

	DOCUMENTO DE SEGURIDAD	Código: POTISegDatV01
		Versión: 01
		Fecha : 12/03/2025
		Página: Página 1 de 8

DOCUMENTO DE SEGURIDAD

ÍNDICE

1.	OBJETIVO.....	2
2.	ALCANCE	2
3.	LINEAMIENTOS.....	2
4.	CONTROL DE VERSIONES	¡Error! Marcador no definido.

1. OBJETIVO

Proporcionar lineamientos para una adecuada gestión de la seguridad de la información, así como para la implementación de medidas debidamente alineadas a los estándares y buenas prácticas con la finalidad de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la organización.

2. ALCANCE

Es aplicable a todos los trabajadores que prestan su servicio a la empresa, clientes y proveedores que utilicen los recursos o información que sean propiedad de la organización.

3. LINEAMIENTOS

- La Política de Seguridad de la Información y sus documentos relacionados son revisados y actualizados por lo menos una vez al año o cuando ocurren cambios significativos, asegurando su idoneidad y adecuación.
- La Política es comunicada, entendida e implementada en toda la organización y es de conocimiento por las partes interesadas.
- Todo colaborador notifica los incidentes de seguridad de la información conforme a los canales de comunicación establecidos.
- Todo acceso y salida de la información a través de dispositivos portátiles de almacenamiento, como discos duros externos, dispositivos USB y demás dispositivos de almacenamiento externo, así como a través del correo electrónico, se encuentran sujetos a un control y su cumplimiento es de acuerdo a un análisis y evaluación de riesgos.
- Todos los servicios de tecnología de la información se encuentran sujetos a monitoreo y en caso de detectarse un mal uso o abuso de los sistemas por parte de los trabajadores, estos últimos serán sancionados de acuerdo a la falta.

Identificación y Descripción del banco de datos personales

Deltron ha implementado esta política de Seguridad para salvaguardar los datos personales que maneja en cumplimiento con la Ley N°29733 - Ley de Protección de Datos Personales y su reglamento correspondiente, garantizando la seguridad y confidencialidad de los datos personales procesados sea de clientes, proveedores o personal directo, así como los derechos fundamentales de los titulares de los datos.

De acuerdo con el artículo 47, Deltron reconoce la importancia de adoptar medidas de seguridad para prevenir y mitigar el acceso no autorizado, la alteración, destrucción o pérdida de datos personales, asegurando que esta información se mantenga en condiciones de confidencialidad. Resaltando que la data está salvaguardada en los ordenadores ubicados en las instalaciones internas de Deltron.

Funciones y Obligaciones del personal

De acuerdo con el artículo 47 de la Ley N° 29733, la responsabilidad de implementar medidas de seguridad recae en Deltron como responsable del tratamiento de los datos personales. Las responsabilidades se designan de la siguiente manera:

1. Oficial de Protección de Datos: Es el encargado de asesorar y supervisar el cumplimiento de la Ley de Protección de Datos, así como el correcto funcionamiento e implementación de seguridad según corresponda.
2. Titular del Banco de Datos: Aplica medidas tecnológicas para contener el incidente de seguridad y reporta a la Autoridad Nacional de Protección de Datos Personales y a los afectados.
3. Responsable del área afectada: Notifica el incidente y coopera en la mitigación.

Todos los accesos a los recursos de información están basados en la necesidad y perfil de puesto del usuario, razón por la cual se toman en cuenta los siguientes aspectos:

- ✓ Acceso basado en grupos y roles.
- ✓ Segregación de roles de control de acceso.
- ✓ Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.

- ✓ Requisitos para la autorización formal de las solicitudes de acceso.
- ✓ Administración de derechos de acceso privilegiado.
- ✓ Revisión periódica de los controles de acceso.
- ✓ Revocación de los derechos de acceso.
- ✓ Control de acceso a correo electrónico.
- ✓ Control de Acceso y salida de información realizada a través de dispositivos USB, disco duro externo, y demás periféricas de almacenamiento externo, VPN, Anydesk según acceso dependiendo del cargo del personal y/o autorización por parte de su jefe a cargo.

El acceso a la red corporativa es controlado mediante políticas de seguridad aplicadas según perfiles de usuario para los colaboradores y personal externo, además los colaboradores bloquean el equipo cada vez que se retiren de su puesto de trabajo de forma manual.

Estructura de los bancos de datos y descripción de los sistemas de información

Se ha establecido una clasificación para la información la misma que puede ser tratada como confidencial, interna o pública, conforme lo establecido a continuación:

- ✓ Confidencial: Esta información, por su grado de sensibilidad para la organización, puede generar pérdidas económicas, problemas legales o daños al derecho de la privacidad y datos personales (trabajadores, proveedores o clientes). Cualquier persona u organización que solicite acceder a este tipo de información deberá solicitarlo por los canales de comunicación establecidos y la organización determinará si puede ser revelada de conformidad con la normatividad vigente.
- ✓ Interna: Es la información que genera, utiliza y controla la organización continuamente. Las atribuciones de generación, modificación y eliminación están limitadas de acuerdo a las funciones o roles de cada colaborador. Este tipo de información también puede ser compartida con las partes interesadas según lo crea conveniente el coordinador de área. Por ello, cada colaborador tiene la responsabilidad de

custodiar la seguridad de la información concedida en cualquier medio de soporte (digital o físico).

- ✓ Pública: Es la información que la organización considera que sea de conocimiento interno y externo.

Para el caso de Deltron, la misma empresa se encarga de crear el software para almacenar los datos de clientes, proveedores y personal interno teniendo como facilidad o ventaja la autonomía del control y monitoreo de la base de datos, y manejar la seguridad y confidencialidad dentro de la empresa.

Procedimientos de notificación, gestión y respuesta ante incidencias

Toda información interna o confidencial es almacenada dentro de un servidor compartido, así como la información contenida en dispositivos de almacenamiento (USB) son guardadas en un lugar seguro.

Los trabajadores velan por la seguridad y confidencialidad de la información contenida en sus equipos, especialmente cuando se encuentren fuera de las dependencias de la organización. Adicional a ello, no destruyen o eliminan registros o información importante sin la aprobación respectiva de los propietarios de información.

Se requiere la autorización del jefe inmediato para la publicación de fotografías y videos de carácter confidencial e interno, realizado dentro las instalaciones de la empresa.

La información almacenada en la Base de Datos se proporciona a las personas autorizadas por la Gerencia responsable.

Antes que se den de baja a las computadoras, se asegura que la información ubicada en los discos duros de estos haya sido administrada de manera segura de modo que su recuperación sea irreversible.

Por último, si ocurre una incidencia relacionada a la protección de datos el área de sistemas envía el reporte de incidencias mediante un correo a ss_soporte@deltron.com.pe para poder documentar y realizar el reporte correspondiente, con la finalidad de tener un registro y monitoreo adecuado.

Cualquier empleado que detecte una posible fuga tiene que reportarlo inmediatamente.

- **Acciones inmediatas:**

- Notificar al Oficial de Protección de Datos Personales (DPO) y al equipo de TI.
- Registrar el hecho en el **Registro de Incidentes de Seguridad**.
- Documentar detalles como:
 - Fecha y hora del incidente.
 - Tipo de información comprometida.
 - Personas afectadas.
 - Posibles causas del incidente.

- **Notificación Interna:**

- El DPO informará a la Alta Dirección sobre el incidente y coordinará las acciones correctivas.

Para mitigar un posible incidente de seguridad en datos personales se deben realizar las siguientes acciones:

Acciones del equipo de TI y Seguridad:

- Desconectar o restringir el acceso a la base de datos comprometida.
- Bloquear cuentas o credenciales comprometidas.
- Implementar cambios de contraseñas y medidas de refuerzo de seguridad.
- Si el incidente fue causado por un ataque cibernético, activar protocolos de defensa (firewalls, análisis de malware, auditoría de accesos).

Acciones de mitigación:

- Revisar si los datos filtrados son sensibles y determinar el alcance del impacto en los titulares de datos personales.
- Identificar si el incidente de seguridad afectó a clientes, proveedores o trabajadores.
- Evaluar si se pueden recuperar y/o eliminar los datos expuestos.

Procedimiento de realización de copia de respaldo y recuperación de datos

Las copias de seguridad de la información son realizadas, registradas y controladas periódicamente. Adicional a ello, este proceso se realiza por duplicado:

- ✓ Se realizan copias de seguridad en el servidor diariamente.
- ✓ Se realizan copias en cinta al menos una vez al mes, las cuales son resguardadas en un local diferente al de la empresa.

Los ambientes donde se almacenen o resguarden las copias de seguridad cumplen las condiciones de almacenamiento, llevando el control en un cuaderno de la entrada y salida del personal que traslada los respaldos de la información. El personal autorizado para el traslado de los respaldos de información forma parte del área de sistemas de la empresa. Cabe resaltar, que el mantenimiento o la actualización de back ups dentro de las instalaciones de Deltron se realiza de manera diaria.

Medidas de seguridad implementadas


Se identifican las áreas restringidas y se establecen políticas de acceso señaladas en la Política de Seguridad y Control de Accesos e Instalaciones. Por otro lado, todo visitante que se encuentre dentro de las instalaciones porta su pase de visita.

Se debe contar con autorización para el retiro de equipos, de información o software de propiedad de la organización.

Sistema de alimentación ininterrumpida (UPS) en el data center.

Se protegen a los equipos informáticos de fallas por falta de suministro de energía y otras anomalías eléctricas.

Por otro lado, para tener una seguridad en la protección de datos, todo usuario creado para el acceso a los sistemas internos cuenta con una contraseña, la cual debe ser cambiada con una periodicidad trimestral y debe ser distinta a la anterior. Además, las contraseñas son de uso personal e intransferible. Ningún trabajador debe solicitar las contraseñas de otros trabajadores.

	DOCUMENTO DE SEGURIDAD	Código: POTISegDatV01
		Versión: 01
		Fecha : 12/03/2025
		Página: Página 8 de 8

Identificación del responsable del documento de seguridad

Para cualquier consulta relacionada con la protección de datos personales, interesados pueden ponerse en contacto con el titular del banco de datos de la empresa al siguiente correo electrónico: alberto.orojeza@deltron.com.pe

Designación del Oficial de Datos Personales

En concordancia con el artículo 37° del Nuevo Reglamento de Protección de Datos Personales, DS N° 016-2024-JUS, se ha designado como Oficial de Datos Personales al señor Jaime Rolando Reyes Aldana, identificado con DNI N° 07631125.