

POLÍTICA DE PRIVACIDAD – FRIOTEAM

FRIOTEAM S.A.C., identificada con RUC No. 20534470402, con domicilio en Carretera Panamericana Sur, Km 298, distrito de Subtanjalla, provincia y departamento de Ica, es responsable del tratamiento de los datos personales recopilados a través de su sitio web <http://www.frioteam.pe> y de otros canales digitales o físicos.

Esta Política de Privacidad detalla cómo se recopilan, utilizan, almacenan y protegen los datos personales de usuarios, clientes, proveedores y postulantes, cumpliendo con la Ley No. 29733 – Ley de Protección de Datos Personales del Perú y considerando buenas prácticas internacionales (RGPD).

El uso del sitio web implica la aceptación de esta Política de Privacidad.

DE LA IDENTIDAD Y RESPONSABILIDAD DEL TRATAMIENTO:

TITULAR	FRIOTEAM S.A.C.
IDENTIFICACIÓN FISCAL	20534470402
DOMICILIO FISCAL	Carretera Panamericana Sur Km 298, distrito de Subtanjalla, Ica
DOMICILIO COMERCIAL	Av. 28 de julio Nro. 753, Oficina 802, Miraflores, Lima.
APODERADO	Alvaro Alejandro Chavez Girao
ÁREA RESPONSABLE	Comunicación e Imagen Institucional
CONTACTO	Pablo Flores Chavez
CORREO ELECTRÓNICO	pflores@frioteam.pe
SITIO WEB	http://www.frioteam.pe

DE LOS PRINCIPIOS APLICADOS SOBRE EL TRATAMIENTO DE DATOS:

- Licitud, Lealtad y Transparencia: Para FRIOTEAM resulta fundamental requerir a sus clientes, proveedores, socios comerciales, trabajadores, terceros vinculados directa o indirectamente, entre otros, su consentimiento para el tratamiento de los datos personales para fines específicos.
- Minimización de Datos: Solo requerimos de los datos cuando resulten estrictamente necesarios.
- Limitación del Plazo de Conservación: Conservamos los datos solo por el tiempo necesario.
- Integridad y Confidencialidad: Adoptamos medidas técnicas y organizativas para garantizar la seguridad de los datos personales.

DE LA OBTENCIÓN DE DATOS PERSONALES:

Recopilamos datos personales en los siguientes casos:

- Formularios de contacto o consultas comerciales.

- Procesos de contratación o postulaciones.
- Interacción con nuestro sitio web mediante cookies.

DE LA FINALIDAD RESPECTO AL TRATAMIENTO DE DATOS PERSONALES:

- Gestión Comercial: Envío de cotizaciones, seguimiento de ventas, atención al cliente entre otra información y/o documentación para el cumplimiento de los fines que correspondan.
- Relación Contractual: Ejecución de contratos, facturación, gestión de cobranzas de pagos entre otros relacionados a esta actividad.
- Reclutamiento: Evaluación de candidatos, gestión de nóminas entre otros.
- Análisis Estadístico: Elaboración de informes, estudio de mercados, análisis de sectores entre otros.

DE LA LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS

- Consentimiento: Es la manifestación de voluntad, libre, específica, informada e inequívoca por la cual el titular de los datos acepta que FRIOTEAM, trate sus datos personales para uno o varios fines determinados.

Ejemplo: i) Un cliente potencial completa un formulario de contacto en el sitio web para solicitar información sobre el diseño y construcción de plantas de refrigeración y marca la casilla aceptando recibir comunicaciones comerciales de FRIOTEAM. ii) Un usuario se suscribe al boletín informativo de FRIOTEAM y da su consentimiento para recibir actualizaciones sobre la empresa, noticias del sector y ofertas especiales. iii) Un postulante a un puesto de trabajo en FRIOTEAM autoriza el tratamiento de sus datos personales (incluyendo datos sensibles, como los relativos a su salud, de ser el caso) para el proceso de selección y evaluación.

- Ejecución de Contratos: Refiere al tratamiento de datos necesarios para la ejecución de un contrato donde el titular de los datos forma parte directa o indirecta para la aplicación; a petición de este último, de medidas precontractuales.

Ejemplo: i) Un cliente proporciona sus datos personales (nombre, dirección, datos de contacto, información financiera) para la formalización de un contrato de construcción de una planta de refrigeración industrial con FRIOTEAM. ii) FRIOTEAM trata los datos de un proveedor (nombre del contacto, datos de la empresa, datos bancarios) para la gestión de la relación contractual, incluyendo la realización de pagos y el seguimiento de los servicios prestados. iii) FRIOTEAM trata los datos de un trabajador (datos de identificación, datos de contacto, datos bancarios, datos laborales) para la gestión de su contrato de trabajo, incluyendo el pago de salarios, la gestión de beneficios y el cumplimiento de obligaciones laborales.

- Cumplimiento de Obligaciones Legales: Es el tratamiento de datos necesarios para el cumplimiento de una obligación legal aplicable a FRIOTEAM.

Ejemplo: i) FRIOTEAM comunica los datos de sus trabajadores a las autoridades tributarias para el cumplimiento de obligaciones fiscales (por ejemplo, retenciones de impuestos). ii) FRIOTEAM proporciona información a las autoridades judiciales o administrativas en el marco de un procedimiento legal. iii) FRIOTEAM conserva los datos de facturación de sus clientes durante el plazo exigido por la legislación mercantil y tributaria.

- Interés Legítimo: El tratamiento de datos es necesario para la satisfacción de intereses legítimos perseguidos por FRIOTEAM o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular de los datos.

Ejemplo: 1) FRIOTEAM realiza un tratamiento de datos de clientes para enviarles información sobre productos o servicios similares a los que ya han contratado, basándose en su interés legítimo en mantener la relación comercial (siempre que el cliente no se haya opuesto a recibir dichas comunicaciones). ii) FRIOTEAM utiliza sistemas de videovigilancia en sus instalaciones para garantizar la seguridad de sus empleados, bienes e instalaciones, basándose en su interés legítimo en proteger su patrimonio. iii) FRIOTEAM realiza análisis estadísticos de los datos de navegación de los usuarios de su sitio web para mejorar su funcionamiento y optimizar la experiencia del usuario, basándose en su interés legítimo en mejorar su negocio online.

RESPECTO A LA CONSERVACIÓN DE LOS DATOS:

Los datos se conservarán mientras sean necesarios para las finalidades descritas o conforme a los plazos legales:

1. PLAZO DE CONSERVACIÓN:

- Datos de Clientes:
 - Información necesaria para la facturación: Conservar durante plazo exigido por la legislación tributaria (generalmente, varios años).
 - Datos de contacto y comerciales: Conservar mientras se mantenga la relación comercial activa. Si no hay actividad, (ej.: 4 años) se anonimiza o elimina, a menos que exista una obligación legal de conservarlos por más tiempo.
 - Comunicaciones y consultas: Conservar por un plazo razonable para atender posibles reclamaciones o consultas futuras (e.: 2-3 años)
- Datos de Proveedores:
 - Datos necesarios para la gestión de contratos y pagos: Conservar durante el plazo de vigencia del contrato y el tiempo necesario para cumplir con obligaciones legales (ej., plazos de prescripción).
 - Datos de contacto: Mantener actualizados mientras se mantenga la relación comercial.
- Datos de Empleados:

- Contratos de trabajo y documentación laboral: Conservar según lo exija la legislación laboral y de seguridad social (los plazos varían según el tipo de documento).
- Datos de planilla: Conservar durante el plazo exigido por la legislación tributaria y laboral.
- Currículums de candidatos no seleccionados: Conservar por un plazo limitado (ej., 6 meses o 1 año) con el consentimiento del candidato para posibles futuras oportunidades.
- Datos de usuarios del sitio WEB:
 - Datos de navegación (cookies): El plazo de conservación dependerá del tipo de cookie (de sesión, persistentes, etc.), tal como se especifique en la Política de Cookies.
 - Datos de formularios de contacto: Conservar por el tiempo necesario para atender la consulta y, si se obtiene consentimiento para comunicaciones comerciales, hasta que el usuario retire su consentimiento.

2. CRITERIOS PARA DETERMINAR LA CONSERVACIÓN:

- Obligaciones Legales:
 - Cumplimiento de la legislación tributaria, laboral, mercantil y otras normativas que establezcan plazos de conservación específicos.
 - Plazos de prescripción de acciones legales (ej.: para reclamaciones contractuales).
 - Requisitos de conservación de documentos contables y financieros.
- Necesidad Operativas de FRIOTEAM:
 - Tiempo necesario para la gestión de la relación con clientes y proveedores.
 - Necesidad de mantener registros para la defensa en caso de reclamaciones.
 - Utilidad de los datos para análisis estadísticos y mejora de los servicios (siempre que se anonimicen cuando sea posible).
- Derecho de los Titulares de los Datos:
 - Equilibrar los plazos de conservación con el derecho a la supresión de los datos (derecho al olvido).
 - Informar a los titulares sobre los criterios utilizados para determinar los plazos de conservación.
- Consideraciones de Seguridad:
 - Minimizar el tiempo de conservación de los datos para reducir el riesgo de incidentes de seguridad.
 - Implementar medidas de seguridad adecuadas durante todo el período de conservación.

3. PROCESO DE ELIMINACIÓN Y/O ANONIMIZACIÓN:

- Eliminación:
 - Procedimiento técnico para la eliminación segura de los datos (ej.: borrado seguro, destrucción física de soportes).

- Aseguramiento que la eliminación sea completa e irreversible.
- Documentar el proceso de eliminación para demostrar el cumplimiento.
- Establecer calendario o sistema para la eliminación periódica de los datos que hayan cumplido su plazo de conservación
- Anonimización:
 - Definición de técnicas para la anonimización que será utilizada en el proceso para la disociación, generalización y/o supresión).
 - Asegurar que la anonimización sea efectiva y que los datos anonimizados ya no permitan identificar al titular.
 - Especificar qué datos se pueden anonimizar y en qué casos se prefiere la anonimización a la eliminación (ej.: para análisis estadísticos)

RESPECTO A LOS DERECHOS DE LOS TITULARES DE DATOS PERSONALES:

Esta sección describe a detalle los derechos que las personas (titulares de los datos) tienen sobre su información personal que FRIOTEAM. recopila y procesa. Estos derechos permiten a los individuos tener control sobre sus datos, incluyendo la capacidad de acceder a ellos, corregirlos si son inexactos, eliminarlos en ciertas circunstancias, oponerse a su uso para determinados fines, limitar su procesamiento y, en algunos casos, solicitar la transferencia de sus datos a otro proveedor de servicios.

El objetivo de esta sección es informar a los titulares sobre cómo pueden ejercer estos derechos y cómo FRIOTEAM se compromete a responder a sus solicitudes de acuerdo con la legislación vigente. Asimismo, si un titular considera que el tratamiento de sus datos personales infringe la normativa vigente, tiene derecho a presentar una reclamación ante la Autoridad Nacional de Protección de Datos Personales (ANPDP), órgano competente en Perú para la protección de datos personales y la supervisión del cumplimiento de la Ley N° 29733.

1. DERECHO DE ACCESO:

- Definición: El derecho de acceso permite al titular de los datos obtener confirmación de si FRIOTEAM está tratando datos personales que le conciernen y, en tal caso, obtener una copia de dichos datos y cierta información sobre su tratamiento.
- Consideraciones para FRIOTEAM:
 - Informar sobre las categorías de datos que se tratan (ej.: datos de identificación, datos de contacto, datos financieros).
 - Detallar las finalidades del tratamiento.
 - Indicar los destinatarios o las categorías de destinatarios a quienes se comunican o comunicarán los datos.
 - Especificar el plazo previsto de conservación de los datos o, si no es posible, los criterios utilizados para determinar este plazo.
 - Informar sobre la existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento, y a oponerse al tratamiento.

- Detallar el derecho a presentar una reclamación ante la autoridad de control (la Autoridad Nacional de Protección de Datos Personales en Perú).
- Indicar, en su caso, la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento.
- Proporcionar una copia de los datos personales objeto del tratamiento.
- Procedimiento:
 - Establecer un procedimiento claro y sencillo para que los titulares puedan ejercer su derecho de acceso (ej., mediante un formulario de solicitud, por correo electrónico, etc.).
 - Fijar un plazo de respuesta razonable (plazo legal en Perú es 20 días hábiles).
 - Proporcionar la información en un formato claro y fácilmente comprensible.

2. DERECHO DE RECTIFICACIÓN:

- Definición: El derecho de rectificación permite al titular de los datos obtener la rectificación de los datos personales inexactos que le conciernen o a que se completen los datos personales que sean incompletos.
- Consideraciones para FRIOTEAM:
 - Informar sobre el derecho a rectificar los datos inexactos.
 - Establecer un procedimiento para que los titulares puedan comunicar los datos que desean rectificar y proporcionar la documentación acreditativa necesaria.
 - Realizar la rectificación sin dilación indebida.
 - Comunicar la rectificación a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado.
- Procedimiento:
 - Definir un canal de comunicación para las solicitudes de rectificación.
 - Establecer un plazo de respuesta para la rectificación.
 - Implementar mecanismos internos para verificar la exactitud de los datos rectificados.

3. DERECHO A LA SUPRESIÓN (Derecho al olvido):

- Definición: El derecho de supresión (o derecho al olvido) permite al titular de los datos obtener la supresión de los datos personales que le conciernen en determinados supuestos.
- Consideraciones para FRIOTEAM:
 - Informar sobre los supuestos en los que procede la supresión:
 - Los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados.
 - El titular retira el consentimiento en que se basa el tratamiento y este no se basa en otra base legal.

- El titular se opone al tratamiento y no prevalecen otros motivos legítimos para el tratamiento.
- Los datos personales han sido tratados ilícitamente.
- Los datos personales deben suprimirse para el cumplimiento de una obligación legal.
- Informar sobre las excepciones al derecho de supresión (ej., cuando el tratamiento es necesario para el cumplimiento de una obligación legal, para el ejercicio del derecho a la libertad de expresión e información, etc.).
- Adoptar medidas razonables para informar de la solicitud de supresión a los responsables que estén tratando los datos personales.
- Procedimiento:
 - Establecer un procedimiento para que los titulares puedan solicitar la supresión de sus datos.
 - Evaluar si procede la supresión en función de los supuestos y excepciones aplicables.
 - Realizar la supresión de forma segura y completa.
 - Informar al titular sobre la decisión adoptada.

4. DERECHO DE OPOSICIÓN:

- Definición: El derecho de oposición permite al titular de los datos oponerse al tratamiento de los datos personales que le conciernen en determinadas circunstancias.
- Consideraciones para FRIOTEAM:
 - Informar sobre el derecho a oponerse al tratamiento basado en el interés legítimo de FRIOTEAM o de un tercero.
 - Informar sobre el derecho a oponerse al tratamiento con fines de mercadotecnia directa, incluida la elaboración de perfiles relacionada con dicha mercadotecnia.
 - Atender la oposición del titular, salvo que FRIOTEAM acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.
- Procedimiento:
 - Establecer un procedimiento para que los titulares puedan ejercer su derecho de oposición.
 - Evaluar los motivos alegados por el titular para oponerse al tratamiento.
 - Informar al titular sobre la decisión adoptada y, en su caso, sobre los motivos legítimos imperiosos que justifican el tratamiento.

5. DERECHO DE LIMITACION DEL TRATAMIENTO:

- Definición: El derecho de limitación del tratamiento permite al titular de los datos obtener la limitación del tratamiento de los datos personales que le conciernen en

determinados supuestos, en cuyo caso FRIOTEAM solo podrá tratar los datos para determinadas finalidades.

- Consideraciones para FRIOTEAM:

- Informar sobre los supuestos en los que procede la limitación del tratamiento:
 - El titular impugna la exactitud de los datos personales, durante un plazo que permita a FRIOTEAM verificar la exactitud de los mismos.
 - El tratamiento es ilícito y el titular se opone a la supresión de los datos personales y solicita en su lugar la limitación de su uso.
 - FRIOTEAM ya no necesita los datos personales para los fines del tratamiento, pero el titular los necesita para la formulación, el ejercicio o la defensa de reclamaciones.
 - El titular se ha opuesto al tratamiento, mientras se verifica si los motivos legítimos de FRIOTEAM prevalecen sobre los del titular.
- Informar sobre la obligación de FRIOTEAM de comunicar la limitación del tratamiento a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado.

- Procedimiento:

- Establecer un procedimiento para que los titulares puedan solicitar la limitación del tratamiento.
- Verificar si se cumple alguno de los supuestos que justifican la limitación.
- Limitar el tratamiento de los datos a las finalidades permitidas.
- Informar al titular sobre la decisión adoptada.

6. DERECHO A LA PORTABILIDAD DE DATOS:

- Definición: El derecho a la portabilidad de los datos permite al titular de los datos recibir los datos personales que le incumben, que haya facilitado a FRIOTEAM, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin impedimentos por parte de FRIOTEAM, cuando el tratamiento se base en el consentimiento o en un contrato y se efectúe por medios automatizados.

- Consideraciones para FRIOTEAM:

- Informar sobre el derecho a la portabilidad de los datos y las condiciones para su ejercicio.
- Proporcionar los datos personales en un formato estructurado, de uso común y lectura mecánica (ej.: CSV, JSON).
- Facilitar la transmisión directa de los datos a otro responsable del tratamiento, cuando sea técnicamente posible.
- Informar sobre el derecho a obtener que los datos personales se transmitan directamente de FRIOTEAM a otro responsable del tratamiento, siempre y cuando sea técnicamente posible.

- Procedimiento:

- Establecer un procedimiento para que los titulares puedan solicitar la portabilidad de sus datos.
- Verificar si el tratamiento se basa en el consentimiento o en un contrato y si se efectúa por medios automatizados.
- Proporcionar los datos en el formato adecuado y facilitar la transmisión, en su caso.
- Informar al titular sobre la decisión adoptada

RESPECTO A LOS DESTINATARIOS DE LOS DATOS PERSONALES:

Esta sección de la Política de Privacidad informa a los titulares de los datos sobre quiénes pueden recibir o acceder a sus datos personales. Esto incluye tanto a entidades internas dentro de FRIOTEAM, como a organizaciones o individuos externos. Se detalla la identidad de estos destinatarios y las razones por las cuales se comparten los datos, los tipos específicos de datos, las medidas de seguridad que se implementan para proteger los datos durante la transferencia (especialmente cuando se trata de transferencias internacionales) y las responsabilidades de estos destinatarios en relación con la protección de los datos personales. Dentro de este ámbito tenemos a) Servicios tecnológicos como lo son proveedores de alojamiento web (hosting), de servicios de correo electrónico, de almacenamiento en la nube, proveedores de software de gestión de clientes (CRM), proveedores de software de gestión de recursos humanos (HRM), proveedores de servicios de análisis web, proveedores de servicios de marketing digital, entre otros y b) Autoridades competentes a quienes se les comparte información de datos personales (ej., autoridades judiciales, administrativas, reguladoras) cuando existe una obligación legal de hacerlo o en el marco de un procedimiento legal.

Todo lo antes mencionado se desarrolla bajo las obligaciones de confidencialidad y seguridad debiendo FRIOTEAM asegurar que los destinatarios de los datos personales se comprometerán a: i) tratar los datos personales de acuerdo con las finalidades establecidas, ii) mantener la confidencialidad de los datos personales y iii) implementar medidas de seguridad adecuadas para proteger los datos personales.

RESPECTO A LA SEGURIDAD DE LOS DATOS PERSONALES:

Esta sección describe las medidas que FRIOTEAM tiene para proteger los datos personales contra accesos no autorizados, pérdida, alteración, destrucción o cualquier otra forma de tratamiento ilícito. Asimismo, detalla tanto las medidas técnicas (como el cifrado y los firewalls) como las medidas organizativas (como las políticas de seguridad y la formación del personal), abarcando aspectos de seguridad física, lógica y administrativa. Además, explica los procedimientos establecidos para la gestión y respuesta ante incidentes de seguridad, asegurando la confidencialidad, integridad y disponibilidad de la información.

1. MEDIDAS DE SEGURIDAD FÍSICA:

- Control de acceso físico a nuestras instalaciones:

- El acceso a nuestras oficinas está controlado mediante tarjetas de acceso y sistemas de identificación biométrica.
- Los centros de datos cuentan con sistemas de vigilancia las 24 horas y personal de seguridad.
- FRIOTEAM cuenta con: Controles de acceso (tarjetas, códigos, biometría, llaves), Registro de ingresos y salidas, Vigilancia (cámaras, personal de seguridad), Protección contra desastres naturales (incendios, inundaciones, terremotos).

Cabe precisar que FRIOTEAM como parte de la seguridad física ha implementado sistemas de videovigilancia en sus instalaciones con el fin de garantizar la seguridad de sus empleados, visitantes, bienes e infraestructura, basándose en su interés legítimo. Este tratamiento de datos se lleva a cabo en cumplimiento de la Directiva de Protección de Datos Personales para Sistemas de Videovigilancia (Resolución 019-2020-JUS/DGPDP), que establece los principios de finalidad, proporcionalidad, calidad y seguridad en el uso de imágenes captadas. Las grabaciones son conservadas por un periodo máximo de 30 días calendario (salvo que deban conservarse por más tiempo debido a un procedimiento interno o legal) y se encuentran protegidas mediante medidas técnicas y organizativas adecuadas. Los titulares pueden ejercer sus derechos respecto a las imágenes captadas, conforme a lo dispuesto en esta política

- Seguridad de los soportes de información:

- Los ordenadores portátiles y dispositivos móviles de la empresa están protegidos con contraseñas y cifrado de disco.
- Los archivos físicos se almacenan en armarios cerrados con llave y en salas con acceso restringido.
- Cifrado de dispositivos y soportes de almacenamiento.
- Procedimientos para la destrucción segura de documentos y dispositivos.
- Control de la salida de dispositivos de la empresa.

2. MEDIDAS DE SEGURIDAD LÓGICA:

- Control de acceso a sistema informático:

- El acceso a nuestras bases de datos está restringido a personal autorizado y se realiza mediante credenciales únicas y contraseñas seguras.
- Implementamos un sistema de gestión de identidades y accesos (IAM) para controlar los permisos de los usuarios.
- Autenticación de usuarios (contraseñas, autenticación de dos factores).
- Autorización de usuarios (control de permisos y privilegios).
- Registro de la actividad de los usuarios (logs de acceso).
- Políticas de contraseñas seguras.

- Protección contra malware:

- Todos los equipos de la empresa cuentan con software antivirus actualizado.
- Implementamos firewalls para proteger nuestra red de accesos no autorizados.

- Software antivirus y antimalware.
- Firewalls.
- Sistemas de detección y prevención de intrusiones (IDS/IPS).
- Actualizaciones de seguridad periódicas
- Cifrado de datos:
 - La transmisión de datos a través de Internet se realiza mediante protocolos seguros (HTTPS).
 - Los datos sensibles se cifran tanto en tránsito como en reposo.
 - Cifrado de datos en tránsito (SSL/TLS).
 - Cifrado de datos en reposo (cifrado de bases de datos, cifrado de archivos).
- Copias de seguridad y recuperación:
 - Realizamos copias de seguridad diarias de nuestras bases de datos y las almacenamos en ubicaciones seguras.
 - Contamos con un plan de recuperación ante desastres para garantizar la continuidad del negocio.
 - Frecuencia y tipo de copias de seguridad.
 - Ubicación de las copias de seguridad (local, remota, en la nube).
 - Procedimientos de restauración de datos.
 - Pruebas periódicas de los procedimientos de recuperación

3. MEDIDAS DE SEGURIDAD ADMINISTRATIVAS

- Políticas y procedimientos de Seguridad:
 - Contamos con una Política de Seguridad de la Información que establece las normas y responsabilidades en materia de protección de datos.
 - Implementamos procedimientos para la gestión de incidentes de seguridad, el acceso a la información y la destrucción de datos.
 - Política de Privacidad.
 - Procedimientos de acceso, uso, almacenamiento y eliminación de datos.
 - Procedimientos de gestión de incidentes de seguridad.
 - Política de contraseñas.
- Formación y concientización del personal:
 - Todos los empleados reciben formación periódica sobre protección de datos.
 - Realizamos campañas de concienciación sobre los riesgos de seguridad y las buenas prácticas.
 - Simulacros de incidentes de seguridad.
 - Materiales de concienciación (folletos, carteles, etc.).
 - Evaluación de la eficacia de la formación.
- Responsabilidad y Roles:
 - Designación de un responsable de Protección de Datos (DPO) que supervisa el cumplimiento de la normativa.
 - Cada departamento es responsable de la seguridad de los datos que trata.

- Definición de roles y responsabilidades en la Política de Seguridad.
- Mecanismos de supervisión y control
- Auditorías de seguridad:
 - Realizamos auditorías de seguridad internas y externas periódicas para evaluar la eficacia de nuestras medidas de seguridad.
 - Alcance de las auditorías.
 - Acciones correctivas derivadas de las auditorías.

4. PROCEDIMIENTOS PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD:

- Detección y notificación:
 - Contamos con un procedimiento para la detección y notificación de incidentes de seguridad que establece los pasos a seguir en caso de una brecha de seguridad.
 - Los empleados están obligados a informar inmediatamente cualquier incidente de seguridad que detecten.
 - Mecanismos de detección (IDS, SIEM).
 - Canales de notificación (correo electrónico, teléfono).
 - Plazos de notificación.
 - Responsabilidades en la notificación.
- Evaluación y respuesta:
 - Se realiza una evaluación del impacto del incidente y se implementan medidas de contención y recuperación.
 - Se informa a las autoridades competentes y a los interesados afectados, si procede.
- Registro de seguimiento:
 - Se mantiene un registro de todos los incidentes de seguridad, incluyendo la fecha, la descripción, el impacto y las medidas adoptadas.
 - Se realiza un seguimiento de las acciones correctivas implementadas para evitar la recurrencia de los incidentes.
 - Análisis de la causa raíz.

En resumen, este punto tiene como objetivo informar a los titulares de los datos sobre el compromiso de FRIOTEAM con la seguridad de su información y las acciones concretas que se llevan a cabo para protegerla.

RESPECTO AL USO DE COOKIES:

Nuestro sitio web utiliza cookies. Consulte la Política de Cookies en <https://frioteam.pe/politica-de-cookies>.

RESPECTO A LOS CAMBIOS EN LA POLITICA DE PRIVACIDAD:

Nos reservamos el derecho de modificar esta política para adaptarla a cambios legislativos o prácticos.