Política de Seguridad de la Información

Gerencia General
Corredores Viales S.A.

corredores viales

corredores viales	TIPO DE DOCUMENTO	CÓDIGO
	POLÍTICA	PSI–GG–04
	TÍTULO DEL DOCUMENTO	VERSIÓN
Área responsable	SEGURIDAD DE LA INFORMACIÓN	01
Gerencia General		APROBACIÓN
		29/08/2023

1. INTRODUCCIÓN:

La información es un activo que, como otros bienes y servicios requeridos para el cumplimiento de los objetivos de la empresa, resulta esencial para el desarrollo de las actividades de competencia. En consecuencia, necesitará ser protegida adecuadamente.

Dicha información puede presentarse en diversos formatos (impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos o como contenido multimedial, entre otros). Por lo tanto, y sin perjuicio del formato en que se encuentre y del soporte que se utilice, deberá estar apropiadamente protegida desde su creación, durante todo su ciclo de vida y hasta su eventual destrucción, desuso o archivo definitivo.

La seguridad de la información es la protección de la información de un rango amplio de amenazas, con el objeto de minimizar los riesgos a los que se encuentra expuesta y asegurar la continuidad de la operación normal de la empresa. Tiene por objetivos la preservación de la confidencialidad, integridad y disponibilidad de la información.

Dicho estado de protección adecuada se logrará implementando un conjunto de mecanismos de seguridad o controles que incluirán, entre otros, procesos, políticas, procedimientos, estructuras organizacionales, software y hardware. Se necesitará establecer, implementar, monitorear, revisar y mejorar estos mecanismos para fortalecer el cumplimiento de los objetivos de seguridad específicos. Esto se deberá realizar en forma coordinada con otros procesos de gestión de la organización.

Del mismo modo, los procesos, sistemas y redes de apoyo también son activos importantes. Definir, lograr, mantener y mejorar la seguridad de la información será esencial para preservarlos, mantener la eficacia en la operación, cumplir con el marco legal y las normas internas, y preservar la imagen institucional de la Empresa Pública y del Estado Nacional en su conjunto.

La empresa, como cualquier organización, enfrenta amenazas de seguridad en sus sistemas y redes de información, cada vez más frecuentes y sofisticadas. La seguridad de la información será importante para el desarrollo de actividades y para proteger las infraestructuras críticas de información que proveen servicios esenciales.

La impresión del presente documento se considera como COPIA NO CONTROLADA.

Para asegurarse sobre la versión y actualización del documento, comuníquese con el Responsable de Calidad y siempre tenga presente tomar el mismo de la CARPETA DEL SISTEMA definida para tal fin.

El presente es un documento de carácter CONFIDENCIAL. Queda prohibida su divulgación a terceros sin autorización expresa de la empresa CVSA

2. OBJETIVO:

La presente Política de Seguridad de la Información –en adelante, PSI– establece las directrices y líneas de actuación en materia de seguridad de la información que establecen el modo en que la empresa deberá gestionar y proteger los datos a los que dé tratamiento, los recursos tecnológicos que utilice y los servicios que brinde. Detalla también lineamientos respecto a la comunicación e implementación de esta Política a los funcionarios y empleados bajo cualquier modalidad de contratación y demás involucrados internos y externos.

El objetivo principal de esta PSI es definir el propósito, la dirección, los principios, las reglas básicas y los mecanismos de comunicación para la protección de la información de la empresa, así como de los recursos utilizados en su tratamiento.

Una adecuada gestión de la seguridad de la información permitirá proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad de la información, así como el cumplimiento de las normas aplicables.

3. ALCANCE:

Esta PSI será aplicable en todo el ámbito de la organización, a sus recursos y a la totalidad de los procesos, ya sean internos o externos, vinculados a la entidad a través de contratos o acuerdos con terceros.

La misma deberá ser comunicada fehacientemente y cumplida por todos los funcionarios y agentes que forman parte de la organización. Se encontrarán comprendidos en su alcance tanto el personal que desempeñe funciones directivas, como administrativas o técnicas, cualquiera sea su vínculo/relación contractual, su nivel jerárquico, su situación de revista y las tareas que desempeñe.

Asimismo, deberá ser conocida y cumplida por todas aquellas personas, ya sean internas o externas, vinculadas a la entidad a través de contratos, convenios, acuerdos o cualquier otro instrumento válido para establecer la relación con terceros, en la medida en que les sea aplicable y en las secciones que le correspondan.

La impresión del presente documento se considera como COPIA NO CONTROLADA.

Para asegurarse sobre la versión y actualización del documento, comuníquese con el Responsable de Calidad y siempre tenga presente tomar el mismo de la CARPETA DEL SISTEMA definida para tal fin.

El presente es un documento de carácter CONFIDENCIAL. Queda prohibida su divulgación a terceros sin autorización expresa de la empresa CVSA

4. PRINCIPIOS BÁSICOS:

Los principios de la seguridad de la información serán la **confidencialidad, la integridad y la disponibilidad de la información** a la que le dan tratamiento y de los activos de información utilizados para su gestión. La protección de los derechos de los titulares de los datos personales procesados, así como de la información propia de la empresa, será el objetivo central de esta PSI.

Los contenidos de este documento estarán alineados y se complementarán con el resto de las políticas y normativas internas de la organización, que entenderá la importancia de gestionar eficazmente la seguridad de la información. En consecuencia, esta última declara su compromiso y total apoyo a la gestión de la seguridad de la información como parte integrante de la gestión del resto de los procesos establecidos en su ámbito.

Asimismo, sus autoridades se comprometerán a liderar la mejora continua de los procesos de gestión de seguridad de la información, asegurando su eficacia y eficiencia.

En el mismo sentido, la empresa se comprometerá a cumplir con la normativa legal y reglamentaria aplicable a todos los niveles, así como a adaptarse a futuras normas y requisitos del contexto interno o externo y a aquellos que emanen de la vinculación con terceros involucrados.

El incumplimiento de esta política tendrá como resultado la aplicación de sanciones disciplinarias, conforme a la magnitud y característica del aspecto no cumplido, de acuerdo con la normativa aplicable.

Al respecto, y de acuerdo con la normativa vigente, se establecerá como falta el incumplimiento de los lineamientos y disposiciones de esta PSI, por parte de los agentes y funcionarios. Para ello, se establecerá una graduación en las responsabilidades y sanciones administrativas que se aplicarán de acuerdo con la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.

La empresa establecerá sus requisitos de seguridad de la información en base a la evaluación y posterior gestión de riesgos de seguridad sobre sus activos de la información.

La impresión del presente documento se considera como COPIA NO CONTROLADA.

Para asegurarse sobre la versión y actualización del documento, comuníquese con el Responsable de Calidad y siempre tenga presente tomar el mismo de la CARPETA DEL SISTEMA definida para tal fin.

El presente es un documento de carácter CONFIDENCIAL. Queda prohibida su divulgación a terceros sin autorización expresa de la empresa CVSA

5. GLOSARIO:

Seguridad de la Información: la seguridad de la información se entenderá como la preservación de las siguientes características principales:

- **Confidencialidad:** se asegurará que la información sea accesible sólo a aquellas personas autorizadas.
- **Integridad:** se salvaguardará la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se asegurará que los usuarios autorizados tengan acceso a la información y a los recursos relacionados, toda vez que lo requieran.

6. REVISIÓN Y ACTUALIZACIÓN:

La empresa: la organización se comprometerá a revisar esta PSI anualmente, adaptándola a nuevas exigencias organizativas o del entorno, así como a comunicarla a su planta de personal y a los terceros involucrados. También dispondrá las medidas necesarias para que esté a disposición de los alcanzados en todo momento.

Adicionalmente, la organización procederá a llevar a cabo su revisión y eventual modificación, cada vez que se produzca un cambio significativo en la plataforma tecnológica, una modificación de la normativa vigente aplicable, un cambio en los objetivos estratégicos de la empresa o cualquier otro evento que lo amerite.

7. LINEAMIENTOS ESPECÍFICOS:

7.1– Organización de la Seguridad de la Información:

La empresa le asignará a la Gerencia de Innovación, Planificación y Control las responsabilidades relativas a la seguridad de la información, que tendrá a su cargo la coordinación de todas las actividades tendientes a la implementación de la presente PSI. Dicha unidad organizativa velará por una adecuada segregación de funciones, por un abordaje de la seguridad de la información en todos los proyectos y programas de la empresa y por el establecimiento de adecuados procedimientos de seguridad, en base a un plan de tratamiento de riesgos.

Las autoridades de la empresa se comprometerán a impulsar las iniciativas que el área competente proponga, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información que gestione. Asimismo, requerirá a las áreas competentes la inclusión en contratos, Términos de Referencia o instrumentos similares, de cláusulas que contemplen el cumplimiento de la presente PSI.

La impresión del presente documento se considera como COPIA NO CONTROLADA.

Para asegurarse sobre la versión y actualización del documento, comuníquese con el Responsable de Calidad y siempre tenga presente tomar el mismo de la CARPETA DEL SISTEMA definida para tal fin.

El presente es un documento de carácter CONFIDENCIAL. Queda prohibida su divulgación a terceros sin autorización expresa de la empresa CVSA

7.2– Seguridad Informática de los Recursos Humanos:

El personal será considerado un recurso central para la protección de la información, motivo por el cual deberá ser adecuadamente entrenado en caso del personal técnico y concientizado a través de programas específicos, para quienes no realicen actividades de ese tenor. A tal fin, se establecerán las medidas necesarias en los procesos de selección de personal, durante la vinculación laboral y al momento de la desvinculación, pudiendo inclusive excederlo. En todo momento, se protegerán los derechos individuales de los empleados, especialmente aquellos relacionados con la privacidad.

Se establecerá la obligatoriedad de la suscripción de compromisos de confidencialidad en función de las responsabilidades que correspondan y a las funciones que se desarrollen. Los permisos de acceso serán otorgados en función de cada perfil de trabajo y se deberán mantener actualizados.

7.3– Gestión de Activos:

La gestión y protección efectiva de los activos en función de su clasificación por criticidad será una prioridad para la empresa. Entre los activos se incluirán tanto el hardware como el software y los dispositivos de comunicación, los elementos de apoyo, la información y los datos en sí mismos, cualquiera sea el soporte y formato en el que se encuentren.

Para la clasificación, se tendrán en cuenta la confidencialidad, integridad y disponibilidad de los datos, así como las funciones que soporta el activo y la normativa aplicable.

Se llevarán inventarios actualizados y se exigirá a todos los agentes y funcionarios, que sean desvinculados, la devolución de los activos de información en su poder. En el mismo sentido, se procederá a una destrucción segura de cualquier medio que pueda contener información crítica o datos personales, para lo cual, se contará con procedimientos adecuados.

La impresión del presente documento se considera como COPIA NO CONTROLADA.

Para asegurarse sobre la versión y actualización del documento, comuníquese con el Responsable de Calidad y siempre tenga presente tomar el mismo de la CARPETA DEL SISTEMA definida para tal fin.

El presente es un documento de carácter CONFIDENCIAL. Queda prohibida su divulgación a terceros sin autorización expresa de la empresa CVSA

7.4– Autenticación, autorización y control de Acceso:

La empresa adoptará los mecanismos necesarios para que solo el personal autorizado acceda a los activos de información, bajo la premisa básica de que **"Todo está prohibido a menos que se permita expresamente"** para aquellos activos considerados críticos. El acceso a la información se establecerá en base a la **"necesidad de saber"**, es decir que quienes accedan deben tener un motivo válido para hacerlo en razón de su rol y/o funciones y usando una política de **"Mínimo Privilegio"**. Estos privilegios se otorgan en forma expresa, son autorizados por los niveles competentes y se gestionan adecuadamente las altas y bajas de las cuentas y permisos de acceso, con revisiones periódicas. Se requiere a los empleados, funcionarios y demás usuarios, el uso responsable de los dispositivos y datos de autenticación otorgados por la empresa para el cumplimiento de sus funciones, que no los compartan y que los mantengan siempre seguros, tanto dentro como fuera de la empresa.

7.5– Uso de herramientas criptográficas:

Se utilizarán sistemas y técnicas criptográficas para la protección de la información de la empresa, con el fin de preservar su confidencialidad, integridad, autenticidad y no repudio, tanto para su almacenamiento como para su transmisión.

Para ello, se requerirá el cifrado de toda la información crítica, especialmente cuando ésta se transmita fuera de la empresa o se encuentre contenida en medios de almacenamiento que se trasladen fuera de la organización. Asimismo, se protegerán las claves criptográficas durante todo su ciclo de vida y se utilizarán certificados digitales válidos en los sitios web institucionales.

7.6– Seguridad física y ambiental:

La empresa protegerá sus instalaciones y activos físicos, incluyendo sus puestos de trabajo, en función de la criticidad de la información que éstos gestionen, mediante el establecimiento de perímetros de seguridad, áreas protegidas y controles ambientales, en la medida en que se considere necesario.

Además, se monitorearán los accesos físicos para permitir sólo ingresos y egresos debidamente autorizados y se mantendrá un registro actualizado de los activos físicos que procesan información. Se implementarán y harán cumplir medidas de seguridad para los activos físicos que deberán llevarse fuera de la empresa, manteniéndose el registro correspondiente.

La impresión del presente documento se considera como COPIA NO CONTROLADA.

Para asegurarse sobre la versión y actualización del documento, comuníquese con el Responsable de Calidad y siempre tenga presente tomar el mismo de la CARPETA DEL SISTEMA definida para tal fin.

El presente es un documento de carácter CONFIDENCIAL. Queda prohibida su divulgación a terceros sin autorización expresa de la empresa CVSA

7.7– Seguridad operativa:

Las operaciones de la empresa se desarrollarán en forma segura, en todas las instalaciones de procesamiento de información, asignándose las debidas responsabilidades y desarrollando procedimientos acordes. Se adoptarán medidas para minimizar los riesgos de acceso y cambios no autorizados o pérdida de información y para proteger las instalaciones y plataformas tecnológicas contra infecciones de código malicioso.

Las vulnerabilidades serán gestionadas de manera apropiada y se controlará la actividad de administradores y operadores.

7.8– Seguridad de las comunicaciones:

La empresa adoptará las medidas necesarias para proteger adecuadamente la información que se comunique por sus redes informáticas y para minimizar los riesgos que pudieran afectar la infraestructura de soporte. Toda información que se transfiera fuera de la empresa, incluyendo la que se transmitiera a través de los servicios de correo electrónico, será protegida de acuerdo con su nivel de criticidad.

Se asignarán cuentas institucionales a todos los empleados y funcionarios, quienes estarán obligados a utilizarlas para toda comunicación vinculada a sus funciones. Dicho personal será informado por sus respectivas autoridades sobre los riesgos de incumplir este requerimiento, y se les exigirá la firma de acuerdos de confidencialidad y no divulgación, en los casos en los que la empresa lo considere necesario.

7.9– Adquisición de sistemas, desarrollo y mantenimiento de sistemas de información:

La empresa adoptará las medidas de seguridad necesarias para proteger por defecto y desde el diseño todas las aplicaciones que se desarrollen internamente, utilizando una metodología de desarrollo seguro, e incorporará requerimientos y evaluaciones de seguridad en el proceso de contratación de aplicaciones a terceros. Esto se aplicará especialmente a aquellas que se utilicen para brindar servicios o realizar trámites por parte de la ciudadanía e involucren el tratamiento de datos personales.

La seguridad de las aplicaciones será evaluada antes de ponerlas productivas.

La impresión del presente documento se considera como COPIA NO CONTROLADA.

Para asegurarse sobre la versión y actualización del documento, comuníquese con el Responsable de Calidad y siempre tenga presente tomar el mismo de la CARPETA DEL SISTEMA definida para tal fin.

El presente es un documento de carácter CONFIDENCIAL. Queda prohibida su divulgación a terceros sin autorización expresa de la empresa CVSA

7.10– Relación con proveedores:

La empresa incluirá en los Pliegos de Bases y Condiciones Particulares cláusulas vinculadas a la seguridad de la información, de cumplimiento efectivo y obligatorio por parte los cocontratantes. Estas disposiciones considerarán los aspectos pertinentes a la protección de la información y los servicios que se brinden, desde el inicio del proceso contractual hasta su finalización. Los requisitos a incluir serán acordes a la criticidad de la información y los servicios, la evaluación de riesgos y el cumplimiento de todas las normas legales y contractuales aplicables.

7.11– Gestión de incidentes de seguridad:

La empresa adoptará las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información. Las debilidades en los procesos serán debidamente identificadas, comunicadas, y minimizadas de forma tal que se apliquen las acciones correctivas en el menor tiempo posible.

Cuando los empleados detectasen un evento que podría constituir un incidente de seguridad, lo deberán comunicar al Departamento de Soporte Técnico de la Subgerencia de Tecnologías de la Información. De producirse el incidente, y que éste hubiera afectado información o datos personales de terceros, la empresa informará públicamente tal ocurrencia, de acuerdo a lo dispuesto por la normativa vigente.

7.12– Aspectos de seguridad para la continuidad de la gestión:

Se contemplarán todos los aspectos de seguridad requeridos en los procedimientos de continuidad de la gestión de la empresa que se desarrollen, especialmente cuando se trate de información, servicios o sistemas críticos. Se realizará un análisis de impacto y se identificarán las ventanas de recuperación requeridas en los procesos críticos.

7.13– Cumplimiento:

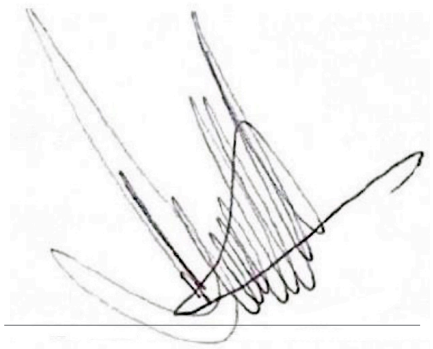
La empresa cumplirá las disposiciones legales, normativas y contractuales que le sean aplicables y promoverá el acatamiento de las políticas y normas de seguridad que se aprueben en su ámbito. En el mismo sentido, atenderá y dará cumplimiento a las recomendaciones correspondientes a los hallazgos de las auditorías internas y externas que sean realizadas, adoptando las medidas correctivas que correspondan.

La impresión del presente documento se considera como COPIA NO CONTROLADA.

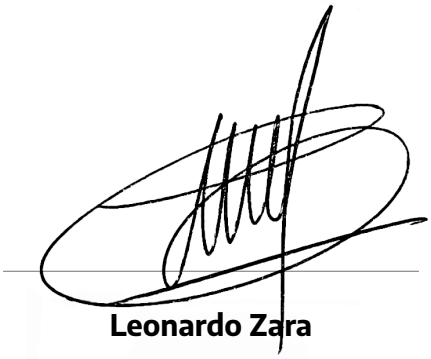
Para asegurarse sobre la versión y actualización del documento, comuníquese con el Responsable de Calidad y siempre tenga presente tomar el mismo de la CARPETA DEL SISTEMA definida para tal fin.

El presente es un documento de carácter CONFIDENCIAL. Queda prohibida su divulgación a terceros sin autorización expresa de la empresa CVSA

corredores viales	TIPO DE DOCUMENTO	CÓDIGO
	POLÍTICA	PSI–GG–04
	TÍTULO DEL DOCUMENTO	VERSIÓN
Área responsable	SEGURIDAD DE LA INFORMACIÓN	01
Gerencia General		APROBACIÓN
		29/08/2023



Daniel Moffa
Gerente de Innovación,
Planificación y Control



Leonardo Zara
Gerente General

La impresión del presente documento se considera como COPIA NO CONTROLADA.

Para asegurarse sobre la versión y actualización del documento, comuníquese con el Responsable de Calidad y siempre tenga presente tomar el mismo de la CARPETA DEL SISTEMA definida para tal fin.

El presente es un documento de carácter CONFIDENCIAL. Queda prohibida su divulgación a terceros sin autorización expresa de la empresa CVSA