

	<p align="center">POLÍTICA DE LA SEGURIDAD DE LA INFORMACION</p>	<p>Código: SGC-RRHH-09</p>
<p>Versión: 01</p>		<p>Fecha: 12/02/2025</p>

El objetivo de esta política es establecer los principios, directrices y responsabilidades relacionadas con la seguridad de la información en **BC Tecnología Perú S.A.C.**, garantizando la confidencialidad, integridad y disponibilidad de la información manejada por la empresa, sus empleados, proveedores y clientes.

Alcance:

Esta política aplica a todas las personas dentro de la organización, incluyendo empleados, contratistas, proveedores y cualquier otra parte que acceda, maneje o controle la información de la empresa. Asimismo, se extiende a todos los sistemas informáticos, aplicaciones, bases de datos, infraestructuras tecnológicas y procesos operativos utilizados para almacenar, procesar y transmitir información.

1. Principios Fundamentales de Seguridad de la Información:

- **Confidencialidad:** Garantizar que la información solo sea accesible a aquellos que tengan autorización para hacerlo, protegiendo datos sensibles y confidenciales, tanto internos como externos.
- **Integridad:** Asegurar que la información sea precisa y esté completa, protegiéndola contra alteraciones no autorizadas.
- **Disponibilidad:** Asegurar que la información esté accesible cuando sea necesario, evitando la pérdida de datos o interrupciones en los sistemas críticos de la empresa.
- **Autenticidad:** Garantizar que la información y las transacciones sean verificables y legítimas.
- **Responsabilidad:** Todos los empleados y partes involucradas deben estar al tanto de su responsabilidad en la protección de la información, asegurándose de seguir las normativas y buenas prácticas establecidas.


2. Gobernanza y Responsabilidad:

La seguridad de la información es responsabilidad de todos los empleados de **BC Tecnología Perú S.A.C.**, sin embargo, el **Responsable de Seguridad de la Información** (CISO, o equivalente) tendrá la responsabilidad primaria de coordinar, implementar y mantener las políticas y medidas de seguridad en la empresa.

3. Clasificación de la Información:

La información debe ser clasificada según su nivel de sensibilidad, de acuerdo con las siguientes categorías:

- **Información confidencial:** Información sensible que, si se divulga o pierde, podría causar un daño grave a la empresa, sus clientes o sus empleados.
- **Información interna:** Información relevante para las operaciones internas de la empresa que no es pública, pero cuyo acceso está restringido a ciertos grupos dentro de la organización.
- **Información pública:** Información que puede ser compartida sin restricciones y que no compromete la seguridad de la empresa.

	<p style="text-align: center;">POLÍTICA DE LA SEGURIDAD DE LA INFORMACION</p>	<p>Código: SGC-RRHH-09</p>
<p>Versión: 01</p>		<p>Fecha: 12/02/2025</p>

4. Control de Acceso a la Información:

- Los accesos a los sistemas y la información de la empresa deben ser autorizados, autenticados y auditados.
- La asignación de permisos debe estar basada en el principio de **mínimo privilegio**, es decir, cada usuario debe tener acceso solo a la información necesaria para realizar su trabajo.
- Se deben usar mecanismos de autenticación robustos, como contraseñas fuertes y sistemas de autenticación multifactor (MFA).

5. Protección de Datos y Privacidad:

La empresa se compromete a proteger la privacidad de los datos personales de sus clientes, empleados y cualquier otra persona cuya información se maneje. Esto incluye cumplir con las leyes y regulaciones aplicables, como la **Ley de Protección de Datos Personales** en Perú y otros estándares internacionales como el **GDPR** (Reglamento General de Protección de Datos de la Unión Europea) cuando corresponda.

6. Gestión de Incidentes de Seguridad:


En caso de un incidente de seguridad de la información (como pérdida de datos, acceso no autorizado o violación de la seguridad), **BC Tecnología Perú S.A.C.** tiene procedimientos establecidos para:

- Detectar, contener y mitigar el impacto del incidente de manera oportuna.
- Notificar a las partes interesadas y autoridades pertinentes, cuando sea necesario.
- Realizar investigaciones forenses para determinar las causas y tomar medidas correctivas.
- Revisar y mejorar las políticas de seguridad para evitar incidentes futuros.

7. Uso Aceptable de los Recursos Tecnológicos:

Los empleados deben usar los sistemas de la empresa y recursos tecnológicos de manera ética, legal y conforme a las políticas de la organización. Esto incluye:

- No utilizar equipos de la empresa para actividades personales que pongan en riesgo la seguridad de la información.
- No instalar software no autorizado ni acceder a contenido no relacionado con el trabajo.
- Respetar las políticas de uso de contraseñas y seguridad de la red.

	POLÍTICA DE LA SEGURIDAD DE LA INFORMACION	Código: SGC-RRHH-09
Versión: 01		Fecha: 12/02/2025

8. Capacitación y Concienciación en Seguridad:

BC Tecnología Perú S.A.C. implementará programas regulares de capacitación en seguridad de la información para todos los empleados, con el fin de:

- Asegurar que todos comprendan la importancia de la seguridad de la información y las mejores prácticas para protegerla.
- Estar al tanto de las amenazas actuales, como el phishing, el malware, y otras vulnerabilidades.
- Reforzar el cumplimiento de las políticas de seguridad de la información.

9. Evaluación y Mejora Continua:

La seguridad de la información será evaluada de manera continua mediante auditorías internas y externas, pruebas de penetración y análisis de vulnerabilidades. Con base en estos resultados, se tomarán acciones correctivas y preventivas para mejorar las medidas de seguridad de la empresa.

10. Cumplimiento Legal y Normativo:

La empresa se compromete a cumplir con todas las leyes, regulaciones y normativas aplicables relacionadas con la seguridad de la información, tanto a nivel nacional como internacional. Esto incluye la **Ley de Delitos Informáticos** en Perú, normativas sobre protección de datos personales y otras leyes pertinentes.

En BC Tecnología Perú S.A.C., entendemos que la seguridad de la información es crucial para el éxito de nuestras operaciones y la confianza de nuestros clientes. Nos comprometemos a implementar y mantener una cultura de seguridad robusta, garantizando la protección de la información sensible y la continuidad de nuestros servicios tecnológicos de manera responsable y ética.



German José Martin
Berrios Fernández Concha