
# POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

CÁMARA DE COMERCIO DE BARRANQUILLA

## 1. OBJETIVO

La Política de Seguridad de la Información de la CÁMARA DE COMERCIO DE BARRANQUILLA tiene como objetivo principal establecer reglas y lineamientos sobre el uso y protección de la información, en cualquiera de sus formas, así como de los sistemas informáticos y de comunicaciones, de los recursos de información y de la tecnología utilizada para su procesamiento. Igualmente, abarca la protección de los activos intangibles (como la reputación e imagen institucional), todo ello frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información de la CÁMARA DE COMERCIO DE BARRANQUILLA.

Además del objetivo general, se establecen como objetivos adicionales del Sistema de Gestión de Seguridad de la Información (SGSI) de la CÁMARA DE COMERCIO DE BARRANQUILLA los siguientes:

1. Fomentar la cultura de la Seguridad de la Información dentro de la CÁMARA DE COMERCIO DE BARRANQUILLA, fortaleciendo las buenas prácticas y la conciencia de los colaboradores, contratistas, proveedores y demás partes interesadas que hagan uso de los activos de información de la organización.

2. Gestionar de manera eficaz los riesgos de seguridad de la información, con el fin de evitar el impacto negativo en los objetivos estratégicos de la CÁMARA DE COMERCIO DE BARRANQUILLA, especialmente en aquellos procesos misionales que soportan la operación y los servicios a la comunidad empresarial.

3. Monitorear y registrar los incidentes de seguridad que puedan presentarse, garantizando un tratamiento oportuno y eficaz que contribuya a la protección de la información y al mejoramiento continuo de los procesos de seguridad.

4. Identificar y remediar las vulnerabilidades críticas y altas para proteger la infraestructura tecnológica de la CÁMARA DE COMERCIO DE BARRANQUILLA, manteniendo los niveles de seguridad apropiados y cumpliendo con los acuerdos de servicio y la normatividad vigente.

5. Dar cumplimiento al programa de respaldo (backups) de la información, con el fin de asegurar la restauración de los datos y un nivel alto de contingencia ante eventos que comprometan la disponibilidad de la información.

## 2. ALCANCE

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la CÁMARA DE COMERCIO DE BARRANQUILLA, incluyendo todos los sistemas, equipos, instalaciones, procesos y activos de información utilizados dentro de su operación. Su aplicación abarca tanto los activos físicos como digitales, asegurando su protección y correcta gestión conforme a las políticas de seguridad establecidas por la organización.

## 3. DEFINICIONES

**Amenaza:** Causa potencial de un evento no deseado que podría resultar en daños para un sistema u organización.

**Ciberespacio:** Entorno complejo surgido de la interacción entre personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a esta red, el cual no tiene una existencia física.

**Cloud Computing:** Modelo de computación basado en el uso de servidores remotos para el almacenamiento, procesamiento y gestión de datos, accesibles a través de Internet.

**CSIRT (Computer Security Incident Response Team):** Equipo externo a Cámara de Comercio de Barranquilla dedicado a responder a incidentes de seguridad informática. Estos equipos están conformados por gremios o grupos de interés relacionados. Algunos ejemplos en Colombia son CSIRT-PONAL de la Policía Nacional y CSIRT-Financiero de Asobancaria.

**Malware:** Software malicioso diseñado para dañar dispositivos, servicios o redes.

**Riesgo:** Efecto de la incertidumbre en el logro de los objetivos. El riesgo de seguridad de la información está relacionado con la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información, causando así daños a una organización.

**Seguridad de la información:** Conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias utilizadas para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información almacenada, reproducida o procesada en los sistemas informáticos de Cámara de Comercio de Barranquilla.

**SOC (Security Operation Center):** Unidad responsable de monitorear, evaluar y defender los sistemas de información empresarial, incluyendo sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, estaciones de trabajo y otros dispositivos.

**Seguridad de la información:** Conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias utilizadas para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información almacenada, reproducida o procesada en los sistemas informáticos de Cámara de Comercio de Barranquilla.

**Teletrabajo:** Modalidad de trabajo remoto en la que el colaborador accede a los sistemas corporativos desde fuera de las instalaciones de la organización, cumpliendo con los lineamientos de seguridad definidos.

**Trazabilidad:** Marca, signo o evidencia de la existencia, influencia o acción de alguien, algo o algún evento sobre un sistema de información.

**Usuario:** Persona con privilegios específicos que hace uso final de las aplicaciones proporcionadas por la organización para la ejecución de sus actividades, utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos.

**VPN (Virtual Private Network):** Tecnología que permite una conexión segura y cifrada a la red institucional desde ubicaciones remotas.

**Vulnerabilidad:** Debilidad de un activo o control que podría ser explotada por una o más amenazas. Se consideran todas las amenazas que surgen de la interacción de los sistemas en el ciberespacio.

## 4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Alta Dirección de la CÁMARA DE COMERCIO DE BARRANQUILLA reconoce que la información es uno de sus activos más valiosos y, por ende, comprende la importancia de su adecuada gestión. Con este convencimiento, la CÁMARA DE COMERCIO DE BARRANQUILLA se compromete a implementar, operar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), alineado con estándares internacionales, buenas prácticas de la industria, exigencias legales, y orientado al logro de sus objetivos estratégicos. De esta forma, se propicia un marco de confianza en el cumplimiento de las funciones y servicios ofrecidos a todos sus grupos de interés, siempre bajo el estricto cumplimiento de la normatividad nacional y en sintonía con la misión, visión, estrategias y necesidades de la institución.

Para la CÁMARA DE COMERCIO DE BARRANQUILLA, la protección y el uso adecuado de sus activos de información, el fomento de una cultura de seguridad y la atención oportuna de los incidentes de seguridad constituyen elementos fundamentales para minimizar el impacto de las amenazas y riesgos que comprometen la información. Con ello, la CÁMARA DE COMERCIO DE BARRANQUILLA ratifica su compromiso de responder de manera integral por la confidencialidad, integridad y disponibilidad de la información, pilares esenciales de la seguridad de la información.

## 4.1. Características de la Información

**Confidencialidad:** Garantiza que solo las personas, áreas o entidades con autorización puedan acceder o divulgar la información. Este principio es esencial para mantener la privacidad de los datos y cumplir con los requerimientos legales de protección de la información personal y corporativa.

**Integridad:** Busca asegurar que los datos no se modifiquen sin la trazabilidad correspondiente (es decir, toda alteración debe dejar un rastro auditable), garantizando que la información conservada sea completa y exacta en todo momento.

**Disponibilidad:** Exige que la información y los activos que la gestionan estén accesibles para los usuarios legítimos cada vez que lo requieran, facilitando la continuidad operativa y el cumplimiento de la oferta de servicios al sector empresarial y la comunidad en general.

## 4.2. Clasificación de la información

La CÁMARA DE COMERCIO DE BARRANQUILLA reconoce la importancia de clasificar la información de acuerdo con su contenido y nivel de sensibilidad. Para ello, toda la información que es almacenada en repositorios de datos o manejada por colaboradores, contratistas, proveedores y demás partes interesadas, debe clasificarse en tres categorías:

**Confidencial:** La información confidencial de la CÁMARA DE COMERCIO DE BARRANQUILLA es reservada y está destinada exclusivamente al uso de colaboradores autorizados. Su reproducción o utilización para fines distintos a los establecidos está prohibida sin la autorización previa del propietario de la información. Este tipo de información puede ser tanto propia de la CÁMARA DE COMERCIO DE BARRANQUILLA como de terceros, y no es de conocimiento público, presentando una o varias de las siguientes características:

Está protegida por un acuerdo de confidencialidad o cláusulas contractuales.
Su divulgación podría tener un impacto alto o significativo en la CÁMARA DE COMERCIO DE BARRANQUILLA, así como en sus clientes o proveedores.
No se encuentra disponible de forma general al público ni es conocida en medios abiertos.
La divulgación, alteración o destrucción no autorizada de esta información conlleva un riesgo elevado para la CÁMARA DE COMERCIO DE BARRANQUILLA o para terceros.

**Uso interno:** Es aquella que se utiliza para la operación cotidiana y la gestión interna de la entidad. Aunque su divulgación, alteración o destrucción no autorizada puede generar un riesgo de impacto medio o bajo, esta información sigue siendo restringida y debe ser accesible únicamente a los colaboradores de la CÁMARA DE COMERCIO DE BARRANQUILLA o a terceros que cuenten con la debida autorización. Además, el uso de esta información es exclusivo para conocimiento interno, esta puede ser compartida con la autorización o aprobación del responsable del proceso al que pertenece. Su divulgación a terceros sin la debida autorización está prohibida, y cada área es responsable de garantizar un nivel adecuado de protección para estos datos.

**Pública:** La información pública de la CÁMARA DE COMERCIO DE BARRANQUILLA es aquella de conocimiento general que no requiere autorización para su uso o acceso, tanto dentro como fuera de la organización. Su divulgación no impacta negativamente en las operaciones de la CÁMARA DE COMERCIO DE BARRANQUILLA, ya que está autorizada para el público en general. Este tipo de datos puede ser compartido a través de cualquier canal, sin que ello implique un riesgo significativo para la organización, siempre que se respeten los lineamientos éticos y legales vigentes.

La información que pertenezca a terceras partes (por ejemplo, de otras entidades públicas o privadas) y que sea custodiada por la CÁMARA DE COMERCIO DE BARRANQUILLA, deberá ser tratada siempre como confidencial, salvo que se disponga lo contrario en acuerdos específicos. En todo caso, se deben respetar las leyes y disposiciones vigentes (por ejemplo, la Ley 1581 de 2012 sobre protección de datos personales), así como las cláusulas contractuales o acuerdos de confidencialidad pactados.

**Nota:** Cuando la CÁMARA DE COMERCIO DE BARRANQUILLA reciba información de un cliente u otra entidad, y este no haya definido criterios de clasificación, se entenderá por defecto que dicha información es confidencial y se regirá por las políticas de seguridad establecidas.

### 4.3. Principios y lineamientos en la cultura de seguridad de la información

**Formación y concientización:** Todos los colaboradores de la CÁMARA DE COMERCIO DE BARRANQUILLA, independientemente de la modalidad de su contrato, reciben capacitaciones y actualizaciones periódicas sobre las políticas y controles de Seguridad de la Información. Estas acciones de formación tienen como propósito fomentar la cultura de seguridad y asegurar el cumplimiento de la normativa y los procedimientos establecidos.

**Contacto con autoridades y grupos de interés:** El área responsable de la Seguridad de la Información en la CÁMARA DE COMERCIO DE BARRANQUILLA mantendrá comunicación apropiada con autoridades competentes y con grupos externos especializados (por ejemplo, CSIRT - Equipos de Respuesta a Incidentes de Seguridad), además de participar en foros y conferencias profesionales. Así se busca estar al día en cuanto a nuevas amenazas, vulnerabilidades y mejores prácticas de

mitigación.

**Políticas y procedimientos suplementarios:** Además de la presente Política de Seguridad de la Información, la CÁMARA DE COMERCIO DE BARRANQUILLA desarrollará, aprobará y difundirá un conjunto de políticas, normas y procedimientos específicos que apoyen la operación y fortalezcan la cultura de seguridad de la información. Dichos lineamientos serán socializados a todas las partes interesadas para asegurar su entendimiento y cumplimiento.

**Controles y cumplimiento legal:** Los controles establecidos en la presente política, y en las demás políticas de seguridad de la información, buscarán dar cumplimiento a los requerimientos internos de la CÁMARA DE COMERCIO DE BARRANQUILLA, así como a la legislación, regulaciones y normativas nacionales e internacionales aplicables. Cualquier manejo o tratamiento de datos se realizará bajo los principios de confidencialidad, integridad y disponibilidad, en concordancia con las leyes de protección de datos personales y demás disposiciones vigentes.

## 5. USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN

Los recursos informáticos y la información contenida en ellos son propiedad de la CÁMARA DE COMERCIO DE BARRANQUILLA y su uso está restringido exclusivamente a fines institucionales y operativos.

Todos los colaboradores, contratistas y terceros que tengan acceso a estos recursos deben hacer un uso adecuado y responsable, alineado con sus funciones y con las normativas de la entidad. Queda prohibido el uso de estos activos para actividades no relacionadas con las responsabilidades del cargo, así como cualquier acción que pueda afectar la imagen de la CÁMARA DE COMERCIO DE BARRANQUILLA o aumentar el riesgo de exposición a amenazas de seguridad sobre los activos de información.

### 5.1. Uso de Internet

El área de Gestión Tecnológica proveerá el servicio de Internet de forma segura e implementará los controles necesarios de acceso, de acuerdo con los roles y responsabilidades definidos para los colaboradores.

Las disposiciones sobre el uso de Internet son las siguientes:

- El acceso a Internet está restringido exclusivamente a fines laborales y debe utilizarse en el marco de las funciones asignadas a cada usuario.
- Está prohibido visitar sitios considerados inseguros o que representen un riesgo potencial para la seguridad de la información de la CÁMARA DE COMERCIO DE BARRANQUILLA.

- No está permitido descargar música, videos, juegos o cualquier otro contenido no relacionado con las funciones laborales.
- El acceso a páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y otros sitios que representen un riesgo de seguridad será bloqueado mediante herramientas de control establecidas por el área de Gestión Tecnológica.
- Cualquier excepción de acceso a sitios restringidos deberá ser solicitada por el jefe inmediato del colaborador, con la debida justificación y aprobación del área de Seguridad de la Información.
- El acceso a Internet por parte de personal externo dentro de las instalaciones de la CÁMARA DE COMERCIO DE BARRANQUILLA será gestionado en segmentos de red separados para evitar accesos no autorizados a la información.
- No está permitido utilizar Internet para infringir derechos de propiedad intelectual, lo que incluye derechos de autor, marcas registradas, software, imágenes, investigaciones, patentes, publicidad y otros contenidos protegidos legalmente.

### 5.2. Uso de Correo Electrónico Corporativo

El servicio de correo electrónico corporativo es una herramienta de comunicación oficial de la CÁMARA DE COMERCIO DE BARRANQUILLA y su uso está restringido a fines estrictamente laborales.

Las disposiciones sobre el uso del correo electrónico son las siguientes:

- El acceso y uso del correo electrónico debe ser autorizado por el jefe inmediato y gestionado por el área de Gestión Tecnológica.
- Cualquier correo sospechoso o de dudosa procedencia debe ser reportado de inmediato al área de Seguridad de la Información.
- El acceso al correo electrónico será revocado en caso de terminación del vínculo laboral o contractual del colaborador o contratista.
- La CÁMARA DE COMERCIO DE BARRANQUILLA podrá monitorear y auditar el uso del correo electrónico, con el fin de garantizar la seguridad de la información y prevenir incidentes.
- Está prohibido usar el correo electrónico para enviar o recibir información no relacionada con las funciones laborales, así como para compartir información confidencial fuera de los protocolos establecidos.
- No se debe asociar el correo electrónico corporativo a redes sociales, cuentas bancarias u otros servicios personales, salvo que estén directamente relacionados con funciones laborales autorizadas.

Para garantizar un uso seguro del correo electrónico, se deben seguir las siguientes buenas prácticas:

- No almacenar contraseñas en navegadores.
- No abrir correos electrónicos de remitentes desconocidos.
- No reenviar correos en cadena.
- No responder a mensajes de spam o de procedencia dudosa.
- Cambiar la contraseña del correo al menos cada tres meses.

### 5.3. Uso de conexiones remotas y teletrabajo

El acceso remoto y el teletrabajo en la CÁMARA DE COMERCIO DE BARRANQUILLA deben realizarse bajo estrictos controles de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información corporativa.

Las disposiciones generales son:

- Los colaboradores autorizados para trabajar en modalidad remota deben utilizar únicamente equipos proporcionados por la entidad, evitando el uso de dispositivos personales.
- Todas las conexiones remotas deberán realizarse exclusivamente a través de una VPN institucional para proteger la transferencia de datos y evitar accesos no autorizados.
- Se restringirá el acceso remoto solo a los sistemas necesarios para el desempeño de las funciones laborales, limitando el acceso a información sensible.
- Los equipos corporativos asignados para teletrabajo no podrán ser utilizados por terceros o familiares, asegurando que el acceso sea exclusivo del usuario autorizado.
- El área de Gestión Tecnológica debe validar periódicamente la efectividad de los controles de acceso remoto, asegurando que se mantengan actualizados y alineados con las políticas de seguridad de la entidad.
- Se prohíbe el uso de redes públicas o no seguras al momento de acceder a los sistemas de la entidad, reduciendo riesgos de filtraciones o ataques cibernéticos.
- Las redes y sistemas críticos serán objeto de auditorías periódicas para evaluar el cumplimiento de los controles de seguridad y minimizar posibles vulnerabilidades.

### 5.4. Uso de Hardware y Software

El uso de hardware y software en la CÁMARA DE COMERCIO DE BARRANQUILLA está sujeto a los lineamientos establecidos por el área de Gestión Tecnológica, con el fin de garantizar la integridad, disponibilidad y seguridad de los activos informáticos.

Las disposiciones sobre el uso de hardware y software son las siguientes:

- El área de Gestión Tecnológica es responsable de definir las especificaciones técnicas de los equipos de cómputo, así como de gestionar la instalación, configuración y mantenimiento del software corporativo.
- Está prohibido abrir, retirar o cambiar componentes de los equipos sin la debida autorización del área de Gestión Tecnológica.
- No se podrán instalar dispositivos o periféricos sin aprobación previa, incluyendo memorias USB, discos duros externos o cualquier otro medio de almacenamiento externo.
- La instalación de software o sistemas solo podrá ser realizada por el área de Gestión Tecnológica, la cual llevará a cabo las pruebas técnicas necesarias antes de su implementación.
- Queda prohibida la instalación y uso de software no autorizado, ya que podría comprometer el funcionamiento del equipo o la seguridad de la información.
- Cada usuario es responsable de organizar y mantener sus archivos de manera ordenada, asegurando que su equipo cuente con el espacio suficiente para operar correctamente.
- El software licenciado y autorizado por la CÁMARA DE COMERCIO DE BARRANQUILLA solo podrá ser utilizado para las funciones asignadas a cada usuario y bajo las condiciones establecidas por la entidad.

### 5.5. Uso de Información Impresa

El manejo del material impreso debe seguir los mismos estándares de seguridad que los datos almacenados electrónicamente, con el fin de prevenir accesos no autorizados y proteger la confidencialidad de la información de la CÁMARA DE COMERCIO DE BARRANQUILLA.

Las disposiciones sobre el uso de información impresa son las siguientes:

- No se debe dejar material impreso desatendido en impresoras, escáneres, fotocopiadoras u otros dispositivos de reproducción, ya que podría ser accesible por personas no autorizadas.
- Los documentos que contengan información sensible deben ser retirados de inmediato tras su impresión o reproducción.
- El envío de documentos con información confidencial o restringida deberá realizarse utilizando servicios que permitan su trazabilidad y seguimiento, como el correo certificado o sistemas internos de gestión documental.
- En ninguna circunstancia se debe reutilizar material impreso que contenga información interna, confidencial o restringida.
- Se recomienda el uso de trituradoras o métodos de eliminación segura para la destrucción de documentos sensibles una vez que ya no sean necesarios.

## 5.6. Uso de Contraseñas

El uso adecuado de contraseñas y claves de acceso es fundamental para garantizar la seguridad de los activos de información de la CÁMARA DE COMERCIO DE BARRANQUILLA.

Las directrices específicas para la gestión de contraseñas están establecidas en el documento "Política de Gestión de Contraseñas", donde se detallan los lineamientos que deben seguir todos los usuarios para el manejo seguro de credenciales de acceso a los sistemas de la entidad.

Se recomienda que todas las contraseñas:

- Cumplan con los requisitos mínimos de seguridad, como longitud y combinación de caracteres.
- Sean cambiadas periódicamente para reducir riesgos de compromiso.
- No sean compartidas ni almacenadas en ubicaciones inseguras, como navegadores web o notas visibles.

## 5.7. Uso de Medios de Almacenamiento Extraíbles y Respaldo de Información

El uso de dispositivos de almacenamiento extraíbles representa un riesgo significativo para la seguridad de la información. Por ello, su uso en la CÁMARA DE COMERCIO DE BARRANQUILLA está estrictamente regulado.

Las disposiciones sobre el uso de medios extraíbles son las siguientes:

- El uso de dispositivos de almacenamiento externo (USB, discos duros portátiles, tarjetas SD, etc.) está restringido y solo será permitido para funcionarios o terceros autorizados por el área de Seguridad de la Información y Gestión Tecnológica.
- El área de Gestión Tecnológica será responsable de gestionar la aprobación, uso y retiro de los dispositivos extraíbles de manera segura.
- Se mantendrá un registro actualizado de las personas autorizadas para el uso y transporte de medios de almacenamiento extraíbles.
- Cada usuario autorizado es responsable de la seguridad y custodia del medio extraíble bajo su uso, evitando accesos no autorizados, daños, pérdida de información o extravío del dispositivo.
- Toda información almacenada en medios extraíbles y que ya no sea requerida debe ser eliminada de forma segura, en cumplimiento con la Política de Eliminación y Destrucción de Información.

- El área de Gestión Tecnológica implementará mecanismos para restringir el uso de medios extraíbles en equipos institucionales, promoviendo alternativas seguras como servidores de archivos, almacenamiento en la nube o carpetas compartidas controladas.
- Todos los archivos críticos deberán contar con copias de respaldo gestionadas por el Área de Gestión Tecnológica.
- Se podrá auditar el almacenamiento y acceso a los datos para prevenir riesgos de seguridad.
- Se establecerán controles para regular el acceso y uso de dispositivos de almacenamiento en la infraestructura tecnológica de la entidad, minimizando riesgos de fuga de información o infecciones por malware.

## 5.8. Seguridad en la Nube (Cloud Computing)

Para la gestión segura de los servicios en la nube, se establecen las siguientes directrices:

- Solo podrán utilizarse servicios de almacenamiento en la nube aprobados por el Área de Gestión Tecnológica.
- La información en la nube deberá estar protegida mediante autenticación de múltiples factores y cifrado.
- Se realizarán auditorías periódicas para garantizar el cumplimiento de las medidas de seguridad.
- En caso de migración o baja de un servicio en la nube, la información almacenada deberá eliminarse de forma segura.

## 5.9. Auditoría y monitoreo del uso de recursos

La CÁMARA DE COMERCIO DE BARRANQUILLA se reserva el derecho de auditar y monitorear el uso de sus activos de información para garantizar el cumplimiento de esta política. Esto incluye:

- Se analizarán los registros de acceso y uso de recursos para detectar posibles incidentes de seguridad.
- El uso del correo institucional podrá ser monitoreado para prevenir el mal uso o filtraciones de información.
- Se implementarán mecanismos de control para restringir el acceso a sistemas en caso de detectar actividades sospechosas.
- Los usuarios deberán reportar cualquier actividad anómala al Área de Seguridad de la Información.

### 5.10. Lineamientos para Proveedores y Terceros

Las siguientes reglas aplican a proveedores y terceros con acceso a los sistemas de información de la CÁMARA DE COMERCIO DE BARRANQUILLA:

- Todo proveedor con acceso a sistemas corporativos deberá firmar acuerdos de confidencialidad y cumplir con los lineamientos de seguridad establecidos.
- Los proveedores sólo podrán acceder a la información estrictamente necesaria para el cumplimiento de sus funciones.
- Las actividades realizadas por terceros en los sistemas de la organización estarán sujetas a auditoría.
- No está permitido instalar software no autorizado, transferir datos fuera de los entornos corporativos ni utilizar cuentas de usuario compartidas.

## 6. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

La CCB entiende la importancia de la definición de roles, responsabilidades y autoridades. Cada miembro del personal debe conocer su papel en la protección de la información y en el cumplimiento de las políticas de seguridad establecidas. Esto la asignación de responsabilidades específicas a cada área, asegurando que todos los colaboradores participen activamente en la gestión de la seguridad de la información. La claridad en estas funciones es fundamental para fomentar una cultura de seguridad y para garantizar que se tomen las decisiones adecuadas en materia de protección de datos.

## 7. SANCIONES POR INCUMPLIMIENTO

El incumplimiento de esta política será considerado una falta grave y podrá derivar en las siguientes sanciones:

- Advertencia formal: En caso de infracciones leves, el usuario será notificado para corregir su conducta.
- Restricción o revocación de acceso: Si se detecta un uso indebido de los recursos informáticos, se podrá restringir o revocar el acceso a los sistemas corporativos.
- Medidas disciplinarias: El incumplimiento reiterado o grave podrá dar lugar a sanciones conforme a la normativa interna de la organización.
- Acciones legales: Si el incumplimiento afecta la confidencialidad, integridad o disponibilidad de los activos de información, podrá derivar en acciones legales contra el infractor.

## 8. PLANIFICACIÓN

La organización ha definido los objetivos de seguridad de la información en alineación con su estrategia general, habiendo identificado previamente las necesidades y expectativas de las partes interesadas. Se han establecido políticas y procedimientos que guían la operación y el mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando el cumplimiento de los requisitos legales y reglamentarios aplicables.

## 9. ACCIONES PARA ABORDAR LOS RIESGOS Y OPORTUNIDADES

La identificación y gestión de riesgos y oportunidades han sido implementadas como parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI). La organización ha llevado a cabo un análisis exhaustivo de los riesgos potenciales que pueden afectar la confidencialidad, integridad y disponibilidad de la información. A partir de esta evaluación, se han desarrollado acciones específicas para mitigar los riesgos identificados y aprovechar las oportunidades que se han presentado para fortalecer la seguridad de la información.

## 10. EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La realización de la evaluación de riesgos de seguridad de la información permitió identificar y priorizar las amenazas que enfrenta la organización. Este proceso involucró la recopilación y análisis de información sobre los activos de información, así como las causas asociadas, además del impacto potencial de los incidentes de seguridad. Los resultados de esta evaluación han proporcionado una base sólida para la toma de decisiones informadas sobre las medidas de seguridad implementadas, lo que permite a la organización gestionar de manera eficaz los riesgos asociados a su información y fortalecer su postura de seguridad.

## 11. TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La CCB ha seleccionado las medidas de control más apropiadas, basándose en la evaluación de riesgos y considerando la efectividad, los costos y la viabilidad de cada acción. Esto ha incluido la implementación de controles técnicos, administrativos y físicos, así como la capacitación del personal en prácticas de seguridad. Además, se han establecido procedimientos para el monitoreo y revisión continua de los controles implementados, asegurando que se mantenga un nivel adecuado de protección frente a las amenazas y vulnerabilidades. Este enfoque integral fortalece la capacidad de la organización para gestionar los riesgos asociados y proteger sus activos de información de manera efectiva.

## 12. EVALUACIÓN DEL DESEMPEÑO

Se ha realizado seguimiento, medición, análisis y evaluación con el fin de mantener un Sistema de Gestión de Seguridad de la Información (SGSI) eficaz y alineado con los objetivos organizacionales. La organización ha establecido procedimientos para recopilar datos relevantes sobre el desempeño del SGSI, garantizando que se realicen auditorías y revisiones periódicas.

## 13. MEJORA

### 13.1. Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.

### 13.2. No conformidad y acción correctiva

## 14. MARCO DE REFERENCIA

ISO/IEC 27001:2022 - Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos.