Documento Técnico de Seguridad para la empresa

Cobranza AAS S.C.

Elaborado por.

Brandan Jimenez

Nestor Rubio

Juan Urmeneta

El presente documento tiene como objetivo ser la documentación de seguridad para los obligados en la realización de la actividad de cobranza por parte de AAS S.C. En el cumplimiento a las disposiciones del artículo 35, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado X y sus Municipios.

Es importante señalar que este documento es obligatorio para los sujetos obligados, ya que serán los responsables del tratamiento de los datos personales. Este documento puede sufrir cambios dependiendo de la evolución del sistema y la necesidad tanto del cliente como del usuario.

ÍNDICE

[Tipos de seguridad](#_47as17mqqx3a)

[Medidas de seguridad implementadas](#_tkky2o9y5hva)

[Implementación de acciones](#_6wgwq0jtgkwk)

[contra inyección SQL.](#_6wgwq0jtgkwk)

[Supervisas las modificaciones](#_uife6irh4xpf)

[automáticas en las aplicaciones](#_uife6irh4xpf).

[Proporcionar una protección](#_3kzpbgwkxouo)

[al servidor](#_3kzpbgwkxouo).

[Blindaje de la base de datos e](#_nlvbyqp5zwzy)

[implementación de Blockchain](#_nlvbyqp5zwzy).

[Aseguramiento de la BD](#_j1a0inw2wpwn)

[por medio de contraseñas.](#_j1a0inw2wpwn)

[Manera en que las claves](#_834j1m2kbzwv)

[se cifran en la BD](#_834j1m2kbzwv)

[Manera en que los campos de](#_93ewyqz7zmnx)

[entrada son validado](#_93ewyqz7zmnx)

[Utilización de protocolos de](#_mw37de26l6i4)

[comunicación seguros.](#_mw37de26l6i4)

# Tipos de seguridad

Es importante aclarar las diferencias que existen entre las medidas de seguridad administrativa, física y técnica.

*a) Las medidas de seguridad administrativa son aquellas que deben implementarse para la correcta función del capital humano de la empresa:*

• **Política de seguridad**. Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado, en este caso los gestores de cobranza y la administración.

• **Cumplimiento de la normatividad.** Los controles establecidos para evitar violaciones de la normatividad vigente (art. 35), obligaciones contractuales o la política de seguridad interna de la organización AAS S.C. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable, especialmente el artículo 35 de la Ley Federal de Protección de Datos.

• **Organización de la seguridad de la información.** Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna de los gestores y administradores, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, considera aspectos externos como la identificación de riesgos relacionados con terceros.

• **Seguridad relacionada a los recursos humanos.** Controles orientados a que el personal (gestores y administradores) conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral de gestores de cobranzas.

• **Administración de incidentes.** Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.

• **Continuidad de las operaciones.** Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación de cobranza del sujeto obligado(gestor y administrador).

*b) Las medidas de seguridad física atañen a las acciones que deben implementarse para contar con buenas prácticas del ambiente físico donde está montado el sistema:*

• **Seguridad física y ambiental.** Establecimiento de controles relacionados con los perímetros de seguridad física y el entorno ambiental de los activos, con el fin de prevenir accesos no autorizados, daños, robo, entre otras amenazas. Se enfoca en aspectos tales como los controles implementados para espacios seguros y seguridad del equipo de la organización.

*c) Las medidas de seguridad técnica son las aplicables al sistemas de cobranza para la empresa AAS S.C. para el uso técnico de seguridad en el programa de la empresa*

# Medidas de seguridad implementadas

## Implementación de acciones contra inyección SQL.

## 

## Supervisas las modificaciones automáticas en las aplicaciones

Todos los implicados en la creación de la aplicación web deben conocer los riesgos asociados a estas vulnerabilidades. De esta manera, se debe proporcionar información y capacitación a todo el personal involucrado en estos procesos.

Supervisar las modificaciones automáticas en las aplicaciones, es decir, comprobar mediante un script PHP los datos esperados. El proceso de filtrado se encarga de ignorar caracteres especiales.

No generar ningún mensaje de error externo que pueda revelar información sobre el sistema o la estructura de la base de datos utilizada

Utilizar Prepared Statements los cuales reducen el riesgo de ataques de inyección SQL debido a su esctructura de instrucciones con parámetros que transmiten el comando SQL real a la base de datos, así que el propio sistema de gestión de la base de datos los ejecuta y enmascara automáticamente los caracteres especiales.

## 

## Proporcionar una protección al servidor

Además de respetar la decisión que los datos estén en servidores propios de la empresa ASS S.C. La siguiente medida de seguridad que se recomienda es el endurecimiento del sistema operativo de acuerdo al patrón:

* Instala y activa únicamente las aplicaciones y servicios que son fundamentales para la base de datos.
* Elimina todas la cuentas de usuarios que no estén en uso y ya no sean relevantes para la empresa.

Es necesario que conforme evolucione el desarrollo o aplicación web se le instalen sistemas de detección de intrusiones (IDS) o sistemas de prevención de intrusiones (IPS) los cuales detectan ataques contra el servidor a tiempo y alerta al administrador en el caso de detectar un ataque en contra del servidor a tiempo.

La implementación de una capa en la aplicación (Aplication Layer Gateway) que monitore directamente, en nivel aplicación, el tráfico entre las aplicaciones y el navegador web.

## Blindaje de la base de datos e implementación de Blockchain

Configurar una cuenta de base de datos que está destinada únicamente para el acceso desde la web y que tenga derechos de acceso mínimos. Almacenar toda la información confidencial de las contraseñas de manera cifrada en la base de datos bajo un gestor de tecnología blockchain. Esto le permitirá al administrador tener varias contraseñas robustas y complejas y poder cambiarlas cada cierto tiempo dentro de una misma base de datos distribuida. Esto hace que la probabilidad de ser descifradas sea muy escasa

## 

## Aseguramiento de la BD por medio de contraseñas.

Las contraseñas serán cambiadas cada cierto tiempo y serán gestadas por el administrador con un gestor de contraseñas blockchain.

## Manera en que las claves se cifran en la BD

“El método deberá solicitarle al usuario una contraseña que sirva para crear esta clave de cifrado. Deberá utilizarse un método que compruebe que la contraseña introducida por el usuario cumple con los requisitos de longitud de contraseña. Se recomienda que la contraseña tenga entre 8 y 32 caracteres. Debe mezclar letras mayúsculas, minúsculas y al menos un número o caracter especial [2]. El usuario crea la base de datos cifrada indicando la clave de cifrado en el proceso, posteriormente, para conectarse y utilizarla deberá ingresar dicha clave.”(Villalobos, 2021)

## Utilización de protocolos de comunicación seguros.

* **“HTTP** (REST/JSON) (*Hypertext Transfer Protocol*) es un protocolo cliente/servidor sin conexión presente en las TIC y en la web. Es un protocolo muy accesible por ser de código abierto, además de poseer numerosas librerías. Es efectivo para enviar grandes cantidades de información, como por ejemplo lecturas de sensores minuto a minuto o cada hora; aunque no es adecuado ni para enviar actualizaciones en periodos de tiempo del orden de milisegundos ni para enviar información de video. Es muy recomendable asegurar la información transmitida aplicando el protocolo criptográfico SSL/TLS sobre HTTP, lo que genera el protocolo de aplicación HTTPS. No obstante, el método más seguro consiste en incluir en el dispositivo IoT solo un cliente HTTP, no un servidor HTTP, de manera que el dispositivo IoT pueda iniciar conexiones a un servidor web, pero no sea capaz de recibir solicitudes de conexión.”()

Referencias

n.a.. (septiembre 4, 2019 ). Inyección SQL: la importancia de proteger tu sistema de base de datos. Abril 24, 2021, de Digital Guide Ionos Sitio web: <https://www.ionos.mx/digitalguide/servidores/seguridad/inyeccion-sql-principios-y-precauciones/>

n.a.. (diciembre 26, 2013 ). Ataques de inyección SQL: qué son y cómo protegerse

. Abril 24, 2021, de Hostalia Sitio web: <https://pressroom.hostalia.com/white-papers/ataques-inyeccion-sql/>

Minero, J.. (2011). Mejores prácticas para evitar inyecciones SQL en proyectos PHP y PostgreSQL. En Identificación y Clasificación de las Mejores Prácticas para Evitar la Inyección SQL en Aplicaciones Desarrolladas en PHP y PostgreSQL(50). Zacatecas, Zac: CIMAT.

Padrón, A. Prieto, R., Herrera, A., Calva, G.. (Octubre, 2014). Implementación de Protocolos de Comunicación Seguros: Escenarios. ResearchGate, ISSN 2395-8499, 9. 2021, Abril 24, De Google Scholar Base de datos.

n.a.. (febrero 08, 2019 ). [IoT: protocolos de comunicación, ataques y recomendaciones](https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones)

. Abril 24, 2021, de Incibe-cert Sitio web: <https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones>

n.a.. (noviembre 04, 2020 ). Protocolos de comunicación de redes. Abril 24, 2021, de Kio Network Sitio web: <https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes>

n.a.. (julio 02, 2018 ). [Así es B.Lock, un gestor de contraseñas basado en Blockchain más seguro](https://www.redeszone.net/2018/07/02/b-lock-gestor-contrasenas-blockchain/). Abril 24, 2021, de RZ Redes Zone Sitio web: <https://www.redeszone.net/2018/07/02/b-lock-gestor-contrasenas-blockchain/>