1 OBJETIVO

La política general de seguridad y privacidad de la información identifica responsabilidades y establece la base general para proteger, conservar y asegurar la información, el buen uso de las herramientas tecnológicas utilizadas para su generación, procesamiento y disposición, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de la Organización.

2 ALCANCE

Esta política establece los lineamientos principales que deben seguir y aplicar todos los usuarios de la Organización, para preservar la confidencialidad, integridad y disponibilidad de la información de la Organización.

3 DEFINICIONES

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Activos de información: Recurso del sistema de información que tiene valor para la organización, bases de datos, documentación física y digital, software, hardware, equipos de comunicación, servicios informáticos y de comunicaciones, infraestructura (iluminación, energía, aire acondicionado, etc.).

Autenticación: Garantía de que una parte de una transacción informática no es falsa. La autenticación normalmente lleva consigo el uso de una contraseña, un certificado, un número de identificación personal u otra información que se pueda utilizar para validar la identidad en una red de equipos.

Firewall: Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno.

Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal.

Inteligencia artificial (IA): Es tecnología que permite que las computadoras simulen la inteligencia y las capacidades humanas de resolución de problemas.

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras.

Seguridad de la Información: La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta.

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información.
- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados.

Usuario: se refiere a todos los empleados, contratistas, consultores, trabajadores temporales, y cualquier otra persona o entidad que utilice los Recursos de Computación de la Organización.

4 CUMPLIMIENTO

Es de total y obligatorio cumplimiento para todos los usuarios, así como para todas las Organizaciones aliadas, filiales o que hacen parte de esta empresa.

Las reglas y obligaciones descritas en este documento aplican a todos los usuarios de la red de computación de la Organización, sin importar su ubicación.

Las violaciones a las políticas aquí establecidas comprometerán de manera grave la responsabilidad del contraventor y podrán generar acción disciplinaria interna, incluyendo terminación con justa causa del contrato de trabajo o terminación del contrato de servicios profesionales sin perjuicio de las acciones civiles y penales a que haya lugar.

5 REVISIÓN

Las políticas se revisan anualmente para comprobar su efectividad por parte de Gerente TI y jefe Service Delivery, Infraestructura y Seguridad de acuerdo con los siguientes factores:

1.1 Incidentes de seguridad.
1.2 Nuevas vulnerabilidades detectadas.
1.3 Cambios de la infraestructura organizacional o tecnológica.
1.4 Cambios en los procesos, en los objetivos del sistema o de la Organización.
1.5 Cambios normativos que en materia de seguridad de la información emita el gobierno nacional a través del Ministerio de las tecnologías de la Información y Comunicaciones

6 PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las responsabilidades frente a la seguridad y privacidad de la información serán definidas, compartidas, publicadas y aceptadas por todos los funcionarios definidos en el alcance establecido en el presente documento.

La Organización protege la información generada, procesada o resguardada por los procesos de sus sistemas de información y activos de información que hacen parte de estos, controla la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

La Organización protege la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos operativos o legales, debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

La Organización protege la información de las amenazas originadas por parte de los usuarios internos y externos, garantiza el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en materia de seguridad y privacidad de la información.

La Organización protege la infraestructura tecnológica y sistemas de almacenamiento que soportan sus procesos críticos, implementa controles de acceso a la información, sistemas de información y recursos de red.

7 GENERALIDADES

La dirección entiende la importancia de una adecuada gestión de la información, está comprometida con la implementación de un sistema de gestión de seguridad y privacidad de la información, buscando establecer un marco de confianza en ejercicio de sus actividades.

Para la Organización la protección de la información es una prioridad, busca la disminución del impacto generado sobre sus activos, minimizando los riesgos identificados a través de controles establecidos en todos sus procesos, con objetivo de preservar la integridad, confidencialidad y la disponibilidad de la información, acorde con la satisfacción de las necesidades de nuestros clientes y demás asociados de negocio (accionistas, colaboradores, contratistas, subcontratistas, comunidad y proveedores), ofreciendo servicios que cumplan con estándares de calidad y garantizando la seguridad en toda la cadena de suministro.

8 OBJETIVOS

La Organización establece las siguientes objetivos y lineamientos para el cumplimiento y protección de todos los activos de información:

- Minimizar el riesgo en todos los ciclos de manejo de información en los procesos.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los clientes externos.
- Incentivar la innovación tecnológica.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios.
- Garantizar la continuidad del negocio frente a incidentes de seguridad informática.

9 CONDICIONES GENERALES

9.1 Derechos de uso de activos informáticos

Los activos informáticos son de propiedad de la Organización y pueden ser utilizados únicamente para propósitos legítimos del negocio. Se permite que los usuarios utilicen estos Recursos para facilitarles el desempeño de sus tareas. El uso de estos Recursos es un privilegio que puede ser revocado en cualquier momento.

9.2 No expectativa de privacidad

Los usuarios no deben tener una expectativa de privacidad en relación con cualquier material que creen, almacenen, generen o reciban en el sistema de computación. Este sistema pertenece a la Organización y solo debe ser utilizado para propósitos relacionados exclusivamente con el negocio.

9.3 Renuncia a derechos de privacidad

Los usuarios renuncian expresamente a la privacidad en relación con cualquier material que ellos creen, almacenen, manden o reciban en el computador, a través de Internet o de cualquier otra red. Los usuarios dan su consentimiento para que, de ser necesario, funcionarios autorizados por la dirección puedan acceder y revisar cualquier tipo de material que los usuarios creen, almacenen, manden o reciban en el computador, a través de internet o de cualquier otra red. los usuarios entienden y aceptan que la Organización. puede utilizar procedimientos y recursos manuales o automáticos para monitorear la utilización de sus recursos de computación.

9.4 Uso personal

No podrán usarse los equipos para uso personal, ni para almacenamiento de información personal, comercial, publicidad, programas destructivos (virus), material político o cualquier otro uso que no esté autorizado de terceros ajenos a la Organización y/o a las operaciones de esta. No obstante, lo anterior, si por alguna circunstancia al momento de auditar los computadores y llegase a encontrar o evidenciar información o documentación de esta índole se tomarán las medidas disciplinarias correspondientes.

9.5 Material inapropiado o ilegal:

El material que tenga carácter fraudulento, que pueda llegar a generar sentimientos de acoso u hostigamiento, o que por su naturaleza sea embarazoso, sexualmente explícito, difamatorio, ilegal o inapropiado, no podrá ser enviado por correo electrónico o cualquier otra forma de comunicación electrónica (tales como sistemas de boletines informativos, grupos de noticia, grupos de chat) o exhibido o almacenado en los computadores de la Organización. Los Usuarios que encuentren o reciban este tipo de material deben reportarlo en forma inmediata a Tecnologia.

9.6 Desperdicio de recursos de cómputo.

Los usuarios no deben realizar intencionalmente actos que impliquen un desperdicio de los recursos de cómputo o monopolicen o acaparen los recursos para excluir a otros. Estos actos incluyen, pero no se limitan a, envió de correo electrónico masivo, envío de correo de cadena, gastar tiempo excesivo en el internet, juegos, grupos de chat, impresión de copias múltiples de documentos, bajar archivos de gran tamaño, o crear tráfico de red innecesario.

9.7 Derechos de propiedad intelectual

La Organización en pleno cumplimiento de la protección de derechos de autor (Ley 23 de 1982) dispone las siguientes directrices:

Los Usuarios no podrán efectuar cualquiera de las siguientes labores sin previa autorización escrita de la Organización:

(1) Copiar software para utilizar en sus computadores en casa; (2) proveer copias de software a contratistas, empleados temporales, amigos, parientes o cualquier otra tercera persona; (3) instalar software en cualquier computador o servidor de la Empresa; (4) bajar software de internet u otro servicio en línea a cualquier computador o servidor; (5) modificar, revisar, transformar o adaptar cualquier software; o (6) descompilar o ingeniería de reverso en cualquier software.

Los Usuarios deberán informar a su jefe inmediato de cualquier conocimiento que tengan de cualquier violación al uso adecuado y legal del software o de los derechos respectivos de autor.

9.7.1 Aplicaciones licenciadas

No se permite el uso, instalación y/o ejecución de software no licenciado en ningún equipo o servidor de la Organización esto, con la finalidad de proteger, mantener y salvaguardar la protección de los derechos de autor dispuestos (Ley 23 de 1982).

9.7.2 Comunicación de secretos del negocio.

A menos que esté expresamente autorizado por las Directivas de la Organización, está estrictamente prohibido divulgar, propagar, copiar o almacenar información de propiedad de la Organización. secretos del negocio o cualquier otra información confidencial. El incumplimiento de esta norma puede resultar en responsabilidad civil y penal. (Arts. 238, 288 y 289 del Código penal).

9.7.3 Acceso de archivos de otros usuarios.

Los Usuarios no podrán alterar o copiar un archivo perteneciente a otro Usuario sin el previo consentimiento del dueño del archivo. La capacidad de poder leer, alterar o borrar un archivo perteneciente a otro usuario, no implica que se tenga el permiso para leer, alterar o borrar ese archivo.

9.8 Acceso a otros computadores y redes

La capacidad de un Usuario de conectarse a otro sistema de cómputo, a través de la red o de módem, no implica que tenga el derecho de conectarse a esos sistemas o de hacer uso de estos, a menos que tengan autorización específica por parte de los operadores de esos sistemas y de la Empresa.

9.9 Seguridad de Cómputo

Cada Usuario es responsable de asegurar que el uso de computadores y redes externas, tal como Internet, no comprometa la seguridad de los Recursos de Computación de la Organización. Esta responsabilidad incluye, pero no se limita a, prevenir que intrusos tengan acceso a los Recursos de Computación y de prevenir la introducción y propagación de virus.

9.10 Internet

Algunos funcionarios pueden ser otorgados permisos de acceso a Internet para asistirles en el desarrollo de sus tareas. Internet puede ser un recurso valioso de información. Adicionalmente, el correo electrónico puede proveer un excelente medio de comunicación con otros empleados, clientes, proveedores, asesores, etc. Sin embargo, el uso de Internet debe ajustarse al sentido común y ética. El uso indebido de este recurso puede implicar que se le remueva el acceso al mismo. Igualmente, puede resultar en acción disciplinaria, incluyendo posible terminación del contrato por justa causa, así como responsabilidad civil y criminal.

La utilización de Internet se rige además por lo siguiente:

9.10.1 Negación de responsabilidad por uso de Internet

La Organización no es responsable por el material que los Usuarios acceden o bajen de Internet. Internet es una red mundial con una amplia gama de información. Los Usuarios deben ser precavidos ya que el contenido de estas páginas puede ser ofensivo, sexualmente explícito e inapropiado. Los Usuarios que se conecten a Internet lo hacen bajo su propia responsabilidad.

9.10.2 Monitoreo del uso de los recursos de computación

La Empresa tiene el derecho, mas no la obligación, de monitorear todos los aspectos relacionados con sus sistemas de cómputo, incluyendo, pero no limitándose a, grupos de chat, y de noticias, revisión de material bajado de Internet, monitoreo de sitios visitados en Internet, revisión del correo enviado, recibido por los usuarios y localización de los equipos.

9.10.3 Bloqueo de contenido inapropiado

La Empresa utiliza software para identificar y bloquear sitios de internet con material inadecuado, violento y sexualmente explícito. En el evento, que el Usuario encuentre este tipo de material en Internet, deberá desconectarse del sitio en forma inmediata, sin importar si el sitio ha sido bloqueado o no por el software.

9.11 Correo electrónico

El correo electrónico se ha convertido rápidamente en uno de los métodos de comunicación más importantes entre funcionarios, clientes, proveedores, contratistas y consultores. Con el fin de maximizar el beneficio y minimizar los riesgos asociados, la Organización, ha creado las siguientes pautas. Tener en cuenta que estas pautas no han sido diseñadas para desalentar la utilización de este, sino más bien para asegurar su uso con responsabilidad y discreción:

9.11.1 Comunicaciones electrónicas como privadas o seguras

El correo electrónico puede ser almacenado en un número indefinido de computadores y copias de sus mensajes pueden ser reenviados a otros, ya sea electrónicamente o en papel. Así mismo, correo electrónico enviado a usuarios inexistentes o equivocados implica que este correo sea de conocimiento de terceras personas

9.11.2 Precaución antes de enviar un mensaje

Al redactar un correo electrónico es importante utilizar el mismo cuidado y discreción que se utiliza en otros tipos de comunicación escrita. Una característica, y peligro, del correo electrónico es que es tratado de más informalmente que otro medio de comunicación de negocios. Cualquier correo o documento creado o almacenado en un computador puede, y probablemente, ser revisado por otros.

9.11.3 Material inapropiado

No se podrá enviar por correo electrónico material de carácter fraudulento, que pueda llegar a generar sentimientos de acoso u hostigamiento a juicio de la Organización, o que por su naturaleza sea embarazoso, sexualmente explícito, difamatorio, ilegal o inapropiado. Si un Usuario encuentra este tipo de material deberá reportarlo a su jefe inmediato

9.11.4 Alteraciones

Nunca deberá alterar la línea “De” (autor del correo) u otra información relacionada con los atributos de origen del correo electrónico. Mensajes anónimos o cuasi - anónimos están prohibidos.

9.11.5 Pie de página

El siguiente pie de página debe incluirse en cada mensaje enviado fuera de la Empresa:

Estimado Cliente, contáctenos en nuestro proceso de Servicio al Cliente: E-MAIL: servicioalcliente@abcrepecev.com, Tel: (57) 321 4509481. El contenido de este mensaje no puede ser interpretado como asesoría puntual. Si recibe este mensaje por error, por favor comunicarlo al remitente y eliminarlo. El presente e-mail no constituye aceptación de la oferta comercial, ni promesa de celebrar contrato u orden de compra, la aceptación de esta incluirá la respectiva orden del bien o servicio por separado, según el art. 851 del Código de Comercio. Esta organización no se hace responsable de las alteraciones que pudieran hacerse al mensaje una vez enviado. Consulte nuestras políticas y tratamiento de la información en https://abcrepecev.com/services-grid, donde se podrá visualizar la política de tratamiento de información.

9.12 Devolución de activos

Devolver todos los activos de información (correo, equipos de cómputo, información electrónica, archivos Excel, Word, información física, etc.) y activos informáticos de la Organización que estén en su posesión o bajo su responsabilidad al final del cumplimiento de sus labores, ya sea por terminación del contrato, cambio de área u obligaciones, ya que, estos activos son de propiedad de la Organización.

Eliminar la información de los medios que contengan información confidencial o clasificada mediante técnicas de borrado seguro; en caso de que los activos informáticos presenten daños parciales o totales por mala manipulación, el proceso de TI reportará estos eventos al área de recursos humanos con el diagnóstico del daño

9.13 Uso de la inteligencia artificial (IA)

La inteligencia artificial (IA) desempeña un papel muy importante en la actualidad, generando un efecto cambiante en la forma de generar tareas y procesos de manera automática, es de suma importancia que los sistemas de IA se hayan creado para proporcionar una experiencia útil, segura y de confianza para todos, por tal motivo la Organización toma las siguientes medidas:

Se prohíbe a todos los usuarios el uso de todo activo de información CONFIDENCIAL y CLASIFICADA perteneciente a la Organización, en cualquier plataforma digital, aplicativo, chat, etc., de inteligencia artificial (IA), para garantizar la privacidad y protección de información.

Se debe dar un uso responsable a las herramientas de IA para la generación de contenido respetando la normatividad vigente sobre la protección de derechos de autor (Ley 1915 de 2018)

10 DOCUMENTOS RELACIONADOS

- Ley 23 de 1982: Sobre derechos de autor.
- Arts. 238, 288 y 289 del Código penal
- Ley 1915 de 2018: se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- ISO/IEC 27001: 2022 Sistema de gestión en Seguridad de la información

ELABORÓ:	**REVISÓ:**	**APROBÓ:**
Luis Miguel Zocadagui Diaz	James Patiño	John Miranda
CARGO: Analista en Infraestructura, Seguridad y Compliance	**CARGO:** Jefe Service Delivery, Infraestructura y Seguridad	**CARGO:** Gerente IT