POLITICAS PARA LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN EN COOMULDESA

OBJETIVOS

Coomuldesa define las políticas, procesos, procedimientos y controles que deben aplicar los empleados, practicantes, aprendices, proveedores, asociados y clientes de COOMULDESA, que puedan tener acceso a los activos de información de la entidad, asegurando su adecuada divulgación para preservar la Confidencialidad, Integridad y Disponibilidad de la información y garantizar la continuidad de las actividades de la entidad, protegiendo dicha información y mitigando los riesgos que la puedan afectar, optimizando la asignación y el uso de recursos o tecnologías para protegerla.

Mediante el presente documento COOMULDESA adopta una política de buenas prácticas en materia de seguridad de la información, para:

a) Establecer principios básicos de actuación que rigen a Coomuldesa para la protección de la integridad, confidencialidad y disponibilidad de sus activos de información, así como de la privacidad de los datos tratados.

b) Identificar y gestionar los riesgos operativos físicos y tecnológicos, así como la posible materialización de incidentes de seguridad que pongan en riesgo la confidencialidad, integridad y disponibilidad de los activos de información.

c) Adoptar de manera preventiva los mecanismos de control que minimicen su impacto, como un elemento que fortalezca la confianza de los asociados y el sector solidario frente a la entidad.

d) Establecer los roles y responsabilidades en términos de la seguridad de la información.

e) Proteger los activos de información, tecnológicos y físicos de la entidad.

f) Monitorear la Seguridad de la Información de la empresa.

g) Garantizar la continuidad del negocio frente a incidentes.

h) Fortalecer la confianza de las contrapartes en la entidad, en temas de seguridad de la información.

i) Sensibilizar a los responsables de los activos de información de la Cooperativa, sobre el uso correcto y el cuidado de los mismos.

j) Procurar aplicar las buenas prácticas de seguridad de la información que señala la ISO 27001.

POLÍTICAS

Política de No Repudio

El no repudio es la capacidad de demostrar o probar la participación de las partes (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.

Política de Integridad

Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

Política de Disponibilidad del Servicio

COOMULDESA cuenta con un plan de continuidad del negocio que procure por asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

Política de Auditoría para la Seguridad de la Información

- COOMULDESA podrá auditar de forma controlada y acorde a cualquiera de las partes interesadas (asociados, clientes, proveedores, aliados estratégicos, órganos de control, entre otros), cuando así lo desee, sin previo aviso, el cumplimiento de la normatividad que emita en materia de seguridad de la información.
- COOMULDESA podrá tomar medidas administrativas en contra de directivos y empleados que incumplan lo dispuesto en la normatividad que la entidad emita en materia de seguridad de la información.

Política de Comunicación y Sensibilización

- COOMULDESA cuenta con unos lineamientos para difundir, entre las partes interesadas, las políticas que se emitan en materia de seguridad de la información.
- COOMULDESA desarrolla un plan de capacitación para sensibilizar a directivos, empleados, aprendices, practicantes, proveedores, asociados y clientes, en materia de seguridad de la información, en armonía con sus funciones y/o su rol frente a la entidad, para fortalecer la cultura organizacional.

ROLES Y RESPONSABILIDADES

Proveedores

Los proveedores que, para el desempeño de la labor contratada, tengan acceso a la información sobre la cual COOMULDESA actúe en calidad de responsable, deben cumplir con todas las normas que integren el SGSCI de COOMULDESA y le sean aplicables. El líder del proceso con el cual tenga relación el proveedor, responde por asegurar el uso adecuado de los activos de información. Los proveedores deben aceptar por escrito los términos y condiciones de uso de los activos de información, así como el cumplimiento estricto del SGSCI antes de su acceder a la información.

Partes Interesadas

Se define como partes interesadas, aquellos roles y/o cargos que, en cumplimiento de sus funciones, puedan tener acceso a la información sobre la cual COOMULDESA actúe en calidad responsable. En relación el SGSCI este rol debe:

a) Cumplir con todas las responsabilidades que le hayan sido asignadas en el SGSCI y en los demás documentos normativos de COOMULDESA, así como en los contratos que puedan haber suscrito con la entidad.

b) Proteger la información a la cual la entidad le haya concedido acceso.

c) Firmar un acuerdo de confidencialidad y/o no divulgación antes de iniciar formalmente sus labores dentro de la entidad, cuando aplique.

d) Firmar aceptación sobre el entendimiento de las políticas, procedimientos, manuales y formatos de seguridad del Sistema de Gestión de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información de la entidad.

e) Cumplir con las políticas y procedimientos del SGSCI.

f) Utilizar de manera segura y adecuada los activos de información y los recursos de la entidad, dentro del desempeño de sus funciones.

RESPONSABILIDADES Y RECURSOS

Proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial

El SGSCI contempla la obligación de iniciar procesos disciplinarios en caso de presentarse alguna infracción contra las políticas de seguridad de la información de COOMULDESA por parte de empleados, aprendices, practicantes y otros colaboradores de la entidad; para el caso de los proveedores, Coomuldesa podrá iniciar procesos de responsabilidad. Sin perjuicio de las demás normas y condiciones contractuales para la actuación entre COOMULDESA y sus contrapartes, se consideran graves las siguientes faltas:

- Negativa o reticencia a firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- Generar, facilitar o no reportar la ocurrencia de incidentes de información, a las áreas encargadas de asegurar la seguridad de la información, según se haya documentado en los Manuales, Instructivos y/o Circulares que integren el SGSCI.
- No mantener la confidencialidad de las contraseñas de acceso que le hayan sido asignadas.
- Recaudar, copiar, transferir, transmitir, modificar, reproducir, suprimir o acceder a información sobre la cual no tenga los correspondientes permisos o privilegios.
- Generar y/o facilitar la pérdida o facilitar el acceso por parte de terceros, sobre la información a la cual tenga acceso acorde a sus funciones.
- No hacer entrega de los documentos de archivos que se encuentren a cargo de los empleados y contratistas, debidamente inventariados, cuando se presente su retiro o traslado.

- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Calificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- Intentar vulnerar los sistemas tecnológicos y de seguridad de COOMULDESA con el uso de herramientas o técnicas para atentar contra la información y los activos que la contienen.
- Desarrollar, fomentar, facilitar o participar en la ocurrencia de incidentes categorizados como:
  - ✓ Violaciones a la privacidad de la información.
  - ✓ Piratería informática.
  - ✓ Fraude y espionaje industrial.