carozzi

Política de

# Seguridad de la Información

La información que mantiene y gestiona la compañía, debe conservar su integridad, confidencialidad y disponibilidad para alcanzar los objetivos estratégicos del negocio.

Dado que la mayor parte de la información se procesa y distribuye a través de medios informáticos, se hace imprescindible que todos los colaboradores, contratistas, proveedores de servicio, entre otros, que trabajan o colaboran en la compañía, observen y adhieran a las normas de seguridad de la información, contribuyendo con su protección ante las variadas amenazas y vulnerabilidades existentes.

**Objetivo**

El objetivo de esta política es establecer los principios, lineamientos y normas para resguardar la información o activos de información (en adelante información) que son de propiedad de la compañía, en relación con su manipulación, envío, recepción, almacenamiento y distribución. Lo mismo aplica para la administración de información relacionada a terceros, que la compañía mantenga en sus sistemas que soportan sus procesos de negocio.

**Alcance**

Estarán sujetos al cumplimiento de esta política todos los colaboradores de Empresas Carozzi S.A. y subsidiarias nacionales e internacionales, así como terceros que presten servicios y accedan a los sistemas de información de la compañía.

La presente política está referida a toda la información que se genera, intercambia, transporta y almacena, ya sea en forma local o en la nube, alcanzando tanto al ámbito de las tecnologías de la información (TI) como al de tecnologías operacionales y/o industriales (TO). Asimismo, esta política aplica a toda la información de la compañía que se almacena y gestiona a través infraestructura provista por proveedores externos.

carozzi

Política de

# Seguridad de la Información

**Principios**

Es esencial que la compañía determine los requerimientos de seguridad de la información a través de estas tres fuentes:

I. La evaluación de riesgos de la organización, teniendo en cuenta su estrategia y objetivos generales de negocio, esto puede ser realizado a través de una evaluación específica de riesgos de seguridad de la información.

II. Los requerimientos legales, estatuarios, regulatorios y contractuales que la compañía y sus partes interesadas tienen que cumplir.

III. Objetivos y requerimientos de negocio, en todas las etapas del ciclo de vida de la información, que la compañía ha desarrollado para sostener su operación.

Por otra parte, los conceptos base que determinan la estrategia de seguridad de la Información son:

- **Confidencialidad:** Tiene como objetivo garantizar que la información almacenada o en tránsito sea accesible solo para personas o sistemas autorizados, protegiéndola contra la divulgación no autorizada y el uso indebido.

- **Integridad:** Tiene como objetivo garantizar la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada

- **Disponibilidad:** Su objetivo es asegurar la fiabilidad y el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados, es decir, que lo necesitan para desenvolver sus actividades.

carozzi

Política de

# Seguridad de la Información

## Clasificación de la información

La clasificación de la información es un proceso que ordena y dispone los activos de información por categorías que consideran diferentes niveles de protección para su almacenamiento, transmisión y/o divulgación. Dado lo anterior es que toda la información de la compañía deberá ser clasificada de acuerdo con la siguiente tabla:

| Clasificación | Descripción | Restricciones |
|---|---|---|
| **Confidencial** | Información sensible de la compañía que no pueden compartidos con personas no autorizadas. | Se debe disponer de autorización para compartir. |
| **Uso Interno** | Información de la compañía que no debe salir de la organización y que se utiliza para comunicaciones y gestión interna. | Los documentos o archivos solo pueden ser compartidos en forma interna. |
| **Pública** | Información de la compañía que puede ser compartida dado que se encuentra disponible al público ya sea en sitios web de la compañía o de terceros, u otros debidamente autorizados. | Ninguna. |

carozzi

Política de

# Seguridad de la Información

**Marco normativo y legal**

Esta política está basada en las buenas prácticas indicadas en la norma ISO 27.002, vigente a la fecha, por lo cual, se implementarán los controles que resulten aplicables, según las características del negocio y la gestión de riesgos corporativos.

Respecto de normativa legal, la compañía tiene el compromiso de velar por el cumplimiento de la legislación vigente en materia de protección de datos y seguridad de la información aplicable en sus procesos de negocio.

**Uso de tecnologías de inteligencia artificial**

La compañía reconoce el valor estratégico de las tecnologías de Inteligencia Artificial (IA) para mejorar la eficiencia operativa, la toma de decisiones y la innovación. No obstante, su uso debe alinearse con los principios establecidos por la compañía.

Tales principios aplican a todos los sistemas, servicios, modelos y herramientas de IA utilizados, desarrollados o integrados por la organización, ya sea internamente o a través de terceros.

En esta política se establece las directrices y controles para el uso seguro, ético y responsable de las herramientas y sistemas basados en Inteligencia Artificial (IA) por parte de todos los colaboradores de la organización.

carozzi

Política de

# Seguridad de la Información

Lineamientos de uso de la IA

- Toda solución de IA debe ser evaluada y autorizada por el equipo de Seguridad Informática.
- Prohibición estricta de introducir cualquier información de la compañía o de sus clientes en una herramienta de IA no autorizada.
- Prohibición estricta de utilizar una herramienta IA para fines laborales que no esté autorizada por la compañía.

Cumplimiento Normativo y Legal

- El uso de la IA no debe infringir leyes, regulaciones, derechos de autor, ni los principios éticos de la organización. Esto incluye la prohibición de crear contenido que sea discriminatorio, ofensivo, o que vulnere la privacidad de terceros.

**Responsabilidades**

La gestión efectiva de la seguridad de la información es una responsabilidad compartida por todos los colaboradores, por lo cual, se pide:

- Cumplir con los controles de seguridad que se establecen en la presente política.
- Reportar cualquier incidente de seguridad.
- Cumplir con las capacitaciones relativas a seguridad de la información que determine la compañía, ya sean cursos, charlas, correos, ejercicios u otros.
- Cumplir con lo establecido en el Reglamento interno de orden, higiene y seguridad.
- Velar por el resguardo en términos de la confidencialidad, integridad y disponibilidad de la información de la compañía.

carozzi

Política de

# Seguridad de la Información

**Controles de seguridad de la información**

Colaboradores

- Mantener bajo resguardo las claves de ingreso de todos los sistemas, especialmente SAP, dado el carácter personal, confidencial e intransferible que revisten las autorizaciones de acceso.
- Hacer uso responsable de su equipo y aplicaciones que se instalen, las cuáles deben estar autorizados por la Empresa.
- Mantenerse alerta a correos sospechosos, cumplir con las recomendaciones instruidas por la compañía.
- No registrar el correo electrónico corporativo en sitios o servicios que no tengan relación con el trabajo (Facebook, LinkedIn, Twitter, bancos, etc.).
- No utilizar el reenvío de correos a cuentas personales.
- Visitar únicamente sitios web confiables y considerar el uso criterioso de internet, ya sea a través del computador asignado o a través del celular corporativo, en caso de que haya sido otorgado por la compañía.
- No se podrá utilizar ninguna herramienta intrusiva (hacking) u otra, con el objetivo de descifrar contraseñas o descubrir vulnerabilidades.
- Utilizar sólo aplicaciones o software validados por el área de informática, sin descargar ni instalar programas desde fuentes desconocidas o no autorizadas.
- Evitar la conexión a redes wifi-públicas o a conexiones inalámbricas desconocidas.
- No revelar, directa ni indirectamente, información de la empresa, sus clientes o proveedores, que no sea de conocimiento público.

**Compañía**

- Los controles de esta política estarán circunscritos a los dominios definidos en la norma ISO 27.001. Cada uno de estos controles serán desarrollados a través de normativas específicas en cada uno de los dominios de control.