

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

COOPETRABAN adopta buenas prácticas y estándares normativos en materia de seguridad de la información, permitiéndole identificar los riesgos operativos tecnológicos y la potencial materialización de incidentes de seguridad que pongan en riesgo la confidencialidad, integridad y disponibilidad de los activos tecnológicos y de información de la organización. De manera preventiva, se adoptan los mecanismos que minimicen el impacto. La seguridad y privacidad de la información son aspectos fundamentales para la prestación de los servicios y la toma de decisiones eficientes, razón por la cual, COOPETRABAN se compromete a la implementación de los requerimientos necesarios para una práctica adecuada en busca de la seguridad de la información. Así mismo, es compromiso de la organización la revisión periódica del Sistema de Seguridad de la Información, teniendo en cuenta los lineamientos establecidos por la normatividad vigente.

Por otro lado, COOPETRABAN manifiesta su disposición para hacer cumplir los estándares de seguridad de la información. La omisión por parte de los colaboradores está contemplada como falta disciplinaria en el “Código de Ética y Conducta”, velando de esta forma porque estos mantengan una cultura de seguridad. La organización se compromete adicionalmente, a publicar en los canales adecuados, la información concerniente a la seguridad y privacidad de la información, para que ésta pueda ser interiorizada y revisada por las partes interesadas.

COOPERABAN realiza una administración de riesgos encaminada a la consolidación de una cultura de seguridad consciente con las necesidades actuales, teniendo en cuenta los requerimientos de la Superintendencia de la Economía Solidaria. Con el propósito de asegurar una mejora continua, se establecen políticas específicas de seguridad de la información, las cuales conforman los lineamientos generales que adopta COOPETRABAN para el desarrollo del Sistema de Seguridad de la Información.

Políticas Específicas

- Es responsabilidad de los dueños de la información crítica no dejar copias impresas o documentos físicos en lugares de fácil acceso a personal no autorizado.
- Todo colaborador de COOPETRABAN debe firmar un acuerdo en el que acepte las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información.
- Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Cooperativa sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y el centro de cómputo de la Cooperativa.
- El personal interno o externo podrá acceder a las áreas restringidas, siempre y cuando se encuentren acompañadas por lo menos de un responsable del área, y previamente cuente con la debida autorización del Líder de Tecnología o del encargado del área de Logística.
- Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura tecnológica de la Cooperativa. De igual forma, deberán proteger la información reservada o confidencial, que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la Cooperativa o hacia redes externas como Internet.
- Los usuarios de la Cooperativa que hagan uso de equipos de cómputo deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red, ransomware, spyware.
- Las cuentas de ingreso a los sistemas y los recursos de cómputo que son propiedad de COOPETRABAN se usarán exclusivamente para actividades relacionadas con la empresa.

- Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, su identificador de usuario y password necesarios para acceder a la información y la infraestructura tecnológica de la Cooperativa, por lo cual deberá mantenerlos de forma confidencial.
- El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de la Cooperativa debe ser proporcionado por el líder de proceso al cual pertenezca el cargo, y queda establecido que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.
- El área de Tecnología de COOPETRABAN tiene como una de sus funciones principales, proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.
- COOPETRABAN asegura la información en las redes y mantiene la seguridad de la información transferida dentro de la organización y con cualquier entidad externa.
- COOPETRABAN realiza protección a los datos usados para pruebas.
- COOPETRABAN garantiza una gestión adecuada de los eventos e incidentes de seguridad y las debilidades asociadas con los activos de Información.
- COOPETRABAN garantiza la disponibilidad de su infraestructura tecnológica, de los procesos de negocio y la continuidad de su operación ante la materialización de incidentes de seguridad de la Información, para garantizar el cumplimiento de los requisitos de disponibilidad de sus partes interesadas.
- COOPETRABAN garantiza el cumplimiento de las obligaciones legales, regulatorias, normativas y contractuales establecidas, relacionados con seguridad de los activos de información, privacidad y seguridad de la información de datos personales, derechos de propiedad intelectual, y uso de software patentado.
- COOPETRABAN garantiza que la seguridad de la información se implemente y opere de acuerdo con las políticas, procesos y procedimientos organizacionales.

Aspectos No permitidos

Se consideran aspectos no permitidos para todos los colaboradores de la Cooperativa las siguientes acciones:

- La transmisión de contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante o acosador.
- Interceptar, recopilar o almacenar datos sobre terceros sin su conocimiento o consentimiento.
- Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.
- Enviar mensajes no solicitados (spam), virus, o ataques internos o externos.
- Obtener acceso no autorizado a equipos, sistemas o programas, tanto al interior de la red como fuera de ella. Tampoco se podrá utilizar la red WIFI para obtener, manipular y compartir cualquier archivo de tipo musical o filmográfico, sin tener los derechos de propiedad intelectual.
- Dañar equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red. Utilizar la red con fines de lucro, actividades comerciales o ilegales, por ejemplo, hacking; y/o utilizarla para crear o colocar un virus informático o malware en la red.
- Transmitir, copiar y/o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil, material amenazante u obsceno o material protegido por secreto comercial o patentes.

Prestación de Servicios por Terceras Partes

Cuando COOPETRABAN requiera la contratación de prestación de servicios por terceras partes debe, como mínimo:

- Firmar el documento de acuerdo de confidencialidad antes de iniciar la prestación del servicio.

- Elaborar los contratos o acuerdos de prestación de servicios donde se especifiquen claramente las condiciones.
- Cuando existan cambios en los servicios que prestan las terceras partes, estos deben ser documentados e incluidos en los acuerdos de servicios o contratos.

Aprobado por el Consejo de Administración acta 1.187 del 14 de Julio de 2022

(Original Firmado)

ÁLVARO DE JESÚS MEJÍA MOLINA
Presidente

(Original Firmado)

JUAN MANUEL MOSQUERA ARBELAEZ
Secretario