Tabla de Contenido

1. INTRODUCCIÓN

En la era digital actual, la información se ha convertido en uno de los activos más valiosos para cualquier organización. En Empocaldas S.A. E.S.P., reconocemos que la integridad, confidencialidad y disponibilidad de la información son fundamentales para mantener nuestra competitividad, garantizar la continuidad del negocio y preservar la confianza de nuestros clientes y colaboradores. Por ello, hemos desarrollado este Manual de Políticas de Seguridad de la Información, cuyo propósito es establecer directrices claras y efectivas para la protección de nuestros activos informáticos.

El rápido avance de las tecnologías de la información y las comunicaciones ha transformado la manera en que gestionamos y compartimos la información. Sin embargo, también ha incrementado los riesgos asociados, como las amenazas cibernéticas, el fraude y las vulnerabilidades en los sistemas. En este contexto, es imperativo contar con un marco de políticas y procedimientos que nos permita mitigar estos riesgos y asegurar un entorno de trabajo seguro y eficiente.

2. OBJETIVO

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la "**Política General de Seguridad de la Información de la Entidad**" con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de Empocaldas S.A. E.S.P.

3. ALCANCE

El presente manual de políticas aplica a funcionarios, contratistas, terceros, usuarios y visitantes de EMPOCALDAS S.A. E.S.P. por alguna razón tengan cualquier tipo de interacción con los activos de información.

4. RESPONSABILIDAD

Los funcionarios, contratistas, terceros, usuarios y visitantes de EMPOCALDAS S.A. E.S.P. deben conocer y adherirse estrictamente a todas las políticas y procedimientos establecidos en el manual, asegurando que su comportamiento y uso de los recursos tecnológicos estén alineados con las directrices de seguridad. Esto incluye el manejo adecuado de información confidencial, la protección de contraseñas, la prevención de acceso no autorizado y la notificación inmediata de cualquier incidente de seguridad. Además, deben participar activamente en las capacitaciones y actualizaciones proporcionadas por la empresa para estar al tanto de las mejores prácticas y las nuevas amenazas. El cumplimiento de estas políticas no solo protege la información de la empresa, sino que también contribuye a crear un entorno de trabajo seguro y eficiente.

5. TERMINOLOGÍA

- **Activo de Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- **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.
- **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.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

- **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.
- **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.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Inventario de activos de información:** es una lista ordenada y documentada de los activos de información pertenecientes al EMPOCALDAS.
- **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.
- **Propietario de la información:** es la unidad organizacional o proceso donde se crean los activos de información.
- **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 EMPOCALDAS S.A. E.S.P.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **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.
- **Vulnerabilidades:** son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por EMPOCALDAS (amenazas), las cuales se constituyen en fuentes de riesgo.

6. POLÍTICAS INTERNAS

EMPOCALDAS S.A. E.S.P., establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

6.1 POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

- Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.
- Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acta de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.

6.2 POLÍTICAS DE GESTIÓN DE ACTIVOS

- Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de EMPOCALDAS S.A. E.S.P.
- Los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad de EMPOCALDAS S.A. E.S.P., son activos de la empresa y se proporcionan a los empleados y terceros autorizados, para cumplir con los propósitos del negocio.
- Los activos dispuestos por EMPOCALDAS S.A. E.S.P. Para el apoyo de las labores desempeñada por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización, para ejecución de tareas establecidas en el ámbito laboral de EMPOCALDAS S.A. E.S.P.
- Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de EMPOCALDAS S.A. E.S.P. se encuentran sujetos a auditorías y revisiones por parte de La Departamento de tecnología.
- EMPOCALDAS S.A. E.S.P. identificará, clasificará y gestionará su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados.

- El Departamento de Tecnología es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los empleados y de hacer entrega de estas.
- El Departamento de Tecnología 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 empleados que se retiran o cambian de labores, cuando les es formalmente solicitado.
- Los recursos tecnológicos de EMPOCALDAS S.A. E.S.P. provistos a empleados y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las funciones laborales; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- Los funcionarios, y contratistas no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de EMPOCALDAS S.A. E.S.P.
- Los usuarios de los recursos tecnológicos y los sistemas de información de EMPOCALDAS S.A. E.S.P. realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

6.3 POLÍTICAS DE CONTROL DE ACCESO LÓGICO

- Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.
- Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan, dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- Los usuarios no deben compartir sus cuentas de usuario y contraseñas con otros empleados o con personal provisto por terceras partes.
- Todos los funcionarios, contratistas y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de EMPOCALDAS S.A. E.S.P. deben acogerse a lineamientos para la configuración de contraseñas implementados.
- La Departamento de tecnología de EMPOCALDAS S.A. E.S.P. velará porque los recursos de la plataforma tecnológica y los servicios de red sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

6.4 POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

- EMPOCALDAS S.A. E.S.P. adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
- EMPOCALDAS S.A. E.S.P. definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.
- Todas las personas que ingresen a las instalaciones de EMPOCALDAS S.A. E.S.P. deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

6.5 POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

- Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. EMPOCALDAS S.A. E.S.P. planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

6.6 POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

- El Departamento de Tecnológica e la Información, establecerá los controles para acceso lógico y protección de las redes del EMPOCALDAS S.A. E.S.P., con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la alta dirección.
- Se solicitará autorización por parte del jefe inmediato, para permitir la conexión a las redes empresariales de los equipos personales de los funcionarios o colaboradores de EMPOCALDAS S.A E.S.P.
- El Departamento de Tecnología definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.
- El Departamento de Tecnología establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

- El Departamento de Tecnología debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de EMPOCALDAS S.A. E.S.P.
- El Departamento de Tecnología debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de EMPOCALDAS S.A. E.S.P.
- El Departamento de Tecnología debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

6.7 POLÍTICAS DE ACCESO A REDES Y RECURSOS DE RED

- El Departamento de Tecnología de EMPOCALDAS S.A. E.S.P., como responsables de las redes de datos y los recursos de red, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico
- El Departamento de Tecnología debe asegurar que las redes inalámbricas de EMPOCALDAS S.A. E.S.P. cuenten con métodos de autenticación que evite accesos no autorizados.
- El Departamento de Tecnología debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de EMPOCALDAS S.A. E.S.P., así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad y Privacidad de la Información por parte de estos.
- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de EMPOCALDAS S.A. E.S.P. deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

6.8 POLÍTICAS DE ACCESO A CUENTAS INSTITUCIONALES

- Cada jefe de área o sección debe solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los empleados que laboran en sus áreas, acogiéndose al procedimiento establecidos para tal fin.
- Previa solicitud de los jefes inmediatos, el Departamento de Tecnología procederá con la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información de EMPOCALDAS S.A. E.S.P.

6.9 POLÍTICAS DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACIÓN

- El Departamento de Tecnología debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.
- El Departamento de Tecnología debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- El Departamento de Tecnología debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- El Departamento de Tecnología debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

6.10 POLÍTICAS DE NORMAS SEGURAS

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por el departamento de tecnología; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.
- El Departamento de Tecnología debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible o en su defecto con la utilización del software de control de acceso.
- El Departamento de Tecnología debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- El Departamento de Tecnología debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma

tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

- El Departamento de Tecnología debe velar porque los recursos de la plataforma tecnológica de EMPOCALDAS S.A. E.S.P. ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.
- El Departamento de Tecnología debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.
- El Departamento de Tecnología debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de EMPOCALDAS S.A. E.S.P.
- El Departamento de Tecnología debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de EMPOCALDAS S.A. E.S.P.

6.11 POLÍTICAS DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

- El Departamento de Tecnología debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de EMPOCALDAS S.A. E.S.P.
- El Departamento de Tecnología debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de EMPOCALDAS S.A. E.S.P.
- El Departamento de Tecnología debe generar estándares de configuración segura para los equipos de cómputo de los empleados de EMPOCALDAS S.A. E.S.P. y configurar dichos equipos acogiendo los estándares generados.
- El Departamento de Tecnología debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de EMPOCALDAS S.A. E.S.P. y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

- El Departamento de Tecnología debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los empleados de EMPOCALDAS S.A. E.S.P., ya sea cuando son dados de baja o cambian de usuario.
- El Departamento de Tecnología debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de EMPOCALDAS S.A. E.S.P. cuente con la autorización documentada y aprobada previamente por el responsable del recurso.
- El Departamento de Tecnología es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de EMPOCALDAS S.A. E.S.P.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los empleados y personal provisto por terceras partes deben acoger las instrucciones técnicas de proporcione el departamento de tecnología.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de EMPOCALDAS S.A. E.S.P. el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior del Departamento de tecnología, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de EMPOCALDAS S.A. E.S.P., solo puede ser realizado por los funcionarios del Departamento de tecnología, o personal de terceras partes autorizado por dicha dirección.
- Los funcionarios de EMPOCALDAS S.A. E.S.P. y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
- Los funcionarios de EMPOCALDAS S.A. E.S.P. y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.
- Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- En caso de pérdida o robo de un equipo de cómputo de EMPOCALDAS S.A. E.S.P., se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

- Los empleados de EMPOCALDAS y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

6.12 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- El Departamento de Tecnología e información, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

6.13 POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

- EMPOCALDAS S.A. E.S.P. establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
- Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesaria durante y después del contrato.

6.14 SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

- EMPOCALDAS S.A. E.S.P. establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.
- El Departamento de TIC generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP).

6.15 POLÍTICAS DE GESTIÓN DE INCIDENTES

- Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar al Grupo/Proceso de TICS por cualquiera de los medios dispuestos para tal fin.

- Sera responsabilidad del Grupo de Tecnología y las Comunicaciones seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.

6.16 POLÍTICAS DE CUMPLIMIENTO

- EMPOCALDAS S.A. E.S.P. velará por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

6.17 ESCRITORIO LIMPIO

- No deberán dejarse documentos críticos en el “Escritorio” tanto físico como el Escritorio virtual (se denomina “Escritorio” al espacio digital en los equipos de cómputo).
- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

6.18 USO ADECUADO DE INTERNET

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Estará limitado el acceso a redes sociales en general.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
- El Departamento de TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

6.19 USO ADECUADO DE CORREO ELECTRÓNICO

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a EMPOCALDAS S.A. E.S.P., por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- La oficina/grupo de tecnología podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

6.20 USO DE USUARIOS Y CONTRASEÑAS

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.
- Las credenciales son personales e intransferibles.
- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).
- Utiliza combinaciones de letras mayúsculas y minúsculas, números y símbolos.
- No utilices datos relacionados a tu empresa o a ti (fecha de creación, nombre personal, fecha de nacimiento… entre otros).
- Usa una única contraseña para cada sitio Web.
- Rechaza guardar la contraseña en navegadores públicos.
- No envíes nunca una contraseña por medios que no tengan seguridad fiable.
- No compartas las contraseñas con nadie.
- Emplea contraseñas que sean fáciles de recordar para ti, pero difícil de adivinar para otros usuarios.

6.21 SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

EMPOCALDAS S.A. E.S.P., definirá un “Plan de Comunicación en Seguridad de la Información” a través de su oficina de comunicación interna y externa y el Departamento TIC, donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de la oficina TIC y/o el Oficial de Seguridad de la información.

6.22 CAPACITACIONES EN SEGURIDAD

EMPOCALDAS S.A. E.S.P. a través de sus áreas/procesos de Talento Humano y el Departamento de tecnología, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, el grupo TIC y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones.

6.23 APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por el Comité Institucional de Gestión y Desempeño y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de EMPOCALDAS S.A. E.S.P.

6.24 SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de EMPOCALDAS S.A. E.S.P. de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

i. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

ii. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

iii. El Departamento de Tecnología e información será el encargado de recopilar y entregar a la Oficina de Control Disciplinario EMPOCALDAS S.A. E.S.P. las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las Politicas.

7. DESCRIPCIÓN GENERAL DE ACTIVIDADES

Las actividades se encuentran enmarcadas en el cumplimiento de cada una de las políticas.

8. NORMAS Y/O REFERENCIAS

- ✓ Ley 1581 de 2012 (Ley de Protección de Datos Personales): Esta ley establece las disposiciones generales para la protección de datos personales. Define los principios, derechos y obligaciones para el tratamiento de datos personales, y obliga a las organizaciones a implementar medidas de seguridad adecuadas para proteger estos datos.

- ✓ Decreto 1377 de 2013: Reglamenta la Ley 1581 de 2012, proporcionando directrices adicionales para la protección de datos personales. Este decreto establece la necesidad de implementar políticas y procedimientos que garanticen la seguridad y privacidad de la información.

- ✓ Ley 1266 de 2008 (Ley de Habeas Data): Regula el manejo de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Aunque se enfoca principalmente en datos crediticios, también establece principios y obligaciones para la protección de datos personales.

- ✓ Ley 1273 de 2009: Modifica el Código Penal para crear tipos penales relacionados con la protección de la información y los datos, estableciendo sanciones para delitos informáticos y fortaleciendo la protección de la privacidad de la información digital.

- ✓ Ley 527 de 1999 (Ley de Comercio Electrónico): Regula y da validez jurídica a los mensajes de datos y a la firma electrónica. Establece la importancia de garantizar la autenticidad, integridad y confidencialidad de la información en las transacciones electrónicas.

- ✓ Circular Externa 038 de 2016 de la Superintendencia de Industria y Comercio (SIC): Esta circular proporciona directrices sobre las medidas de seguridad de la información para la protección de datos personales. Incluye recomendaciones para la implementación de políticas de seguridad y la gestión de incidentes.

9. CONTROL DE CAMBIOS

DATOS DE CREACIÓN DEL DOCUMENTO	
Fecha de elaboración	2024-08-05
Nombre de quien elaboró	Sebastián López Ciro
Cargo	Contratista Departamento de Tecnología e Información CIO

Elaboró	Revisó	Aprobó
Sebastian Lopez Ciro Contrato 082 Chief Information Security Officer	Coordinadora de Procesos	Jefe Depto. de Tecnología e Información CIO