PANDAPÉ

# Seguridad de la información y Protección de datos personales

PANDAPÉ

# Somos líderes mundiales en soluciones digitales de RRHH

Estamos comprometidos con ayudar a nuestros clientes a seleccionar y gestionar el mejor talento. Por eso, creamos **Pandapé**, la suite de soluciones de RRHH más popular en Latinoamérica.

Diseñamos **Pandapé** para que puedas agilizar, transformar y mejorar tus procesos de selección. Con **Pandapé**, podrás digitalizar la gestión de talento, mejorar la comunicación y aumentar el rendimiento.

En el centro de nuestro éxito está nuestro enfoque en la seguridad de la información y protección de datos.

# Tabla de Contenido

## Seguridad

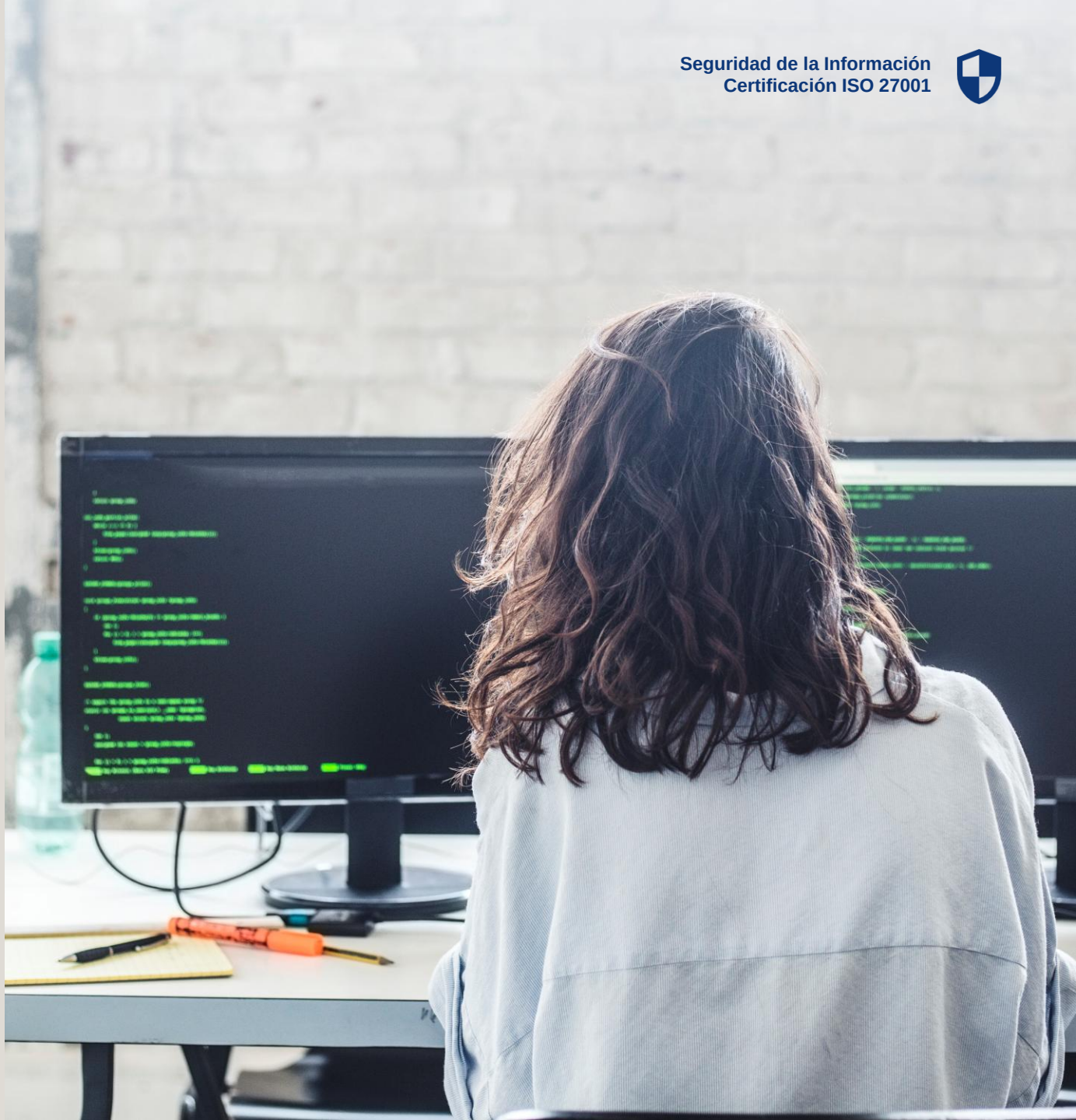


## Protección de datos

# Estamos comprometidos con la seguridad de la información en nuestros servicios

Contamos con un Sistema de Gestión de Seguridad de la Información (SGSI) certificado bajo la **norma ISO/IEC 27001:2022** para los servicios que ofrecemos ofrece. Esto incluye a **Pandapé**.

Nuestros procesos y sistemas están sujetos a auditorías periódicas, pruebas de penetración, detección y prevención de intrusiones. Monitoreamos y mejoramos nuestra tecnología, infraestructura y procesos para garantizar la máxima calidad, eficiencia y seguridad.



# Seguridad en la nube

**AWS** y **Azure** son **nuestros proveedores de cómputo en la nube**.
Nos apoyamos en la experiencia, recursos y reputación de Amazon y Microsoft para garantizar la seguridad, robustez y confiabilidad de la operación en la nube

### Equipo de seguridad

Tenemos un equipo técnico dedicado a monitorear nuestra infraestructura. Nuestros sistemas funcionan 24/7 para garantizar seguridad del servicio

### Protección de la red

Utilizamos cortafuegos, NACL, NACL y HTTPS para el transporte seguro en la red. Tenemos sistemas (IDS/IPS) que detectan y bloquean tráfico malicioso y ataques

### Arquitectura de la red

Dividimos nuestra arquitectura de seguridad por zonas (DMZ). Utilizamos las DMZ entre internet o subredes públicas (load balancers)

### Cortafuegos

Filtramos el tráfico de red entrante con cortafuegos. Identificamos y denegamos conexión con tráfico no autorizado

### Pruebas de penetración

Terceros externos realizan una amplia prueba de penetración anual en nuestras redes públicas y privadas y auditorías trimestrales de producto

### Acceso lógico

El acceso a todas nuestras redes y sistemas de administración se basa en roles. Cada usuario debe identificarse y autenticarse

### Mitigación de DDoS

Supervisamos el tráfico en todas las entradas HTTP y utilizamos WAF para bloquear automáticamente las técnicas DDoS en la capa 7 y ataques en capas 3 y 4

# Seguridad en las operaciones

**Gestión de cambios**
Gestionamos todos los cambios en los sistemas a través de un procedimiento de gestión de cambios. Controlamos los cambios, analizamos sus riesgos y aprobamos sus impactos.

**Actualizaciones**
Con Azure DevOps, automatizamos actualizaciones mediante pipelines. Hacemos tests para desplegar nuevas versiones y hacemos rollbacks automáticos si hay fallos del servicio.

**Gestión de recursos**
Monitorizamos la demanda actual y futura de recursos tecnológicos para optimizar rendimiento, planificar capacidad y gestionar la demanda de servicios.

**Control contra malware**
Implementamos soluciones antimalware que actualizamos continuamente. Monitoreamos constantemente nuestros activos para protegerlos de amenazas cibernéticas.

**Respuesta ante incidentes de seguridad**
Ante alertas, nuestros equipos 24/7 de operaciones, redes y seguridad escalan incidencias. Informamos al Cliente de cualquier impacto en la seguridad en máximo 48hr.

**Registro y monitoreo**
Recopilamos extensos registros de eventos. Nuestro sistema envía alertas al equipo de seguridad ante eventos correlacionados para investigación y respuesta

**Cifrado en tránsito**
Ciframos todas nuestras comunicaciones con el protocolo Transport Layer Security (TLS) a través de redes públicas de nuevos conjuntos de cifrado no débiles.

**Cifrado en reposo**
Ciframos todos los archivos y almacenes de datos con sistemas de gestión de claves basados en algoritmos robustos y programas de rotación según estándares de la industria

# Desarrollo seguro

Como parte de nuestro Secure Development Life Cycle (SDLC), contamos con varias herramientas que usamos en cada etapa de desarrollo software para garantizar la seguridad de nuestros servicios desde su concepción hasta su implementación y mantenimiento

## Lenguaje

Nuestro stack de software se basa en varios lenguajes de programación para nuestras webs y API. Azure DevOps soporta lenguajes de programación con una alta escalabilidad, fiabilidad y seguridad.

## Formación en seguridad

Formamos internamente a nuestros desarrolladores en materias de seguridad en código, en el diseño, en seguir las mejores prácticas para combatir ataques comunes y en usar controles de seguridad.

## Quality Assurance

Nuestro equipo de QA revisa y prueba nuestro código, integrando varias pruebas manuales y automatizadas para que solo se implemente el código que ha sido evaluado y aprobado.

## Audit logs

Mantenemos registros de todos los accesos y de los cambios que realiza cada usuario (audit logs). El registro se encuentra almacenado bajo acceso restringido, y es únicamente consultable en caso de incidencia.

## Controles de seguridad OWASP

Alineamos nuestro desarrollo software con las prácticas de la industria OWASP. Estas incluyen controles que reducen nuestra exposición a Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) e Inyección SQL (SQLi), entre otros.

## Entornos separados

Separamos física y lógicamente los entornos de prueba, preparación y desarrollo. Hacemos esta separación a través del aislamiento de red, firewalls y NACL. No usamos datos de producción reales en el entorno de desarrollo o prueba.

# Disponibilidad y continuidad

# Gestión de vulnerabilidades

Contamos con varias herramientas que nos permiten detectar vulnerabilidades técnicas

## Escaneo dinámico interno de vulnerabilidades

Empleamos herramientas de seguridad calificadas de terceros para escanear continua y dinámicamente nuestras aplicaciones en contra de reglas OWASP, entre otros. Todos los controladores HTTP tienen un WAF activo que bloquea todos los OWASP conocidos y las reglas principales conocidas en tiempo real.

## Escaneo de vulnerabilidad dinámica externa

Utilizamos tecnologías de escaneo estándar de la industria, personalizadas para probar la infraestructura y el software de manera eficiente y, al mismo tiempo, minimizar los riesgos potenciales asociados con el escaneo activo. Realizamos pruebas y escaneos bajo demanda según sea necesario. Las exploraciones se realizan durante las ventanas que no son pico.

## Análisis de código estático

Nuestros repositorios de código fuente se escanean continuamente en las pruebas y revisan las etapas en los Pipelines y Flow de CI/CD (integración continua), y se integran con todos los flujos de QA.

## Pruebas de penetración de seguridad

Nos apoyamos en terceros externos expertos en seguridad para realizar pruebas de penetración detalladas y análisis de código dinámico.

# Funciones de seguridad en nuestros servicios

Estas funcionalidades nos permiten preservar la seguridad de la información que circula o se almacena por el uso de nuestros servicios.

| Función | Descripción |
|---|---|
| Opciones para autenticación | Para las aplicaciones WebGUI, ofrecemos inicio de sesión de cuenta con 2FA. Para las API de productos y/o integraciones de clientes, ofrecemos un flujo de autenticación con claves de API y/o secret/tokens para autenticar y autorizar todas las llamadas y acciones de API con el backend. Los usuarios que accedan a la herramienta son identificados de forma única y exclusiva, mediante el sistema de autentificación obligatorio, compuesto de un usuario único y una clave de acceso o contraseña. El sistema genera automáticamente una clave o contraseña inicial que deberá ser cambiada en el primer acceso. Por seguridad se requerirá que la clave o contraseña contenga un formato específico para evitar claves débiles. |
| Autenticación de dos factores (2FA) | Se requiere la autenticación de 2 factores (2FA) para agentes y administradores. La autenticación 2FA proporciona otra capa de seguridad a su cuenta, lo que dificulta que otra persona inicie sesión como usted. |
| Política de contraseñas | Las contraseñas solo pueden ser restablecidas por el usuario final con una dirección de correo electrónico. El usuario final puede generar una URL de restablecimiento de contraseña temporal en la página de inicio de sesión. Las políticas de contraseñas siguen las recomendaciones principales para garantizar su seguridad. |
| Almacenamiento seguro de credenciales | Seguimos las mejores prácticas de almacenamiento seguro de credenciales. Todas las contraseñas se almacenan cifradas, es decir, nunca se almacenan en formato legible por humanos. Se usa un hash seguro y unidireccional, con cifrado en reposo y de todas las operaciones en tránsito al backend. |

# Funciones de seguridad en nuestros servicios (cont.)

Estas funcionalidades nos permiten preservar la seguridad de la información que circula o se almacena por el uso de nuestros servicios.

| Función | Descripción |
|---|---|
| Privilegios y roles de acceso | El acceso a los datos se rige por derechos de acceso y se puede configurar para definir privilegios de acceso granulares. Las aplicaciones tienen varios niveles de permisos para los usuarios (propietario, administrador, agente, usuario final, etc.) y una granularidad de roles por grupo. |
| Alta disponibilidad y acceso del producto | Para garantizar una baja latencia y una alta disponibilidad en la entrega de contenido, se utiliza una red de entrega de contenido (CDN), lo que a segura una baja latencia y alta disponibilidad. |
| Datos del cliente | Los datos y la documentación de cada cliente son almacenados de forma cifrada en un espacio lógico propio e independiente. |
| Archivos adjuntos privados | De forma predeterminada, todas las instancias de nuestras aplicaciones están protegidas, todos los activos y archivos adjuntos son privados y se requiere un inicio de sesión y un permiso / rol. Además, todos los activos y archivos adjuntos se almacenan en un almacén de datos cifrados. |

# Nuestra prioridad es apoyarte en proteger los datos personales de tus candidatos y colaboradores

En **Pandapé**, entendemos tus obligaciones como el responsable del tratamiento de datos personales de tus candidatos y colaboradores. Por eso, te ofrecemos soluciones que te ayudan a cumplir con tus responsabilidades y sean respetuosas de la privacidad.

Desde nuestros inicios, nos hemos enfocado enfocado en desarrollar soluciones centradas en la protección de datos personales. Esto significa que, en la práctica, desarrollamos herramientas, implementamos medidas y proveemos información para que las personas tomen decisiones informadas y siempre tengan control sobre sus datos personales.

Nos das instrucciones de qué datos tratar y por qué tratarlos en un **contrato de encargo**

Para el Perú, Computrabajo Perú SAC actúa como encargado

Para LatAm, DGNET LTD actúa como encargado

**Tú** eres el **responsable** del tratamiento porque determinaste

El **medio** a través del cual se hace el tratamiento, esto es el Software como Servicio de Pandapé

La **finalidad** del tratamiento, esto es, en general, seleccionar y gestionar talento

de los datos personales de

**Tus candidatos**
Aquellos individuos que aplicaron a tus vacantes de empleo y cuya postulación gestionas en **Pandapé**

**Tus colaboradores**
Aquellos individuos que tienen una relación de trabajo contigo, la cual gestionas en **Pandapé**

# Principios

Como encargados procuramos que nuestra relación contigo, responsable, se base en que

- **Licitud**: Siempre debes tener un fundamento legal para tratar datos personales
- **Finalidad**: Trates datos personales para lograr propósitos claros, específicos y actuales que decidas
- **Proporcionalidad**: Trates los datos personales que sean estrictamente necesarios
- **Transparencia**: Proveas información accesible, comprensible, concisa y relevante
- **Calidad**: Mantengas datos completos, precisos, exactos y que reflejen la realidad
- **Responsabilidad**: Puedas cumplir con tus obligaciones como responsable y puedas probarlo
- **Seguridad**: Mantengas la integridad, confidencialidad y disponibilidad

# Pandapé es *privacy-friendly*

Hemos diseñado y desarrollado **Pandapé** de forma que tú, como responsable, puedas dar a tus candidatos y colabores el control de sus datos personales y sepan qué ocurre con ellos. No toleramos prácticas invasivas, engañosas, confusas que afecten la privacidad.

## Privacidad en el diseño

En cada etapa de desarrollo, hemos tomado decisiones para:

- Garantizar la confidencialidad integridad, disponibilidad y resiliencia permanente de los sistemas y servicios
- Restaurar la disponibilidad y el acceso en caso de incidentes de seguridad
- Verificar, evaluar y valorar continuamente la eficacia de las medidas técnicas y organizativas implantadas

## Privacidad por defecto

La configuración original de cuentas de **Pandapé** es respetuosa de la privacidad, por ejemplo:

- Hay temporizadores configurables de borrado permanente de datos personales
- Ofrecemos una plantilla de política de privacidad para tus candidatos y/o colaboradores
- Varios mensajes de alertas y novedades permiten a sus destinatarios darse de baja

# Tratamiento de datos que hacemos bajo tus instrucciones

# Finalidades

Como **responsable** del tratamiento de datos, **tú eres quien determina cómo y para qué vas a tratar los datos personales**. De manera que es tu deber responderte a *"¿por qué quiero Pandapé?"* y *"¿qué voy a hacer con los datos de mis candidatos y colaboradores?"*

Nosotros, como **encargados**, **no podemos decirte cuál es el propósito y la manera de tratar los datos**. Pero, por la naturaleza de nuestras soluciones, creemos que:

✓ Pandapé ATS te ayudará a:
- Gestionar el proceso de selección de tus candidatos
- Comunicarte con el candidato para conversar sobre los procesos de selección
- Buscar candidatos adecuados para cubrir las vacantes que tengas disponibles

✓ Pandapé HCM te ayudará a:
- Gestionar la relación de trabajo con tus colaboradores
- Comunicarte con tus colaboradores sobre temas de interés laboral
- Hacer seguimiento al desempeño y rendimiento

En el diseño de Pandapé incluimos un menú de configuraciones de privacidad donde autónomamente puedes gestionar tiempos de retención, actualizaciones de tu política de privacidad y más.

Gracias a esto, tus candidatos y colaboradores pueden tener información actualizada y completa sobre los tratamientos de datos personales que haces e información sobre cómo ejercer sus derechos.

# Derechos

Como encargados podemos ayudarte a que, como responsable, contestes de fondo solicitudes relacionadas con derechos de

- **Acceso**: Derecho a que confirmes si tratas datos personales, cuál es el tratamiento y des una copia de los datos
- **Rectificación**: Derecho a que actualices, rectifiques o modifiques datos para que sean completos, precisos y actuales
- **Cancelación**: Derecho a que borres los datos que tratamos, sin perjuicio de las excepciones que por ley apliquen
- **Limitación**: Derecho a que limites o restringas, por un tiempo, el tratamiento de todos o algunos datos
- **Oposición**: Direito de se opor ao tratamento de dados pessoais de acordo com o contexto do tratamento
- **Portabilidad**: Derecho a obtener los datos de manera estructurada, en formato de uso común y lectura mecánica
- **No ser sujeto de decisiones automatizadas**: Siempre tener intervención humana en decisiones que pueden impactar libertades o derechos

# Como responsable, eres quien decide por cuánto tiempo conservar los datos personales

Por ejemplo, esto puede significar

- Para candidatos: el período para el proceso de selección
- Para colaboradores: la duración de la relación de trabajo
- El candidato o trabajador NO hayan solicitado la cancelación
- Prescripción en obligaciones legales o de acciones judiciales

Los usuarios administradores que asignes en **Pandapé** podrán borrar del sistema los datos para los que se haya cumplido el período de conservación que tu determines

# Compartimos datos  únicamente cuando es necesario para cumplir con las finalidades determinadas

Estos son los terceros con quienes compartimos datos personales. Algunas veces estos terceros están en países diferentes al de tus candidatos o colaboradores.

Hacemos nuestros mejores esfuerzos por tener proveedores que estén en países declarados como adecuados por las autoridades de protección de datos. En ausencia de esta declaración, implementamos cláusulas contractuales tipo u otros mecanismos para mantener el mismo nivel de protección que los datos tienen desde su lugar de origen.

## Subencargados

Son terceros o empresas de nuestro grupo empresarial  que, bajo nuestra instrucción realizan actividades de tratamiento. Por ejemplo: nube, soporte, análisis.

## Autoridades oficiales

Son entidades públicas que en ejercicio de sus funciones legales y/o reglamentarias nos pueden ordenar compartir datos personales de sus usuarios. En estos casos trabajaremos contigo para dar repuesta.

# Sobre los subencargados del tratamiento

Para prestar el servicio de **Pandapé**, subcontratamos con terceros que nos apoyan a tratar datos personales en tu nombre. Sin ellos, no podemos prestar el servicio.  Estos terceros son **subencargados del tratamiento de datos personales**. Estas son las medidas que contamos con respecto a ellos:

## Debida Diligencia

Como mínimo, nuestros expertos legales, en seguridad y protección de datos revisan:

- Políticas, procesos y procedimientos de ciberseguridad
- Medidas técnicas y organizativas de protección de datos
- Acuerdos de servicio y soporte

## Reputación

Preferimos terceros que:

- Tengan certificaciones de ciberseguridad y/o calidad
- No tengan investigaciones abiertas o multas en los últimos 5 años
- Publiquen reports de auditoría
- Tengan buena reputación global
- Estén en un país declarado como adecuado

## Contrato

Formulamos contratos de encargo de tratamiento que tengan como mínimo:

- Obligación de seguir instrucciones del responsable
- Auditorías
- Comunicación de incidentes
- Apoyo a resolver solicitudes de ejercicio de derechos
- Protección para transferencias internacionales de datos
- Autorización para subencargados

## Seguimiento

Después de firmar el contrato, monitoreamos la relación con el encargado para:

- Actualizar cambios en la relación comercial
- Incluir en el contrato nuevas obligaciones legales
- Monitorear las políticas de conservación de datos
- Reconocer cambios en los subencargados

# Medidas de seguridad

Estas son las prácticas y herramientas que implementamos para garantizar la confidencialidad, integridad y disponibilidad de los datos personales de candidatos y usuarios profesionales.

## Medidas organizativas

- Tenemos políticas y procedimientos internos de desarrollo *privacy friendly*
- Tenemos un Delegado/Oficial de Protección de Datos
- Realizamos Evaluaciones de Impacto de Protección de Datos para tratamientos de alto riesgo
- Capacitamos nuestros colaboradores
- Tenemos una política de seguridad de la información
- Mantenemos un registro de actividades de tratamiento
- Nos enfocamos en recolectar y tratar los datos mínimamente necesarios
- Seguimos la regulación aplicable en materia de gestión de incidentes

## Medidas técnicas

- Ciframos los datos en tránsito y en reposo
- Controlamos el acceso al portal mediante autenticación de usuarios
- Tenemos firewalls, sistemas de detección/prevención de intrusiones (IDS/IPS).
- Actualizamos nuestros antivirus
- Implementamos tecnologías DLP
- Almacenamos los datos personales en AWS (ISO 27001).
- Implementamos sistemas de monitoreo automático para detectar y responder a actividades sospechosas
- Utilizamos técnicas de separado, seudonimización, enmascaramiento u otros, según sea necesario

# Gestión de incidentes

Nos tomamos muy en serio la seguridad de los datos personales que tratamos en tu nombre. Nunca escatimamos recursos en protegerlos, pero sabemos que el riesgo nunca es cero. Algo puede ocurrir. Pero si pasara, esto haremos:

Gracias por confiar en Pandapé. La suite de gestión de RRHH líder en Latinoamérica.

Si tienes preguntas contacta a tu ejecutivo asignado.

PANDAPÉ