RESOLUCION No. 22
(05 de Diciembre de 2019)

POR MEDIO DEL CUAL SE ADOPTA LA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION DE CENTRALES ELECTRICAS DEL CAUCA – CEDELCA S.A. ESP.

EL GERENTE SUPLENTE DE CENTRALES ELÉCTRICAS DEL CAUCA CEDELCA S.A E.S.P., en uso de sus facultades legales y estatutarias, en esencial las conferidas en la Ley 142 de 1994 y

CONSIDERANDO

Que el título V de la ley 594 de 2000 fue reglamentada mediante decreto 2609 de 2012, así como, parcialmente los artículos 58 y 59 de la ley 1437 del 2011 y se dictaron otras disposiciones en materia de gestión documental para todas las entidades del estado.

Que de conformidad con lo dispuesto en el artículo 6 de la Ley 962 de 2005, todas las entidades y organismos de la administración pública deberán poner en conocimiento de los ciudadanos los trámites y procedimientos de su competencia en la forma prevista en las disposiciones vigentes o emplear cualquier medio tecnológico o documento electrónico de que dispongan, para lo cual podrán implementar las condiciones y requisitos de seguridad que para cada caso sean procedentes.

Que la Ley 1437 de 2011 en el capítulo IV artículos 53 y siguientes reguló la utilización de medios electrónicos en el procedimiento administrativo, razón por la cual se requiere fortalecer la Seguridad Informática y la Continuidad del Negocio para dar cumplimiento a dicho precepto legal.

Que la Ley 1712 de 2014, creó la ley de transparencia y del derecho de acceso a la información pública Nacional aplicable a las entidades públicas de cualquier orden y regula el derecho de acceso a la información pública, procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicación de información.

Que el Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones,

en el Título 9, capitulo 1, estrategia de Gobierno Digital, en la sección 2, Instrumentos y responsables; establece como uno de los componentes de la estrategia, la Seguridad y privacidad de la información, que comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

Que los sistemas de Información constituyen el conjunto de tecnologías informáticas, procedimientos diseñados, mecanismos de control implementados y asignación de responsables de la captura, procesamiento, administración y distribución de datos e información.

Que Centrales Eléctricas Del Cauca S.A. E.S.P. en comité de gerencia del 09 de Octubre del 2019 creó el Comité de Tic's que dentro de sus funciones debe aprobar la política de seguridad de la información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos asignados a cada uno de los servidores de la Empresa.

En concordancia con lo anterior se hace necesario implementar y unificar las políticas de seguridad de la información y las políticas de gestión de la información.

Como consecuencia de lo anterior,

RESUELVE

ARTÍCULO PRIMERO. Adoptar la política de seguridad y gestión de la información de CENTRALES ELECTRICAS DEL CAUCA CEDELCA S.A E.S.P., las cuales hacen parte integral de la presente resolución, así como los lineamientos del manejo y uso de la información.

ARTÍCULO SEGUNDO. La política adoptada en la presente resolución aplica a todos los trabajadores, contratistas y pasantes de CEDELCA S.A E.S.P., y demás partes relacionadas que utilicen recursos e infraestructura de tecnologías de la información y las comunicaciones de la Empresa en cumplimiento de las disposiciones legales vigentes y basada en la norma ISO 27001 del 2013 con el ánimo de gestionar adecuadamente la seguridad de la información en los procesos, en los activos, en sistemas informáticos y lógicos, partes interesadas, la infraestructura de red de la Empresa, instalaciones físicas y del entorno.

ARTÍCULO TERCERO. Los Jefes de Oficina, deben asegurarse que los procedimientos de seguridad dentro de su área de responsabilidad sean realizados

correctamente en cumplimiento con la política de seguridad de que trata la presente resolución y velaran para que sean cumplidas por los trabajadores, contratistas y pasantes de su área.

ARTÍCULO CUARTO. El área de Informática y Tecnología será el Líder responsable de verificar el cumplimiento de las políticas de Seguridad de la información, así como de su evaluación y actualización con el apoyo del Comité de Tic's.

ARTÍCULO QUINTO: La presente resolución rige a partir de la fecha de su expedición.

Dada en Popayán el día Cinco (05) del mes de Diciembre de dos mil diecinueve (2019).

YANAMILETH TOVAR DIAZ
Gerente Suplente
CEDELCA S.A. ESP

Proyectó: Pablo Pardo / Profesional I - Informática y Tecnología
Revisó: Leonardo Cobo / Profesional II – Informática y Tecnología.

POLITICAS DE SEGURIDAD

DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se agrupan las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en CEDELCA S.A E.S.P.

POLÍTICA 1: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta política garantizará que existen responsabilidades claramente asignadas en todos los niveles organizacionales para la gestión de seguridad de los activos de la información; se contará con un comité de seguridad de la información conformado por personal idóneo (Comité de TICS), que apoyará como asesor interno de seguridad, con el objetivo de direccionar y hacer cumplir los lineamientos de la empresa, en la materia y revisar las posibles incidencias y acciones que se deben tomar.

Todos los trabajadores, contratistas, pasantes y externos con acceso a los activos de información de la empresa, tendrán el compromiso con la seguridad de cumplir las políticas y normas que la empresa dicte, así como reportar los incidentes que se pueda detectar.

- Los trabajadores, contratistas, y pasantes de CEDELCA S.A E.S.P. son responsables de la información que manejan y deberán cumplir con los lineamientos generales y especiales dados por la empresa y por la ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

• Todo trabajador, contratista y/o pasante que labore en la empresa y detecte el mal uso de la información (copia indebida, transferencia a terceros sin autorización, daño, información oculta, adulteración o incumplimiento de la política), está en la obligación de reportar el hecho al área de informática y tecnología y/o Control Disciplinario Interno.

POLÍTICA 2: GESTIÓN DE ACTIVOS

Identificación y clasificación de activos:

• La empresa realizará la identificación, clasificación y actualización de los activos de información, de acuerdo a las directrices establecidas en el decreto 103 de 2015-Vigente "Por el cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones", Artículos 37 y 38, este se actualizará de acuerdo a los lineamientos establecidos en el programa de Gestión Documental.

• Toda la información de la empresa, así como los activos donde se procesa y se almacena deberá ser inventariada y asignada a un área responsable; se realizará y se publicará el inventario de activos de información, el índice de información clasificada y reservada y el esquema de publicación de acuerdo a las directrices de la Ley 1712 de 2014 del Ministerio de tecnologías y comunicaciones MINTIC-Vigente "por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones" y decreto 103 de 2015.

• El inventario de activos de información, el índice de información clasificada y reservada y el esquema de publicación debe ser actualizada cuando se presenten cambios en la información o normatividad que pueda afectarla.

• Todo trabajador, contratista o pasante que utilice los sistemas de información, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Devolución de los Activos:

Es deber de todo trabajador, contratista y/o pasante que labore en la empresa, al dejar de prestar sus servicios, entregar toda información del producto del trabajo realizado y hacer entrega de los equipos y recursos tecnológicos en perfecto estado, conforme al procedimiento PRGR 03 VERSION 2 para los trabajadores, los contratistas y pasantes de acuerdo a

las condiciones establecidas en el contrato o convenio. Una vez retirado, debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante la gestión en la empresa, directamente o a través de terceros.

Gestión de Medios Removibles:

• La empresa se reserva el derecho de restringir el uso de medios removibles; mientras esté permitido es responsabilidad de los trabajadores de contrato laboral, contratistas, pasante y/o terceros que el medio removible conectado esté libre de virus y/o código malicioso, que pueda poner en riesgo la Integridad, confidencialidad y disponibilidad de la información y de los recursos tecnológicos de la empresa.

Disposición de los Activos:

• Ningún funcionario de la empresa está autorizado para realizar labores de mantenimiento y/o reparación de los equipos de cómputo, redes, cámaras, GPS y demás dispositivos electrónicos, para tal fin se debe comunicar con la dependencia responsable.

• Los funcionarios deben velar por el buen uso de los recursos tecnológicos asignados, pues son los directamente responsables de cualquier daño. En caso de presentar falla física o lógica se deberá notificar al área de informática y tecnología por medio de sinergy o al personal responsable de dar servicio a los mismos para que los revisen, corrijan la falla o de ser necesario ordenen la reparación de los mismos.

• Cualquier cambio que se requiera realizar en los equipos de cómputo de la empresa (cambios de procesador, adición de memoria, discos duros o tarjetas) debe tener previamente una evaluación técnica y autorización del área informática y tecnología.

• La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

• Los computadores corporativos son asignados a los trabajadores de contrato laboral, contratista o pasante, con el propósito de mejorar su ambiente de trabajo, mecanizar funciones y procesar información oficial, por lo cual se prohíbe el uso de los mismos para fines personales.

• Los usuarios sólo podrán utilizar los programas con que cuenta el computador que se le asignó, toda modificación del sistema será realizada bajo supervisión del área de informática y tecnología.

• Todo recurso tecnológico cuando cumpla su vida útil ya sea por obsolescencia o daño debe ser reintegrado Al área informática y tecnología, la cual hará el procedimiento correspondiente para la devolución o reintegro al Almacén.

• Se debe cerrar las sesiones abiertas de los diferentes Sistemas de Información, Correo Electrónico y demás aplicaciones al finalizar la jornada de trabajo y apagar el computador, estación de trabajo, portátil, etc., a excepción de los servidores y equipos del área de servidores, los cuales deben permanecer activos las 24 horas.

POLÍTICA 3: CONTROL DE ACCESO

• En el caso de personas ajenas a la empresa deban ingresar a algún activo informático, la Secretaría General, Gerencia y Jefes de Oficina deben autorizar sólo el acceso indispensable de acuerdo con el trabajo a realizar por estas personas, previa justificación y autorización.

• En todos los contratos deberá hacerse taxativa la cláusula de confidencialidad, responsabilidad, integridad, buen uso, etc., sobre la información institucional que el funcionario en desarrollo de su trabajo deba utilizar.

• El otorgamiento de acceso a la información está regulado mediante el procedimiento de administración de cuentas de usuario.

• Todos los accesos y permisos para el uso de los sistemas de información de la empresa deben terminar inmediatamente después de que el trabajador, contratista o pasante cesa de prestar sus servicios a la empresa.

• Los proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

• Todo usuario de los sistemas de información deberá tener asignado una cuenta y una contraseña para su utilización, de acuerdo a los estándares que maneja el área de informática y tecnología, previa solicitud de la Oficina de unidad de personal para funcionarios y del Supervisor, Director o Jefe para contratistas. El uso de la misma es responsabilidad de la persona o la que está asignada, es de carácter personal e intransferible.

• La cuenta de usuario administrador dispone a todos los privilegios y características que le permiten administrar completamente el equipo, por tal motivo dicha cuenta debe manejarse únicamente por el personal del área informática y tecnología.

• Se debe reportar oportunamente a través del Sinergy, los eventos relacionados con traslados vacaciones, ingresos, retiros de funcionarios de la entidad que ameriten activar y/o desactivar códigos de usuario, crear y/o modificar perfiles y roles de otros existentes, activar y/o desactivar servicios, etc.

POLÍTICA 4: SEGURIDAD DE LOS SERVICIOS INFORMÁTICOS

Uso del Correo Electrónico:

• Los buzones de Correo electrónico asignados a los trabajadores, contratista, pasantes o dependencias, deben ser usados solamente para el envío o recepción de documentos relacionados con las actividades propias del cumplimiento de las funciones institucionales.

• El usuario titular de la cuenta de correo es el único y directo responsable de todas las acciones y mensajes que se envíen a través de dicha cuenta.

• Los usuarios del servicio de Correo Electrónico de la empresa no pueden enviar, distribuir, difundir y participar en la propagación de "cadenas" de mensajes o propaganda comercial.

• El Correo Electrónico no se debe utilizar para enviar o distribuir ningún mensaje que pueda ser considerado difamatorio, acosador, o explícitamente sexual, o que pueda ofender a alguien con base en su raza, religión, género, nacionalidad, orientación sexual, política o discapacidad.

• Los mensajes masivos solamente podrán ser enviados siempre y cuando se trate de temas de carácter oficial y de interés general evitando en lo posible enviar archivos anexos de gran tamaño y solamente por personas autorizadas para tal fin. Esto debe hacerse con la autorización del Jefe de Oficina.

• La empresa se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico Institucional para cualquier propósito. Para este efecto el funcionario, contratista o pasante autorizará a la empresa para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

• Todo uso indebido del correo electrónico, acarrea suspensión temporal de la cuenta de acuerdo al nivel de la falta cometida.

Uso y manejo de Internet:

• Los funcionarios de la empresa no deben descargar archivos que puedan ser nocivos para los sistemas como virus, software espía, programas maliciosos capaces de alojarse en computadores permitiendo el acceso a usuarios externos y atacantes que pongan en riesgo la seguridad de la información, así mismo no deben acceder a sitios desconocidos o de baja confianza, ni aceptar los mensajes sobre instalación de software que ofrezcan las diferentes páginas sin la debida autorización del área informática y tecnología.

• Para evitar la congestión en los canales de comunicación, la empresa se reserva el derecho de restringir el acceso a ciertas páginas (no oficiales, categorías maliciosas y otras), aplicar limitación de ancho de banda a páginas web, como redes sociales y almacenamiento en la nube no oficial. Si por requerimiento del trabajo se requiere utilizar algunas de las páginas restringidas se debe solicitar la autorización a el área informática y tecnología, por medio de comunicado oficial.

• Se prohíbe el uso de software que omita las políticas de seguridad de la información, como proxy, Tunel, VPN no autorizada, entre otros.

Uso Red Inalámbrica:

• La Red Inalámbrica de la empresa permitirá el acceso solo al personal autorizado, ya sean trabajadores, contratistas, pasantes o usuarios invitados.

• La gerencia y el área de informática y tecnología se reserva el derecho de negar el acceso a la Red Inalámbrica en caso que se requiera.

Escritorios Limpios:

• Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel.

• Todo trabajador, contratista, pasante y/o colaborador de la empresa que se retire de su escritorio por un tiempo prolongado, deberá garantizar el bloqueo de la pantalla del computador, PC, estación de trabajo, servidor u otro equipo con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

POLÍTICA 5: SEGURIDAD DE COMUNICACIONES Y OPERACIONES

• Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la empresa, deberán ser consideradas y tratadas como información confidencial. Su diseño, administración, operación y mantenimiento está a cargo del Proceso de informática y tecnología.

• Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la empresa, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

• Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar autorizado por el área de informática y tecnología.

• Los equipos, Servidores, Equipos de Comunicaciones no deben moverse o reubicarse sin la aprobación previa del área de informática y tecnología.

• Para seguridad de los equipos tecnológicos, debe tenerse en cuenta que la conexión eléctrica debe realizarse a las tomas de corriente regulada (identificadas con color naranja).

• Los trabajadores, contratistas y pasantes se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que genere caídas de la energía.

• Los particulares en general, entre ellos, los familiares de todos los funcionarios, no están autorizados para utilizar los recursos informáticos de la empresa.

• Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad vigentes en la empresa. CEDELCA S.A E.S.P. se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos.

• El área de informática y tecnología se reserva el derecho de monitorear el tráfico de la red con el fin de garantizar el uso productivo del espacio (ancho de banda), detectar y prevenir fallas, estudiar tendencias de tráfico y detectar y prevenir el acceso no autorizado a los diferentes sistemas de información.

Adquisición de Recursos Tecnológicos:

• Toda adquisición de recursos tecnológicos debe estar avalado por el Comité de TIC´S siguiendo los lineamientos del manual de contratación de la empresa, quienes deberán participar en todo el proceso para garantizar las características tecnológicas mínimas, su compatibilidad, confiabilidad y adaptabilidad de los mismos con la infraestructura tecnológica de la empresa.

Acceso al centro de cómputo:

• Para el ingreso al cuarto de servidores del personal encargado de actividades como: mantenimiento del aire acondicionado, instalación y mantenimiento de servidores, instalación y mantenimiento de software, los visitantes y el personal de limpieza deberán estar identificados plenamente en sus actividades, y deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal responsable.

• Todo cambio relacionado con modificación de acceso, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

• Las áreas de cableados que la empresa considere críticas como por ejemplo el cuarto de servidores, deben ser lugares de acceso restringido.

POLÍTICA 6: SOFTWARE

• Está prohibida la descarga y uso de software no autorizado.

• Los usuarios no pueden descargar y/o emplear archivos de imagen, sonido o similares que estén o puedan estar protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

• Se realizará seguimiento o revisión para ejercer control sobre el uso de Software legalmente adquirido y licenciado por la empresa.

• Está prohibida la reproducción de cualquier software perteneciente a la empresa, bien sea que se haya adquirido o desarrollado internamente, para beneficio personal de cualquiera de sus usuarios o de terceras partes.

• La entrega de software desarrollado(en caso tal de que sea desarrollado en la empresa) a otras entidades debe estar autorizado por la Gerencia de la empresa.

• Antes de que un nuevo sistema se desarrolle o se adquiera, el comité de TIC´S, deberán definir las especificaciones y requerimientos de seguridad necesarios.

POLÍTICA 7: ALMACENAMIENTO Y RESPALDO

• La información que es soportada por la infraestructura de tecnología de CEDELCA S.A E.S.P. deberá ser almacenada y respaldada de acuerdo a lo establecido en el procedimiento "PGRIT-03 generación de Backups", de tal forma que se garantice su disponibilidad.

• Los trabajadores, contratistas y pasantes son responsables de los respaldos de la información almacenada localmente en el computador asignado.

POLÍTICA 8: DOCUMENTOS ELECTRÓNICOS

• El sistema generador de documentos electrónicos de la empresa es el Sistema de Información Documental de CEDELCA S.A E.S.P. – SINERGY.

• Para garantizar la integridad y autenticidad de los documentos cargados en el sistema de gestión documental SINERGY, se utilizará el estampado electrónico y la firma digital.

• Los documentos generados o cargados al Sistema de Gestión Documental SINERGY, deben incorporar condiciones de seguridad mediante la utilización del formato PDF con seguridad.

• Los documentos generados electrónicamente deben tener un número consecutivo de radicado generado automáticamente por el Sistema de Gestión de Documentos SINERGY.

• Las firmas digitales de CEDELCA S.A E.S.P. y asignadas a los Directivos, Jefes y/o autorizados, son personales e intransferibles y sólo se pueden utilizar para firma de documentos pertinentes a la empresa.

• Una vez terminado el vínculo laboral de los directores, Jefe y/o autorizados la firma digital será cancelada.

• Todas las comunicaciones externas que se envíen por correo electrónico, deberá ser enviadas a través de correo electrónico certificado institucional a través de SINERGY.

• La información generada en SINERGY debe ser almacenada y respaldada, de acuerdo con el procedimiento "PGRIT-03 generación de Backups" establecido por el área de informática y tecnología.

• El sistema debe contar con metadatos que garanticen las búsquedas, roles, controles, recuperación, acceso y administración de la información y documentación electrónica generada.

• Establecer estrategias de preservación digital para garantizar que la información almacenada pueda permanecer en el futuro, pese a los cambios tecnológicos u otras causas que puedan alterar la información que contiene, manteniendo su confidencialidad, integridad y disponibilidad.

• El tiempo de retención y disposición final de las series documentales generadas en el sistema estarán definidos en las Tablas de Retención Documental de la empresa.

• Los lineamientos y directrices para la conformación de expedientes híbridos y digitalización de documentos se establecerán en el Manual de Gestión Documental de la empresa.

• Los Manuales, instructivos, procesos y procedimientos se verificarán y ajustarán de manera periódica, con el fin de garantizar la preservación digital de los documentos.

POLÍTICA 9: REGISTRO Y AUDITORIA

• Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la empresa, como son sistemas de información en ambiente productivo, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar registros de auditoría.

• Todos los archivos de auditorías deben proporcionar suficiente información para apoyar el monitoreo, control y seguimiento que se requiera y preservarse por períodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

POLÍTICA 10: DISPONIBILIDAD DEL SERVICIO DE LA INFORMACIÓN (PLAN DE CONTINUIDAD)

El Proceso de Informática y Tecnología definirá, preparará, mantendrá actualizado y probado de forma periódica el Plan de Contingencia, de tal manera que permita a las aplicaciones críticas y sistemas de información, sistemas de cómputo y comunicación, garantizar la continuidad del negocio en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación, fallas eléctricas u otros riesgos que se puedan cristalizar.

POLÍTICA 11: CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

• Es responsabilidad del Comité de TIC´S evaluar, actualizar, verificar y socializar las políticas de seguridad de la información, conforme a esto, el presente documento tendrá una revisión anual, o antes en caso de ser necesario.

• Estas políticas deben ser socializada de acuerdo a las actualizaciones que puedan llevarse a cabo, y publicarla en la intranet y pagina web de la empresa para conocimiento de todo el personal objetivo e incluirla en el proceso de inducción de nuevos funcionarios, contratistas y pasantes.

• El líder del Proceso de Gestión Tecnologías de la Información a través de los funcionarios responsables de administrar la infraestructura de las Tecnologías de la Información y las Comunicaciones será el responsable de efectuar el seguimiento al cumplimiento de las Políticas de Seguridad de la Información con el fin de verificar y controlar que se esté aplicando adecuadamente. Los casos de incumplimiento serán reportados a la Gerencia, para ser aplicadas las sanciones a que haya lugar.

CEDELCA
Centrales Eléctricas del Cauca S.A E.S.P

POLITICAS DE COMUNICACIONES INTERNAS Y EXTERNAS

PRESENTACIÓN

La imagen de CEDELCA S.A E.S.P. es la proyección de nuestra misión, visión y objetivos institucionales, que son percibidos por los públicos internos y externos, como resultado de la gestión de la comunicación, el diseño de estrategias, acciones y mensajes emitidos a través de los canales de comunicación.

Por ello, en la empresa se propende por una comunicación transparente, oportuna y eficaz, que nos permita relacionarnos con nuestros públicos y emitir mensajes e información útil y de interés de manera permanente y/o cuando se requiera.

Es así como la comunicación hace parte de nuestro quehacer diario y por ello trabajamos en el adecuado manejo de mensajes y canales. Para ello, La comunicación en CEDELCA S.A E.S.P. se considera transversal a todas las actividades institucionales y es facilitadora de procesos de toma de decisión y de proyectos estratégicos y contribuye al clima laboral y sentido de pertenencia.

LAS COMUNICACIONES EN CEDELCA S.A E.S.P.

La gestión de comunicaciones en CEDELCA S.A E.S.P. vela por la imagen de la Institución y su posicionamiento entre los públicos internos y externos (stakeholders).

Esta labor se realiza mediante el diseño de estrategias, la creación de mensajes y dispositi-vos de comunicación coherentes con la misión y los objetivos institucionales. La presencia institucional se promueve a través del buen nombre de la identidad corporativa, la conducción de relaciones con las entidades estratégicas, la realización de medios y procesos de comunicación eficaces que proyecten el que hacer de la empresa.

Por otro lado, considerando la naturaleza misional de CEDELCA S.A E.S.P., la entidad debe contar con una Política de Comunicaciones que permita anticipar y reaccionar de manera asertiva ante cualquier evento.

POLÍTICAS DE COMUNICACIÓN

De los públicos de interés:

Públicos: Audiencias o grupos de personas con quien debemos comunicarnos o relacionar-nos. Basados en los objetivos de comunicación que tenemos con cada uno de éstos y en sus particularidades, es que direccionamos los mensajes y las estrategias de comunicación.

La Empresa mantendrá informados a sus públicos de interés sobre políticas, objetivos, resultados, decisiones, programas y proyectos misionales mediante mensajes y dispositivos de comunicación coherentes con la misión institucional.

Se consideran públicos internos: funcionarios, contratistas, directivas y consejo directivo.

Son públicos externos los inversionistas, gobierno, medios de comunicación, sector empresarial y en general, la comunidad. Son considerados públicos intermedios proveedores, familiares de públicos internos y potenciales inversionistas nacionales y extranjeros.

El objetivo de la comunicación con cada uno de nuestros públicos es:

Contratistas y Proveedores:	Alianzas, mejoras en los servicios
Comunidades:	Vínculo emocional: ciudadano y Empresa
Gobierno e Instituciones:	Mejora en relaciones y colaboración
Prensa:	Mejora en relaciones y colaboración
Trabajadores CEDELCA S.A E.S.P.:	Transmitir compromiso, orgullo y pertenencia.

De los voceros de la Empresa:

El principal vocero de la empresa es el gerente de la Empresa, seguido por la secretaria general. El Gerente, a través de la unidad de apoyo al personal y secretaria general, determinará los voceros ante los medios de comunicación, de acuerdo con los temas y pertinencia de los pronunciamientos.

De la identidad Institucional:

La unidad de apoyo al personal vela por el cumplimiento y buen uso de la identidad institucional en cada una de las piezas de promoción, publicidad y medios con impacto en los públicos objetivo de la empresa.

Es política de la Empresa propender por la imagen institucional y protocolo en los eventos realizados por la misma, de cualquiera de sus áreas misionales y administrativas.

De los canales de comunicación internos y externos:

La Empresa mantendrá mecanismos de comunicación de carácter institucional que permitan el flujo e intercambio de mensajes en las áreas misionales y administrativas, mientras se promueve el conocimiento, el clima organizacional y el sentido de pertenencia.

Es política de la Empresa administrar y conservar relaciones con los medios de comunicación a largo plazo, por lo que se establecerán planes y estrategias de comunicación que consolidan el posicionamiento de la Empresa, mientras se fortalecen las relaciones con los medios de comunicación locales, regionales, nacionales e internacionales.

La Gerencia es la única dependencia que cuenta con la facultad de emitir comunicaciones institucionales a los medios de comunicación y periodistas. Ya que es quien entiende las implicaciones legales y públicas en el momento de suministrar información o hacer declaraciones a audiencias externas.

La creación de medios y formas de comunicación con el público externo deberá ser aprobada por la Gerencia (avisos de prensa – publicaciones y especiales).

La comunicación en la Empresa se constituye como uno de los pilares estratégicos de la misma con sus servidores, por esto, su rol principal es el de posicionar la imagen a través de iniciativas, medios y canales de comunicación atractivos e innovadores que permitan la transmisión efectiva de los mensajes.

La creación de medios y formas de comunicación con el público interno deberá ser aprobada por la Gerencia.

Los canales de comunicación son herramientas usadas por la empresa con el fin de transmitir comunicaciones e información a todos los públicos de interés y buscar espacios de interacción y comunicación con ellos. Cuando la Empresa se comunica con ellos, es muy cuidadosa con la información que suministra, los canales usados y el vocero que suministra esta información.

A continuación, se relacionan los canales de CEDELCA S.A E.S.P.:

MEDIOS EXTERNOS	MEDIOS INTERNOS
Página web, redes sociales Facebook, Twitter	Intranet
Correos Electrónicos Personales, Genéricos, Línea telefónica	Correos Electrónicos institucionales,
Videos Institucionales	Carteleras Virtuales
Publicaciones e Impresos (Brochures-Publicaciones-Folletos)	Publicaciones Internas a traves de los diferentes canales
Cartas Personales, Informes	Correos Masivos
Presentaciones	Manuales
Eventos, Congresos, Talleres, Foros Celebraciones y Reuniones	Reuniones, Comités, Eventos y Celebraciones Internas

PREMISA DE COMUNICACIONES

En CEDELCA S.A E.S.P. creemos que una comunicación direccionada y efectiva es vital para llegar a nuestros públicos. Estar conscientes de los canales con que contamos para conseguir que nuestros públicos entiendan de la forma que queremos un determinado mensaje, es una herramienta poderosa que es muy útil conocer y manejar.

En este sentido, presentación, contenido, intención, expresión, contexto, ambiente y todos los detalles presentes en un acto comunicativo se integran para decir algo sobre alguien o algo, y es fundamental propender que nada quede al azar y, sobre todo, que la integración de todos los elementos emita un mensaje coherente.

Esto no sólo contribuye a mejorar las relaciones laborales, sino que aporta un grado importante de valor a las relaciones interpersonales dentro de la empresa.

La comunicación dentro de un equipo de trabajo, y entre los diferentes equipos, es reflejo del clima laboral, del compromiso de las personas con su trabajo, de su integración con la cultura organizacional y de su conocimiento de la misión de la empresa. Asimismo, es un aliado estratégico para la misión de la Empresa y un motor de transformación cultural que permite generar trabajadores alineados con los objetivos. Siendo la comunicación efectiva un eje de la gestión de CEDELCA S.A E.S.P., es fundamental que sus trabajadores compartan un lenguaje común, tanto en

lo técnico y operativo como en lo intangible (misión, visión, valores de la empresa y cultura organizacional).

ESTRUCTURACIÓN DE LAS COMUNICACIONES

De los públicos de interés:

La empresa busca estructurar y coordinar los procesos y requerimientos de comunicación de manera planeada, unificada y coherente, y por tal motivo sigue la siguiente estructura:

- Define cual es la necesidad de comunicación y cómo se debe actuar.

- Define un responsable de comunicaciones para que diseñe y ejecute el plan, producto o acción de comunicación.

- Formaliza y registra todas las acciones de comunicación con el propósito de construir memoria de la empresa.

Este responsable a su vez debe definir:

- **QUÉ:** mensaje (s) claves que deben ser comunicados
- **QUIEN o (S):** son las audiencias o públicos a quienes debe llegar el mensaje
- **COMO:** va a comunicar o transmitir el mensaje
- **CUANDO:** será comunicada o transmitida la información
- **EFECTO O ACCIÓN:** que se quiere lograr una vez se efectúe la comunicación.

VALORES QUE RIGEN LA POLÍTICA DE COMUNICACIÓN

- Responsabilidad en nuestro actuar comunicacional.
- Participación y Colaboración con los procesos de comunicación.
- Respeto por los públicos con los que nos comunicamos.
- Veracidad, relevancia y transparencia en la información y mensajes que transmitimos.
- Coherencia entre lo que pensamos, decimos y hacemos.

MENSAJES CLAVES

Los mensajes claves son aquellas ideas o enunciados correctamente construidos, que reflejan qué es nuestra empresa (valores, misión, visión, objetivos y metas), que nos sirven como discurso único para generar recordación e inciden en nuestra identidad y reputación.

Además, en CEDELCA S.A E.S.P., los mensajes claves tienen el propósito, de dar respuesta de manera estratégica a las dudas manifestadas por las distintas audiencias, así como también el de generar una opinión pública positiva.

COMPROMISOS CON LA POLÍTICA DE COMUNICACIONES

La claridad de la información y el transparente acceso a ésta por parte de los trabajadores, es vital para el ambiente laboral, por tal motivo en CEDELCA S.A E.S.P. la información de tipo institucional se genera de forma descendente, asegurando que el gerente y los jefes de área la transmitan a sus equipos de trabajo. Así mismo, la línea del gerente tiene el rol de generar el vínculo entre los colaboradores y los directivos de la organización.

Todos los trabajadores de la Empresa deben informar y consultar con los respectivos responsables de los canales internos y externos cualquier necesidad o acción de comunicación que se requiera con cualquiera de los públicos de la empresa.

Todos los colaboradores de la Empresa son responsables por el manejo adecuado tanto de la información como de los medios de comunicación que la empresa ha puesto al servicio.

Mantener canales de comunicación abiertos y responsables con las externas es el eje de acción en comunicación externa, por lo cual se hace de forma responsable, coherente y coordinada.

En caso que algún colaborador de la empresa sea contactado por audiencias externas tales como miembros de la comunidad, inversionista, analistas y prensa, entre otros, y sea requerido para entregar información de la empresa que sea de carácter sensible como por ejemplo datos o cifras de producción, financieras, proyectos de inversión, etc., deberá comunicarlo a la Gerencia de ésta.

BUENAS PRÁCTICAS EN COMUNICACIÓN

Tanto los Directivos de la Empresa como cada uno de sus trabajadores se comunican de diversas formas y cualquiera que sea, comunicación verbal, escrita y no verbal, debe hacerse siguiendo los valores que rigen esta política.

- Las comunicaciones transmitidas a través de canales impersonales o masivos, tales como el correo electrónico, páginas web, publicaciones e impresos tienen la capacidad de transferir información rápida y efectiva a nuestros públicos de manera consistente. No obstante, estás no deben sustituir la comunicación personal (cara a cara).

- En lo posible la comunicación personal, debe ser nuestra forma de comunicación más importante ya que estimula el diálogo y un ambiente abierto y de confianza.

- Sentido común, buenos modales, cortesía, respeto y tolerancia, reglas que se deben seguir en nuestra comunicación diaria, deben también tenerse en cuenta cuando nos comunicamos de manera impersonal. Al otro lado de la pantalla o del medio que se esté usando, hay un ser humano.

- Todos somos embajadores de la imagen de la entidad, la manera como nos comportamos y nos relacionamos día a día, dentro y fuera de la oficina, habla de ella.

LOS EVENTOS, EL PROTOCOLO Y LA ETIQUETA INSTITUCIONAL

En CEDELCA S.A E.S.P. todos los eventos son importantes, pues reflejan la personalidad de nuestra empresa y expresan la planeación y el desarrollo institucional en cada una de las áreas, Por eso "hacer" un evento significa "organizarlo", prever los detalles, visionar el momento o tiempo en que queremos que se realice y cómo deseamos presentarlo ante nuestros invitados.

La unidad de apoyo al personal es responsable de la organización de eventos de alto impacto institucional, los que convocan a diversos públicos y aquellos que de manera especial vinculan a la empresa. La unidad de apoyo al personal actúa como soporte o asesor de la realización de eventos que organicen directamente las áreas misionales de la Empresa.

La empresa debe establecer un conjunto de normas o reglas de cortesía, buenas prácticas y fórmulas que refuercen las relaciones humanas dentro y fuera de la empresa, logrando con todo ello un estilo propio que la caracterice, que cuide todos los detalles de una forma armoniosa, sutil e institucional.