Política de seguridad de Aureo Job

Titular legal	Producto	Versión
Aureo Technologies	Aureo Job	1.2
Tipo	**Jurisdicción**	**Vigente desde**
Política de seguridad	Estados Unidos	24/07/2026 · Última actualización: 24/07/2026

Esta política describe las medidas técnicas y organizativas que Aureo Technologies aplica para proteger Aureo Job. Su objetivo es explicar nuestros controles con claridad; no representa por sí sola una certificación de seguridad.

Alcance

Abarca la aplicación Aureo Job, sus páginas públicas, servicios de soporte, herramientas administrativas internas y la infraestructura que Aureo Technologies controla para operar el producto.

Responsabilidad compartida

Aureo Technologies protege la plataforma y su infraestructura. Cada empresa cliente administra a sus usuarios, roles, dispositivos, datos cargados, consentimientos y decisiones operativas. Los clientes deben asignar el acceso mínimo necesario y retirar accesos cuando una persona ya no los requiera.

Identidad y acceso

Las contraseñas se almacenan mediante funciones criptográficas unidireccionales, no como texto legible. El registro público exige verificación del correo antes de crear la cuenta. Los enlaces de restablecimiento se almacenan como hash, vencen y solo pueden utilizarse una vez. El inicio de sesión tiene limitación de intentos y bloqueo temporal después de intentos fallidos repetidos. Los permisos se aplican por rol y pueden ajustarse por usuario. La administración interna privilegiada de Aureo Technologies requiere autenticación de dos factores.

Sesiones y seguridad web

En producción, Aureo Job usa HTTPS y cookies de sesión con atributos Secure, HttpOnly y SameSite. Los formularios y acciones protegidas usan defensa CSRF. Las respuestas sensibles se marcan para no almacenarse en caché y la Política de Seguridad de Contenido limita la ejecución de scripts no autorizados. Las rutas protegidas exigen autenticación y autorización.

Aislamiento entre empresas

Los registros operativos se asocian a una empresa mediante company_id. Las consultas, permisos y validaciones de propiedad limitan el acceso al ámbito de la empresa autenticada. Los controles de autorización también se aplican al consultar recursos por identificador para reducir el riesgo de acceso directo indebido.

Archivos y evidencias

Las cargas tienen límites de tamaño y validaciones de nombre, extensión y tipo permitido. Las imágenes se normalizan antes de conservarse. Las evidencias privadas se guardan fuera de los activos públicos y se entregan mediante rutas autorizadas; las respuestas privadas se sirven sin caché cuando corresponde.

Secretos e integraciones

Las credenciales de infraestructura y proveedores se mantienen fuera del repositorio y de los archivos públicos. Las contraseñas, tokens de verificación, enlaces de acceso y estados OAuth se almacenan como hash o se protegen según su función. El acceso a integraciones se limita a usuarios autorizados.

Pagos

Stripe procesa los datos de tarjeta y las operaciones de suscripción. Aureo Job conserva referencias y estados necesarios para la operación, pero no almacena números completos de tarjeta.

Auditoría y monitoreo

Las acciones sensibles registran, según corresponda, usuario, empresa, fecha, dirección IP, agente de usuario, recurso y metadatos no secretos. Los eventos principales de auditoría se enlazan mediante hashes para facilitar revisiones de integridad. La plataforma mantiene registros operativos, controles de salud y revisión de errores para detectar fallas.

Respaldos y recuperación

El proceso de respaldo de la base de datos genera copias con permisos restringidos y valida que el archivo pueda ser leído por la herramienta de restauración. Aureo Technologies mantiene procedimientos de recuperación y revisa periódicamente la vigencia de los respaldos y las pruebas de restauración.

Cambios y vulnerabilidades

Los cambios pasan por pruebas funcionales y de seguridad proporcionales al riesgo antes de su despliegue. Las dependencias y configuraciones se revisan durante el mantenimiento del servicio. Los hallazgos confirmados se priorizan según su impacto y posibilidad de explotación.

Respuesta a incidentes

Los eventos de seguridad se registran, clasifican, investigan y contienen. Cuando un incidente afecta datos o servicios de un cliente, Aureo Technologies evalúa el alcance, conserva evidencia y realiza las comunicaciones exigidas por los contratos o la ley aplicable. Los reportes pueden enviarse a security@aureotechnologies.com.

Datos, retención y eliminación

El tratamiento, la retención, exportación y eliminación de datos se rigen por la Política de privacidad, el DPA, las instrucciones válidas del cliente y las obligaciones aplicables. Las solicitudes de privacidad pueden enviarse a privacy@aureotechnologies.com.

Revisión de esta política

Ningún sistema puede garantizar seguridad absoluta. Aureo Technologies revisa esta política al menos una vez al año y cuando existe un cambio material en los controles o en la operación de Aureo Job.