Worky

Seguridad de la información en Worky

Índice:

01 - Introducción

Acerca de Worky:

Worky es el software de RH. que es inteligente, sencillo y te libera del estrés. Automatiza e integra tus procesos de Recursos Humanos y Nómina en solo lugar. Más de 50,000 usuarios y empresas en diferentes industrias depositan su confianza en nosotros.

Acerca de este Documento:

El siguiente documento describe la arquitectura de seguridad, políticas y procedimientos que Worky emplea en el desarrollo de su plataforma, ejecución de procedimientos operativos y de la operación en la nube de su infraestructura Cloud de la Plataforma Worky.

En Worky queremos siempre brindar un servicio excepcional para que nuestros clientes puedan cumplir todos sus objetivos de gestión de todo el ciclo de RH. Es por esto que aseguramos que ellos y sus datos estén seguros 24/7. Worky está comprometido con la transparencia acerca de sus prácticas de seguridad y con ayudar a sus clientes a comprenderlas.

02 - Seguridad organizacional

Worky posee un programa de seguridad dedicado a asegurar que cada cliente pueda tener el máximo nivel de confianza en la custodia de sus datos. El programa de seguridad de Worky está alineado con las prácticas del estándar ISO 27001 y es regularmente auditado.

Seguridad del Personal:

Las políticas de seguridad de la empresa son conocidas y aplicadas por todos los empleados (colaboradores) que poseen acceso a la información de clientes. Todos los colaboradores deben aceptar y cumplir nuestras normas de seguridad. Todos los colaboradores tienen firmado en sus contratos laborales estrictas cláusulas de confidencialidad y seguridad de la información.

Antes de tener acceso a los sistemas, todos los colaboradores deben aceptar los términos de confidencialidad y ser sometidos a un chequeo de sus antecedentes, además de acudir a un entrenamiento de seguridad. Este entrenamiento cubre temas de privacidad y seguridad, además del uso aceptable del equipamiento tecnológico de la empresa, prevención de malware, seguridad física, privacidad de los datos, gestión de cuentas, reporte de incidentes entre otros.

Al terminar su relación laboral con Worky, todos los accesos y permisos son revocados inmediatamente en nuestro sistema de autenticación y autorización.

Entrenamientos en Seguridad y Privacidad

Durante la vigencia de su contrato, todos los colaboradores de Worky deberán asistir a los entrenamientos de privacidad y seguridad al menos una vez por año. También será requerido que lean y firmen las Políticas de Seguridad y Privacidad de Worky. Es mandatorio para todo el personal activar un segundo factor de autenticación en todos los servicios usados según sus funciones. Todos los colaboradores que posean privilegios especiales (con mayor acceso a la información de clientes) recibirán además un entrenamiento especializado según su rol y función.

Todos los colaboradores tienen el deber de reportar incidentes de seguridad a los equipos internos apropiados. Los colaboradores serán oportunamente informados si en algún momento violan alguno de los términos que puedan incurrir en consecuencias, incluyendo su desvinculación con la empresa.

Profesionales Dedicados de Seguridad

Por medio del Área de Seguridad e Infraestructura, Worky dispone de un equipo dedicado, el cual es responsable de la implementación y el cumplimiento de las Políticas de Seguridad. El Área de Seguridad e Infraestructura es liderada por el *Chief Product and Technology Officer* (CPTO) de Worky con quién se definen y aprueban las políticas, procedimientos y planes de mejora a ser implementados.
Se definen los siguientes aspectos críticos de seguridad:

- **Seguridad del Producto**
  - Establecer estándares y prácticas seguras de desarrollo de *software*
  - Asegurar que existan procesos de detección y documentación de riesgos a nivel de proyecto.
  - Proveer de revisiones de diseño y código fuente para la detección oportuna de posibles fallas de seguridad.
  - Entrenar a los desarrolladores en las mejores prácticas de codificación segura.
- **Seguridad Operacional**
  - Construye y opera toda la infraestructura crítica de seguridad, incluyendo los servicios de autenticación y monitoreo de eventos.
  - Mantiene un archivo de los logs relevantes para las inspecciones de seguridad.
  - Aseguramiento de las configuraciones seguras en los entornos de producción.
  - Responder a alertas en caso de eventos de seguridad.
  - Manejar incidentes de seguridad
- **Riesgo y Cumplimiento**
  - Coordinar los test de penetración.
  - Manejar los escaneos de vulnerabilidades y sus remediaciones.
  - Coordinar las evaluaciones de riesgos regulares y darle seguimiento a los riesgos identificados.
  - Coordinar la auditoría y mantención de las certificaciones de seguridad.
  - Revisar y calificar la seguridad de los proveedores.

Todos los miembros del Área de Seguridad e Infraestructura de Worky se encuentran en un proceso continuo de aprendizaje y capacitación, cuenta con la certificaciones internacionales entre las cuales se destacan ISO/IEC 27001, especialidad en seguridad en la nube y ciclo de vida de desarrollo seguro (DevSecOps).

03 - Políticas y Estándares

Worky posee Políticas de Seguridad bien definidas que son aceptadas por la totalidad de sus empleados las cuales proveen las reglas básicas para la operación del negocio. Con ellas Worky asegura que sus clientes puedan confiar en sus empleados en cuanto a su ética y comportamiento al operar los diferentes servicios ofrecidos.

Las Políticas de Seguridad de Worky incluyen temas como:

- **Reglamento interno de trabajo.** Obligaciones y responsabilidades adquiridas por los empleados en el uso de la información.
- **Ciclo de vida de desarrollo.**
- **Plan de Continuidad del Negocio.**
- **Plan de Recuperación de Desastres.**
- **Gestión de Copias de Seguridad**

Estas políticas se encuentran en constante mejora, publicadas en un canal interno y son regularmente revisadas y actualizadas, según corresponda.

Auditorías:

Worky es auditado regularmente de forma interna y por empresas externas de seguridad, quienes se encargan de realizar inspecciones de seguridad a los procesos y políticas internas, así como también a la tecnología utilizada en los distintos productos de la empresa. Los resultados de las auditorías podrán ser compartidos con Worky, quienes se encargan de dar resolución a todos los hallazgos encontrados por los clientes y/o empresas externas de seguridad contratadas por los clientes o Worky.

Tests de Penetración:

Worky realiza pruebas de penetración a la plataforma Worky al menos dos veces al año. Estas pruebas son de tipo “caja negra” y podrán ser ejecutadas por el equipo interno de seguridad o a través de empresas externas de seguridad. El equipo de Seguridad e Infraestructura de Worky revisa y cataloga los resultados para su oportuna resolución. Los resultados de estas pruebas internas se tratan como información confidencial al interior de la organización.

Código fuente y data operativa:

Worky y sus empresas afiliadas son fabricantes y dueños de la propiedad intelectual de los productos principales y herramientas de apoyo necesarias para garantizar la operación. Worky proveerá a través de sus canales y productos, los mecanismos necesarios a sus clientes para que estos puedan consultar data operativa relevante a la función establecida en el contrato y acuerdos de niveles de servicio. Cualquier solicitud de acceso adicional a información generada por nuestras tecnologías y herramientas de apoyo deberá ser gestionada a través del KAM-AM *(Key Account Manager - Account Manager)* asignado a la cuenta. El Comité de Datos decidirá el alcance, mecanismos de entrega y restricciones de dichos activos información .

04 - Seguridad de aplicaciones Worky

Infraestructura Cloud

Worky opera toda su infraestructura de producción y ambientes previos en **Google Cloud Platform (GCP)**, quienes son líderes en la industria del *cloud computing* y ofrecen los mayores estándares y certificaciones de seguridad perimetral en sus data centers. Como parte de nuestra operación de tecnología, nos adherimos a las mejores prácticas de ISO27001 incluidas dentro del sello de seguridad *Google Cloud Architecture Framework*. Worky cumple con el 100% de las recomendaciones de dicho framework en sus pilares.

De manera adicional, Worky busca incorporar prácticas de cumplimiento con altos estándares del software, dichos estándares nos permiten cubrir escenarios de control y auditoría necesarios para que nuestros clientes puedan contar con entornos seguros. Finalmente para contar con un modelo estándar hemos adoptado el marco de control de prevención y detección de auditoría para responder a potenciales incidentes de seguridad en el marco de nuestra arquitectura de referencia.

Seguridad Perimetral:

El acceso a la infraestructura tecnológica de Worky es protegido por un *firewall* de red que se encuentra en el perímetro y permite proteger de ataques como DDoS *(Distributed Denial-of-Service Attack),* exploit's, ataques de hombre en el medio *(Man in the Middle)*, escalamiento de privilegios en la red, además de controlar el acceso a solo a direcciones IP permitidas. Por otra parte todo el tráfico WEB (https) que se recibe en el *firewall* de red es enviado a nuestro WAF *(Firewall de aplicaciones)*, debido a que es este el especialista en evaluar los posibles ataques a los servicios WEB existentes en la actualidad. Algunos de los ataques de los que nos protege el WAF son: inyecciones de SQL, Ataques XSS, Cross Site Request Forgery (CSRF), autenticaciones automatizadas, carga de contenido malicioso, entre otros.

Worky segmenta sus sistemas en su propia red VPC *(Virtual Private Cloud)*, a su vez este puede poseer hasta 2 entornos VPC diferentes configurados (producción y certificación), todos los componentes de cada sistema nuestro están completamente aislados el uno del otro. Sólo una pequeña parte de la infraestructura de producción y preproducción *(staging)* puede ser accedida directamente desde direcciones IPs autorizadas por personal calificado de Worky para tareas de operación y mantenimiento.

Monitoreo de Sistemas, Logs y Alertas:

Worky almacena de forma centralizada todos los logs de los sistemas en producción, tanto de los servidores utilizados por las aplicaciones productivas, como las aplicaciones auxiliares de uso interno. La información de los logs es utilizada para configurar alertas operacionales y realizar investigaciones internas, con una retención de 3 años.

Para todos los sistemas configurados en la nube de **Google Cloud Platform (GCP)** existe una política permanente de monitoreo mediante las herramientas de **Google Cloud Audit Logs** para el control de eventos, **Google Cloud Security Command Center** para la seguridad de redes, y **Google Cloud Security Scanner** para instancias. Adicionalmente, utilizamos un **APM** *(Application Performance Monitoring)* como Google Cloud Monitoring para monitorear absolutamente todas las instancias y bases de datos productivas.

Ciclo de vida de desarrollo:

Todo las fuentes y configuraciones de los productos Worky y aplicaciones auxiliares desarrolladas por la empresa se encuentran en un sistema de control empresarial de código fuente (Version Control System) protegido con segundo factor de autenticación (2FA), el cual se encarga de que el trabajo producido por los equipos revisado y aprobado por al menos dos miembros del equipo (antes de que sea integrado al proyecto), previo a la ejecución de nuestros CD *pipelines*.

En Worky hacemos *Continuous Delivery*, esto significa que todo el ciclo de vida de desarrollo se encuentra automatizado, y es orquestado por el "*deployment pipeline*". El *pipeline* se encarga de garantizar que todas las fases del paso a producción de un cambio en nuestras aplicaciones, se haga en el orden correcto y ejecutando pruebas automatizadas definidas por el equipo de desarrollo, arquitectura, seguridad, QA y devops.

Las fases de nuestro ciclo de vida de desarrollo y sus respectivas pruebas son:

1. **Fase de *commit*:** En esta fase se corren automáticamente tests unitarios, tests de integración y detección de bugs.
2. **Fase de aceptación:** Tests automáticos de todos los escenarios funcionales de la aplicación bajo análisis. En esta fase se realizan también pruebas de escenarios de seguridad enfocados en la integridad de la data transaccional.
3. **Fase de *release*.** En esta fase se envían los cambios a un ambiente pre productivo (staging) en donde se realizan revisiones manuales especiales del equipo de producto y seguridad.
4. **Producción. Masificación de los cambios a todos los clientes.** En esta fase se realizan monitoreos de todos los componentes en producción (salud, consumos, memoria, red). Adicionalmente se revisan las alertas automáticas en caso de eventos de seguridad y estabilidad. En caso de ser necesario hacer un rollback, nuestro deployment pipeline se encarga de llevarnos a la última versión estable del sistema previo al último release.

Reporte de Incidencias:

Worky posee un canal especial para el reporte de incidencias de seguridad, el cual está a cargo del Área de Seguridad e Infraestructura de Worky. Los clientes de Worky también tienen a su disposición la página de estatus además pueden reportar incidencias por medio del help center o también a través del correo soporte@worky.mx. Todas las incidencias serán valoradas por nuestro equipo de Seguridad e Infraestructura quienes tendrán las herramientas para poder hacer remediaciones inmediatas en la infraestructura tecnológica o harán el respectivo escalamiento a las células de desarrollo según lo determine el análisis.

Procesos de críticos de negocio

Ya en el marco del proceso de negocio, una vez que nuestros clientes o usuarios interactúan con nuestra tecnología, establecemos varios procesos de cobertura y prevención a nivel tecnológico, en este sentido, las condiciones de seguridad se automatizan para garantizar que se cuente con un proceso de detección de anomalías en el que los procesos de control se activan tanto para la originación (*onboarding*), como para los procesos críticos del negocio; nómina (*payroll*) y gestión de asistencia (*time and attendance*).

En este sentido, realizamos validaciones de seguridad enmarcadas en los siguientes procesos:

1. **Conocimiento de cliente (KYC) para Hiring y Payroll.** Validación de la información proporcionada a través de catálogos oficiales y terceros que se conectan a organismos gubernamentales como el IMSS y SAT.
2. **Prueba de Vida. Time and Attendance:** Comprobación de la similitud del documento de identidad frente a una selfie o un breve vídeo creando umbrales de confianza personalizados y haciendo pruebas de vida en tiempo real.
3. **Aceptación de términos y firma electrónica:** Firma digital de documentos de forma simple y compatible con dispositivos móviles.

Estos procesos aplican también para nuestros colaboradores, aplicamos un proceso de conocimiento del colaborador en el que adicionalmente se verifican sus antecedentes legales y criminales.

Protección de Datos de Clientes:

El objetivo del programa de seguridad de Worky es el de prevenir el acceso no autorizado a los datos de clientes. Para ello el equipo de Operaciones, en conjunto con las demás áreas, toman exhaustivos pasos para identificar y mitigar riesgos de seguridad, así como de implementar las mejores prácticas y evaluar constantemente nuevas formas para mejorar.

El equipo de operaciones realiza esta función basados en nuestro modelo de gobierno de datos.

Acceso a sistemas de información internos:

Existe una política del mínimo privilegio en Worky. Todas las configuraciones y desarrollos de la solución se realizan de forma automática con scripts de aprovisionamiento sin necesidad de tener accesos a las consolas de administración ni tampoco accesos privilegiados. Worky no entrega acceso a los datos de clientes a ningún colaborador a menos que este lo requiera en el estricto cumplimiento de sus funciones. El equipo de Seguridad e Infraestructura audita cada tres meses los accesos y privilegios a los sistemas de información.

Cuando un colaborador ingresa a trabajar a Worky sólo posee acceso a los sistemas básicos de correo y comunicaciones corporativas. Todo nuevo acceso a activos de información por parte de un colaborador, debe ser analizado por el *data steward* quien dará vía libre al equipo de infraestructura de proceder a hacer la asignación.

En Worky implementamos un modelo de autenticación y autorización basados en Single-Sign-On (SSO). Esto implica que todos los accesos a los sistemas de información propios o de terceros en Worky, se deben acceder con las mismas credenciales y políticas de acceso. Si un empleado deja la entidad o Worky decide revocar un determinado permiso en nuestro sistema de SSO, inmediatamente el empleado pierde el acceso a todos los sistemas de información. Todos los empleados de Worky deben configurar el segundo factor de autenticación (2FA) obligatoriamente (configuración default).

Cifrado de Datos.

Toda la comunicación entre Worky y los clientes es encriptada vía HTTPS TLS 1.3, este enlace seguro garantiza que todos los datos transferidos permanezcan privados.

Por la parte de comunicación en red, nuestro cliente web cuenta con un certificado de seguridad de 2048 bits, similar a la seguridad que se utiliza en las conexiones con los bancos, por lo que aseguramos que información en tránsito y así evitar el robo de información.

Backups de los datos.

Toda la información generada en nuestros sistemas de información cuentan con una política de retención y una configuración de sus respectivos backups. La ejecución de estos backups se realiza por medio de scripts automáticos en nuestra infraestructura tecnológica, dejando también un log de auditoría con el resultado de la ejecución.
La información cargada a Worky es automáticamente respaldada cada 24 horas, lo que permite prepararnos para cualquier tipo de eventualidad y actuar para restablecer los servicios a nivel plataforma.

Respuesta a Incidentes:

Worky posee políticas y protocolos para dar respuesta a potenciales incidentes de seguridad. Todos los incidentes son gestionados por el Área de Seguridad e Infraestructura. Worky define y clasifica los tipos de eventos que deberán ser manejados por el proceso de respuesta según su severidad. La atención y posteriores seguimientos se realizarán por medio la página de estatus así como del help center Worky y/o por medio del correo soporte@worky.mx.

Los protocolos de respuesta a incidentes son revisados y actualizados, según corresponda, de forma anual por el equipo de seguridad informática y Comité de Datos.

Destrucción de Datos:

Worky destruye toda la información de producción de los clientes que no posean contratos de usuarios activos. Todos los respaldos de información en bases de datos no podrán ser almacenados por más de 365 días una vez que la relación con el cliente haya terminado, eliminando su identidad en producción.

Seguridad de Equipos de Trabajo:

Worky posee Políticas de Seguridad que explican acerca del uso aceptable y seguro de los equipos de trabajo. Todos los equipos de trabajo deben estar encriptados y protegidos por una contraseña segura, la cual además deberá ser requerida cada vez que el equipo se encuentre en inactividad por un periodo corto de tiempo. La única forma de poder acceder a las herramientas internas de operación de los productos Worky es a través del agente instalado en los equipos que requieran accesos especiales. Este agente se encuentra asociado a nuestro SSO el cual obliga a todos los empleados a usar un segundo factor de autenticación.

Control de Sistemas Operacionales:

Todos los cambios al código y configuraciones de los sistemas de Worky son supervisados por procesos de aprobación de cambios y de revisión de código estático para prevenir la introducción de código malicioso a los repositorios.

Todos los servidores y sistemas utilizados en la operación de la plataforma y sus proceso de operación poseen los servicios que no son requeridos deshabilitados, removiendo las credenciales y cuentas por defecto.

El 100% del acceso a los sistemas de información internos o externos se debe hacer siempre a través de nuestro SSO. De esta misma forma, todos los logs de auditorías a los sistemas de información quedan centralizados utilizando el modelo de SSO mencionado en puntos anteriores.

05 - Recuperación ante Desastres y Continuidad Operacional

Worky opera siguiendo las mejores prácticas de Google Cloud Platform (GCP). Todos los sistemas operan de forma redundante en al menos dos zonas de disponibilidad y los respaldos de información en al menos dos regiones geográficas distantes entre sí.

Los servicios que por motivos de costos y eficiencia no sean requeridos para operar en modalidad de alta disponibilidad deberán al menos contar con un respaldo verificado para poder ser recreados en caso de pérdida.

Para más detalle acerca de los planes y estrategias de continuidad operacional favor referirse a los documentos; Plan de Continuidad de Negocios (BCP) y Plan de Recuperación de Desastres (DRP).

Modelo de Responsabilidad Compartida:

En el uso de los canales móviles, web, APIs u otros (con o sin uso de VPNs), Worky garantiza la seguridad perimetral de su solución de nube, custodia de propiedad intelectual de códigos fuentes y datos sensibles de usuarios, siguiendo las mejores prácticas de seguridad de la industria.

No obstante lo anterior, será responsabilidad de cada cliente realizar validaciones de seguridad e integridad en la data utilizada para transaccionar en los canales y monitorear los posibles usos fraudulentos de sus servicios expuestos. Worky no será responsable por el uso indebido de los canales y servicios expuestos en los puntos de integración operados por los clientes ni por perjuicios ocasionados por vulnerabilidades en sistemas que escapan de su control.