SEAJAL
Sistema Estatal Anticorrupción de Jalisco
Secretaría Ejecutiva

Dirección de Tecnologías y Plataformas

Recomendaciones de Seguridad Informática en la instalación y uso del SiDECLARA SESAJ

Contenido

Presentación

SiDECLARA SESAJ es un sistema de información desarrollado por la Secretaría Ejecutiva del Sistema Anticorrupción de Jalisco, que permite la captura de la declaración de situación patrimonial, de intereses y constancia de presentación de la declaración fiscal, para dar cumplimiento a lo establecido por la LGRA.

Implementa los nuevos formatos de uso obligatorio a partir de mayo del 2021.

El sistema es desarrollado con herramientas de software libre y basado en Linux para servidores, es intuitivo, de navegación sencilla, incluye ayudas, tips, y preguntas frecuentes, además es personalizable a la imagen institucional de cada ente público.

El sistema también facilita la conexión e interoperabilidad con la PDN, al incluir el API correspondiente. Incluye un módulo de administración que distingue a los usuarios con los roles de Administrador y de Órgano Interno de Control.

En este documento se presentan algunas recomendaciones de seguridad que pueden ser implementadas por el ente público y se divide en dos partes, la primera de ella son las relacionadas directamente con el SiDECLARA SESAJ, en la segunda parte se presentan recomendaciones generales no relacionadas directamente con el SiDECLARA SESAJ pero que pueden ayudar a contar con un esquema de seguridad más robusto para el ente público.

Este documento contiene solo algunas recomendaciones de seguridad, para alguna de ellas se menciona “el qué hacer” más no “el cómo hacerlo” ya que esto dependerá del tipo de infraestructura, así como de la arquitectura y configuración de la red, sistemas operativos y servicios asociados.

Este documento no pretende ser un documento exhaustivo o sustituir reglamentos, estándares o normas de seguridad de la industria de la tecnología de la información y comunicación.

SiDECLARA SESAJ por sí mismo implementa los siguientes mecanismos de protección.

- Aislamiento en una máquina virtual, a través de Dockers en donde el único punto de acceso es el puerto de NGINX.
- Ocultamiento de las variables de la BD como son el usuario y contraseña, manejadas a través de variables de entorno.
- Ocultamiento del tipo de BD, el sistema utiliza un ORM (Object Relational Model) que utiliza un lenguaje optimizado y oculta los detalles de la BD utilizado.
- Uso del protocolo OAUTH2 para la conexión con la PDN, a través de tokens y de control de aplicaciones.
- Establecimiento de un mecanismo de protección contra ataques DDoS.

Consideraciones de uso y responsabilidades

La descarga de la copia del código fuente del SiDECLARA SESAJ para su uso, se realiza a título gratuito, y sin fines de lucro, esto no comprende la cesión de los derechos de autor patrimoniales, ni morales, mismos que se encuentran contemplados en la legislación vigente y en los tratados internacionales de los que nuestro país forma parte de los Derechos de Autor.

El ente público o usuario que utilice o descargue el SiDECLARA SESAJ no está autorizado a ofrecer la redistribución, compartición o venta del software, por lo que, queda prohibida la copia, distribución, comunicación pública, instalación, acceso y cualquier otra forma de reproducción y/o explotación parcial o total del software denominado SiDECLARA SESAJ.

El ente público es el responsable de la seguridad física y lógica de la infraestructura donde instale el SiDECLARA SESAJ, así también como del resguardo de la información, datos o documentación que se encuentre contenida en las declaraciones patrimoniales que se alojen en el software, misma que será utilizada exclusivamente para los fines establecidos en las Leyes General de Responsabilidades Administrativas y de Responsabilidades Políticas y la análoga de su entidad, así como cualquier otra normativa que resulte aplicable.

El sistema SiDECLARA SESAJ se proporciona en las condiciones que se encuentra, no obstante que la Secretaría Ejecutiva del Sistema Anticorrupción de Jalisco ha hecho el mejor de sus esfuerzos, no es posible garantizar que el sistema esté libre de fallas.

La Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco no será en ningún caso considerado responsable de los daños, directos o indirectos, o pérdidas (pérdidas lucrativas, actividad interrumpida, pérdida de información u otras pérdidas de tipo económico, incluyéndose, sin límite, los que deriven de pérdida de beneficios, interrupción de la operación, pérdida de información o cualesquiera otras pérdidas pecuniarias) originadas como consecuencia de la utilización o imposibilidad de utilización del SiDECLARA SESAJ.

Considerando que el SiDECLARA SESAJ es distribuido y puesto a disposición sin ningún costo, la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco no se encuentra obligada a brindar ningún tipo de servicio de soporte técnico, sin embargo, voluntariamente y de acuerdo con su disponibilidad de recursos podrá brindar asesoría bajo un esquema de “mejor esfuerzo” o convenios de participación con el ente público.

Para más información al respecto, favor de consultar los Términos y Condiciones de Uso del SiDECLARA SESAJ

1. Recomendaciones propias del SiDECLARA SESAJ

Deshabilitar el modo debug en Django

En algunos casos, sobre todo durante el proceso de instalación y puesta a punto, SiDECLARA SESAJ es recomendable ejecutar el sistema con el modo de depuración web activo Django (DEBUG = True).

El modo de depuración permite la visualización de páginas de error de forma detallada. Lo que facilita la corrección de errores e implementación de mejoras en el funcionamiento del sistema, como se muestra a continuación:

Imagen 1: Página de error obtenida cuando se encuentra el modo debug activado

Sin embargo, utilizar el modo depuración en un sistema productivo, representa un riesgo de seguridad, ya que un atacante puede obtener información sobre el funcionamiento del sistema y utilizarla para propósitos maliciosos.

Una vez que el sistema entre en operación, **ES ALTAMENTE RECOMENDABLE** deshabilitar el modo DEBUG esto se hace editando el archivo “settings.py”, en la ruta proyecto\declaraciones\declaraciones, y estableciendo el siguiente valor DEBUG = False.

Referencia:
https://docs.djangoproject.com/en/1.8/ref/settings/#std:setting-DEBUG.

Cambiar el password por defecto de la cuenta admin

Es de uso común incluir establecer una contraseña genérica por defecto en los equipos y sistemas informáticos, esto es para facilitar el acceso la primera vez que se utilizan.

Sin embargo, **ES ALTAMENTE RECOMENDABLE** cambiar el password inmediatamente, tal como se señala en el manual de instalación. En el directorio donde se encuentra el archivo de instalación se encuentra el script de creacion de superusuararios, llamado asi createsuperuser responda a las preguntas para crear un superusuario.

Con estas claves entre al panel de administración y desactive o elimine el usuario de admin admin que viene por default. El no realizar este cambio representa un potencial y grave problema en la seguridad.

Cambio de password de usuario de base de datos

Otra de las recomendaciones de seguridad, incluidas en el manual de instalación, es la de cambiar el usuario y password por defecto de la base de datos que se incluye en el código del SiDECLARA SESAJ.

Para esto, previo a la instalación, se debe editar el archivo oculto en la ruta proyecto/.env y ajustar los campos “user” y “password” así como el nombre de la base de datos.

También, dependiendo de la cantidad de usuarios y del diseño de la arquitectura de la infraestructura, se puede separar la base de datos del servidor del aplicativo, esto ayudará a proteger la información en caso de que el servidor donde se instaló el SiDECLARA SESAJ falle.

Actualizaciones del SiDECLARA SESAJ

Como todo sistema complejo, el SiDECLAR SESAJ evoluciona en gran medida gracias a las observaciones de ustedes, por lo que eventualmente se requieren actualizaciones para reflejar esos cambios necesarios. El SiDECLARA ya tiene un grado de madurez tal que sus actualizaciones son muy sencillas,

El proceso de actualización se encuentra en el sitio privado del SiDECLARA SESAJ. Aplicar las actualizaciones no impacta o modifica la base de datos, por lo que esto se realiza de manera rápida y sencilla.

Habilitar / configurar función recaptcha

SiDECLARA SESAJ cuenta con el mecanismo de recaptcha, el cual es utilizado para prevenir ataques automatizados que puedan afectar el funcionamiento del sistema por tener que atender peticiones en volumen.

El SiDECLARA permite inhibir el uso de esta característica en caso de que la institución así lo decida. En este caso el captcha no se despliega en las pantallas de entrada y se corre el riesgo de ser atacado, esta es una decisión de la entidad

En caso de requerir el captcha para asegurar la protección, es necesario obtener el código del sitio y la clave secreta que Google proporciona para activar esta característica. Para obtener este código y claves seguir las instrucciones en la liga https://developers.google.com/recaptcha/docs/display

Para habilitar y configurar la función recaptcha, es necesario entrar a la página de personalización del sitio en http://TUSITIO/admin/sitio/sitio_personalizacion/1/change/

Contraseña de usuarios

El SiDECLARA SESAJ tiene configurada algunas políticas de contraseñas de usuarios para hacer más segura su operación, entre ellas:

- La contraseña no puede asemejarse tanto a otra información personal
- La contraseña debe contener al menos 8 caracteres.
- La contraseña no puede ser una clave utilizada comúnmente
- La contraseña no puede ser totalmente numérica.

Protección ataques DDoS en NGINX

SiDECLARA SESAJ habilita un mecanismo de limitación de carga para la defensa de ataques DDOS (Distributed Denial Of Services), este mecanismo se basa en la configuración de NGINX para limitar la carga que el sistema puede manejar y rechazar las peticiones fuera de estos límites.

Para este propósito el NGINX que es el servidor de web HTTP, requiere del siguiente código para habilitar este mecanismo.

Este código se reparte en dos archivos:

- En el archivo serv_prox/nginx.conf línea 18, insertar el código #limit_req_zone $binary_remote_addr zone=zone1:10m rate=30r/s;
- En el archivo serv_prox/conf/default.conf linea 19, insertar el código #limit_req zone=zone1;

Inicialmente se ha configurado para 30r/s o 30 peticiones por segundo, dependiendo de su servidor y de la carga que recibe, será necesario ajustar este limite

Términos y condiciones (PDF)

Otra de las funciones del SiDECLARA SESAJ relacionadas con la seguridad de la información, en este caso relacionado con el cumplimiento de la Ley General de Protección de Datos Generales en posesión de sujetos obligados; la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios y leyes relacionadas en la materia; es la de poder configurar un documento totalmente personalizable de “Términos y condiciones” donde se especifique el uso y protección que el ente público dará a los datos recabados.

Este documento podrá ser consultado por cualquier usuario previo al registrar su cuenta en la página: /declaracion/registro/nuevo

Este documento debe ser generado por la institución y debe reflejar desde el aviso de privacidad de los datos, así como la obligación de cada servidor de presentar sus declaraciones en el tiempo y forma establecido en la Ley General de Responsabilidades Administrativas.

Este documento puede ser personalizado, seleccionando el documento apropiado.

2. Recomendaciones generales o fuera del alcance del SiDECLARA SESAJ

Implementación o configuración de un firewall

Se recomienda implementar o bien configurar un mecanismo de control de acceso al servidor donde se aloje el SiDECLARA SESAJ.

Como sugerencia se deberá restringir el acceso a solo las direcciones IP específicas que deban acceder al servidor de forma pública, o en su defecto a rangos de direcciones IP.

También se recomienda utilizar una política de abrir solamente los puertos TCP/UDP mínimos indispensables para el funcionamiento del servidor.

Evaluar limitar acceso desde cualquier parte del mundo

Como un punto de mejora para la seguridad de la información del sistema SiDECLARA y su infraestructura tecnológica que lo soporta, y debido a que el sistema puede tener solo un alcance local para ser accedido desde una región o país en específico, en caso de ser posible y de acuerdo con las reglas de operación del sistema, se recomienda incorporar restricciones adicionales de conexiones por países, regiones o lugares desde los cuales no se espera tener conexión alguna o solo permitirlos para los lugares, países o regiones desde los cuales si se realizará una conexión.

Este tipo de restricciones puede ayudar a limitar los ataques provenientes de otros lugares que no deben tener acceso al sistema.

Incluso puede llevarse al extremo de solo permitir el acceso a sistema desde una computadora o una red privada local (ejemplo 192.168.X.X).

Usar llaves secretas

Este valor [la configuración SECRET_KEY] es la clave para proteger los datos firmados; es vital que lo mantenga seguro, o los atacantes podrían usarlo para generar sus propios valores firmados.

(También se hace referencia a esta sección de la documentación de Django para la configuración "SECRET_KEY").

La API de firma criptográfica en Django está disponible para cualquier aplicación para firmas criptográficamente seguras en valores. El propio Django hace uso de esto en varias funciones de nivel superior:

Firma de datos serializados (por ejemplo, documentos JSON).

Tokens únicos para una sesión de usuario, solicitud de restablecimiento de contraseña, mensajes, etc.

Prevención de ataques entre sitios o de reproducción agregando (y luego esperando) valores únicos para la solicitud.

Generando una sal única para funciones hash.

La respuesta genérica es: hay muchas cosas en una aplicación de Django que requieren una firma criptográfica, y la configuración "SECRET_KEY" es la clave que se usa para eso. Debe tener una cantidad de entropía criptográficamente fuerte (difícil de adivinar para las computadoras) y única entre todas las instancias de Django.

Generación de llaves secretas

Para generar una llave secreta utilizar el script secret.py proporcionado en el ZIP. Ejecutarlo con el siguiente comando :

Python secret.py > key

Editar el archivo key, copiar el valor guardado en el archivo. Editar el archivo proyecto/declaraciones/.env en el espacio de la variable SECRET_KEY.

Habilitar el tráfico encriptado usando el protocolo HTTPS

Debido a que el SiDECLARA SESAJ maneja información sensible como usuario y password, así como todos los datos que se envía y se reciben, se recomienda deshabilitar el puerto 80 o bien redirigir el tráfico al puerto de un protocolo seguro como lo es HTTPS.

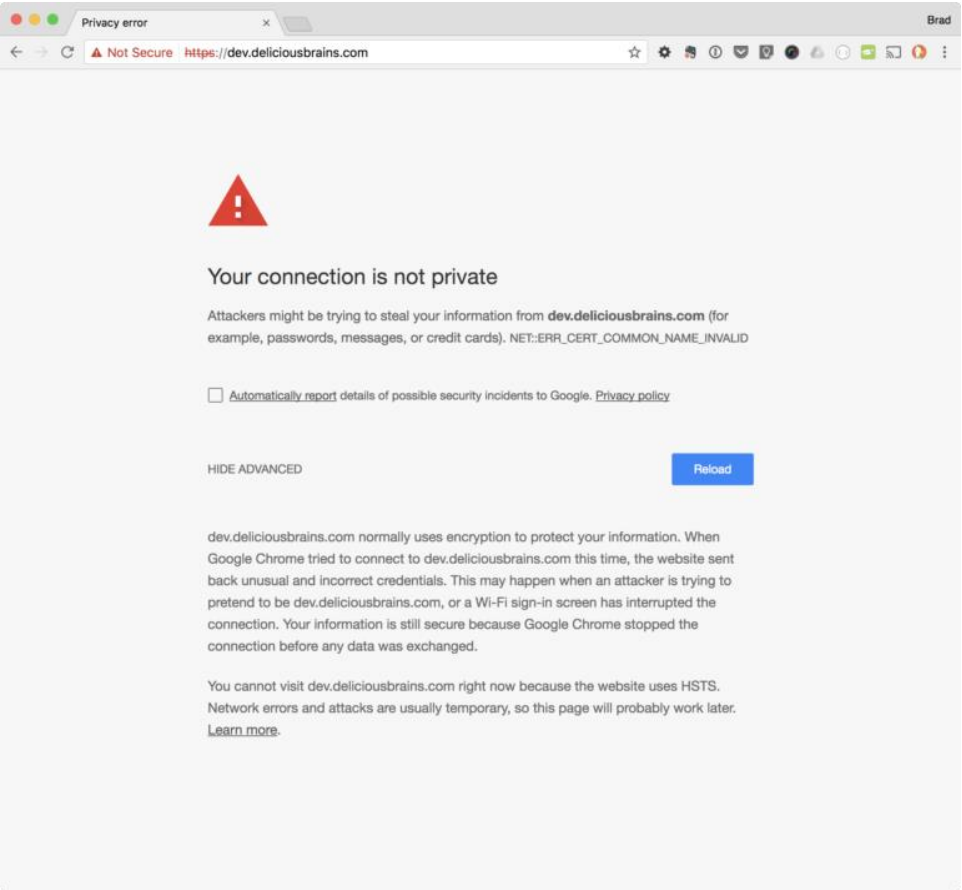
El puerto 80 o el uso del protocolo HTTP, no maneja cifrado y toda la comunicación se realiza en texto plano, esto lo hace susceptible a posibles ataques de “sniffing”.

Para habilitar el uso del protocolo https es posible hacerlo por cualquiera de las dos vías siguientes:
A) utilizar un browser como proxy, que redireccione el tráfico del puerto 443 y que maneje los certificados ssl y toda la comunicacion encriptada y la redireccione al puerto 80 en donde escucha el sistema.

B) Modificar al sistema, en el docker-compose.yml exponer el puerto 443 y configurar los certificados en los archivos del NGINX. Para este proceso pueden ustedes guiarse con la ayuda de los siguientes links.
https://faun.pub/setting-up-ssl-certificates-for-nginx-in-docker-environ-e7eec5ebb418
https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-nginx-in-ubuntu-16-04

Se aclara que para habilitar el protocolo HTTPS se requiere la generación de un certificado SSL. Estos certificados pueden ser provistos por el provedor de Internet o generados por ustedes mismos https://deliciousbrains.com/ssl-certificate-authority-for-local-https-development/

Se recomienda acudir a una autoridad certificadora (verisign, godaddy, su ISP) para no sufrir errores como los mostrados en a imagen



Actualización de Sistema Operativo y aplicativos

Las actualizaciones en el Sistema Operativo y aplicaciones instalan mejoras en el funcionamiento y en la seguridad del software.

En muchos casos las actualizaciones permiten solucionar errores, solucionar vulnerabilidades e incluir nuevas funciones.

No actualizar el sistema operativo del servidor puede provocar que éste quede expuesto a fallas y vulnerabilidades de seguridad que facilitan el robo de información personal y la invasión de privacidad.

EL uso de dockers de alguna manera aisla al sistema de cambios en el entorno del sistema operativo, Por lo que si se tiene una buena política de respaldos las actualizaciones del SO no lo afectan.

Diseño de la arquitectura / capacidad suficiente del servidor

SiDECLARA SESAJ está desarrollado con software libre, es decir, no se requiere el pago de licenciamiento de software, sin embargo, se requiere un hardware mínimo para un buen desempeño del sistema, el cual se puede consultar en https://seajal.org/declaraciones

Dependiendo de la cantidad de usuarios a manejar, y particularmente para un número elevado de los mismos (por ejemplo, más de 5mil usuarios) se sugiere el diseño de una arquitectura especializada en alto rendimiento y alta disponibilidad; ejemplo de soluciones que pueden aplicarse son: balanceadores de carga, replicadores de información, o incorporar distintas zonas de disponibilidad.

Durante la fase de producción del sistema, será necesario monitorear el desempeño del servidor y en su caso ajustar la capacidad de procesamiento, almacenamiento y memoria conforme al número de usuarios crezca o se capturen mayor número de declaraciones.

Conocimientos básicos sobre las aplicaciones

Finalmente se recomienda adquirir conocimientos mínimos básicos de las aplicaciones sobre las que corre el SiDECLARA SESAJ, esto ayudará con la instalación del sistema, comprender mejor el funcionamiento su funcionamiento, corregir y prevenir errores de operación. Entre los sistemas/tecnologías sobre las que se recomienda capacitación se encuentra:

- Uso del sistema operativo Linux, en particular uso de la consola de comandos, así como configuración de permisos de archivos, directorios y cuentas de usuarios.
- Uso de contenedores: Docker, Docker compose
- Conocimiento sobre base de datos
- Configuración de servidor web NGINX
- Conocimiento básico de configuración de redes