemas de información de Comfenalco Valle Delagente, deberán sincronizar su hora con el servidor principal de directorio activo.

12.5 CONTROL DE SOFTWARE OPERACIONAL

12.5.1 Instalación de software en sistemas operativos

Normas dirigidas a: Tecnología de información

- Solo el personal autorizado de Tecnología de Información realizará la actualización del software operacional aplicaciones y librerías.

12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

12.6.1 Gestión de las vulnerabilidades técnicas

Normas dirigidas a: Tecnología de información

- Definir, actualizar y revisar el listado de vulnerabilidades técnicas conocidas dentro de la Corporación.
- Establecer las acciones preventivas y correctivas de las vulnerabilidades conocidas y establecer un esquema de revisión periódica, para asegurar la integridad y disponibilidad de los sistemas de información, así como la integridad, confidencialidad y disponibilidad de los datos personales que estén en uso o almacenamiento dentro de los sistemas de información de la Corporación.
- Comunicar periódicamente a todos los interesados, las actualizaciones sobre las vulnerabilidades, las acciones correctivas y preventivas, y establecer los mecanismos de registro y capacitación.
- Planificar la realización de pruebas paralelas al sistema de información para la explotación de vulnerabilidades y llevar un registro de la gestión realizada que incluya las lecciones aprendidas.
- Verificar del estado de los sistemas junto con el estado de las vulnerabilidades técnicas.
- Notificar cualquier cambio en la configuración o actualización de los sistemas de información, previa verificación del impacto de los cambios a realizar.
- Aplicar e informar las revisiones, acciones correctivas y preventivas comunicadas a los coordinadores de área, así mismo debe realizar las capacitaciones y gestionar los registros necesarios, con el fin de asegurar el funcionamiento correcto de los sistemas de información.

Normas dirigidas a: Líderes de Área

- Llevar un control sobre los registros de capacitación, notificar cualquier incidencia en los sistemas de información que pueda indicar un fallo producido por la explotación de alguna vulnerabilidad, notificar la necesidad de cualquier cambio que considere necesario para que el área de Tecnología de Información valide si los cambios propuestos pueden incluir nuevas vulnerabilidades en los sistemas de información y sus estructuras de soporte.

12.6.2 Restricciones sobre la instalación de software

Normas dirigidas a: Tecnología de información

- Solo el personal de soporte y tecnología autorizado, podrá instalar software en los equipos de cómputo asignado a los trabajadores, este software debe ser el avalado por el

área de Tecnología de Información y hacer parte del listado de software autorizado que se encuentra publicado en la intranet en la sección de documentos.

- Ningún trabajador diferente al autorizado por soporte y tecnología, deberá tener permisos de administrador para la instalación de software en los computadores asignados para su desempeño.

12.7 CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN

12.7.1 Controles sobre auditorias de sistemas de información

Normas dirigidas a: Auditoria interna

- El acceso a sistemas y datos por parte del personal de Auditoria interna se debe acordar con el área auditada.
- Todos los accesos otorgados al personal de Auditoria interna en los aplicativos de la Corporación deben ser de solo lectura.
- Las pruebas de auditoria que puedan afectar la disponibilidad de los sistemas de deberán realizar en horas no laborales y concertado con el área de Tecnología de Información.

13. SEGURIDAD DE LAS COMUNICACIONES

La Corporación establecerá a través del área de Tecnología de información los mecanismos de control necesarios para la disponibilidad de las redes de datos y servicios que de ellas dependan, así mismo contará con mecanismos de seguridad que protejan la confidencialidad e integridad de la información que se transporta a través de nuestras redes de datos.

13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES

13.1.1 Controles de redes

Normas dirigidas a: Tecnología de información

- Coordinar los mecanismos de control implementados para los dominios de seguridad definidos.
- Aprobar y aplicar medidas de control para las excepciones que permitan accesos desde otros dominios hacia los servidores de la red corporativa.
- Mantener la seguridad en el intercambio de información y software dentro de la Corporación y con cualquier otra entidad externa.
- Toda conexión de dispositivos de terceros a la red de Comfenalco Valle Delagente, deberá pasar a través de un dispositivo de seguridad (firewall) y el control deberá ser definido por el área de Tecnología de información.
- Cualquier equipo que represente un riesgo para el funcionamiento de la red, deberá ser desconectado inmediatamente de la misma por el área de Tecnología de información.
- Crear, administrar e instalar certificados o herramientas de cifrado en los correos electrónicos, establecer canales de red privados cuando se transmitan datos personales por redes públicas e implementar controles criptográficos cuando se usen aplicaciones de mensajería instantánea corporativas.

- Autorizar los métodos de cifrado a utilizar en los sistemas de información, aplicaciones, bases de datos y comunicaciones.

13.1.2 Seguridad en los servicios de red

Normas dirigidas a: Tecnología de información

- Se controlará el acceso a los servicios de red tanto internos como externos. El Área Tecnología de información tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red.
- Las redes que ofrezcan servicios a personal ajeno a Comfenalco Valle Delagente, pero que presten servicios en nuestras instalaciones, deberán ser aisladas mediante elementos de seguridad y/o deberá separarse en lo posible físicamente de la infraestructura de Comfenalco Valle Delagente.
- Los contratos que impliquen interconexión de redes de terceros con Comfenalco Valle Delagente, deben de incluir cláusulas de deberes y responsabilidad del tercero frente a la confidencialidad y establecer procedimientos sobre incidentes de seguridad y/o disponibilidad de los servicios, que puedan ser generados por dicha interconexión.

Normas dirigidas a: Líderes de Área

- Solicitar los permisos de red para los colaboradores.

13.1.3 Separación de las redes

Normas dirigidas a: Tecnología de información

- Se deberá mantener la segmentación de la red y la instalación de un “firewall”, para filtrar el tráfico entre las diferentes redes y bloquear el tráfico no autorizado.

13.2 TRANSFERENCIA DE INFORMACIÓN

13.2.1 Política de transferencia de información

Normas dirigidas a: Tecnología de información

- Ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.
- Tener protección contra el código malicioso que pueda ser transmitido a través del uso de transacciones telemáticas.
- Definir buenas prácticas en el uso de las instalaciones de comunicación electrónicas.
- Definir responsabilidades a los usuarios, contratistas y terceros para no ver comprometida la imagen de Comfenalco Valle Delagente, a través de difamación, hostigamiento, personificación, reenvío de cadenas y redes sociales.

Normas dirigidas a: Propietarios de información

- Los propietarios de los activos de información deben velar porque la información de la Corporación o de sus afiliados sea protegida de divulgación no autorizada por parte de

los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

- Los propietarios de los activos de información deben asegurar que los datos requeridos de los titulares sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- Los propietarios de los activos de información deben verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada.

Normas dirigidas a: Terceros

- Los terceros con quienes intercambia información la Corporación deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de Comfenalco Valle Delagente y de las condiciones contractuales establecidas.
- Los terceros con quienes se intercambia información de Comfenalco Valle Delagente deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

Normas dirigidas a: Todos los usuarios

- Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la Corporación o de sus afiliados.
- No está permitido el intercambio de información sensible por vía telefónica.

13.2.2 Acuerdos sobre transferencia de información

Normas dirigidas a: GI

- Definir los modelos de Intercambio de Información entre la Corporación y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la Corporación a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.

Normas dirigidas a: Líderes de Área

- Para los contratos en los que se realice transmisión de información se debe incluir las cláusulas de transmisión de información personal suministradas por el área de GI.

13.2.3 Política para uso de red inalámbrica

Normas dirigidas a: Tecnología de información

- Todos los equipos que intervienen en la red inalámbrica deberán ser instalados o desinstalados solamente por el personal de Tecnología de información o por proveedores autorizados con supervisión del área de Tecnología de información.
- La red inalámbrica pública que ofrece Comfenalco Valle Delagente, será aislada de la red corporativa.

Normas dirigidas a: Líderes de Área

- El acceso a la red inalámbrica de Comfenalco Valle Delagente que tiene permisos para acceder a los recursos de nuestra red interna, deberá ser autorizada por los líderes de área.

13.2.4 Política para el uso de correo corporativo

Normas dirigidas a: Tecnología de información

- Proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- Establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

Normas dirigidas a: Todos los usuarios

- El correo electrónico sólo puede ser usado por el personal autorizado por la Corporación.
- Está prohibido por medio del correo electrónico realizar las siguientes actividades:
  - ✓ El uso que debe hacerse del correo electrónico es estrictamente corporativo y no personal. Se trata de una herramienta de trabajo que debe ser respetada. No promueva disputas y polémicas por este medio.
  - ✓ Envío de cartas de cadena.
  - ✓ Está prohibido reenviar material de tinte político cualquiera que este sea, chistes, cadenas, consejos, promociones comerciales, materiales pornográficos y semejantes.
  - ✓ Transmisión de material ilegal, de acoso, difamatorio, amenazador, nocivo, vulgar, obsceno o de cualquier otra manera censurable.
  - ✓ Divulgar o promover ideales políticos, religiosos o sociales.
  - ✓ Transmitir cualquier material que contenga virus o mensajes que puedan generar daños en el funcionamiento de los equipos de cómputo.
  - ✓ Interferir o causar trastornos en redes conectadas a este servicio o infringir las regulaciones, directivas o procedimientos de tales redes.
  - ✓ Transmisión de material diferente al requerido para la ejecución de las funciones propias del trabajo asignado.
  - ✓ Suplantar o intentar engañar a otras personas con la identidad del remitente u origen del mensaje.
  - ✓ Infringir cualquier ley colombiana relativa a la transmisión de datos técnicos a través del servicio.
  - ✓ Difamar, abusar, acosar, acechar, amenazar o de otra forma infringir los derechos (tales como los derechos a la intimidad y a la propia imagen) de terceros.

- ✓ Cargar o poner a disposición de otras personas, archivos que contengan imágenes, fotografías, software u otro material protegido por las leyes sobre propiedad intelectual e industrial, incluyendo o a modo de ejemplo a menos que usted sea titular de los derechos respectivos o haya recibido todos los consentimientos necesarios para hacerlo.
- ✓ Falsificar o eliminar avisos de derechos de autor, avisos legales o cualquier otro aviso relevante, designación o etiqueta indicativa del origen o la fuente del software u otro material contenido en un archivo que esté cargado.
- ✓ Recoger o de cualquier manera recopilar información acerca de terceros, incluidas direcciones de correo electrónico.
- ✓ Utilizar, descargar o de otra manera copiar o proporcionar a una persona física o jurídica, cualquier directorio de los usuarios de Sitios o Servicios informáticos de Comfenalco Valle Delagente.
- ✓ Los empleados de Comfenalco Valle Delagente que reciban correos con contenido prohibido de otro empleado de Comfenalco Valle Delagente, debe de notificar al área de GI.
- ✓ Está prohibido él envió de masivo de correo por los trabajadores a cuentas de correo externo desde nuestras plataformas de correo, sin que haya una autorización por parte del área de Tecnología de información.

- Está prohibido el envío o transmisión de cualquier tipo de información propietaria, secretos del negocio o cualquier otra información confidencial de la organización a menos que tenga la autorización de realizarlo.
- Adicional a estas políticas se debe de tener en cuenta el documento “normas uso correcto de correo electrónico” que se encuentra publicado en la intranet en la sección “Políticas de Comunicaciones”.

13.2.5 Política sobre el uso de internet

Normas dirigidas a: Líderes de Área

- El acceso a Internet, medios de mensajería instantánea (por ejemplo, Microsoft Messenger, Yahoo! Messenger, MS Chat, Skype o NetMeeting, Google Hangouts o similares), medios de almacenamiento en la nube (por ejemplo: sky drive, google drive y Dropbox entre otros) y redes sociales (por ejemplo, Facebook y Twitter entre otros) sólo se asignará a aquellos cargos que lo requieran para su desempeño laboral, y deberá ser aprobado por los líderes de área.

Normas dirigidas a: Tecnología de información

- Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- El área de Tecnología de información podrá suspender o disminuir el ancho de banda o la calidad de un servicio que atente contra el desempeño de otros servicios de internet en general.
- Diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- Debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

- Debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Normas dirigidas a: Todos los usuarios

- Está prohibido utilizar internet para actividades diferentes a las laborales.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el líder de área y el área de Tecnología de información, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- No está permitido el intercambio no autorizado de información de propiedad de Comfenalco Valle Delagente de sus clientes y/o de sus colaboradores, con terceros.

13.2.6 Autenticación del usuario para conexiones externas VPN

Normas dirigidas a: Líderes de Área

- El servicio de VPN para los trabajadores de Comfenalco Valle Delagente, debe ser autorizado por el líder de área.
- El servicio de VPN para personal ajeno a Comfenalco Valle Delagente, deberá ser solicitado por el líder encargado de proyecto o soporte y debe de tener una fecha de inicio y final de actividades.

Normas dirigidas a: Tecnología de información

- Solo se debe de utilizar el cliente de VPN, autorizado por Comfenalco Valle Delagente.
- Los equipos conectados a las VPN de Comfenalco Valle Delagente, serán desconectados después de 30 minutos de inactividad.

Normas dirigidas a: Todos los usuarios

- Es responsabilidad de los usuarios con privilegios VPN impedir que otras personas sin autorización, ingresen a nuestra red por medio de las credenciales que les fueron asignadas o por dejar el equipo donde está accediendo desatendido.
- Los usuarios que se conectan a la VPN de Comfenalco Valle Delagente con equipos personales, deben de comprender que estos equipos en el momento de conexión, son una extensión de la red corporativa y están sujetos a las mismas reglas y regulaciones que aplican a los equipos de Comfenalco Valle Delagente.

- Los trabajadores que accedan a Comfenalco Valle Delagente por medio de la VPN a la red de Comfenalco Valle Delagente deberán hacerlo única y exclusivamente por los equipos asignados por la Corporación, o por los equipos autorizados por el área de Tecnología de Información.

13.2.7 Política de compartir carpetas y archivos

Normas dirigidas a: Líderes de Área

- Los procesos del negocio que requieran carpeta o archivos compartidos deberán realizar la solitud al área de Tecnología de información.
- Si algún proceso de negocio requiere compartir carpetas o archivos en un equipo de cómputo asignado a un trabajador, deberá de ser autorizado por el área de Tecnología de información.

Normas dirigidas a: Todos los usuarios

- Las carpetas Compartidas en los servidores de la infraestructura de Comfenalco Valle Delagente, solo deberán contener información relacionada al ámbito laborar.

13.2.8 Acuerdos de confidencialidad o de no divulgación

Normas dirigidas a: GI

- Definir los modelos de Acuerdos de Confidencialidad entre la Corporación y terceras partes y empleados incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la Corporación a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.
- El área Jurídica debe incluir en los contratos que se celebren con terceros las cláusulas de confidencialidad establecidas.

Normas dirigidas a: Compensación y Beneficios

- Incluir en los contratos de trabajo de los colaboradores las cláusulas de confidencialidad suministradas por el área de GI.

Normas dirigidas a: Todos los usuarios

- Cumplir con las cláusulas de confidencialidad y de seguridad de la información establecidas por la Corporación.

14. ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La Corporación propenderá por garantizar que el software adquirido y desarrollado al interior como por terceras partes, cumpla con los requisitos de seguridad y calidad establecidos.

14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

14.1.1 Análisis y especificación de requisitos de seguridad de la información

Normas dirigidas a: Propietarios de los sistemas de información

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de la Corporación formalmente asignada.
- Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

Normas dirigidas a: Tecnología de información

- Establecer las actualizaciones de los sistemas operativos, según su criticidad y verificar el control de versiones, con el fin de determinar si la actualización puede interferir con el funcionamiento de los sistemas de información.
- Realizar las actualizaciones o coordinar su instalación.
- Informar cualquier fallo y hacer las pruebas iniciales de las aplicaciones.
- Gestión y conservación de las técnicas criptográficas y claves utilizadas en los sistemas de información.
- Garantizar el licenciamiento, calidad del software desarrollado y la inclusión de cláusulas de seguridad de la información en los contratos con terceros que fabriquen software.
- Crear e implementar controles en los sistemas de información desarrollados al interior de la Corporación o por terceros.
- Hacer seguimiento al cumplimiento de los controles establecidos para el desarrollo y mantenimiento de los sistemas de información.
- Definir procedimientos para el control de cambios en los sistemas, la verificación de seguridad en cada uno de los sistemas y bases de datos asociadas.
- Establecer los requisitos de seguridad del sistema de información, en los siguientes ámbitos:
  - ✓ Especificaciones técnicas de los equipos de soporte del sistema de información.
  - ✓ Desarrollo y adquisición de software.
  - ✓ Diseño de pruebas.
  - ✓ Uso de red.
  - ✓ Protocolos de seguridad de los datos personales.
  - ✓ Roles y responsabilidades.
  - ✓ Formación y capacitación.
- Ejecutar y coordinar los cambios que han sido planeados para las aplicaciones.
- Instalar los nuevos Sistemas de Información o las actualizaciones en los ya existentes.
- Realizar el análisis de los requerimientos de cambios solicitados en primera instancia, en caso de ser viable se notifica a los desarrolladores, aprobando las pruebas después de los cambios y ejecutando los cambios en el respectivo servidor.
- Coordinar y supervisar los cambios realizados en la infraestructura de comunicaciones y los sistemas de información.
- Atender las solicitudes y requerimientos de los usuarios ante incidentes y cambios inadecuados en los sistemas de información.

- Crear y monitorear un entorno de red en el que se realicen las pruebas y se analice el funcionamiento de los sistemas de información antes de pasarlo a producción.
- Definir e implementar políticas de desarrollo seguro para proteger los datos personales en el ambiente de desarrollo de software.
- Implementar procedimientos que permitan la realización de pruebas con datos personales, siempre que se respete el mismo nivel de seguridad de las bases de datos a los que pertenecen los datos objeto de pruebas, de conformidad con lo previsto en la ley de protección de datos personales.
- Supervisar las acciones de pruebas en los sistemas que realizan los desarrolladores.
- Realizar un informe del estado actual de la red y de los sistemas de información, con el propósito de dimensionar y establecer las necesidades y prioridades que debe suplir el sistema de información a implementar.
- Implementar los cambios técnicos para la instalación, prueba y puesta en marcha del nuevo sistema de información.
- Realizar el monitoreo continuo del sistema de información implementado y llevar un registro de incidencias de seguridad o fallas técnicas.
- Debe definir el procedimiento interno para ejecutar los cambios solicitados.
- Realizar pruebas en los sistemas de información después de hacer los cambios y actualizar el manual técnico y/o de usuario.

Normas dirigidas a: Líderes de Área

- Realizar las capacitaciones informadas por el área de Tecnología de información y verificar que el personal que usa o tiene acceso al nuevo sistema de información, acate y cumpla las normas y recomendaciones operativas y de seguridad de la información, especificadas.
- Debe llevar un registro de fallas e incidencias de seguridad, además debe verificar y registrar la asignación, alta, baja, o modificación de usuarios, credenciales y privilegios de acceso para el personal que interactúe con el nuevo sistema de información.

Normas dirigidas a: Desarrolladores (internos o externos)

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

Normas dirigidas a: Todos los usuarios

- Deben realizar reportes de cualquier falla, inconsistencia o cambio no documentado en el funcionamiento de las aplicaciones después de la actualización.

14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

14.2.1 Política de desarrollo seguro

Normas dirigidas a: Propietarios de los sistemas de información

- Los propietarios de los sistemas de información son responsables de realizar las pruebas 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. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas.
- El área de Tecnología de información debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Corporación.
- El área de Tecnología de información debe generar 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.
- El área de Tecnología de información, a través de sus colaboradores, debe 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.

Normas dirigidas a: Desarrolladores (internos o externos)

- Los desarrolladores de los sistemas de información deben 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 producción.
- Los desarrolladores 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.
- Los desarrolladores deben asegurar que los sistemas de información 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, entre otros.
- Los desarrolladores deben suministrar mecanismos de desconexión o cierre de sesión de los aplicativos que permitan finalizar completamente la sesión iniciada.
- Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

- Los desarrolladores deben garantizar que no se divulgue información sensible en mensajes de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios y propender por implementar mensajes de error genéricos.
- Los desarrolladores deben 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.
- Los desarrolladores y gestión informática, no podrán acceder a los ambientes de producción con fines de modificación de programas o datos propios de las aplicaciones previo un mecanismo de autorización de acceso.

14.3 DATOS DE PRUEBA

14.3.1 Protección de datos de prueba

Normas dirigidas a: Tecnología de información

- En los casos que se tenga que usar datos reales de debe tener en cuenta los siguientes requisitos:
  - ✓ Al definir las características de una aplicación, se deben implementar medidas de seguridad para garantizar la integridad, confidencialidad y disponibilidad de los datos personales que contendrán las bases de datos asociadas.
  - ✓ Crear entornos separados de prueba con datos reales.
  - ✓ Restringir el acceso a los desarrolladores al entorno de producción desde los entornos de desarrollo. Si el personal de desarrollo necesita acceder al entorno de producción a realizar tareas de mantenimiento o de otro tipo, debe estar autorizado por el Responsable de Tecnología de información.
  - ✓ Solo se pueden usar datos reales en las pruebas cuando se disponga de la autorización expresa del Área de Tecnología de información.
  - ✓ Prohibir la realización de pruebas con datos reales en entornos que no cumplan con los requisitos de seguridad de la Corporación.
  - ✓ El Jefe de Soporte y tecnología es el encargado de otorgar privilegios a los desarrolladores para ejecutar tareas en el ambiente de producción.
  - ✓ Identificación y autenticación de usuarios.
  - ✓ Control de accesos.
  - ✓ Bases de datos que estén en soportes enviados fuera de las instalaciones de la Corporación o sean transmitidas deben estar cifradas (en caso de datos privados o sensibles).
- El área de Tecnología de información debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

15. RELACIONES CON LOS PROVEEDORES

La Corporación establecerá mecanismos de control en sus relaciones con terceros, asegurando que la información a la que tengan acceso, así como servicios que sean suministrados por los mismos, cumplan las políticas de seguridad de la información.

Los colaboradores encargados de la interventoría con terceros se asegurarán de la divulgación de las políticas de seguridad de la información a terceros.

15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

15.1.1 Política de seguridad de la información para las relaciones con los proveedores

Normas dirigidas a: GI

- El área de GI y el área Jurídica deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir los proveedores de servicios o terceros. Dicho modelo, debe ser divulgado a todas las áreas que para su utilización en caso de requerir.
- El área de GI y el área Jurídica deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con proveedores y terceros. Se debe tener en cuenta la responsabilidad civil como penal para los proveedores y terceros contratados.

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información debe establecer las condiciones de conexión adecuadas para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Corporación.
- El área de Tecnología de información debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.

Normas dirigidas a: Interventores de contratos

- Los interventores de contratos con proveedores y terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de la Corporación a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas y lineamientos de seguridad de la información.

15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES

15.2.1 Seguimiento y revisión de los servicios de los proveedores

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Corporación.
- El área de Tecnología de información debe verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.

Normas dirigidas a: Interventores de contratos

- Los interventores de contratos con proveedores y terceros deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los proveedores y de servicios.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Corporación promoverá entre los colaboradores y terceros el reporte de incidentes relacionados con la seguridad de la información, así como también asignara responsables para el tratamiento de incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar, solucionar y documentar los incidentes reportados.

El equipo CSIRT es el único autorizado para definir si es un incidente de seguridad y si amerita reporte ante la Superintendencia de Industria y Comercio.

16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

16.1.1 Tratamiento y reporte de incidentes de seguridad

Normas dirigidas a: GI

- Será el responsable de realizar el registro de los incidentes de seguridad de la información y el reporte de estos en los aplicativos de los entes de control, en los casos que sean necesarios.
- Es el encargado del seguimiento, documentación y análisis de los incidentes de seguridad de la información encontrados, así como la comunicación al Comité de Gestión de Seguridad de Datos Personales (SGSDP), en caso de que amerite.
- Debe crear y coordinar un equipo que se encargue de la gestión y respuesta a incidentes de seguridad de la información CSIRT.
- Así mismo, junto con el Área de Desarrollo, Selección y Personal, son responsables de poner en conocimiento los procedimientos de gestión de incidentes a los colaboradores contratados al inicio de la relación laboral.
- Liderar el Equipo de Respuesta a Incidentes de Seguridad de la Información.
- Velar por el correcto funcionamiento y operación de la Gestión de Incidentes de Seguridad de la Información.

Normas dirigidas a: Tecnología de información

- Registrar, clasificar y asignar responsabilidad de solución a los incidentes de Seguridad de la Información.
- Implementar una plataforma tecnológica para la adecuada atención y registros históricos de incidentes de seguridad de la información.
- Generar reportes necesarios para el monitoreo de los incidentes de seguridad de la información.
- Monitoreo constante de la oportuna solución de los Incidentes de seguridad de la información.

Normas dirigidas a: Lideres de área

- Deben atender las convocatorias, solicitudes y consultas realizadas por el Responsable de Gobierno de Información, bajo el marco de la atención a incidentes de seguridad que puedan comprometer la integridad, disponibilidad y confidencialidad de la información.

Normas dirigidas a: Todos los usuarios

- Todo el personal de la Corporación es responsable de reportar debilidades e incidentes de seguridad oportunamente al área GI o CSIRT equipo de respuesta a incidentes de seguridad.
- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los colaboradores deben notificarlo al área GI o CSIRT equipo de respuesta a incidentes de seguridad para que se registre y se le dé el trámite necesario.

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

La Corporación proporcionara los recursos suficientes para tener una respuesta efectiva de colaboradores y procesos en caso de una contingencia o un evento catastrófico que se presente en la Corporación y que afecten la continuidad de la operación.

17.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Normas dirigidas a: Riesgo corporativo

- El área de Riesgo Corporativo deberá reconocer las situaciones que serán identificadas como emergencia o desastre para la Corporación, los procesos o las áreas y realizar los análisis de impacto al negocio, riesgos de continuidad para posteriormente, apoyar en el levantamiento de posibles estrategias de recuperación, en caso de activarse el plan de contingencia o continuidad.

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información debe elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.
- El área de Tecnología de información debe participar activamente en las pruebas de recuperación ante desastres.

Normas dirigidas a: Lideres de área

- Los líderes de área deben identificar y generar al interior de sus áreas, la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

17.2 REDUNDANCIAS

17.2.1 Disponibilidad de instalaciones de procesamiento de información.

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la Corporación y la plataforma tecnológica que los apoya.
- El área de Tecnología de información debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de los negocios de la Corporación.
- El área de Tecnología de información, a través de sus colaboradores, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la Corporación.

18. CUMPLIMIENTO

La Corporación velara por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información.

18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Normas dirigidas a: GI

- El área debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Corporación y relacionados con seguridad de la información.

Normas dirigidas a: Tecnología de información

- El área de Tecnología de información debe certificar que todo software que se ejecuta en la Corporación, está protegido por derechos de autor y requiere licencia de uso, o, en su lugar, sea software de libre distribución y uso.
- El área de Tecnología de información debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la Corporación para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Normas dirigidas a: Todos los usuarios

- Los usuarios no deben instalar ningún tipo de software en los equipos de trabajo que se le asignaron para el desarrollo de sus actividades laborales.
- Los usuarios deben cumplir con las leyes de derecho de autor y acuerdos de licenciamiento de software.

18.1.2 Privacidad y protección de datos personales

Normas dirigidas a: Comité del sistema de gestión de seguridad de datos personales

- Asegurar que las áreas de la Corporación que tratan datos personales lo realicen conforme a las indicaciones generales de la Política de Tratamiento de la Información, según los diversos protocolos y recomendaciones del SGSDP y, en especial, atendiendo a la tipología de los datos en cada proceso del tratamiento.
- Supervisar el cumplimiento de todos los protocolos en materia de protección de datos personales.

Normas dirigidas a: Demás áreas que realizan tratamiento de datos personales

- Acoger e implementar los lineamientos contenidos en la Política de Tratamiento de la Información y en los protocolos que complementan el SGSDP.