Política de seguridad

devengo

Versión 1.1 Última edición 22/09/2021

Índice

Política de seguridad 3

Objetivos 4

People 5

Activos y equipos 6

Datos 7

Legal 8

Plataforma tecnológica 9

Auditoría y registro 10

Disponibilidad 11

Gestión de incidentes y continuidad 12

Datos de contacto y resolución de dudas 13

Política de seguridad

Devengo en un servicio financiero en la nube para que las empresas den liquidez a sus trabajadores que la necesiten.

Por la propia naturaleza de sus servicios, Devengo procesa información confidencial de sus clientes y empleados acerca de sus trabajadores, contratos, salarios, bajas, etc. Por tanto, proteger esta información es tan importante para Devengo como transferir el dinero de la manera más rápida posible cuando un empleado lo necesita.

Devengo está decidido a implementar y hacer cumplir controles efectivos en su Sistema de Gestión de Seguridad de la Información así como mejorarlo continuamente.

En línea con esta declaración de intención, Devengo declara que:

- Protege de manera sistemática los datos confidenciales que gestiona por medio de diversos medios de monitorización y registro de acceso a dicha información, incluyendo la encriptación de aquellos datos considerados sensibles.

- Tiene un control sobre la integridad de dichos datos confidenciales para protegerlos de cualquier acceso o modificación no autorizada o pérdida.

- Realiza un seguimiento y registro exhaustivo seguro de todas las operaciones de pago para garantizar la trazabilidad en caso de ser necesaria.

- Dispone de una infraestructura robusta que permita el acceso y gestión de la información de manera constante.

Devengo controla, restringe y monitoriza que solo los empleados y partners autorizados acceden a estar información confidencial y sensible y que únicamente lo hacen al conjunto mínimo de información necesario.

Devengo está comprometida con proteger la información personal de los empleados de sus clientes de acuerdo a la Regulación General de Protección de Datos (RGPD), procesando en todo momento la información que recibe de manera legal, clara y transparente.

El compromiso de Devengo con la seguridad y la privacidad es tal, que todos sus diseños y desarrollos se hacen siempre con un conjunto de metodologías y técnicas que las anteponen ante todo.

Fernando Cabello-Astolfi
CEO

Objetivos

--- Conseguir y mantener el nivel de seguridad óptimo para **garantizar de forma adecuada la continuidad del negocio**, incluso en situaciones adversas.

--- **Incrementar la integración** y el apoyo mutuo de los aspectos físicos y lógicos de la seguridad.

--- Colaborar en la **gestión de las demás disciplinas de seguridad**, incluyendo los aspectos laborales y medioambientales, atendiendo a los criterios que potencien la Responsabilidad Social Corporativa.

--- Establecer **la estructura corporativa de seguridad** definida por los órganos de decisión de Devengo y crear los canales de comunicación adecuados entre todos los implicados.

--- **Cumplir con la normativa** oficial en materia de seguridad y otros requisitos.

--- Establecer e implantar Planes de **Formación y de Divulgación** de Seguridad entre los empleados de Devengo para mejorar la sensibilidad por todos los aspectos relativos a la seguridad.

--- Fijar un compromiso expreso por la mejora contínua.

--- Integrar a los distintos departamentos de la empresa en un sistema de gestión de la seguridad que, bajo criterios comunes, aproveche las sinergias y logre consistencia en los recursos y acciones.

People

--- La responsabilidad última de la seguridad corresponde al equipo directivo, que es quien analiza los riesgos y vulnerabilidades en materias de seguridad que puedan afectar al buen funcionamiento del negocio y el responsable directo de gestionar el desarrollo e implantación de las medidas para mitigarlos.

--- Todos los empleados firman un acuerdo de confidencialidad y su compromiso de seguimiento de la política interna de seguridad digital como parte del proceso de gestión interna.

--- Todo el equipo recibe formación en temas de seguridad y protección de datos en aquellos aspectos relevantes para su tarea y asume la responsabilidad de mantener la seguridad de los activos a su cargo.

--- Existe un procedimiento de entrada de nuevos empleados que no otorga permisos de acceso a información por defecto y de salida que elimina los accesos que hayan adquirido durante su permanencia en la empresa.

Activos y equipos

- Gestión centralizada con inventario global, monitorización y alertas.
- Política global de seguridad remota de los dispositivos con bloqueo, gestión de contraseñas, restricción de instalación de software, protección contra malware, firewall, encriptado de disco, actualizaciones y bloqueo remoto.
- Acceso al código fuente restringido y gestionado por claves privadas.
- Proceso de desarrollo que incluye registro de todo cambio, proceso de revisión de cada cambio y batería de test ejecutada de manera sistemática antes de aceptar cualquier modificación.
- Proceso centralizado de selección, contratación y gestión de proveedores de software-as-a-service.

Datos

--- Todos los datos, incluidos los backups, están almacenados en la Unión Europea.

--- Todos los datos sensibles se almacenan en base de datos con un sistema de protección BCrypt.

--- No se transmite información sensible a sub-procesadores (ej: procesadores de pago) más allá de la estrictamente necesaria y en dichos casos siempre se hace por medios de conexión seguros.

--- Toda comunicación se realiza con un cifrado de todos los datos que se transmiten por Internet (mediante certificado SSL RSA-2048 y conexión segura por HTTPS) o por medio de una VPN.

--- Solo los equipos de onboarding, soporte y el equipo técnico tienen acceso a los datos de los empleados, con una restricción proporcional a las razones para tal acceso, registrándose siempre dicho acceso.

--- La integridad de los datos se asegura por medio de una extensa batería de test que evitan errores de código que los modifiquen.

--- Seguimos buenas prácticas de diseño y desarrollo para prevenir el envío por canales no seguros de cualquier información de carácter protegido.

Legal

--- Contamos con un equipo de asesores que nos ayudan a mantener nuestro servicio siempre alineado con la legalidad en todos los ámbitos de aplicación: laboral, fiscal, contable, protección de datos y servicios financieros.

--- Todo cambio en la plataforma se realiza con las pruebas necesarias para asegurarnos de que eso sigue siendo así.

--- Contamos directa o indirectamente con las autorizaciones necesarias para ofrecer los servicios financieros que ofrecemos.

--- Proteger la privacidad de nuestros clientes y de sus empleados que utilizan nuestros servicios es algo que nos tomamos muy en serio y actuamos siempre dentro del ámbito de la GDPR con un modelo de encargado del tratamiento únicamente.

Plataforma tecnológica

- Toda la plataforma de Devengo está alojada en Amazon Web Services en sus centros de datos de la Unión Europea, siguiendo las directrices y controles de la ISO27001, HIPAA y SOC2 tipo II entre otras certificaciones de seguridad a la que se realizan auditorías con regularidad.

- Dispone del cifrado de todos los datos que se transmiten por Internet (mediante certificado SSL RSA-2048 y conexión segura por HTTPS).

- Los distintos entornos de desarrollo, demo y producción están estrictamente separados a todos los niveles para reducir errores y asegurar la máxima disponibilidad.

- Se realiza una monitorización permanente 24×7 de toda la plataforma para garantizar la salud de la misma y su disponibilidad.

- El acceso a la plataforma está debidamente protegido con las políticas de acceso de AWS y Heroku, protegido con autenticación de dos factores (2FA).

Auditoría y registro

- Utilizamos un registro general de todo uso de nuestra plataforma así como acceso y modificaciones de los datos.
- Registramos también todo tipo de eventos técnicos, como errores o picos de carga, de manera separada para asegurar el buen funcionamiento de la plataforma.
- El acceso a esos registros está debidamente restringido a las personas que lo necesitan y siempre con autenticación de dos factores (2FA).
- Los registros de auditoría se mantienen durante un año salvo aquellos aspectos que por ley puedan requerir un plazo mayor, como los movimientos de dinero.
- Se han definido alertas sobre dichos logs para poder detectar errores, riesgos de seguridad, cambios o seguimiento de la actividad en la plataforma.

No se registran en los logs datos considerados especialmente sensibles que pudieran ser un riesgo posterior en la seguridad, como por ejemplo contraseñas utilizadas por los usuarios al autenticarse.

Disponibilidad

- Todo el proceso de despliegue de la plataforma en Devengo está automatizado de manera que en caso de incidente somos capaces de arrancar una nueva instancia completa de la misma en menos de cinco minutos.

- Devengo dispone de un sistema de escritura en el que cada cambio realizado a los datos se escribe en registros de escritura anticipada, que se envían a un almacenamiento de alta durabilidad de varios centros de datos. En el improbable caso de una falla irrecuperable del hardware, estos registros se pueden 'reproducir' automáticamente para recuperar la base de datos a unos segundos de su último estado conocido.

- Mantenemos además replicada la base de datos principal como maestro-esclavo para asegurar la disponibilidad de los datos en caso de incidente.

- Devengo mantiene una política de copias de seguridad que realiza copias de seguridad incrementales y completas que se prueban regularmente.

- Mantenemos también un sitio con información de nuestro servicio al que pueden suscribirse los clientes que lo deseen.

Gestión de incidentes y continuidad

- Devengo tiene un procedimiento de gestión de incidentes de seguridad y formado a su equipo para responder a ellos.

- Cuando se detecta un incidente de seguridad, se notifica inmediatamente al equipo de guardia en ese momento y se define un plan para dar una respuesta lo más rápidamente posible para mitigar sus consecuencias.

- Tras las primeras acciones se definen las acciones para una solución permanente y se realiza un análisis post-mortem con medidas correctoras que se comparte con el resto de la empresa con el fin de evitar que vuelva a ocurrir en el futuro.

Datos de contacto y resolución de dudas

Si tienes alguna duda o necesitas ampliar información, no dudes en ponerte en contacto con nosotros vía:

Alberto Molpeceres, co-fundador de Devengo

security@devengo.com


devengo