1. RESUMEN

Esta política permitirá sensibilizar a los colaboradores de la organización sobre los criterios de Seguridad en el intercambio de Información, tanto dentro como fuera de la organización, garantizando los principios de confidencialidad, disponibilidad e integridad de la misma.

2. OBJETIVO

El objetivo de este documento es establecer y especificar los lineamientos, políticas y procedimientos para la transferencia de información, con el fin de reducir el riesgo de fuga o pérdida de información confidencial, restringida o sensible que pertenece a la organización.

3. ALCANCE

Esta política se aplica al intercambio de información contenida en los activos de información de la organización. Todos los empleados, colaboradores, contratistas, consultores, temporales y demás trabajadores de la organización son responsables de hacer un uso adecuado y tratamiento de dicha información, en cumplimiento con las políticas, leyes y regulaciones locales y las directrices establecidas por la organización.

4. POLÍTICA

La política y los procedimientos de intercambio de información tienen como objetivo establecer los procedimientos y controles para el intercambio de información a través de diversos servicios de comunicación. En otras palabras, busca crear directrices y consideraciones para el intercambio de información dentro de la organización, entre organizaciones y con terceros. Además, este intercambio debe estar regulado y cumplir con las leyes y normativas aplicables, asegurando así una protección adecuada de la información.

4.1 NORMAS GENERALES APLICABLES A LA TRANSFERENCIA DE INFORMACIÓN

4.1.1 NORMA N°1: INTERCAMBIO DE INFORMACIÓN EN MEDIOS FÍSICOS O LÓGICOS

Es fundamental que, durante el transporte físico o lógico de la información de la organización, ya sea en medios informáticos, esta esté protegida contra accesos no autorizados, usos indebidos o posibles alteraciones. Para ello, se deben considerar las siguientes pautas:

- Siempre utilizar medios de transporte confiables para el intercambio o traslado de información en dispositivos físicos.
- Los equipos físicos que almacenan la información a trasladar deben estar adecuadamente protegidos contra posibles daños físicos durante el transporte. Es obligatorio embalar y proteger correctamente los activos de información con el material adecuado.
- En el caso de dispositivos extraíbles o discos duros que sean trasladados por los colaboradores, estos deben ser cifrados previamente con un sistema de cifrado de disco, como el PGP (Pretty Good Privacy). Sólo el colaborador y el administrador del sistema tendrán las claves privadas para descifrar la información.
- Los empleados de la organización no deben divulgar información confidencial o sensible de la organización o de sus clientes. Esto incluye el uso de teléfonos, correo electrónico, dispositivos extraíbles o cualquier otro canal de comunicación.
- La información confidencial relacionada con los clientes que estos soliciten será entregada en formato impreso y enviada a la oficina correspondiente. Además, la organización tendrá un repositorio de acceso restringido con la información de

cada cliente, el cual podrá ser consultado por el cliente a través de un acceso de doble autenticación: usuario/clave y un mensaje de texto con un ID aleatorio enviado al teléfono registrado del cliente.

- Los empleados no deben dejar mensajes con información sensible o confidencial en buzones de voz o contestadores automáticos, ya que estos pueden ser escuchados por personas no autorizadas.

4.1.2 NORMA N°2: RESPONSABILIDAD DEL PERSONAL

El uso indebido en la transferencia de información que resulte en la fuga de datos confidenciales o restringidos de la organización o de sus clientes será sujeto a:

- Sanciones que podrían incluir la terminación del contrato laboral.
- La organización quedará exenta de cualquier responsabilidad por las acciones legales que se deriven, de acuerdo con las leyes vigentes aplicables.

5. CUMPLIMIENTO DE POLÍTICA

5.1 MEDICIÓN DEL CUMPLIMIENTO

La organización realizará un seguimiento y verificación del cumplimiento de esta política mediante una variedad de métodos, incluyendo:

- Visitas periódicas
- Monitoreo de video
- Informes generados por herramientas comerciales
- Auditorías internas y externas
- Inspecciones

Los resultados de estas actividades serán comunicados al propietario de la política y al gerente de la unidad de negocio correspondiente, con el fin de garantizar el cumplimiento y la mejora continua de la política.

5.2 EXCEPCIONES

Cualquier excepción a esta política deberá ser sometida a aprobación previa por parte del Gerente de área correspondiente y el Grupo Interdisciplinario de Seguridad de la Información (GISI), quienes evaluarán y autorizarán las excepciones de acuerdo con las necesidades y riesgos de la organización.

5.3 INCUMPLIMIENTO

Cualquier empleado que incumpla o viole esta política estará sujeto a medidas disciplinarias, que pueden incluir desde advertencias hasta el despido, dependiendo de la gravedad de la infracción y la discreción de la organización.

6. APROBACIÓN

Elaborado por	Verificado por	Aprobado por
Nombre **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: