DIRECTIVA GERENCIA No. 024 de 2025
(19 de Marzo del 2025)

POR MEDIO DE LA CUAL SE ADOPTAN PROCEDIMIENTOS, FORMATOS, MANUALES, MODIFICACION DEL PROCEDIMEINTO PRGFA 15 Y EL PLAN DE RECUPERACIÓN DE DESASTRES DEL PROCESO DE INFORMÁTICA Y COMUNICACIONES PARA EL SISTEMA INTEGRADO DE GESTIÓN S.I.G. DE CENTRALES ELÉCTRICAS DEL CAUCA CEDELCA S.A. E.S.P.

El Gerente Suplente de CEDELCA S.A E.S.P., en uso de sus facultades legales y estatutarias y considerando que:

Centrales Eléctricas del Cauca CEDELCA S.A. E.S.P., es una sociedad anónima comercial, de nacionalidad colombiana del orden nacional con autonomía administrativa, patrimonial y presupuestal, clasificada legalmente como empresa de servicios públicos mixta, perteneciente al sector minero Energético del Ministerio de Minas y Energía, sometido al Régimen General de las Empresas del sector eléctrico, con régimen especial de derecho privado contemplado en la Ley 142 de 1994.

Puntualmente la Ley 142 de 1994, define en el **ARTÍCULO 46.** "Control interno. Se entiende por control interno el conjunto de actividades de planeación y ejecución, realizado por la administración de cada empresa para lograr que sus objetivos se cumplan.

Igualmente, en este sentido la Ley 142 de 1994, define en el **ARTÍCULO 49.** "Responsabilidad por el control interno. El control interno es responsabilidad de la gerencia de cada empresa de servicios públicos.

En el entendido de que el control interno de este tipo de empresas es el conjunto de actividades de planeación y ejecución, realizado por la administración para lograr que sus objetivos se cumplan, disponiendo de medidas objetivas de resultado, o indicadores de gestión, alrededor de diversos objetivos, para asegurar su mejoramiento y evaluación de responsabilidad de la gerencia. Centrales Eléctricas del Cauca CEDELCA S.A E.S.P. estableció el Sistema Integrado de Gestión SIG, que se compone de procesos, procedimientos y mecanismos de verificación y evaluación con el objetivo de proporcionar un grado de seguridad razonable, y poder conseguir sus objetivos.

En relación a dicho sistema y con el propósito de impulsar la aplicación de buenas prácticas de administración, que permitan legitimar su acción y que redunden en una gestión más eficiente, eficaz y efectiva; mejorando su desempeño y la

capacidad de proporcionar servicios que respondan a las necesidades y expectativas de las partes interesadas, fortaleciendo el control y la evaluación interna y orientar a la Empresa hacia el cumplimiento de la política y objetivos, Centrales Eléctricas del Cauca CEDELCA S.A. E.S.P, ve necesario la modificación del procedimientos PRGFA 15 y la adopción de los siguientes documentos

PROCEDIMIENTOS

PRGFA 54 Procedimiento de Administración de Máquinas Virtuales.
PRGFA 55 Procedimiento de Monitoreo de Infraestructura de Red y Servidores.
PRGFA 56 Procedimiento de Prueba de Restauración de Copias de Seguridad de un Servidor.
PRGFA 57 Procedimiento de Restauración de Configuración de Dispositivos de Red.

FORMATOS

FTGFA 115-Formato de Copias de Seguridad de la Información.
FTGFA 116-Formato Activación Plan de Recuperación de Desastres.
FTGFA 117-Formato Administración de Máquinas Virtuales.
FTGFA 118-Formato de contactos Plan Recuperación de Desastres.
FTGFA 119-Formato de Datos de Proveedores de Servicio.
FTGFA 120-Formato de Eventos de Infraestructura de Red y Servidores.
FTGFA 121-Formato de Inventario Servidores y Dispositivos de Red.
FTGFA 122-Formato de Monitoreo de Infraestructura de Red y Servidores.
FTGFA 123-Formato de Monitoreo de Proveed de Servicios de Internet.
FTGFA 124-Formato de Prueba de Restauración de Copias de Seguridad de un Servidor.
FTGFA 125-Formato de Restauración de Configuración de Dispositivos de Red.

MANUALES

MNGFA03 - Manual de políticas de seguridad y privacidad de la información.
MNGFA04 - Manual de Prueba de Restauración de Copias de Seguridad de un Servidor.
MNGFA05 - Manual de Administración de Máquinas Virtuales.

PLAN

MNGFA06 - Plan de recuperación de desastres.

Los documentos mencionados anteriormente hacen parte del proceso de Informática y Comunicaciones para el fortalecimiento del Sistema Integrado de Gestión SIG mediante el cual opera los diferentes procesos, enmarcado en las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018.

Con el Sistema Integrado de Gestión da cumplimiento a los estándares internacionales de la ISO 45001:2018 y demás requisitos legales aplicables en SG-SST.

Y finalmente frente al Sistema de Gestión de Calidad, en búsqueda de Incrementar la satisfacción de las partes interesadas, mediante el cumplimiento de los requisitos de la norma ISO 9001:2015 para el servicio.

En mérito de lo expuesto,

RESULEVE

ARTÍCULO PRIMERO. MODIFICAR EL PROCEDIMIENTO PRGFA 15, ADOPTAR LOS PROCEDIMIENTOS IDENTIFICADOS COMO PRGFA54 A PRGFA57, ADOPTAR LOS FORMATOS IDENTIFICADOS COMO FTGFA 115 A FTGFA 125, ADOPCIÓN DE LOS MANUALES IDENTIFICADOS COMO MNGFA03 A MNGFA05 Y ADOPCIÓN DEL PLAN IDENTIFICADO COMO MNGFA06 DEL PROCESO DE INFORMÁTICA Y COMUNICACIONES, diseñados para Centrales Eléctricas del Cauca CEDELCA S.A. E.S.P., el cual involucra los requerimientos de los Sistemas de Gestión de Calidad, enmarcado en las normas ISO 9001:2015.

ARTÍCULO SEGUNDO. DOCUMENTOS DEL SISTEMA INTEGRADO DE GESTIÓN. Incluir los procedimientos PRGFA54 A PRGFA57, los formatos FTGFA 115 A FTGFA 125, los manuales MNGFA03 A MNGFA05 y el plan MNGFA06, del proceso de Informática y Comunicaciones, en la información documentada del S.I.G. para la correspondiente socialización e implementación.

ARTÍCULO TERCERO. DIVULGACIÓN, La divulgación de los procedimientos PRGFA54 A PRGFA57, los formatos FTGFA 115 A FTGFA 125, los manuales MNGFA03 A MNGFA05 y el plan MNGFA06, del proceso de Informática y Comunicaciones, se realiza por medio de la publicación en intranet de la empresa, la inducción, reinducción, según aplique y la evaluación correspondiente.

ARTÍCULO DECIMO. VIGENCIA. La presente Directiva rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sen contrarias.

Dada en el municipio de Popayán – Cauca a los diecinueve (19) días del mes de Marzo del año 2025.

PEDRO ELÍAS ROJAS CÁCERES
Gerente suplente

Proyectó: Fernando Andres Estrada Romero – Profesional Universitario II
Revisó: Andrés Caicedo Pérez – Subgerente de Planeación
Revisó: Guillermo Hernán Latorre Cerón – Jefe Oficina Jurídica

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CENTRALES ELÉCTRICAS DEL CAUCA S.A E.S.P. CEDELCA

2025

TABLA DE CONTENIDO

1. COMPROMISO

CEDELCA S.A E.S.P., ha declarado su compromiso con la seguridad y privacidad de la información mediante la elaboración del manual de políticas de seguridad de la información, el cual presenta para el usuario final y los diferentes actores que intervienen en los procesos, los controles que adopta la entidad para el manejo de la información, basado en los estándares internacionales que plantea la norma ISO 27001:2022.

2. OBJETIVO DEL MANUAL

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de **CEDELCA S.A E.S.P.** e implementando las buenas prácticas y socializándolas a todos los actores involucrados.

3. OBJETIVOS ESPECÍFICOS

- Garantizar la disponibilidad, integridad y confidencialidad como principios fundamentales de la seguridad de la información.
- Salvaguardar tanto la información como los activos tecnológicos que pertenecen a CEDELCA S.A E.S.P.
- Concientizar a los funcionarios y contratistas de CEDELCA S.A E.S.P. sobre la correcta utilización de los activos de información asignados para sus funciones diarias, asegurando la protección de la confidencialidad, la privacidad y la integridad de los datos.

4. ALCANCE DEL MANUAL

El presente manual de políticas aplica a colaboradores, contratistas, terceros, usuarios y visitantes de **CEDELCA S.A E.S.P.** que por alguna razón tengan acceso o cualquier tipo de interacción con los activos de información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la entidad.

5. DEFINICIONES

- **Información:** Conjunto de datos que informan sobre algo.
- **Seguridad de la Información:** Entiéndase como la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Activo de Información:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas, etc) que tenga valor para la organización.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.

- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **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.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Código malicioso:** Es un código informático que crea brechas de seguridad para dañar un sistema informático.
- **Privacidad de la información:** El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Terceros**: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.
- **VPN:** Red virtual privada por sus siglas en inglés Virtual Private Network.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- **Alta Dirección:** Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad (ministro, viceministros, secretaria general y direcciones).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Procedimiento:** Es un conjunto documentado de instrucciones específicas y detalladas que describen cómo llevar a cabo una actividad o proceso para garantizar la coherencia, efectividad y cumplimiento con los objetivos de seguridad de la información y los controles establecidos.

6. *POLÍTICAS*

CEDELCA S.A E.S.P., establece a continuación, los siguientes controles de seguridad de la información, los cuales deberán ser cumplidos por todos los colaboradores, 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:

A. Controles organizativos

Políticas de Seguridad de la Información

- Los colaboradores, contratistas, proveedores y todos aquellos que tengan responsabilidades, sobre fuentes, repositorios y recursos de procesamiento de la información de CEDELCA S.A E.S.P., deben adoptar los lineamientos contenidos en el presente documento. Este está compuesto por las políticas que mejor se ajustan a los actuales sistemas tecnológicos de información y a la estructura de la empresa, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad de la información.
- La socialización de la política de seguridad de la información se realiza a través de los canales de comunicación definidos por la entidad entre los que está el correo electrónico, mensajería instantánea entre otros, enfatizando que esta política se encuentra disponible en la intranet y en la página web de la organización.
- Las presentes políticas de seguridad de la información se alinean a las estrategias, el entorno, contratos y las legislaciones aplicables a CEDELCA S.A E.S.P. Se establecen para asegurar los temas de control de acceso, clasificación de información, seguridad física y del entorno, temas orientados a los usuarios finales (uso aceptable de activos, transferencia de información, dispositivos móviles, trabajo en casa, restricciones y otros), copias de respaldo y/o Backups, protección contra código malicioso, gestión de vulnerabilidades, seguridad en las telecomunicaciones, privacidad y protección de información de datos personales, relación con proveedores, entre otros temas de seguridad de la información.

Funciones y Responsabilidades en Materia de Seguridad de la Información

GERENCIA

Promover activamente una cultura de seguridad de la información dentro y fuera de la empresa y el aseguramiento de los recursos, infraestructura y talento humano adecuados para implementar y mantener la Seguridad de la Información y Protección de Datos.

RESPONSABLE DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El responsable de la seguridad y privacidad de la información tendrá las siguientes responsabilidades:

- Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información.
- Coordinar la gestión de riesgos según la periodicidad establecida, incluyendo la actualización de amenazas, vulnerabilidades y riesgos en los activos de información de la organización.
- Dictar lineamientos para controlar el acceso a los sistemas de información y la modificación de los privilegios.

- Hacer seguimiento a las no conformidades y al estado de las acciones correctivas, relacionadas con la seguridad de la información.
- Informar a la Alta Dirección sobre el desempeño del Sistema de Gestión de Seguridad de la Información.
- Coordinar las actividades correspondientes a la gestión de Incidentes de Seguridad de la Información.
- Desarrollar, mantener y comunicar las políticas, estándares y guías de seguridad de la información.
- Realizar el proceso de gestión de incidentes de seguridad que se presenten en la empresa.
- Dar soporte y asesoría a los líderes de proceso en el análisis de riesgos de seguridad de la información, así como consolidar los planes para su tratamiento.
- Elaborar las campañas de sensibilización y socialización de seguridad de la información.
- Configurar y afinar las herramientas de seguridad instaladas.

RESPONSABLE DE INFRAESTRUCTURA

El responsable de infraestructura en aras de asegurar el correcto uso y administración de los recursos tecnológicos de la Empresa y para contribuir a la seguridad de la información en CEDELCA tendrán las siguientes responsabilidades:

- Identificar y actualizar en conjunto con el responsable de la seguridad y privacidad de la información el inventario de activos de información y apoyar al líder del proceso en la valoración y determinarán la criticidad de los activos identificados.
- Planear y ejecutar el plan de mantenimiento de la infraestructura tecnológica de la organización.
- Implementar las mejoras que estén relacionadas con hardware, software, canales de comunicaciones o infraestructura de TI en general.
- Identificar y reportar riesgos, eventos o incidentes de seguridad a través de los canales definidos.
- Gestionar recursos para la mejora continua.

LÍDERES DEL PROCESO

Los líderes de procesos son los responsables y propietarios de los activos de información para todos los aspectos de seguridad de la información y deben cumplir las siguientes responsabilidades:

- Identificar e incluir en el inventario de activos de información, los activos identificados, así como los riesgos asociados.
- Efectuar el análisis de riesgos de seguridad de la información en sus procesos y activos de información y coordinar el plan de tratamiento de los riesgos identificados con el líder de seguridad de la información.
- Identificar oportunidades de mejora en seguridad de la información en sus procesos.

- Realizar acompañamiento al responsable de la seguridad y privacidad de la información y al responsable de infraestructura en la identificación y clasificación de los activos de información.

COLABORADORES

- Los colaboradores y personal provisto por terceras partes que realicen labores en o para CEDELCA S.A E.S.P., tienen la responsabilidad de cumplir de manera estricta con las presentes políticas, normas, procedimientos y estándares referentes a la seguridad de la información.
- Los colaboradores son responsables por los activos que se les haya asignado, incluyendo activos de información.
- Así mismo tienen la responsabilidad de reportar los eventos o incidentes de seguridad de la información que puedan detectar en el desempeño de sus labores y que puedan afectar a la organización.
- Son responsables de la información bajo su custodia y que les haya sido suministrada, por lo que deberán mantener su confidencialidad, integridad y disponibilidad, así como velar porque la misma no llegue a fugarse.

TERCEROS Y/O ALIADOS

Las terceras partes interesadas o aliados de CEDELCA S.A E.S.P., deben ceñirse a las políticas de seguridad de la información descritas en este documento, deben dar un uso responsable bajo un marco de seguridad que proteja la confidencialidad, la integridad y la disponibilidad de la información o datos que se intercambian, en el marco de contratos o alianzas estratégicas.

Segregación de funciones

CEDELCA S.A E.S.P. se encuentra estructurada a través de la cadena de valor, dividida por procesos (estratégicos, misionales y de apoyo), los cuales cuentan con un área funcional que operativiza las actividades acordes con los objetivos empresariales. Para la seguridad de la información, se definen desde la Oficina de Informática y Comunicaciones.
Las funciones del equipo que administra los servidores, aplicativos, redes y telecomunicaciones, seguridad perimetral y otros servicios corporativos, están a cargo de la Oficina de Informática y Comunicaciones.
De acuerdo con el cargo y funciones de cada colaborador se definen los accesos y roles que estos tendrán en los sistemas de información (diversos aplicativos) de CEDELCA S.A E.S.P.
La seguridad física y del entorno es monitoreada por el CCTV (Circuito cerrado de Televisión), el cual es liderado y es responsabilidad del área Administrativa.

Responsabilidades de la dirección

La empresa se compromete en apoyar a la Oficina de Informática y Comunicaciones a través de la directiva para el cumplimiento de las presentes políticas de seguridad de la información, Se comprometen a apoyar los programas educativos en materia de seguridad de la información para los colaboradores tales como seminarios, conferencias, espacios de charlas y difusión a través de los diversos canales de comunicación.

Contacto con las autoridades

CEDELCA S.A E.S.P., mantiene contacto con las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes.
Las principales autoridades en materia de seguridad en el país, Colombia, son las siguientes:

- Centro Cibernético Policial, CCP - Policía http://www.ccp.gov.co
- Grupo de respuestas a Emergencias Cibernéticas de Colombia, ColCERT, Gobierno http://www.colcert.gov.co/index.php

Contacto con grupos de interés especial

Por parte de la Oficina de Informática y Comunicaciones, se debe tener una relación activa y apropiada con grupos especializados en el campo de la seguridad de la información y tecnologías de la información (TI), como foros, grupos, asociaciones, empresas, entre otros, que mantienen actualizado el panorama y tendencias de la seguridad de la información y TI.
Esto se hará con el objetivo de generar espacios donde se compartan conocimientos, charlas o conferencias educativas en materia de seguridad de la información o tecnología para los usuarios finales.

Seguridad de la información en la gestión de proyectos

La seguridad de la información se debe integrar a la gestión de proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de los proyectos. Lo anterior aplica a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los líderes de procesos asegurar que se sigan las siguientes directrices:

a. Incluir objetivos de seguridad de la información en los objetivos del proyecto.
b. Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.
c. Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.

Inventario de la información y otros activos asociados

- Toda información sea física o digital generada, almacenada o transformada por los colaboradores, contratistas o proveedores de la empresa, utilizando los recursos dispuestos por la empresa para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de **CEDELCA S.A E.S.P.**

- Los activos dispuestos por **CEDELCA S.A E.S.P.** para el apoyo de las labores desempeñada por los colaboradores, contratistas, terceros, usuarios y visitantes, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral de **CEDELCA S.A E.S.P.**

Inventario de activos

- Todos los dispositivos de procesamiento de información de la empresa deberán ser registrados en el inventario de equipos de cómputo "FTFGA 75_HV EQUIPOS", en donde se registre información relacionada con Hardware, Sistema operativo y software base instalado, Fecha de compra, Especificaciones generales y Entre otros.

- Los dispositivos identificados como servidores y dispositivos de red que se encuentren en el centro de datos de **CEDELCA S.A E.S.P.** deberán ser registrados en el FTGFA 121-Formato de Inventario Servidores y Dispositivos de Red, ya que ellos son catalogados como activos de información.

- Esta información deberá ser consignada una vez hayan sido recibidos los equipos en cuestión; la actualización del inventario de equipos se llevará a cabo cada vez que se realice cualquier tipo de modificación de software o hardware sobre los mismos.
- El mantenimiento físico y lógico de todos los equipos de CEDELCA S.A E.S.P., las revisiones de mantenimiento de software y revisión de la vigencia de licencias se realizará anualmente y estará a cargo de La Oficina de Informática y Comunicaciones.

Adquisición y asignación de equipos de usuario

- La adquisición, asignación y entrega de equipos la realizará el área Financiera y Administrativa a través de la Oficina de Informática y Comunicaciones.
- Los equipos de cómputo tendrán instalados única y exclusivamente los aplicativos y/o programas debidamente licenciados y aprobados teniendo en cuenta las funciones del usuario que lo utilizará. Adicionalmente se deben aplicar todas las restricciones y realizar las instalaciones de software correspondientes. Hasta tanto el equipo no se encuentre en condiciones adecuadas para su uso, el usuario no podrá utilizarlo.

Propiedad de los activos:

Uso de computadores

- Para no afectar la operación de la empresa se deben utilizar las herramientas autorizadas por parte de la Oficina de Informática y Comunicaciones, las cuales cumplen con los protocolos de seguridad de la información, como almacenamiento Cloud, Correo Electrónico, Chat, SFTP, Repositorios, Unidades Compartidas.
- En caso de ausencia de un colaborador sin reemplazo y de llegarse a necesitar información del computador asignado a éste, se deberá solicitar previa autorización del Gerente. El acceso a estos archivos debe ser informado a la Oficina de Informática y Comunicaciones.

- Se debería tener las precauciones necesarias al comer o beber en el puesto de trabajo para evitar daños al computador, documentos o los elementos de trabajo.
- Está prohibido intercambiar partes entre computadores (mouse, teclados, monitor, etc.), sin previo consentimiento de la Oficina de Informática y Comunicaciones y dejar los registros por correo electrónico o por escrito de dichos cambios.
- No está permitido almacenar en el disco duro del computador, ni en las carpetas de red, archivos (música, videos, fotos, programas y otros) que violen las leyes de propiedad intelectual y que no sean a fin con los propósitos de CEDELCA S.A E.S.P.
- Los funcionarios deben comunicar inmediatamente por medio del formulario de mesa de ayuda toda vulnerabilidad u operación sospechosa que se encuentre en los sistemas, manifestación de malware, virus o programas sospechosos e intentos de intromisión en los sistemas (ej. Bloqueo constante del usuario en los sistemas), no deben revelar este tipo de información ni interna o externamente.
- Está prohibido leer documentos que se especifiquen expresamente o según la clasificación de la información como confidenciales, dirigidos a otros procesos o colaboradores.
- El traslado y movimiento de equipos (excepto los portátiles) debe ser realizado por la Oficina de Informática y Comunicaciones.

Uso de Internet

El servicio de Internet es un servicio de gran importancia en el mundo laboral, de conocimiento y negocios basado en el acceso a diferentes fuentes de información en distintas ubicaciones a través de sistemas de cómputo interconectados en red a nivel local y mundial.
El acceso al servicio de Internet es un permiso otorgado por CEDELCA S.A E.S.P. a sus funcionarios, contratistas o practicantes y así mismo sobrelleva responsabilidades y compromisos para su uso. Se espera que los usuarios de este servicio conserven normas de buen uso, confidencialidad y criterio ético.
El acceso a sitios que no se requieren normalmente para las funciones laborales estará bloqueado si se encuentran en las siguientes categorías.

- Sitios para adultos (Pornografía, Sexo explícito, Citas)
- Violencia, armas, agresión
- Drogas, alcohol y tabaco
- Audio y video (streaming, sitios de video del tipo Youtube o Vimeo, TV en vivo, sitios de divulgación, descarga o distribución de películas, videos, música, audio, webcams, etc).
- Entretenimiento (Humor, cocina, mascotas, astrología, etc.)
- Juegos de cualquier índole
- Chats, blogs, página de contactos, etc.
- Redes sociales (Facebook, Twitter)
- Sitios Maliciosos / ciberdelincuencia, Phishing, Spam.
- Sitios que permitan acceder a software pirata y/o malware

- La Oficina de Informática y Comunicaciones podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

- No se permite utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados.
- Está prohibido compartir en sitios web información propia de CEDELCA S.A E.S.P. clasificada como reservada o clasificada de sus usuarios, funcionarios, contratistas.
- Emplear este servicio para la recepción, envió o distribución de información pública clasificada o reservada de CEDELCA S.A E.S.P. a través de servicios y cuentas de correo públicos no está permitido.
- No está autorizado cargar, descargar, instalar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.
- Se restringe el uso del servicio de Internet/Intranet para propósitos comerciales ajenos a CEDELCA S.A E.S.P.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados por CEDELCA S.A E.S.P. no está permitido.
- Está prohibido comprar o vender artículos personales a través de sitios web o de subastas en línea.
- No está permitido publicar o enviar opiniones personales, declaraciones políticas y asuntos no propios de la entidad, dirigidos a funcionarios, contratistas o practicantes y público en general, del sector oficial, de otras compañías y organizaciones, a través de este servicio.
- No está autorizado descargar, instalar y configurar navegadores distintos a los permitidos por la Oficina de Informática y Comunicaciones.

Uso de correo electrónico y mensajería instantánea

El Correo Electrónico Corporativo es un servicio basado en el intercambio de información a través de la red y el cual es provisto por CEDELCA S.A E.S.P. para los funcionarios, contratistas, previamente autorizados para su acceso.

- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas y practicantes con acceso a este servicio.
- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a **CEDELCA S.A E.S.P.**, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico sólo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- La oficina de Informática y Comunicaciones podrá verificar el contenido de los buzones de los correos electrónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.
- El servicio de correo electrónico tiene como objeto la comunicación a nivel corporativo, con los funcionarios de la misma empresa, proveedores, prestadores o cualquier tercero que tenga relación con CEDELCA S.A E.S.P. La información que se envíe por este medio es propiedad de CEDELCA S.A E.S.P. y por ende cualquier acceso o investigación a ésta, se realizará con autorización expresa de la Gerencia.
- Redactar los contenidos de un mensaje de correo electrónico de tal manera que sea serio, claro, conciso, cortés y respetuoso.

- Está prohibido el envío de archivos tipo MP3, WAV, EXE, LNK archivos de video o cualquier otro tipo de archivo que viole la propiedad intelectual, los derechos de autor, la dignidad humana o que genere daño o perjuicios a terceros.
- El correo electrónico corporativo es para uso laboral, no está permitido darle uso para fines personales y comerciales como promoción de productos, rifas y suscripciones sin autorización de la Gerencia.
- El correo corporativo no debe ser usado para el envío de cadenas ya que pueden traer archivos adjuntos de gran volumen o virus ocultos.
- Está prohibido realizar intentos no autorizados para acceder a otra cuenta de correo electrónico Institucional.
- Está prohibido revelar o publicar cualquier información clasificada o reservada de CEDELCA S.A E.S.P.
- No se permite el envío de correos con contenido que atente contra la integridad humana de las personas o instituciones, tales como: pornográfico, chistes, religiosos, terroristas, hackers, racistas, políticos o cualquier contenido que represente riesgo de virus; código malicioso, etc.
- Las credenciales de acceso a las cuentas de correo electrónico corporativo asignadas a los usuarios son intransferibles, no se pueden compartir los accesos.
- Los accesos a las cuentas de correo electrónico corporativo están protegidos por autenticación de doble factor a cargo de La Oficina de Informática y Comunicaciones.
- El uso de programas de mensajería instantánea de carácter público no está permitido, ya que representan elementos de exposición pública y evaden los controles perimetrales.
- Mantener actualizado el estado de disponibilidad en el sistema para que los demás usuarios puedan saber si están disponibles para ser contactados.
- No se debe participar en actividades de acoso, difamación o intimidación mediante la mensajería instantánea.
- No enviar mensajes difamatorios, ofensivos, obscenos, vulgares, racistas, calumniosos o de contenido sexual, ya sea sobre superiores, compañeros, subalternos o cualquier otra entidad o individuo. Esto puede afectar tanto la reputación personal como de la entidad.
- No compartir información clasificada o reservada de **CEDELCA S.A E.S.P.** o de sus empleados, contratistas o practicantes sin la debida autorización.
- No se debe descargar, instalar y utilizar sistemas de mensajería instantánea que no sean los aprobados y administrados por la Oficina de Informática y Comunicaciones de **CEDELCA S.A E.S.P.**, tales como Yahoo! Messenger, AOL Instant Messenger (AIM), MSN Messenger, eBuddy, ICQ, MySpace, entre otros.
- No compartir documentos o archivos que no estén relacionados con las operaciones de la entidad.
- No se debe intentar modificar la configuración o parámetros de seguridad de los clientes de mensajería instantánea proporcionados por **CEDELCA S.A E.S.P.**
- No se permite participar en actividades que puedan causar congestión o interrupción en los servicios de comunicación de CEDELCA S.A E.S.P. o la normal operación de los servicios de correo electrónico.

- El envío de correos SPAM de cualquier índole no está permitido.
- Está prohibido reenviar correos electrónicos con contenido PHISING.
- No se permite intentar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de CEDELCA S.A E.S.P.
- Se prohíbe utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.
- No se permite usar correos públicos para la recepción, envió o distribución de información pública clasificada o reservada propia de CEDELCA S.A E.S.P.
- Está prohibido distribuir listas de direcciones de correo personales sin expresa autorización de sus dueños.

El uso inapropiado o el abuso en el servicio de correo electrónico ocasionan la desactivación temporal o permanente de las cuentas. La desactivación de la cuenta lleva consigo la imposibilidad de acceder a los mensajes de correo que estén en ese momento en el servidor y la imposibilidad de recibir nuevos mientras no vuelva a ser activada.

Uso de las aplicaciones corporativas

- Las aplicaciones corporativas se deben usar para su propósito, no se debe extraer información de las aplicaciones corporativas con fines personales o en beneficio propio o de terceros no autorizados.
- El acceso a las aplicaciones corporativas está definido por usuario y contraseña para cada colaborador, estos deben propender por proteger sus credenciales de acceso y no deben compartir estos datos con otros colaboradores o terceros.

Uso de la red inalámbrica

- La entidad tendrá una red de invitados para conexión inalámbrica a internet de equipos de visitantes que lo soliciten, esta conexión permite navegación de uso general y cuenta con restricciones de acceso a sitios de categorías que representan amenazas para la empresa, puede ser accedida desde equipos portátiles y dispositivos móviles en iguales condiciones, esta red será aislada de la red LAN, es una red únicamente de acceso a internet.
- En caso de detectar actividad anómala o sospechosa a través de estas redes se debe alertar a la Oficina de Informática y Comunicaciones.
- Las claves de acceso a las redes inalámbricas deben ser cambiadas cada 6 meses o antes si se sospecha que se han divulgado las claves.

Devolución de activos

- El Colaborador es responsable de realizar la devolución de activos y la información con el fin de obtener las firmas del acta de entrega de cargo en señal de paz y salvo a satisfacción por parte de los procesos respectivos.
- La Unidad de Apoyo de Administración de Personal validará dicha devolución de manera previa al trámite del pago de liquidación.

- La tarjeta de acceso físico debe ser devuelta a la Oficina de Informática y Comunicaciones, donde se retirarán los accesos.
- El Colaborador o tercero no podrá extraer, secuestrar mediante cifrado, ni borrar información de propiedad de CEDELCA S.A E.S.P.

Clasificación de la información

La Secretaría General realizará la revisión de las Tablas de Retención Documental de la Empresa, y hará la actualización cuando lo considere necesario.

Transferencia de información

- La información transferida que llega en formatos adjuntos por vía correo electrónico y que es categorizada dentro del mismo como spam o correo altamente peligroso, debe ser comunicada a la Oficina de Informática y Comunicaciones.
- Los colaboradores de **CEDELCA S.A E.S.P.**, en su oficio de recepción de información por entidades externas, deben reportar las inconsistencias encontradas en la información recibida tanto a la entidad externa como en el formulario de mesa de ayuda.
- Toda la Información transferida y recibida mediante dispositivos de almacenamiento de entidades externas debe tener una copia de respaldo realizada por la Oficina de Informática y Comunicaciones y esta permanecerá en custodia.
- Cuando se transfiera información por correo electrónico, se debe guardar el correo electrónico como evidencia de recepción o envío de la información.
- Cuando se transfiera información utilizando almacenamiento en Cloud para ser compartida, previamente se debe realizar copias de respaldo de la información y brindar los roles de solo lectura a las entidades externas.
- No están permitidos los reenvíos de información a cuentas de correo no autorizadas impidiendo la fuga de información de la entidad.
- Se deben implementar procesos de inducción formativos a los colaboradores de **CEDELCA S.A E.S.P.** sobre el correcto uso de la Información y desde el momento de su ingreso a la entidad.
- Se deben establecer en los contratos con terceros las condiciones de manejo de información que provean confidencialidad, integridad y disponibilidad a la información confidencial y de uso interno que se entregue o se reciba.
- La información transmitida y recepcionada, debe ser registrada en el aplicativo de gestión documental y basada en las tablas de retención documental implementadas por **CEDELCA S.A E.S.P.**, descrita en la adopción de Tablas de Retención Documental.
- **CEDELCA S.A E.S.P.**, mantendrá disponible la información durante todo el proceso de transmisión.
- El sistema de mensajería electrónica de **CEDELCA S.A E.S.P.** oficialmente está soportado en el servicio de correo electrónico corporativo, el cual puede ser accedido por medio de Office 365. La Oficina de Informática y Comunicaciones es la encargada de asegurar el correcto funcionamiento de este servicio.
- Al ingresar el colaborador a **CEDELCA S.A E.S.P.**, se le asigna una dirección de correo electrónico con los accesos respectivos. El envío de mensajería electrónica empleando este medió es categorizado como firma electrónica, puesto que el empleado es

identificado. Además, es identificable el correo del remitente y del destinatario, teniendo validez como firma digital con los actos jurídicos según el Decreto 2364 del año 2012 y la Ley 527 del año 1999 en donde se da el reconocimiento jurídico a este tipo de mensajes de datos.

Control de acceso

- 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.
- Se asignarán a los usuarios los accesos definidos para su cargo y los adicionales que le sean solicitados por el líder de proceso para el desarrollo de sus funciones.
- Adicionalmente se evaluarán individualmente y se podrán dar accesos que contribuyan a mejorar el desempeño laboral o formación personal siempre y cuando no representen un riesgo para la seguridad de la información de la entidad.
- Los accesos que puedan representar un riesgo para la seguridad de la información serán brindados bajo los controles necesarios y autorizados siempre por la Gerencia de la empresa, quien compartirá con el colaborador la responsabilidad por las consecuencias que puedan ocasionarse a partir del uso de los accesos; esto aplica para accesos al personal interno de **CEDELCA S.A E.S.P** y para accesos a terceros que solicite el funcionario interventor.
- Para terceros el control de acceso estará regido por las condiciones y cláusulas contractuales y no se podrán extender más allá de la finalización del contrato bajo ninguna circunstancia.
- En caso de eventos y/o incidentes de seguridad de la información se podrán retirar los accesos al o los usuarios involucrados.
- Cada área a través de Directivos o Jefes son responsables de brindar los accesos a los datos e información gestionados bajo su custodia a los colaboradores bajo su cargo, de otros procesos o externos que por cuestiones contractuales se relacionen.

Política de acceso a redes y servicios de red

- Se permite a los usuarios y colaboradores el uso de los canales, servicios y recursos de red previamente autorizados para cumplir funciones requeridas por el cargo o para el proceso, realizar solicitudes de gestión en redes y elementos de conectividad para mejorar su desempeño laboral o formación personal siempre y cuando no representen un riesgo para seguridad de la información de la entidad.
- **CEDELCA S.A E.S.P.** conserva el derecho de almacenar archivos de registro (conocidos como logs) de las actividades de los usuarios al hacer uso de la infraestructura de red, los canales o servicios de internet y revisarlos formal o informalmente por la oficina de Informática y Comunicaciones.
- Está prohibido el uso de datos/información accesible a través de canales de internet para actividades no relacionadas con el cargo, el abuso de privilegios de usuario para acceder a datos o información sobre la que no se tiene autorización, el espionaje por

cualquier medio (electrónico, digital o físico) de las actividades de otros usuarios sin su respectiva autorización y la suplantación de usuarios al ingresar con credenciales ajenos a los asignados por **CEDELCA S.A E.S.P.**

- Las redes inalámbricas corporativas que permitan el acceso a la red LAN de la empresa deben ser administradas por la oficina de Informática y Comunicaciones. Será configurada a los funcionarios que la requieran.
- Las claves de acceso a las redes inalámbricas deben ser cambiadas cada 6 meses o antes si se sospecha que se han divulgado las claves.
- Los servicios y accesos de red referentes a conexiones de red corporativa se autorizan para que puedan consumir diferentes servicios centralizados del Data Center de **CEDELCA S.A E.S.P.**

Política de acceso a redes inalámbricas – WiFi Cedelca corporativa e invitados

- **CEDELCA S.A E.S.P** para la conexión de dispositivos móviles dispone de sus redes inalámbricas corporativas seguras. Las cuales se denomina de la siguiente manera:

  - **WiFi Cedelca Corporativa**

  Consiste en la red inalámbrica controlada, exclusivamente para los colaboradores de **CEDELCA S.A E.S.P.**, y se aplica únicamente en los casos que no se pueda brindar conexión a red cableada. Esta red cuenta con medidas de seguridad especiales para poder brindar acceso seguro a internet y a servicios y sistemas de información corporativos.

  - En la **WiFi Cedelca Corporativa** no se deben conectar dispositivos personales móviles tales como portátiles, celulares o Smartphone, Tablet y relacionados. En caso de que se requiera se debe realizar solicitud formal.
  - Las redes inalámbricas de tipo **WiFi Cedelca Corporativa** pueden ser utilizadas en dispositivos móviles de la Gerencia, Directivos o jefes, bajo revisión previa de seguridad y una correcta configuración por el personal de la Oficina de Informática y Comunicaciones.

  - **WiFi Cedelca Invitados**

  Consiste en la red inalámbrica controlada, para la conexión únicamente a internet de los usuarios y terceros relacionados con **CEDELCA S.A E.S.P.**

  - Las redes inalámbricas de la empresa deben ser controladas por la Oficina de Informática y Comunicaciones, quienes deben aplicar buenas prácticas de implementación y administración de redes inalámbricas seguras.
  - Las redes inalámbricas de **CEDELCA S.A E.S.P** deben contar con control de navegación con el fin de mitigar el riesgo de acceso a sitios no adecuados o peligros tales como sitios de distribución de software malicioso o malware, pornografía, juegos y apuestas, entre otros relacionados.
  - Las redes inalámbricas de tipo **WiFi Cedelca Invitados** pueden ser configuradas a los funcionarios que la requieran, bajo solicitud,

autorización y aprobación formal. La configuración adecuada debe ser realizada por personal de la Oficina de Informática y Comunicaciones.

- Las redes inalámbricas de tipo **WiFi Cedelca Invitados** no deben tener conexión a la red LAN.

Información de autenticación

La asignación de usuarios y contraseñas es un permiso que **CEDELCA S.A E.S.P.** otorga a sus funcionarios, contratistas o practicantes para permitirles el acceso a los recursos tecnológicos, incluyendo plataformas y sistemas de información que facilitan la operación, consulta y resguardo de la información institucional.

Los objetivos específicos de los lineamientos para el uso de usuarios y contraseñas son:

- Proporcionar a todos los funcionarios y contratistas de CEDELCA S.A E.S.P. responsables de la asignación, creación y modificación de usuarios y contraseñas, directrices claras a seguir y verificar su cumplimiento con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información de la institución.
- Concientizar a todos los funcionarios y contratistas sobre los riesgos asociados al uso de credenciales de acceso (usuario y contraseña) y las implicaciones de exponer indebidamente la identidad ante terceros, recordando que las credenciales asignadas a cada funcionario, contratista o practicante son personales e intransferibles.
- Garantizar el manejo adecuado de la información privada de la entidad.
- La asignación de credenciales de acceso: usuarios (Login o User ID) y contraseñas (Clave o Password) para los diferentes funcionarios y contratistas, así como su desactivación en los sistemas, se llevará a cabo de acuerdo con los procedimientos establecidos y según lo solicitado por los Subgerentes, jefes o la Unidad de Apoyo de Administración de Personal
- A través de cláusulas de confidencialidad contractuales el o los usuarios (Colaborador, empleado y/o tercero) deben mantener en privado la información secreta para la autenticación. Dentro de la información secreta se encuentran contraseñas, llaves criptográficas, respuestas de preguntas de recuperación de cuentas y otros relacionados.
- Después de suministrar a los colaboradores la información secreta para la autenticación (contraseñas) de usuario en los equipos de cómputo y otros sistemas, se les solicitará realizar el cambio de esta por una nueva.
- Las cuentas de usuario y sus contraseñas son de carácter individual y las primeras son transferibles sólo en situaciones formales de reemplazos o encargos; no está permitido el uso de cuentas de grupo, cuentas genéricas o cuentas compartidas sin autorización de la Oficina de Informática y Comunicaciones. El colaborador es responsable de custodiar todas las contraseñas que le sean asignadas con el objeto de desarrollar su labor como trabajador de **CEDELCA S.A E.S.P.**, En virtud de lo anterior las contraseñas son personales y no podrán darse a conocer o entregarse a terceros; el sólo hecho de

dar a conocer las contraseñas se tendrá como una falta a las obligaciones; ahora bien, si esto causa perjuicios al empleador la conducta se catalogará como una falta grave.

- Las acciones ejecutadas con las cuentas de usuarios son responsabilidad del propietario de la cuenta.
- Cada líder de proceso es responsable de asegurar que sus funcionarios cuenten con las opciones requeridas en los aplicativos para el desempeño de su labor y deben solicitar oportunamente los ajustes en los perfiles de usuarios para evitar el uso de claves y usuarios que no correspondan.
- Los sistemas estarán configurados para no permitir contraseñas en blanco.

Uso indebido del servicio de usuarios y contraseñas

- Permitir que terceros conozcan las contraseñas asignadas.
- Guardar las credenciales de acceso en libretas, agendas, notas adhesivas, hojas sueltas, u otros medios similares. Si es necesario respaldar las contraseñas en un medio físico, el documento generado deberá ser único y mantenerse bajo resguardo seguro.
- Almacenar las credenciales sin medidas de protección en dispositivos electrónicos personales (tabletas, memorias USB, teléfonos móviles, agendas electrónicas, etc.).
- Intentar acceder sin autorización utilizando un usuario y contraseña diferentes a los asignados personalmente en cualquier sistema de información o plataforma tecnológica.
- Utilizar identificadores de otras personas para acceder a información no autorizada o suplantar al usuario correspondiente.
- Emplear el usuario y contraseña asignados para fines comerciales ajenos a CEDELCA S.A. E.S.P.
- Intentar modificar los sistemas y parámetros de seguridad de la red de CEDELCA S.A. E.S.P.

Derechos de acceso

- Los accesos de usuarios serán suministrados por la Oficina de Informática y Comunicaciones a cada colaborador en particular.
- Una vez la Oficina de Informática y Comunicaciones le informe al funcionario sus datos de acceso, la responsabilidad por el uso y cambio de las contraseñas es del colaborador.
- Las cuentas con altos privilegios deben ser de uso exclusivo y específico. En lo posible las cuentas de usuario de dominio personal no deben tener altos privilegios, esto se revisará de acuerdo con los requerimientos de los aplicativos.
- Una vez al año se revisará que las cuentas de los colaboradores tengan los privilegios establecidos para su cargo, y que los privilegios adicionales que se encuentren hayan sido solicitados formalmente y autorizados.
- Los privilegios no autorizados o vencidos serán retirados hasta tanto se realice la solicitud de asignar nuevamente.

Seguridad de la información en las relaciones con los proveedores

- En los contratos con proveedores y/o aliados externos se deben implementar cláusulas de confidencialidad, no divulgación y privacidad para la protección de datos personales y protección de datos corporativos, derechos de uso de información, cláusulas de destrucción o devolución de la información de **CEDELCA S.A E.S.P.** que fue suministrada una vez se termine el contrato. Esto debe ser implementado por el proceso de Contratación apoyado con la Oficina Jurídica.
- Los procesos a través del personal que haga de interventores de contratos o alianzas deben poner a disposición la presente política de seguridad a las partes externas.
- Se debe contar con la identificación y documentación de los tipos de proveedores, por ejemplo, servicios de TI, logísticos, servicios financieros, componentes de la infraestructura de TI, a quienes la organización permitirá acceso a su información.
- Se debe tener un control de acceso y seguimiento de la información que es accedida por los proveedores.

Gestión de la seguridad de la información en los acuerdos con los proveedores

Los procesos deberán establecer y documentar las relaciones con proveedores que puedan tener acceso, procesar, comunicar, almacenar o suministrar componentes de infraestructura de TI para el sistema de información de **CEDELCA S.A E.S.P.** Adicionalmente se deben considerar los siguientes aspectos.

- Descripción de la información que se va a suministrar o a la que se va a permitir medios de accesos.
- Requisitos legales y de reglamentación, incluida la protección de datos personales, derechos de autor y de propiedad intelectual.
- Se deben acordar grupos de controles de acceso a la información.
- Entre otros que se consideren importantes.

Gestión de la seguridad de la información en la cadena de suministro de las TIC

- Las áreas dentro de acuerdos con proveedores (proveedores de productos o servicios de tecnologías de la información y comunicación) deben establecer requisitos para tratar los riesgos de seguridad de la información asociados.
- Se exigirá a los proveedores que entreguen o divulguen buenas prácticas de seguridad relacionadas a los productos o servicios suministrados.
- Se exigirán manuales de uso de los productos y servicios, con las consideraciones de seguridad para mantener la funcionalidad de los productos y servicios.
- En relación con los productos y servicios se establecerán reglas de comunicación con proveedores, con el fin de evitar inconvenientes, lograr la resolución de problemas oportunamente, lograr informar sobre los funcionamientos.

Monitoreo, revisión y gestión de cambios de los servicios de los proveedores

- Los servicios prestados por proveedores deberán ser monitoreados y revisados con el fin de que se cumplan los términos y condiciones de seguridad de la información, y que se resuelvan incidentes y problemas de forma oportuna y eficiente.

- En relación con el seguimiento y revisión se debe considerar niveles de desempeño, gestión de la capacidad del servicio por parte del proveedor, resolución de problemas identificados, entre otros aspectos relacionados.
- Se debe gestionar los cambios de servicios de los proveedores en base a seguimientos, revisiones de servicios y cumplimientos de los requerimientos exigidos, o también por los cambios de mejora informados por parte de proveedores. En este proceso se deben considerar.
    - Cambios en los acuerdos con los proveedores
    - Cambios realizados por la organización para implementar
    - Cambios en los servicios de los proveedores para implementar

Planificación y preparación de la gestión de incidentes de seguridad de la información

Mediante el formulario de mesa de ayuda se realiza el reporte de evento y/o incidentes, se gestiona principalmente por el punto de contacto - PoC indicando lo sucedido, después de ello la Oficina de Informática y Comunicaciones categoriza el tipo de reporte y direccionará a la persona especialista. Finalmente se entrega un reporte con las acciones o directrices tomadas.

Evaluación y decisión sobre eventos de seguridad de la información

- Los reportes se identificarán y evaluarán según la matriz de riesgos, Tabla de criterios para valoración del impacto organizacional, Matriz de calor del Riesgo, los cuales serán categorizados por el profesional universitario de la oficina de Informática y Comunicaciones, para su respectivo tratamiento.
- En la documentación de evaluaciones de eventos y resolución de estos se detallará el evento, así como las acciones tomadas frente a los mismos.

Respuesta a incidentes de seguridad de la información

- La Oficina de Informática y Comunicaciones determinará si la organización cuenta con la capacidad de resolver un incidente presentado por sí mismo, contando con los especialistas y grupos de apoyo dentro de la empresa o si el incidente debe ser tratado por un equipo externo.
- La Oficina de Informática y Comunicaciones debe hacer seguimiento de los eventos / incidentes presentados y llevar evidencias de cuando un incidente se da por finalizado, tipo de incidencia, las lecciones aprendidas y costos generados.
- Los eventos / incidentes deben ser registrados en los canales designados, los cuales generarán resultados para su seguimiento, lecciones aprendidas para determinar las causas del evento / incidente.

Aprendizaje de los incidentes de seguridad de la información

- Todos los eventos / incidentes deberán ser registrados en el formulario de mesa de ayuda que dispone la empresa para la gestión de reportes, con el fin de llevar un control sobre los mismos, registrando las resoluciones de estos como estrategia de

aprendizaje. Así mismo observar incidentes comunes y tomar acciones diferentes que resulten más afectivas.

- Con estas herramientas se logrará calificar y hacer seguimiento a los diferentes tipos de eventos / incidentes, verificando costos de recuperación, determinando el impacto que puede generar en la organización.
- La evaluación de los eventos / incidentes de seguridad de la información ayuda a que se implementen controles adicionales o mejoras para reducir daños y costos futuros.

Recogida de pruebas

La Oficina de Informática y Comunicaciones realizará la gestión para la recolección, adquisición y preservación de evidencias, de acuerdo con los diferentes tipos de medios, dispositivos, estado de los dispositivos. Se debe tener en cuenta:

- Cadena de custodia
- Sesiones informativas
- Seguridad del personal
- Roles y responsabilidades personal involucrado
- Seguridad de la evidencia
- Competencia del personal
- Documentaciones

Se tomarán acciones para los temas tratados frente a evidencias forenses, copias de datos, preservación de la información y salvaguardas de la integridad.

Identificación de los requisitos legales, reglamentarios y contractuales

La Oficina Jurídica es responsable de informar permanentemente a la Oficina de Informática y Comunicaciones y colaboradores de CEDELCA S.A E.S.P. y demás personal involucrado, sobre la legislación aplicable de seguridad de la información y protección de datos personales a través del normograma estipulado.

- La Oficina Jurídica brindará asesoría respectiva en la implementación de políticas y controles que ayuden al cumplimiento de las leyes y regulaciones.
- La Oficina de Informática y Comunicaciones deberá apoyarse con la Oficina Jurídica para las revisiones de la legislación aplicable sobre seguridad de la información y protección de datos personales.

Derechos de propiedad intelectual

- Todo material utilizado como propiedad intelectual por **CEDELCA S.A E.S.P.** debe ser adquirido cumpliendo con los requisitos legales. Si se requiere la instalación de Software adquirido por terceros, en los equipos de cómputo, se debe solicitar, a la Oficina de Informática y Comunicaciones, adjuntando certificación del tercero, donde se indique que el software ha sido adquirido legalmente y cumple con las obligaciones relativas a los derechos de propiedad intelectual.
- Todo colaborador de **CEDELCA S.A E.S.P.** y partes relacionadas, son responsables de asegurar que todo el material que utilicen con propósito laboral cumpla con la legislación de derechos de propiedad intelectual.
- Está prohibido que usuarios finales instalen Software en los equipos de cómputo de la empresa. Esta función es exclusiva de la Oficina de Informática y Comunicaciones,

quien debe tener un control de las licencias de los programas de software y velar porque no exista un software sin la debida licencia de uso.

- Únicamente la Oficina de Informática y Comunicaciones está autorizada para tomar una copia con propósito de respaldo de los medios originales de los programas de software licenciados.
- La instalación de programas de software en los computadores, por parte de colaboradores de **CEDELCA S.A E.S.P.** o terceras partes, sin la debida autorización la Oficina de Informática y Comunicaciones, es considerado un incidente de seguridad.
- Los colaboradores de **CEDELCA S.A E.S.P.** y terceras partes, no deben descargar o almacenar archivos de música, fotos, vídeos, o material sujeto a propiedad intelectual en los equipos de cómputo sin autorización del propietario.
- Los colaboradores de **CEDELCA S.A E.S.P.** y terceras partes, no deben, descargar, instalar, almacenar o utilizar herramientas de software o hardware como crackers de software, software de descubrimiento de contraseñas, detección de vulnerabilidades o utilidades de cifrado no autorizadas que puedan ser utilizadas para evaluar o comprometer los sistemas de seguridad de la información, sin la autorización de la Oficina de Informática y Comunicaciones.
- Se debe incluir en el programa de concientización de seguridad de la información el cumplimiento de las leyes de propiedad intelectual.

Protección de registros

- Los registros sobre requisitos legislativos, de reglamentación, contractuales y de negocio, deberán ser almacenados y custodiados de forma segura por parte de cada proceso.
- Los registros que se consideren importantes (y que de acuerdo con las directrices de cada líder de proceso), deberán ser almacenados en forma física y digital a través de los sistemas de información y herramientas que se hayan definido.

Privacidad y protección de la información personal

- En atención a la Ley 1581 de 2012 y sus decretos reglamentarios se establece la Política de Protección de Datos Personales y el aviso de privacidad, cuyo cumplimiento es obligatorio.
- Las áreas deberán realizar el respectivo cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios referente a las autorizaciones por parte de afiliados, empleados, proveedores y otros relacionados en el tratamiento de datos personales.

Responsabilidades de cada área

Cada área de la organización tiene un rol clave en garantizar la privacidad y protección de los datos personales. Estas responsabilidades incluyen, pero no se limitan a:

- La **Oficina de Informática y Comunicaciones** será responsable de implementar las medidas técnicas necesarias para proteger la información personal contra accesos no autorizados, pérdidas o alteraciones.

- El **Departamento de Recursos Humanos** supervisará que los datos personales de los empleados se gestionen conforme a la normativa vigente.
- El **Departamento Jurídico** asegurará que los contratos con terceros incluyan cláusulas específicas de protección de datos personales.
- La **Alta Gerencia** garantizará la supervisión y promoción de una cultura organizacional que priorice la protección de datos personales.

Procesos de Monitoreo

Se realizarán revisiones periódicas para verificar el cumplimiento de las políticas de privacidad y la protección de los datos personales, que incluirán:

- Auditorías semestrales sobre el acceso y uso de la información personal almacenada.
- Verificación semestral del cumplimiento de los controles asociados a la Ley 1581 de 2012.
- Validación anual de las medidas de seguridad implementadas, como cifrado y restricciones de acceso, mediante pruebas de vulnerabilidades.

Formatos y Registros

Para garantizar la trazabilidad y evidencia del cumplimiento de los requisitos legales, se usarán los siguientes formatos y registros:

- **Registro de Consentimientos Informados**: Para documentar la autorización explícita de los titulares de los datos.
- **Registro de Incidentes Relacionados con Datos Personales**: Para detallar cualquier incidente de seguridad que afecte la privacidad de la información.
- **Registro de Auditorías**: Para evidenciar los resultados de las auditorías relacionadas con el tratamiento de datos personales.

Estos puntos aseguran que CEDELCA cumpla con las disposiciones de la Ley 1581 de 2012 y el Control 5.37 de la norma ISO 27001:2022, protegiendo los derechos de los titulares y fortaleciendo la confianza de las partes interesadas.

Revisión independiente de la seguridad de la información

Las revisiones independientes pueden realizarse por actores relacionados con la seguridad de la información tales como empresas, consultores externos, grupos de investigación, investigadores independientes y comunidades. Lo anterior bajo el cumplimiento de la ley y las estipulaciones contractuales o de cooperación.
La Oficina de Informática y Comunicaciones deberá hacer la supervisión, interventoría y acompañamiento a las revisiones independientes de seguridad de la información.

Cumplimiento de políticas y normas de seguridad de la información

CEDELCA S.A E.S.P. velará por el cumplimiento de las políticas vigentes 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.

Procedimientos operativos documentados

CEDELCA S.A E.S.P. cuenta con 12 procedimientos documentados para el desarrollo de las funciones de la Oficina de Informática y Comunicaciones. Estos procedimientos aseguran la correcta implementación de los controles y garantizan evidencia de cumplimiento:

- **Requerimientos De Soporte De Software, Hardware Y Asesoría Para Usuarios:** Ser preventivo, predictivo y correctivo con el funcionamiento de los recursos de tecnología, informática y de comunicaciones con los que cuenta la empresa.
- **Administración De Cuentas De Usuario:** Atender las solicitudes de creación, modificación o retiro de cuentas de usuario para la disponibilidad y uso de los recursos tecnológicos como archivos, directorios, aplicaciones, entre otros.
- **Mantenimiento Preventivo De Los Equipos:** Garantizar que los equipos de cómputo con los que cuenta la empresa se encuentren en un nivel funcional, a fin de que todos los procesos puedan ejecutar la información que manejan.
- **Baja De Equipos:** Establecer los lineamientos y actividades para dar de baja los equipos que por su estado de obsolescencia y/o daño físico de hardware o software no cumplan con el objetivo de su adquisición y asignación, por lo que deben ser dados de baja.
- **Administración Del Sitio Web:** Garantizar que el sitio web oficial de la empresa contenga la información institucional necesaria y actualizada.
- **Administración De Las Cámaras De Seguridad:** Regular e identificar los procedimientos para el debido uso de los equipos y las grabaciones de vigilancia que se realizan en las instalaciones de CEDELCA S.A. E.S.P. y el archivo histórico, como medida de seguridad.
- **Administración De Redes Sociales:** Procedimiento mediante el cual se determine cada una de las acciones que se deben ejecutar para administrar la información en redes sociales de CEDELCA SA E.S.P.
- **Procedimiento de Administración de Máquinas Virtuales:** Proporciona directrices para la creación, modificación, administración y eliminación de VM, asegurando la trazabilidad y la autorización adecuada.
- **Procedimiento de Copia de Seguridad de la Información:** Detalla los pasos para realizar y verificar copias de seguridad según la criticidad de los datos y activos.
- **Procedimiento de Monitoreo de Infraestructura de Red y Servidores:** Describe cómo llevar a cabo el monitoreo manual de servidores y redes, identificando eventos que puedan comprometer la seguridad.
- **Procedimiento de Prueba de Restauración de Copias de Seguridad de un Servidor:** Define cómo realizar pruebas periódicas para validar la integridad y disponibilidad de las copias de seguridad.

- **Procedimiento de Restauración de Configuración de Dispositivos de Red:** Incluye pautas para la restauración segura de configuraciones en caso de fallos o incidentes.

B. Controles de personas

Selección de personal

- Se entra en cuenta lo establecido en el procedimiento PRGFA40 – SELECCIÓN Y VINCULACION DE PERSONAL.

Términos y condiciones de empleo

- Como parte de obligación contractual, empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de **CEDELCA S.A E.S.P.** para la seguridad de la información.
- Todo el personal que labore en la empresa o preste servicios a la misma deberá tener incluido en su contrato un acuerdo de confidencialidad, además, conocer y aceptar las políticas definidas y buen uso de los activos de información.

Concienciación, educación y formación en materia de seguridad de la información

- La Oficina de Informática y Comunicaciones realizará constantemente campañas de concientización por medios como correos electrónicos, publicaciones, mensajes, etc., también velará porque los nuevos colaboradores y contratistas reciban inducción en seguridad de la información al ingresar a la entidad.
- Se realizará capacitación a los colaboradores sobre seguridad de la información, amenazas informáticas, tipos de ataques, ingenierías sociales y relacionadas por medio de charlas informativas, cursos virtuales, conferencias y noticias sobre seguridad de la información y seguridad informática.

Proceso disciplinario

- Dentro de la documentación de los procesos disciplinarios se debe incluir un mecanismo de disuasión para prevenir que los empleados o colaboradores violen las políticas y controles de seguridad de la información.
- Todo incidente de seguridad en los activos de información y/o en el manejo de la misma en los que estén involucrados colaboradores, internos o externos, debe ser investigado por el área de Control Interno y Jurídica, en conjunto con la Oficina de Informática y Comunicaciones, para establecer responsabilidades y determinar las sanciones correspondientes.

Responsabilidades después de la terminación o cambio de empleo

- La Unidad de Apoyo de Administración de Personal es la encargada de realizar las gestiones necesarias para los traslados o finalización de las relaciones laborales. Así mismo estos deberán recordar las cláusulas de confidencialidad de la información posterior a la terminación laboral.
- La Unidad de Apoyo de Administración de Personal es responsable de generar las comunicaciones respectivas para informar a las otras áreas de los traslados o retiros de los empleados para que se proceda con las gestiones pertinentes para la seguridad de la información, tales como retiro de permisos, accesos y demás gestiones.

Acuerdos de confidencialidad o no divulgación

- Todo el personal que labore en la empresa o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.
- En los contratos para desarrollos se deben implementar acuerdos de licenciamiento, propiedad del código fuente y derechos de propiedad intelectual. Así mismo cláusulas de confidencialidad, no divulgación y privacidad para la protección de datos personales y protección de datos corporativos, derechos de uso, cláusulas de destrucción o devolución de la información, cláusulas de confidencialidad y los aspectos de seguridad de la información necesarios durante y después del contrato de **CEDELCA S.A E.S.P.** que fue suministrada una vez se termine el contrato. Esto debe ser implementado por el proceso de Contratación apoyado con el área Jurídica.
- Los correos electrónicos deben contener la sentencia de confidencialidad con el siguiente contenido: "AVISO LEGAL: La información contenida en este mensaje electrónico, tiene carácter privado y confidencial. Solo puede ser utilizado por el destinatario. Cualquier copia o distribución, su reenvío total, parcial o su uso sin contar con expresa autorización de su autor, está totalmente prohibida y sancionada por la ley. Si por algún motivo usted ha recibido el presente mensaje electrónico por error a su correo electrónico, por favor elimínelo y comuníquelo al remitente. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida esta comunicación, antes de que llegue a su destinatario, estará sujeto a las sanciones penales correspondientes, al igual que el que en provecho propio o ajeno o con perjuicio de otro, divulgue o emplee la información contenida en la misma. Todas las ideas y reflexiones expresadas en el presente mensaje electrónico corresponden al remitente del mismo y NO representa la posición oficial de **CEDELCA S.A E.S.P.**".

Trabajo a distancia

- El acceso a red VPN corporativa está limitada a aquellos usuarios a quienes se les haya autorizado la conexión formal de este servicio.
- **CEDELCA S.A E.S.P.**, cuenta con una red de telecomunicaciones definida, estructurada y segmentada. Para poder acceder a esta red mediante VPN, los usuarios deben cumplir con criterios de seguridad y de conexión contando con una red de datos

estable, adicional a esto las credenciales de accesos deben ser certificados por parte de la empresa.

Conexiones remotas

Las conexiones remotas aplican a todos los empleados y contratistas de CEDELCA S.A E.S.P. que necesiten y tengan autorización para acceder a terminales o servidores institucionales mediante herramientas VPN, ya sea para realizar sus actividades fuera de los horarios habituales o desde ubicaciones distintas a las oficinas de la empresa.

Los objetivos sobre el uso de conexiones remotas son:

- Asegurar la confidencialidad, privacidad y el uso responsable y adecuado de la información institucional.
- Fomentar la conciencia sobre los riesgos asociados al acceso y manejo de información a través de las plataformas institucionales de forma remota, y cómo mitigarlos siguiendo las directrices aquí establecidas.
- Establecer las recomendaciones y medidas necesarias para proteger tanto la información como los dispositivos utilizados en el acceso y la operación remota.
- Definir las pautas para organizar y resguardar de forma segura las credenciales de acceso y los elementos de protección requeridos para garantizar una conexión remota segura.

Reporte de eventos de seguridad de la información

- Los usuarios deben reportar los eventos, incidentes / vulnerabilidades de seguridad de la información a través del formulario de mesa de ayuda. El Profesional de la Oficina de Informática y Comunicaciones determinará la categoría respectiva e informará a quienes sea pertinente.
- En la identificación y reportes de eventos se deben considerar los siguientes aspectos:
    - Violaciones de acceso.
    - Violaciones de la integridad, confidencialidad y disponibilidad de la información.
    - No cumplimientos de políticas y directrices.
    - Errores humanos.
    - Violaciones de la seguridad física.
    - Otros relacionados a seguridad.
- Las investigaciones especiales adelantadas por los entes de control relacionadas con la seguridad de la información deben ser notificadas a la oficina de Informática y Comunicaciones para realizar la respectiva gestión.
- Los colaboradores de **CEDELCA S.A E.S.P.**, contratistas y usuarios que observen situaciones sospechosas o que claramente sean incidentes de seguridad de la información o cualquier anomalía en los sistemas o servicios tienen la obligación de reportar en el formulario de mesa de ayuda.

C. Controles físicos

Perímetro de seguridad física

- Los colaboradores podrán acceder a las instalaciones de CEDELCA S.A E.S.P. a través de tarjetas de proximidad o lectores biométricos los cuales están instalados en las entradas a las oficinas del edificio, previamente configurados por la Oficina de Informática y Comunicaciones.
- En las instalaciones del tercer piso se tendrá puerta con controles de acceso para proteger las áreas que contienen información y servicios de procesamiento de información.
- En caso de los accesos a visitantes el personal de recepción realiza el respectivo registro de ingreso y entrega una tarjeta de acceso que lo identifica como visitante autorizado para un área determinada de la empresa.
- Las tarjetas de acceso son de carácter personal e intransferible; la pérdida o hurto de las tarjetas de visitante deben ser notificadas inmediatamente a la Oficina de Informática y Comunicaciones.

Controles físicos de entrada

- El personal de recepción podrá permitir el ingreso a los visitantes que han sido previamente autorizados por un colaborador de la entidad.
- El ingreso de visitantes o terceros a la empresa solo se podrá realizar en horario hábil de lunes a viernes de 7:30am a 5:30pm. Los ingresos en horarios adicionales deben ser solicitados con antelación por escrito (correo electrónico u oficio) al jefe inmediato y autorizado por la gerencia.
- El ingreso de visitantes a las áreas donde se procesa información como el centro de datos Datacenter no está autorizado, en caso de requerir el acceso debe estar acompañado del personal autorizado; si se requieren realizar actividades de mantenimiento en el Datacenter por parte de proveedores debe hacerse bajo el acompañamiento y supervisión de personal interno de la empresa.
- Todo colaborador o contratista debe portar una identificación visible, en el caso de los visitantes, deben portar el carnet entregado por recepción que lo identifica como visitante.
- Los proveedores de servicios de internet como ISP u otros servicios relacionados con el centro de cómputo y que requieran acceso físico, están restringidos y solo se les autoriza el ingreso junto con el personal interno autorizado por la entidad

Seguridad de oficinas, salas e instalaciones

El ingreso de colaboradores está permitido en el horario hábil establecido para cada uno, en otros horarios se debe solicitar previamente con el visto bueno del gerente o jefe inmediato.

Protección contra amenazas físicas y ambientales

- Proveer las condiciones físicas y medioambientales necesarias como sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de

incendios, sistemas de descarga eléctrica, sistemas de vigilancia, para certificar la protección y correcta operación de la gestión de la información y de los recursos de la plataforma tecnológica de CEDELCA S.A E.S.P.

- Mantener en buen estado la infraestructura física de los centros de cableado, centros de datos de CEDELCA S.A E.S.P., y en general de las áreas seguras, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, sensores, entre otros.
- Asegurar que el Datacenter, se encuentre separado de las áreas en general, que tengan líquidos inflamables o que corran riesgo de inundaciones o incendios.

Trabajar en áreas seguras

- Se entienden como zonas restringidas o áreas seguras las siguientes:
  - Cuarto de equipos. (Data Center)
  - Oficina de Gerencia.
  - Oficina Subgerencia Financiera y Administrativa
  - Archivo físico Documental.
- Las zonas restringidas deben estar debidamente identificadas, contar con mecanismos de control de acceso, y monitoreo mediante CCTV (Circuito Cerrado de Televisión), solo los funcionarios del proceso correspondiente están autorizados a ingresar a estas zonas. Si un funcionario de otra área requiere ingresar, puede hacerlo bajo autorización y responsabilidad del líder de proceso.

Escritorio y pantalla despejados

La política de escritorios y pantallas despejadas es extensiva para todos los funcionarios, contratistas y practicantes de **CEDELCA S.A E.S.P.** y apoya en la seguridad de la información sensible o crítica de la empresa.

Este parámetro se define en el uso adecuado y ordenado de las áreas de trabajo desde el punto de vista físico como tecnológico entendiéndose para tal fin como escritorio el espacio físico o puesto de trabajo asignado a cada funcionario, contratista o practicante de la entidad y pantalla como el área de trabajo virtual sobre el sistema operativo de su computador, que contiene tanto sus carpetas electrónicas como los archivos y accesos a los diferentes aplicativos Institucionales.

El uso y conservación de los puestos de trabajo (escritorios) y de los fondos de escritorio de sus computadores (pantallas) es una responsabilidad de cada uno de los funcionarios, contratistas y practicantes que tengan acceso a la información de **CEDELCA S.A E.S.P.**, sea de manera temporal o indefinida, en el normal desarrollo de sus actividades. Para su definición y aplicación se define de la siguiente manera:

- Se deben dejar organizados los puestos y áreas de trabajo, para resguardar documentos con información clasificada o reservada evitando que queden a la vista o al alcance de la mano de personal ajeno a la misma.
- En la medida de lo posible los documentos con información clasificada o reservada deben quedar bajo llave o custodia en horas no laborables.

- Los papeles autoadhesivos que contengan información confidencial, especialmente contraseñas están prohibidas.
- Está prohibido escribir las contraseñas de los funcionarios en papeles, debajo del teclado, en cajoneras o sobre el escritorio.
- No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio virtual" al espacio digital en los equipos de cómputo).
- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.
- Al imprimir o fotocopiar documentos con información clasificada o reservada, esta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no debe ser dejada desatendida sobre los escritorios.
- No se debe reutilizar papel que contenga información clasificada o reservada.
- Los computadores o estaciones de trabajo deben ser bloqueados por los usuarios al retirarse de los mismos y estos deben ser desbloqueados por medio del usuario y contraseña asignados para su acceso. Es responsabilidad del usuario, asegurar que el equipo tenga la protección adecuada.
- Las áreas de trabajo virtuales "pantallas" del computador deben tener el mínimo de iconos visibles, limitándose estos a los accesos necesarios para la ejecución de la ofimática, accesos a sistemas de información y a carpetas y unidades de red necesarios para la ejecución de las actividades.

Ubicación y protección de los equipos

- Los equipos portátiles no deberán estar ubicados en áreas públicas, en los casos en los que se requiera deberán estar asegurados con guaya.
- Los equipos de cómputo deben estar libres de amenazas físicas como, electromagnetismo, humedad, robo, incendio entre otras.
- Los colaboradores de la empresa no deben consumir alimentos sobre los equipos de cómputo.
- Es obligatorio realizar el bloqueo de pantalla (Tecla Windows + L) de la estación de trabajo o computador por parte del colaborador cada vez que éste abandone su puesto de trabajo para evitar accesos no autorizados a su información.

Seguridad de los activos fuera de las instalaciones

Se debe prestar especial atención a los dispositivos, tales como: computadores portátiles, discos duros externos, tabletas, teléfonos inteligentes, memorias USB y en general todo dispositivo que contenga información de **CEDELCA S.A E.S.P.**, con los siguientes controles:

- No usar en redes públicas inalámbricas los dispositivos de **CEDELCA S.A E.S.P**. que contengan información confidencial.
- Evitar exponer el equipo a factores externos que comprometen su integridad, tales como, calor extremo, humedad, electromagnetismo, radiación, humo o polución.
- No se debe acceder a los servicios de TI de **CEDELCA S.A E.S.P.** como el Correo, VPN y demás servicios corporativos desde redes de datos en sitios que no sean de confianza, tales como WiFi público, cafés internet y relacionados.

- Los equipos e información no se deben dejar desatendidos o sin vigilancia en lugares públicos.

Seguridad del cableado

El cableado de energía eléctrica y de telecomunicaciones debe ir por ductos y canaletas que impidan daño accidental al mismo.

Mantenimiento de equipos

Asegurar la disponibilidad y óptimo funcionamiento de la infraestructura tecnológica de CEDELCA S.A E.S.P., manteniendo los equipos en condiciones ideales para prevenir posibles fallas o averías. Esto permite garantizar que las labores se realicen con altos estándares de calidad y seguridad.

DESARROLLO

El Profesional de la Oficina de Informática y Comunicaciones, elaborará un programa de mantenimiento preventivo que contemple los siguientes aspectos:

- Hoja de vida de los equipos: Cada equipo contará con un registro detallado que incluirá el programa de revisiones, las actividades de mantenimiento realizadas y las reparaciones efectuadas. Este registro identificará las partes críticas de los equipos y los elementos específicos a revisar.

- Frecuencia del mantenimiento: Los mantenimientos preventivos se realizarán de manera semestral (dos veces al año) para cada equipo. Sin embargo, si se lleva a cabo un mantenimiento correctivo que implique formateo o reinstalación del sistema operativo, este será considerado como parte del mantenimiento preventivo, ya que implica restaurar el equipo a un estado funcional óptimo.

- Resultados de las revisiones preventivas:

    - Si durante una revisión preventiva se detectan anomalías, estas deberán ser notificadas y, cuando sea posible, corregidas de inmediato o programadas para su solución posterior.
    - Las irregularidades encontradas se registrarán en un formulario diseñado para este propósito.
    - Adicionalmente, el personal puede reportar anomalías detectadas en sus equipos mediante un formulario específico establecido para este fin.

PROCEDIMIENTO

- Diagnóstico de Primer Nivel:

    - Realizado por los funcionarios encargados de la infraestructura tecnológica de CEDELCA S.A E.S.P..

- Consiste en verificar el tipo de error o problema presente, y, si es posible, ofrecer una solución directa.

- Diagnóstico de Segundo Nivel:
  - Efectuado por el proveedor externo contratado por la entidad para brindar soporte técnico o realizar el mantenimiento correctivo necesario.

CONDICIONES GENERALES

- Revisión inicial y final: Antes de realizar cualquier servicio de mantenimiento preventivo o soporte técnico, se debe examinar la configuración y estado funcional del PC, servidor u otros equipos tecnológicos mediante una lista de verificación. Después del servicio, se debe corroborar nuevamente su funcionamiento.
- Garantía y contratos vigentes: Los equipos que cuenten con garantía o contratos de soporte técnico/mantenimiento no deben ser abiertos ni intervenidos por personas no autorizadas por la empresa proveedora.
- Informe de irregularidades: Cualquier irregularidad detectada en los equipos, como cambios en las partes internas o externas que no coincidan con el inventario entregado por el almacén al funcionario, debe ser reportada al Coordinador del área correspondiente.
- Actualización del plan: Se debe garantizar que el plan de mantenimiento preventivo para la infraestructura tecnológica permanezca actualizado.

Seguridad en la eliminación o reutilización de equipos

La Oficina de Informática y Comunicaciones debe realizar el formateo al disco duro de todos los equipos que se reciban por devolución, ya sea para reasignar el equipo a otro colaborador, o para darlo de baja.

Uso de dispositivos de captura de imágenes y/o grabación de video

- Concientizar a los empleados, contratistas, practicantes y cualquier persona vinculada con la entidad sobre los riesgos asociados al uso de dispositivos para registro de imágenes y/o videos dentro de las instalaciones de la empresa.
- Reforzar las medidas de seguridad en las áreas que manejan documentación e información sensible o reservada de CEDELCA S.A. E.S.P.
- Garantizar el cumplimiento de las directrices establecidas en la Política de Seguridad de la Información de la institución.
- Restringir el uso de dispositivos de captura de imágenes y/o grabación de video en zonas donde se gestione información clasificada, confidencial o crítica.

Dispositivos de captura de imágenes y/o grabación de video: abarca dispositivos como, pero no limitados a:

- Videocámaras.
- Cámaras fotográficas.

- Teléfonos celulares y smartphones.
- Tablets y PDAs.
- Webcams.
- Escáneres.
- Impresoras y multifuncionales con capacidades de captura de imagen.

Directrices generales:

- La captura de imágenes y/o grabación de video por parte de ciudadanos o visitantes dentro de las instalaciones de CEDELCA S.A E.S.P. debe contar con una autorización expresa de la Subgerencia Administrativa y Financiera.
- Está prohibida la captura de imágenes y/o videos en las instalaciones, así como del personal, por parte de ciudadanos, empleados, contratistas y practicantes, salvo que exista una autorización previa por parte de la Secretaría General.
- El acceso y uso de equipos fotográficos y de video con fines institucionales, de prensa o comunicación, debe estar autorizado previamente por la Dirección Administrativa o la dependencia correspondiente.
- Únicamente las cámaras de seguridad designadas por CEDELCA S.A E.S.P. están permitidas en las áreas sensibles con el objetivo de proteger al personal, la documentación, la información y los activos alojados en dichas áreas.
- En el caso de equipos de cómputo institucionales que dispongan de webcams integradas y dispositivos de videoconferencia, su uso debe limitarse exclusivamente a actividades relacionadas con videoconferencias institucionales y desarrollarse únicamente en las áreas habilitadas.
- Se deben tomar medidas para garantizar que los dispositivos permitidos estén configurados de forma segura, minimizando riesgos de fuga de información.

Uso de dispositivos de almacenamiento externo

El uso de dispositivos de almacenamiento externo, distintos a los medios disponibles en los equipos de cómputo, unidades de red compartidas y servidores de CEDELCA S.A E.S.P., constituye una herramienta útil para la transferencia rápida y directa de información entre los empleados, contratistas y practicantes de la entidad. Sin embargo, su uso también puede exponer información confidencial y sensible de la organización a diversos riesgos y amenazas.

- Sensibilizar a los empleados, contratistas y practicantes de CEDELCA S.A E.S.P. sobre los riesgos asociados al uso de medios de almacenamiento externo, tanto para los sistemas de información como para la infraestructura tecnológica de la empresa.
- Asegurar el adecuado manejo de la información digital almacenada en la institución, garantizando su integridad y protección.
- Establecer restricciones sobre el uso de estos dispositivos en diferentes áreas de la entidad, asegurando el cumplimiento de las normativas internas de seguridad.

CEDELCA S.A E.S.P. reconoce que estos dispositivos son herramientas útiles para el almacenamiento y transporte de información, pero también representan un riesgo, ya que

pueden extraer datos sin dejar un rastro físico ni un registro visible de dicha acción. Por esta razón, CEDELCA S.A E.S.P. establece los siguientes compromisos para el uso de dispositivos de almacenamiento externo, asegurando que la información propiedad de la entidad no sea susceptible a fuga, uso no autorizado, modificación, divulgación o pérdida. Esta información debe ser protegida de acuerdo con su valor, confidencialidad y relevancia.

El uso de dispositivos de almacenamiento externo está permitido en CEDELCA S.A E.S.P. para los empleados, contratistas y practicantes, con el objetivo de facilitar la transferencia y almacenamiento de información que no sea clasificada ni reservada, siempre dentro de las normas y responsabilidades del manejo adecuado de la información institucional.

Dispositivos de almacenamiento externo permitidos: Los dispositivos de almacenamiento externo comprende unidades que se pueden conectar a los equipos de cómputo de CEDELCA S.A E.S.P., como memorias USB, mediante cables de datos o conexiones inalámbricas directas. Algunos ejemplos de estos dispositivos incluyen, pero no se limitan a:

- Memorias Flash USB
- Reproductores portátiles MP3/MP4
- Cámaras con conexión USB
- iPhones/Smartphones
- Tarjetas SD/Mini SD/Micro SD
- PDAs/ Tablets
- Dispositivos con tecnología Bluetooth
- Tarjetas Compact Flash
- Discos duros externos

Uso indebido de dispositivos de almacenamiento externo: Se considerará un uso indebido de los dispositivos de almacenamiento externo los siguientes casos:

- Almacenar o transportar información clasificada o reservada de CEDELCA S.A E.S.P. sin las autorizaciones pertinentes.
- Ejecutar programas no autorizados por la entidad desde cualquiera de los dispositivos de almacenamiento mencionados.
- Descargar archivos sin tomar medidas adecuadas para prevenir la introducción de virus en los equipos y redes de CEDELCA S.A E.S.P..
- Utilizar mecanismos para ocultar o suplantar la identidad del usuario de los dispositivos de almacenamiento.
- Usar dispositivos de almacenamiento externo para almacenar o exponer información sensible o confidencial de los usuarios, empleados, contratistas o practicantes de CEDELCA S.A E.S.P..

D. Controles tecnológicos

Derechos de acceso con privilegios

- Los accesos a aplicativos y privilegios superiores a los definidos para el cargo deben ser solicitados formalmente, autorizados y documentados mediante el formulario de mesa de ayuda.
- Las cuentas pertenecientes a usuarios que ya no laboren para **CEDELCA S.A E.S.P.** o de terceros que finalicen sus actividades, deben ser deshabilitadas de todos los sistemas.

Restricción de acceso a la información

Se deben seguir los lineamientos indicados en la presente política sobre control de acceso a activos de información y sistemas. La información se restringe a partir de los medios de almacenamiento, así como las barreras físicas, lógicas y por software a través de roles definidos que se generan en todos los elementos que componen el sistema de información global de **CEDELCA S.A E.S.P.**

Acceso al código fuente

La lectura de código fuente de programas desarrollados interna y externamente está prohibida, excepto para la Oficina de Informática y Comunicaciones.

Autenticación segura

- 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 cumplir con los siguientes requerimientos:

    - Poseer al menos ocho caracteres.
    - Tener incluido al menos una letra mayúscula.
    - Tener incluido al menos una letra minúscula.
    - Tener incluido al menos un número.
    - Tener incluido al menos un carácter especial.

Copia de seguridad de la información

Usuarios Finales

- Está prohibido realizar sin autorización copias de la información perteneciente a **CEDELCA S.A E.S.P.**, mediante dispositivos de grabación, o a través de cualquier medio de almacenamiento externo (CDs, DVDs, discos duros externos, memorias USB, etc.). Con el fin de controlar la fuga de información utilizando dispositivos de almacenamiento con puertos USB, se bloquearán los puertos USB y las unidades de CD/DVD de los computadores que posee o administra **CEDELCA S.A E.S.P.** Se exceptúan

los colaboradores de la Oficina de Informática y Comunicaciones que por sus funciones requieren tener la posibilidad de utilizar estos dispositivos.

- Cuando se realicen copias de seguridad diferentes a las que realiza la Oficina de Informática y Comunicaciones para salvaguardar la información, éstas deben ser solicitadas y autorizadas por el líder del proceso, se debe solicitar a través del formulario de mesa de ayuda para conceder los permisos necesarios.
- Cuando se realice copia de información a un computador de un colaborador de la empresa, este debe ser informado previa dicha actividad, la copia permanecerá en custodia de la Oficina de Informática y Comunicaciones.

Servidores y Dispositivos de Red

Cedelca S.A E.S.P. en su inventario de servidores cuenta con servidores de rack (físicos) y servidores virtualizados que están alojados en los servidores físicos, como también cuenta con dispositivos de red para manejar el tráfico de datos, dispositivos que se encuentran alojados en el centro de datos de su sede administrativa, los cuales deben poseer respaldos o copias de seguridad de la información.

- Los servidores físicos deben estar respaldados en una arquitectura de réplica, en donde la sincronización entre el servidor principal y la réplica se realice por lo menos una vez al día.
- Los servidores virtuales deben tener una copia instantánea (snapshop) diaria que debe ser almacenada en un sitio local y también en una nube externa, retenciones que deben cumplir los requerimientos indicados en la siguiente Tabla

Tipo de Almacenamiento	Tipo de Retención			
	Diaria	Semanal	Mensual	Anual
Nube Acronis	7 días	4 semanas	12 meses	5 años
Local NAS	2 días	2 semanas	1 mensual	1 año

- Los dispositivos de red dado que es importante la configuración de los mismos se hace necesario que se guarde la información correspondiente a su configuración y se almacene localmente, con una frecuencia de al menos una copia cada seis meses, con una retención de cuatro copias.

Las copias de seguridad de los servidores en la medida de lo posible deberían realizarse con una herramienta que pueda automatizar el proceso, para así de esa manera minimizar los errores que pudiesen generar la intervención de un operador; para garantizar que las copias se estén ejecutando el profesional II debe realizar un seguimiento periódico a la ejecución de las copias el cual debe quedar evidencia del mismo en el FTGFA 115-Formato de Copias de Seguridad de la Información.

Para garantizar la funcionalidad de las copias de seguridad de los servidores se debe realizar las pruebas de restauración, las cuales deben ser por lo menos una vez al año, para ello se debe hacer uso del PRGFA 56 Procedimiento de Prueba de Restauración de Copias de Seguridad de un Servidor; FTGFA 124-Formato de Pruebas de restauración de Copias de

Seguridad de un Servidor; FTGFA 115-Formato de Copias de Seguridad de la Información; restaurando anualmente servidores distintos. Para las pruebas de restauración se pueden tomar alguna de las copias realizadas, que estén almacenadas en el repositorio local o de la nube.

Para garantizar la funcionalidad de las copias de seguridad de las configuraciones de los dispositivos de red, también se deben realizar pruebas de restauración, las cuales deben ser al menos una vez al año, para ello se debe hacer uso del PRGFA 57 Procedimiento de Resta de configuración de Dispositivos de Red; FTGFA 125-Formato de Restauración de configuración de Dispositivos de Red; FTGFA 115-Formato de Copias de Seguridad de la Información; restaurando anualmente un dispositivo de red distinto.

Sincronización de relojes

- Los sistemas de información corporativos se sincronizan contra el servidor de dominio de aplicaciones principales.
- La sincronización de relojes de equipos de municipios o nodos con conexión banda ancha se sincronizará automáticamente y la zona horaria será UTC-05:00 Bogotá.

Uso de programas de utilidad privilegiados

- El acceso a programas utilitarios en sistema está limitado por el controlador de dominio de acuerdo con el tipo de usuario, donde se restringen la modificación de configuraciones del sistema, instalación de programas, entre otros relacionados.
- La Oficina de Informática y Comunicaciones instalará o habilitará los programas en los sistemas en relación con lo requerido para cada usuario.

Instalación de software en sistemas operativos

- La instalación de software en los computadores suministrados por **CEDELCA S.A E.S.P.** y de los equipos conectados a la red corporativa es una función exclusiva de la Oficina de Informática y Comunicaciones. Toda instalación debe tramitarse a través del formulario de mesa de ayuda, quien removerá sin previo aviso los archivos que claramente incumplan con las normas señaladas en esta política.
- Todo software o contenido multimedia utilizado en los equipos propiedad de la empresa, conectados a la red corporativa o que se utilicen en las instalaciones de **CEDELCA S.A E.S.P.** debe poseer las licencias de uso legal, de acuerdo con leyes de protección de propiedad intelectual y derechos de autor.
- Para requerimientos de software no autorizado, la solicitud debe ser realizada por el líder de proceso del colaborador a la Oficina de Informática y Comunicaciones, quien estudiará la viabilidad de la adquisición.
- En el caso de actualizaciones de software que afecten el correcto funcionamiento del sistema, se debe realizar un Rollback regresando a la versión anterior.
- Los medios de instalación de software y firmware de proveedores son directamente descargados de los sitios autorizados por el fabricante o por la Oficina de Informática y Comunicaciones.

Controles de red

- Las redes en CEDELCA S.A E.S.P. son administradas por la Oficina de Informática y Comunicaciones a cargo del Profesional Universitario II.
- Las actividades relacionadas con la administración de redes solo aplican a dispositivos activos de interconexión como Switches, Routers y firewalls propietarios. En el caso de dispositivos de interconexión no propietarios entregados por proveedores a la empresa, el Profesional Universitario II solicitará acceso con roles definidos para poder realizar esta administración, en caso de no poder hacer cambios a través de estos roles por carencia de privilegios, estos deben hacerse directamente por el proveedor del servicio.
- Los accesos y la seguridad en las redes inalámbricas están determinados por el protocolo WPA2 (Acceso Wi-Fi protegido 2) basado en el estándar 802.11 N/ac el cual utiliza el método de cifrado AES (Advanced Encryption Standard).

Seguridad de los servicios de red

- Los servicios publicados hacia Internet que requieran usuario y contraseña para acceder a información confidencial estarán protegidos mediante técnicas de cifrado SSL, TLS, AES o similares, y algunas tecnologías de red como VPN.
- La Oficina de Informática y Comunicaciones, es la encargada de gestionar las conexiones y capacidades de los canales en las redes de comunicación internos y externos, así como la administración y cambios en los dispositivos activos de interconexión de red.

Segregación en redes

- **CEDELCA S.A E.S.P.** contará con métodos de segmentación en sus redes LAN empleando técnicas como redes LAN virtuales (VLANs).
- La separación de redes está dada por los diversos componentes de red, y se controlan principalmente por Firewalls perimetrales.
- Las redes inalámbricas de invitado deben estar aisladas lógicamente del resto de la LAN con restricciones de navegación.

Uso de criptografía

- En el caso de correo electrónico se realiza a través del protocolo TLS (Seguridad en la capa de transporte), el cual proporciona la seguridad de cifrado en los correos para proteger su privacidad, adicional a esto el proveedor del servicio de correo electrónico brinda el servicio de almacenamiento Cloud. Este tipo de cifrado es aplicable a todos los archivos creados o cargados con una encriptación en tránsito y en reposo con el método de cifrado AES de 256 bits.
- Los accesos desde el exterior a la red local interna de **CEDELCA S.A E.S.P.** se realiza mediante VPN (Virtual private network) configurada en el Firewall de la empresa, estableciendo un túnel de comunicación cifrado mediante un agente de conexión

instalado en el equipo cliente y el servidor firewall de la entidad, esta administración es realizada por La Oficina de Informática y Comunicaciones.

Pruebas de seguridad en el desarrollo y la aceptación

- Las pruebas de seguridad de sistemas también pueden ser ejecutadas por proveedores externos competentes, bajo el acompañamiento de la interventoría de contratos y/o el proceso.

Desarrollo externalizado

Cuando se requieran desarrollos externos para **CEDELCA S.A E.S.P.** se deben cumplir con las siguientes directrices de seguridad.

- En los contratos para desarrollos se deben implementar acuerdos de licenciamiento, propiedad del código fuente y derechos de propiedad intelectual. Así mismo cláusulas de confidencialidad, no divulgación y privacidad para la protección de datos personales y protección de datos corporativos, derechos de uso, cláusulas de destrucción o devolución de la información de **CEDELCA S.A E.S.P.** que fue suministrada una vez se termine el contrato. Esto debe ser implementado por el proceso de Contratación apoyado con el área Jurídica.
- Para la contratación de desarrollos externos o servicios de TI que las áreas requieran es de obligatoriedad consultar a La Oficina de Informática y Comunicaciones para garantizar asegurar que los desarrollos o servicios de TI que van a ser contratados se incorporen o integren adecuadamente a la infraestructura tecnológica y sistemas de información de **CEDELCA S.A E.S.P.**, así como también a buenas prácticas de seguridad y tecnologías de la información que se vean necesarias.

Separación de los entornos de desarrollo, prueba y producción

- En los desarrollos de aplicaciones internas se tendrán separados los entornos de desarrollo, pruebas y producción para los aplicativos.
- Los ambientes de desarrollo, pruebas y producción funcionan independientes del tipo de tecnología Hardware, lo que las hace portables en cuanto a infraestructura.
- Los desarrollos de aplicaciones internas y externas son evaluados en un ambiente de pruebas, los cuales cuentan con las mismas tecnologías de producción.
- No se deben realizar pruebas o validación de códigos en los ambientes de producción de aplicaciones y bases de datos, todo desarrollo debe validarse en pruebas.

Cedelca S.A E.S.P para la separación de entornos de desarrollo pruebas y producción cuenta con una arquitectura virtualizada la que permite clonar los servidores productivos y generar máquinas que pueden ser dispuestas para los ambientes mencionados anteriormente, esto para no poner en riesgo los datos de producción, para ello se puede hacer uso del servidor físico productivo (Dell Power Edge R_540, IP 192.168.100.4)en donde se pueden disponer los servidores para realizar pruebas o en su defecto desarrollos, para disponer las copias de estos servidores se puede hacer uso de los procedimientos mencionados a continuación:

- FTGFA 117-Formato Administración de Máquinas Virtuales.

- PRGFA 56 Procedimiento de Prueba de Restauración de Copias de Seguridad de un Servidor.
- PRGFA 15 Procedimiento de Copia de Seguridad de la Información
- FTGFA 124-Formato de Prueba de Restauración de Copias de Seguridad de un Servidor.
- FTGFA 115-Formato de Copias de Seguridad de la Información.

En caso de requerir los servidores de desarrollo y pruebas de forma permanente estos deben quedar referenciados en el FTGFA 121-Formato de Inventario Servidores y Dispositivos de Red y quedará a disposición del profesional II si estos servidores deberán ser incluidos en plan de copias de seguridad y monitoreo de servidores, esto debido a que son servidores que no son productivos, por lo tanto, el riesgo de pérdida de información es bajo.

Gestión del cambio

- Los cambios que se lleven a cabo deben ser evaluados y probados de forma integral y se debe contar con una participación de los administradores de los diferentes componentes de la solución.
- En el proceso de gestión cambios se deben considerar los niveles de servicio y las necesidades de la empresa.
- En el proceso de gestión de cambios se debe incluir la identificación de los riesgos asociados al cambio y las acciones del tratamiento correspondiente.
- Establecer que las configuraciones de sistemas críticos, como las VM, estarán documentadas y respaldadas antes de cualquier cambio.
- Crear un formato específico para solicitudes de cambios en las configuraciones, incluyendo aprobaciones y evidencias de pruebas.
- Asegurar que los cambios sean revisados y aprobados por la Oficina de Informática y Comunicaciones y la Alta Dirección cuando sea necesario.

Formatos para Evidencias de Cumplimiento

Se incluirá una referencia obligatoria a los formatos de seguimiento, que servirán como evidencias documentales:

- **Formato de Administración de Máquinas Virtuales**: Detalla los registros de creación, modificaciones, y eliminaciones de VM.
- **Formato de Copias de Seguridad de la Información**: Asegura que cada copia de seguridad quede documentada, incluyendo la fecha, responsable y ubicación.
- **Formato de Eventos de Infraestructura de Red y Servidores**: Para reportar eventos y evidenciar las acciones correctivas.
- **Formato de Monitoreo de Infraestructura de Red y Servidores**: Para registrar la verificación manual de servidores y redes.
- **Formato de Restauración de Configuración de Dispositivos de Red**: Documenta cada cambio en las configuraciones, incluyendo las aprobaciones requeridas.

E. Gestión de recuperación de desastres

Objetivo:
Establecer los lineamientos para garantizar la recuperación eficiente de los sistemas tecnológicos críticos y la continuidad de las operaciones en caso de desastres o incidentes mayores que afecten la infraestructura tecnológica de CEDELCA S.A E.S.P.
Descripción:
CEDELCA S.A E.S.P. cuenta con un **Plan de Recuperación de Desastres** que detalla los procedimientos necesarios para restaurar la operatividad de los sistemas críticos en situaciones adversas. Este plan:

- Establece los pasos para la activación del plan en caso de emergencia.
- Describe las medidas preventivas y correctivas necesarias para minimizar el impacto de los desastres.

Directrices:

- El Plan de Recuperación de Desastres debe ser consultado y aplicado por los líderes de proceso en coordinación con el área de Tecnología de la Información y Comunicaciones.
- Es obligatorio que todo el personal involucrado en la gestión de incidentes esté capacitado en las acciones contenidas en el plan.
- La implementación del plan será evaluada periódicamente mediante simulacros y auditorías para garantizar su efectividad.

7. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

SENSIBILIZACIÓN Y COMUNICACIÓN

CEDELCA S.A E.S.P. A través de La oficina de Informática y Comunicaciones 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.

CAPACITACIONES EN SEGURIDAD

CEDELCA S.A E.S.P., a través de la unidad de apoyo a personal, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier colaborador y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de la información, La oficina de Informática y Comunicaciones apoyará en dichas inducciones, y como constancia de las capacitaciones se tendrá en cuenta los siguientes aspectos:

- Formato de asistencia y evaluación para las sesiones de capacitación.
- Periodicidad de campañas de concienciación y medios utilizados.
- Inducciones para nuevos empleados con revisión de procedimientos y formatos.

8. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Gerencia 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 **CEDELCA S.A E.S.P.**

9. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de **CEDELCA 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.

- **a.** Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.
- **b.** 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.
- **c.** La Oficina de Informatica y Comunicaciones será la encargado de recopilar y entregar a la Oficina de Control interno 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, la Oficina de Informática y Comunicaciones será la encargada de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.