## Políticas de Seguridad

*Documento emitido en 2020 - 06 – 08*

¡ Su seguridad es muy importante para nosotros !. Aquí hay un resumen de lo que hacemos todos los días para garantizar que sus datos se encuentren seguros y que apliquemos las mejores prácticas de seguridad en nuestra versión alojada en Google Cloud Platform.

# Plataforma de Seguridad en la Nube de MyOwnApps

## 1. Respaldos/Recuperación de desastres

- Mantenemos 14 copias de seguridad completas de cada base de datos de Odoo durante y hasta 3 meses: 1 / día durante 7 días, 1 / semana durante 4 semanas, 1 / mes durante 3 meses (dependerá del plan de suscripción seleccionado).

- También se podrá descargar copias de seguridad manuales de sus datos en tiempo real y a cualquier momento utilizando el panel de control. Esta opción es nuestra mejor recomendación para usted como Cliente (dependerá del plan de suscripción seleccionado).

- **Recuperación de desastres:** cuando finalmente necesite esta estrategia para recuperar su información, nuestro plan consiste en almacenar su última copia de seguridad en nuestra plataforma o, si la suya es más reciente, podrá hacerlo automáticamente a través de su panel de control. Según su uso en nuestro sistema, nuestro tiempo de respuesta podría variar, pero nuestro tiempo de reacción mínimo sería de 24 horas después de que pudiera ocurrir este evento. Desafortunadamente, no podemos garantizar una tasa de recuperación de datos al 100%, se podrían perder datos al realizar una recuperación por desastre.

## 2. Seguridad en la Base de Datos

- Los datos de nuestros clientes son isolados y guardados en la base de datos que los mismos crean en nuestra plataforma. No hay forma de cruzar o compartir estos datos con otros usuarios alojados.

- Las reglas de control de acceso a datos implementan un aislamiento completo entre las bases de datos de clientes que se ejecutan en el mismo clúster, no es posible acceder de una base de datos a otra.

## 3. Seguridad en la Contraseña

- Las contraseñas de los clientes están protegidas con el cifrado PBKDF2 + SHA512 estándar de la industria, pero la seguridad de una contraseña muy segura y fuerte debe comenzar desde el mismo usuario. Por favor, no se asigne una contraseña fácil con palabras del diccionario (por ejemplo, 123456 o el nombre de su mascota). Es su responsabilidad mantener su contraseña segura.

- Nuestro personal nunca tendrá acceso a su contraseña y no podrá recuperarla por usted, la única opción si se le olvida será la de restablecerla. Incluso nuestro propio sistema no podrá acceder a élla ni como texto plano desencriptado.

- Las credenciales de acceso a su panel de control, siempre serán transmitidas de forma segura bajo el protocolo de seguridad HTPPS.

- Nuestra plataforma se ejecuta bajo Odoo versión 12.0, por lo tanto, los administradores de bases de datos de los clientes incluso podrán tener la opción de configurar la limitación de velocidad y la duración de frecuencia de intentos repetidos para poder ingresar e iniciar sesión válida.

- *Políticas de contraseña:* a partir de Odoo 12, los administradores de bases de datos tienen una configuración incorporada para aplicar una longitud mínima de contraseña de usuario. Otras políticas de contraseña como las clases de caracteres requeridas no son compatibles de forma predeterminada porque se ha demostrado que son contraproducentes.

# 4. Acceso del Personal de Trabajo

- Nuestro personal del servicio de asistencia puede iniciar sesión en su cuenta para acceder a la configuración relacionada con algún problema que se requiera soporte. Para esto, se usan propias credenciales especiales que tiene el personal de desarrollo, nunca su contraseña será revelada.

- Este acceso especial del personal mejorará la eficiencia y la seguridad: se puede reproducir inmediatamente cualquier tipo de problema que esté sucediendo, sin la necesidad de compartir su contraseña, ¡ y podemos auditar y controlar las acciones del personal involucrado por separado ! (Dependerá del plan de suscripción y la edición de Odoo).

- Nuestro personal del servicio de asistencia se esfuerza por respetar su privacidad tanto como sea posible, y solo accederá a los archivos y configuraciones necesarias para diagnosticar y resolver su problema o cualquier información que desee proporcionar de forma adicional para que pueda resolverlo a la mayor brevedad posible. Lo mismo aplicaría para un requerimiento.

# 5. Seguridad en el Sistema

- La plataforma MyOwnApps ejecuta una distribución de Linux muy segura con parches de seguridad actualizados.

- Las instalaciones son ad-hoc y mínimas para limitar la cantidad de servicios que podrían contener vulnerabilidades (por ejemplo, sin pila de PHP / MySQL).

- Solo el personal autorizado tiene autorización para administrar los servidores de forma remota, y el acceso solo es posible utilizando un par de claves SSH personal cifrado, desde una computadora con cifrado de disco completo.

# 6. Seguridad Física

La plataforma MyOwnApps está alojada en un centro de datos confiable como lo es Google Cloud Platform, y todo debe exceder nuestros criterios de seguridad física:

- Perímetro restringido, accesible físicamente solo por empleados autorizados del centro de datos.

- Control de acceso físico con distintivos de seguridad o seguridad biométrica.

- Cámaras de seguridad que monitorean las ubicaciones del centro de datos 7/24.

- Personal de seguridad en el sitio 7/24.

# 7. Comunicaciones

- Todas las conexiones web a instancias de clientes están protegidas con un cifrado TLS/SSL de 256 bits de última generación.
- Todos nuestros certificados SSL utilizan un sólido módulo de 2048 bits con cadenas de certificados SHA-2 completas.

# 8. Seguridad en el Software Odoo

Odoo CE (Community Edition) es de código abierto, por lo que los usuarios y colaboradores de Odoo en todo el mundo examinan continuamente toda la base del código. Los informes de errores de la comunidad son, por lo tanto, una fuente importante de comentarios sobre seguridad. Alentamos a los desarrolladores a auditar el código e informar problemas de seguridad.

Los procesos R&D de Odoo presentan pasos de revisión de código que incluyen aspectos de seguridad, para piezas de código nuevas y contribuidas (Se aplica a Odoo Enterprise Edition).

## 8.1 Seguro por diseño

Odoo está diseñado de una manera que evita la introducción de vulnerabilidades en seguridad más comunes:

- Las inyecciones de SQL se evitan mediante el uso de una API de nivel superior que no requiere consultas manuales de SQL.
- Los ataques XSS se evitan mediante el uso de un sistema de plantillas de alto nivel que no interpreta automáticamente los datos inyectados o manipulados.
- La estructura del código impide el acceso de RPC a métodos privados, lo que dificulta la introducción de vulnerabilidades explotables.

## 8.2 OWASP - Principales vulnerabilidades

Aquí es donde Odoo se destaca en la forma de enfrentar un problema de seguridad para las aplicaciones web, según lo enumerado por el Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP - Open Web Applications Security Proyect):

- *Fallas de inyección: las fallas de inyección, particularmente la inyección SQL, son comunes en las aplicaciones web. La inyección se produce cuando los datos proporcionados por el usuario se envían a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante engañan al intérprete para que ejecute comandos no deseados o cambie datos.*

  Odoo se basa en un patron de mapeo relacional de objetos (ORM) que abstrae la creación de consultas y evita las inyecciones SQL de forma predeterminada. Los desarrolladores normalmente no crean consultas SQL manualmente, son generadas por el ORM y los parámetros siempre se protegen correctamente.
- *Cross Site Scripting (XSS): los defectos de XSS ocurren cada vez que una aplicación toma datos proporcionados por el usuario y los envía a un navegador web sin validar o codificar primero ese contenido. XSS permite a los atacantes ejecutar scripts en el navegador de la víctima que pueden secuestrar sesiones de usuario, desfigurar sitios web, posiblemente introducir gusanos, etc.*

  La estructuración de código de Odoo controla y no interpreta por defecto todas las expresiones representadas en vistas y páginas, evitando XSS. Los desarrolladores deben marcar especialmente las expresiones como "seguras" para su inclusión en bruto en las páginas visualizadas.
- *Falsificación de solicitud de sitios cruzados (CSRF): un ataque CSRF obliga al navegador de una víctima que ha iniciado sesión a enviar una solicitud HTTP falsificada, incluida la cookie de sesión de la víctima y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la víctima a generar solicitudes que la aplicación vulnerable cree que son solicitudes legítimas de la víctima.*

# MyOwnApps – Políticas de Seguridad

El motor del sitio web de Odoo incluye un mecanismo de protección CSRF incorporado. Impide que cualquier controlador HTTP reciba una solicitud POST sin el token de seguridad correspondiente. Esta es la técnica recomendada para la prevención de CSRF. Este token de seguridad solo se conoce y está presente cuando el usuario accedió genuinamente al formulario del sitio web relevante, y un atacante no podrá falsificar una solicitud sin este token de seguridad previamente asignado.

● *Ejecución de archivos maliciosos: el código vulnerable a la inclusión remota de archivos (RFI) permite a los atacantes incluir código y datos hostiles, lo que resulta en ataques devastadores, como vulnerar totalmente el servidor.*

Odoo no expone funciones para realizar la inclusión remota de archivos. Sin embargo, permite a los usuarios privilegiados personalizar características agregando expresiones personalizadas que serán evaluadas por el sistema. Estas expresiones siempre son evaluadas por un entorno de espacio aislado y desinfectado que solo permite el acceso a las funciones permitidas.

● *Referencia de objeto directo insegura: una referencia de objeto directo ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, como un archivo, directorio, registro de base de datos o clave, como una URL o parámetro de formulario. Los atacantes pueden manipular esas referencias para acceder a otros objetos sin autorización.*

El control de acceso de Odoo no se implementa en el nivel de la interfaz de usuario, por lo que no existe ningún riesgo al exponer referencias a objetos internos en las URL. Los atacantes no pueden eludir la capa de control de acceso manipulando esas referencias, porque cada solicitud aún tiene que pasar por la capa de validación de acceso a datos.

● *Almacenamiento criptográfico inseguro: las aplicaciones web rara vez usan funciones criptográficas de manera adecuada para proteger datos y credenciales. Los atacantes usan datos poco protegidos para llevar a cabo el robo de identidad y otros delitos, como el fraude con tarjetas de crédito.*

Odoo utiliza el hashing seguro estándar de la industria para las contraseñas de usuario (por defecto PKFDB2 + SHA-512, con estiramiento de clave) para proteger las contraseñas almacenadas. También es posible utilizar sistemas de autenticación externos como OAuth 2.0 o LDAP, para evitar el almacenamiento local de contraseñas de usuario.

● *Comunicaciones inseguras: las aplicaciones con frecuencia no pueden encriptar el tráfico de red cuando es necesario proteger las comunicaciones confidenciales.*

Nuestra plataforma MyOwnApps se ejecuta siempre bajo el protocolo de seguridad HTTPS, como se puede observar en su navegador en estos momentos.

● *Error al restringir el acceso a URL: con frecuencia, una aplicación solo protege la funcionalidad sensible al evitar la visualización de enlaces o URL a usuarios no autorizados. Los atacantes pueden usar esta debilidad para acceder y realizar operaciones no autorizadas accediendo a esas URL directamente.*

El control de acceso de Odoo no se implementa a nivel de la interfaz de usuario, y la seguridad no depende de ocultar URL especiales. Los atacantes no pueden eludir la capa de control de acceso reutilizando o manipulando cualquier URL, porque cada solicitud aún tiene que pasar por la capa de validación de acceso a datos. En casos excepcionales en los que una URL proporcione acceso no autenticado a datos confidenciales, como las URL especiales que utiliza el cliente para confirmar un pedido, estas URL se firmarán digitalmente con tokens únicos y solo se enviarán por correo electrónico al destinatario previsto.