

Computrabajo



**Seguridad de la información y
Protección de datos personales**

Somos líderes mundiales en soluciones digitales de RRHH

Nuestra misión es ayudar a las personas a encontrar un mejor empleo y a las empresas, el mejor talento. Por eso, creamos **Computrabajo**, la bolsa de empleo líder en Latinoamérica. Tenemos 128+ millones de visitas mensuales y 27+ millones de valoraciones sobre empresas.

Estas cifras reflejan la confianza de nuestros usuarios. Honramos y preservamos esa confianza con nuestras medidas de seguridad de la información y de protección de datos personales.





Tabla de Contenido

Seguridad de la información

<u>Certificación ISO 27001</u>	4
<u>Cómputo en la nube</u>	5
<u>Seguridad de las operaciones</u>	6
<u>Desarrollo seguro</u>	7
<u>Disponibilidad y continuidad</u>	8
<u>Gestión de vulnerabilidades</u>	9
<u>Seguridad en los servicios</u>	10

Protección de datos

<u>Compromiso</u>	12
<u>Principios</u>	13
<u>Responsable</u>	14
<u>Privacidad por diseño y defecto</u>	15
<u>Tratamiento</u>	16
<u>Finalidades</u>	17
<u>Derechos</u>	19
<u>Conservación</u>	20
<u>Transferencias</u>	21
<u>Encargados</u>	22
<u>Seguridad</u>	23
<u>Incidentes</u>	24



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 nuestro grupo empresarial ofrece. Esto incluye a **Computrabajo**.

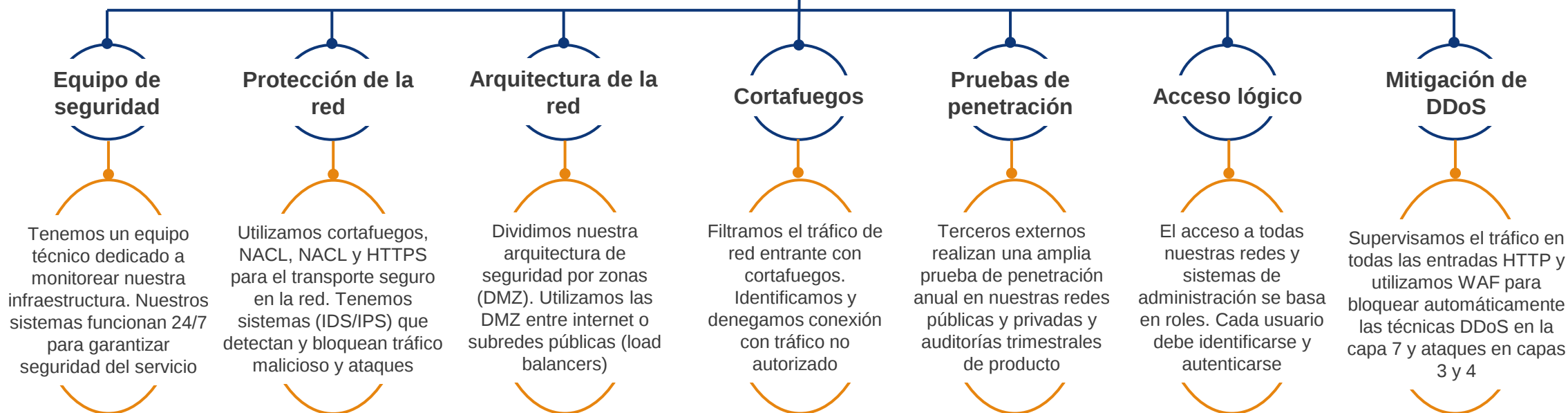
Nuestros procesos y sistemas están sujetos a auditorías periódicas, pruebas de penetración, detección y prevención de intrusiones. Monitoreamos y mejoramos nuestra tecnología, infraestructura y procesos para garantizar la máxima calidad, eficiencia y seguridad.





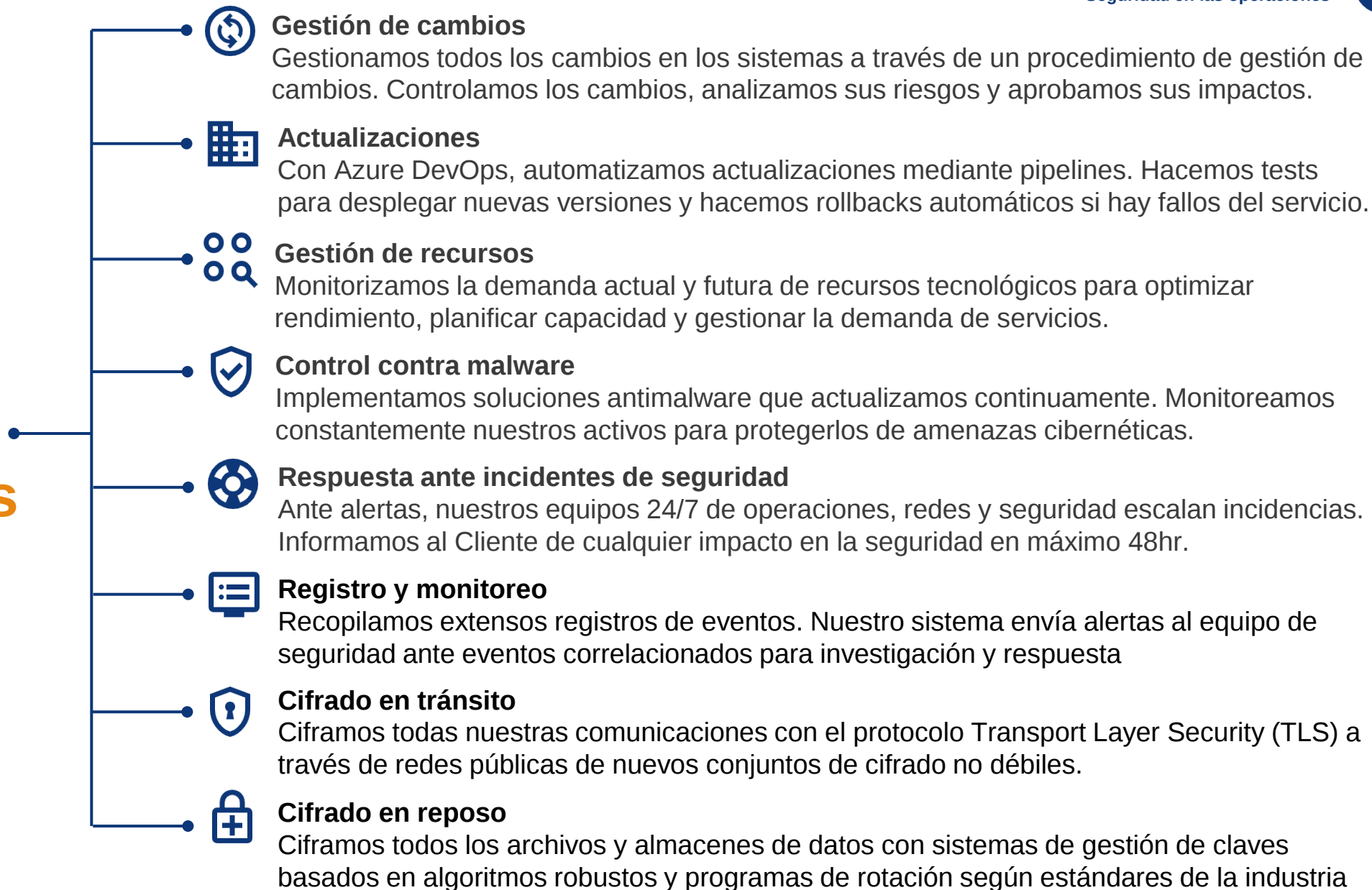
Seguridad en la nube

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





Seguridad en las operaciones





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



Redundancia

La infraestructura de nuestros servicios de producción tiene redundancia para evitar puntos únicos de fallo. Si un sistema primario falla, el hardware redundante lo releva. Usamos agrupación de servicios y redundancia de red para reducir puntos únicos de fallo.



Copia de seguridad

AWS/Azure proveen nuestra infraestructura de respaldo que reside en almacenes de datos de larga duración detrás de redes privadas aseguradas lógicamente y cifradas en reposo. Diariamente hacemos copias de seguridad de información de entornos productivos y semanalmente, a través de una verificación aleatoria, comprobamos la integridad de la copia de seguridad.



Recuperación de desastres

Nuestro plan garantiza la disponibilidad y recuperación de servicios ante desastres, mediante un entorno técnico sólido y planes de recuperación con redundancia de proveedor, según los RTO y RPO que definimos.



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 autenticación 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 asegura 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.



Proteger los datos personales de nuestros usuarios es nuestra prioridad

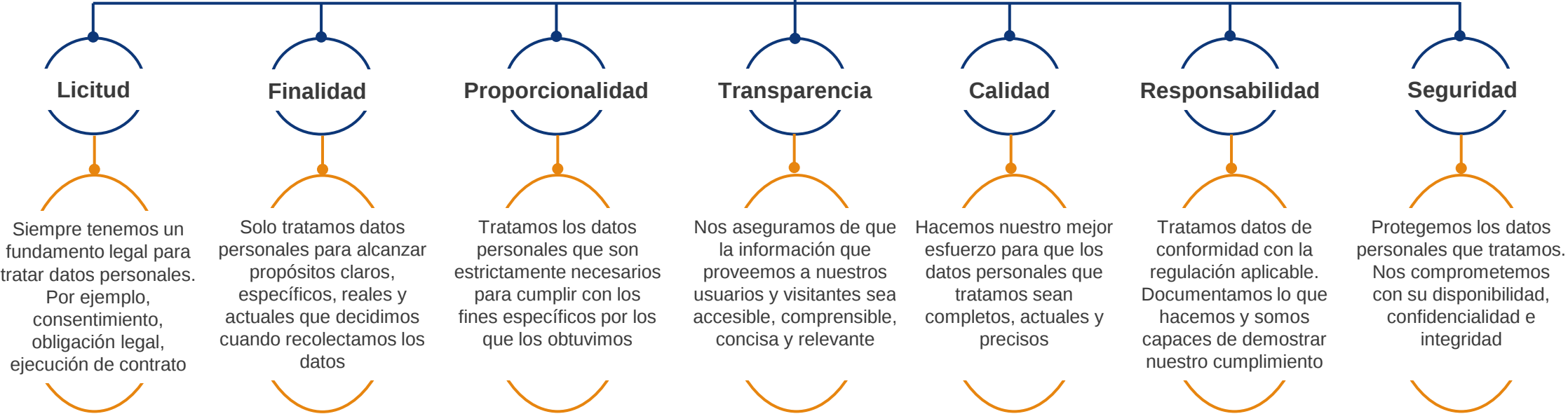
En **Computrabajo**, es de vital importancia proteger los datos personales de nuestros usuarios. Desde nuestros inicios, nos hemos enfocado en desarrollar soluciones centradas en la privacidad y la protección de datos personales.

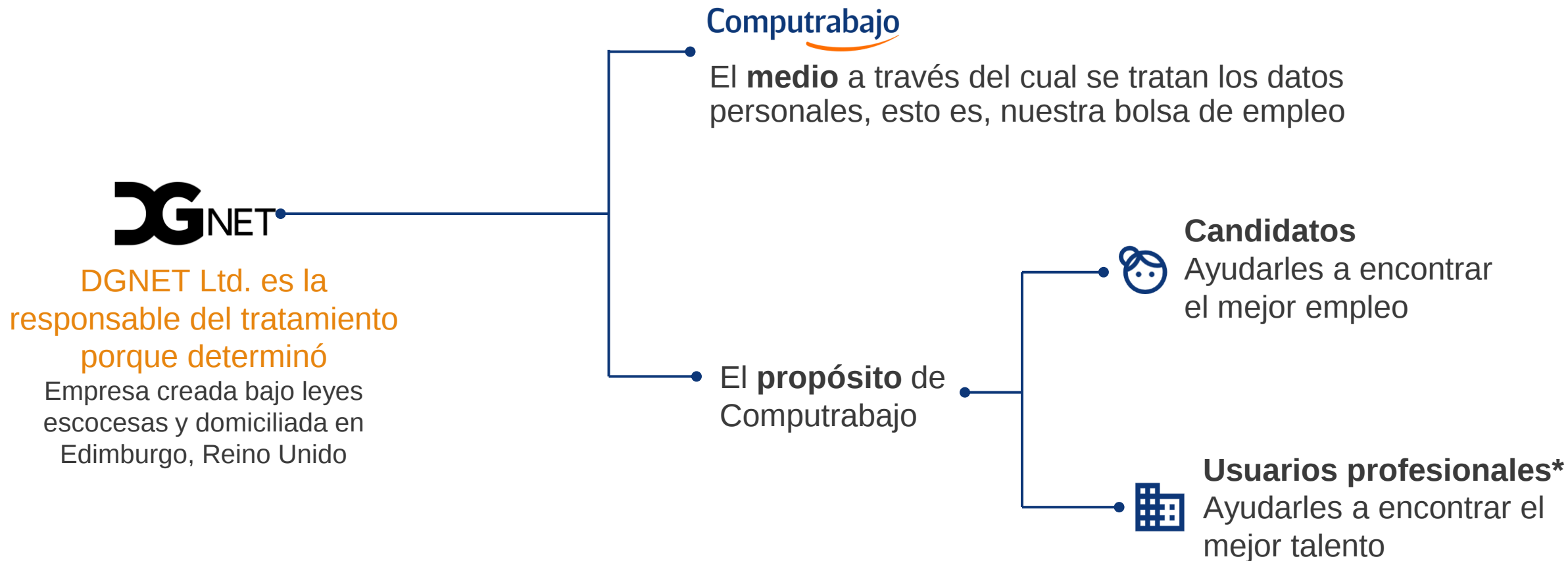
Esto significa, en la práctica, que desarrollamos herramientas, implementamos medidas y proveemos información para que nuestros usuarios puedan tomar decisiones informadas sobre sus datos personales y mantener el control sobre ellos.





Principios





* También llamados "empresas". Solo para efectos de protección de datos, cuando nos referimos a usuarios profesionales nos referimos al individuo que crea y gestiona la cuenta de Computrabajo en nombre y representación de una empresa.



Computrabajo es *privacy-friendly*

Hemos diseñado y desarrollado **Computrabajo** de forma que nuestros usuarios siempre tengan control de sus datos personales y sepan qué estamos haciendo 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



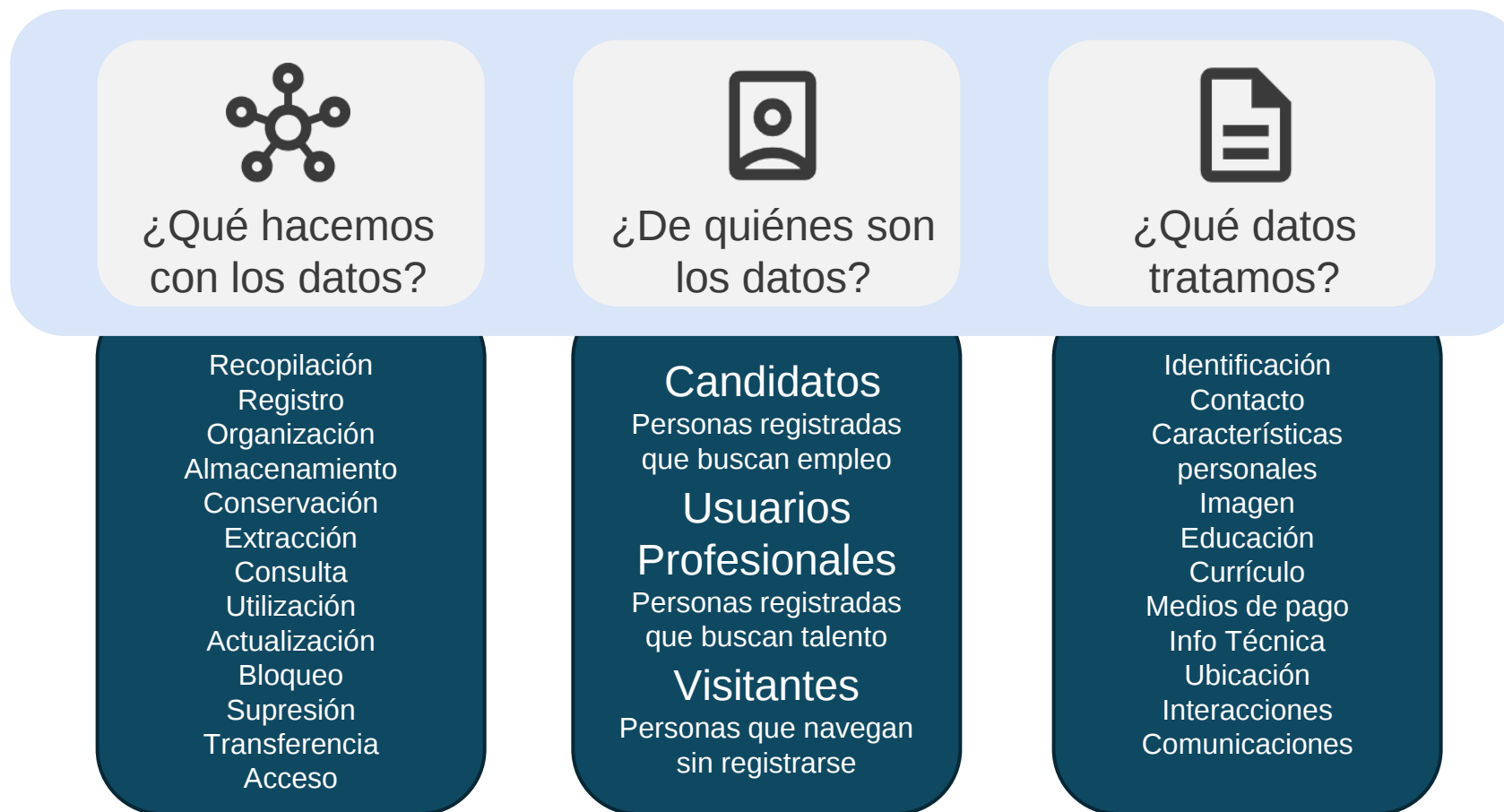
Privacidad por defecto

La configuración original de cuentas de **Computrabajo** es respetuosa de la privacidad:

- Nuestros usuarios deciden cómo y cuándo compartir sus datos
- Nuestros usuarios pueden ejercer fácilmente sus derechos
- Solicitamos la información estrictamente necesaria para la correcta prestación de nuestro servicio



Tratamiento





Finalidades

Te hablamos del principio de finalidad y del propósito de **Computrabajo**. A continuación, detallamos lo que significa ese propósito y los fundamentos legales que tenemos para tratar los datos personales

Finalidades	Fundamentos legales
Gestión de servicios, por ejemplo: • Creación, gestión y edición de cuenta • Contacto entre candidatos y usuarios profesionales • Envío de comunicaciones relativas al funcionamiento de Computrabajo	Ejecución de contrato
Gestión de la suscripción y moderación de contenido	
Mejora de nuestros servicios	
Despliegue de material publicitario personalizado	Consentimiento
Envío de boletines y promociones de otros servicios que ofrecemos	
Generación de información agregada para fines estadísticos y analíticos	
Prevención de fraudes y abusos	Interés legítimo
Cumplimiento de órdenes de autoridades oficiales en ejercicio de sus funciones	
	Obligación legal



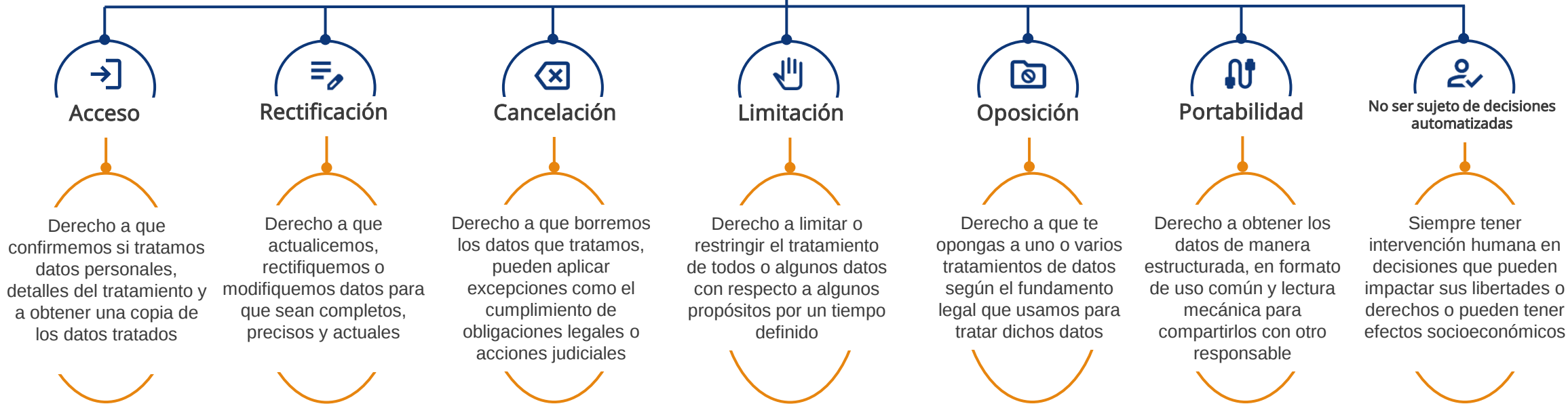
El diseño de nuestro portal hace que los candidatos deban aceptar nuestra política de privacidad para crear una cuenta en Computrabajo.

Gracias a esto, nuestros clientes, registrados en Computrabajo como usuarios profesionales, pueden buscar candidatos, contactarse con ellos y recibir los currículos de aquellos candidatos que se hayan postulado a vacantes publicadas.



Derechos

Nuestros candidatos y usuarios profesionales
pueden ejercer



Conservamos los datos solo por el tiempo necesario para lograr las finalidades de Computrabajo

esto significa



Para candidatos: la cuenta está activa



Para usuarios profesionales: contrato/orden de servicio vigente



El candidato o usuario profesional NO ha solicitado la supresión



Prescripción en obligaciones legales o de acciones judiciales



Compartimos datos únicamente cuando es necesario para cumplir con las finalidades de Computrabajo

Estos son los terceros con quienes compartimos datos personales. Algunas veces estos terceros están en países diferentes al de nuestro usuario.

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.



Encargados

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



Autoridades oficiales

Son entidades públicas que en ejercicio de sus funciones legales y/o reglamentarias nos pueden ordenar compartir datos personales de sus usuarios.



Usuarios profesionales (solo aplica a candidatos)

Cuando un candidato aplica a una vacante laboral, compartimos su currículum con el usuario profesional que ha publicado dicha vacante.



Sobre nuestros encargados del tratamiento

Para prestar el servicio de **Computrabajo**, contratamos con terceros que, bajo nuestras instrucciones, tratan datos personales. Estos terceros son **encargados 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

- La política de protección de datos de **Computrabajo** está disponible para consulta pública
- 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/prevenición 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 de nuestros candidatos y usuarios profesionales. 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
Computrabajo. La bolsa
de empleo líder en
Latinoamérica.**

**Si tienes preguntas
contacta a tu ejecutivo
asignado.**

Computrabajo