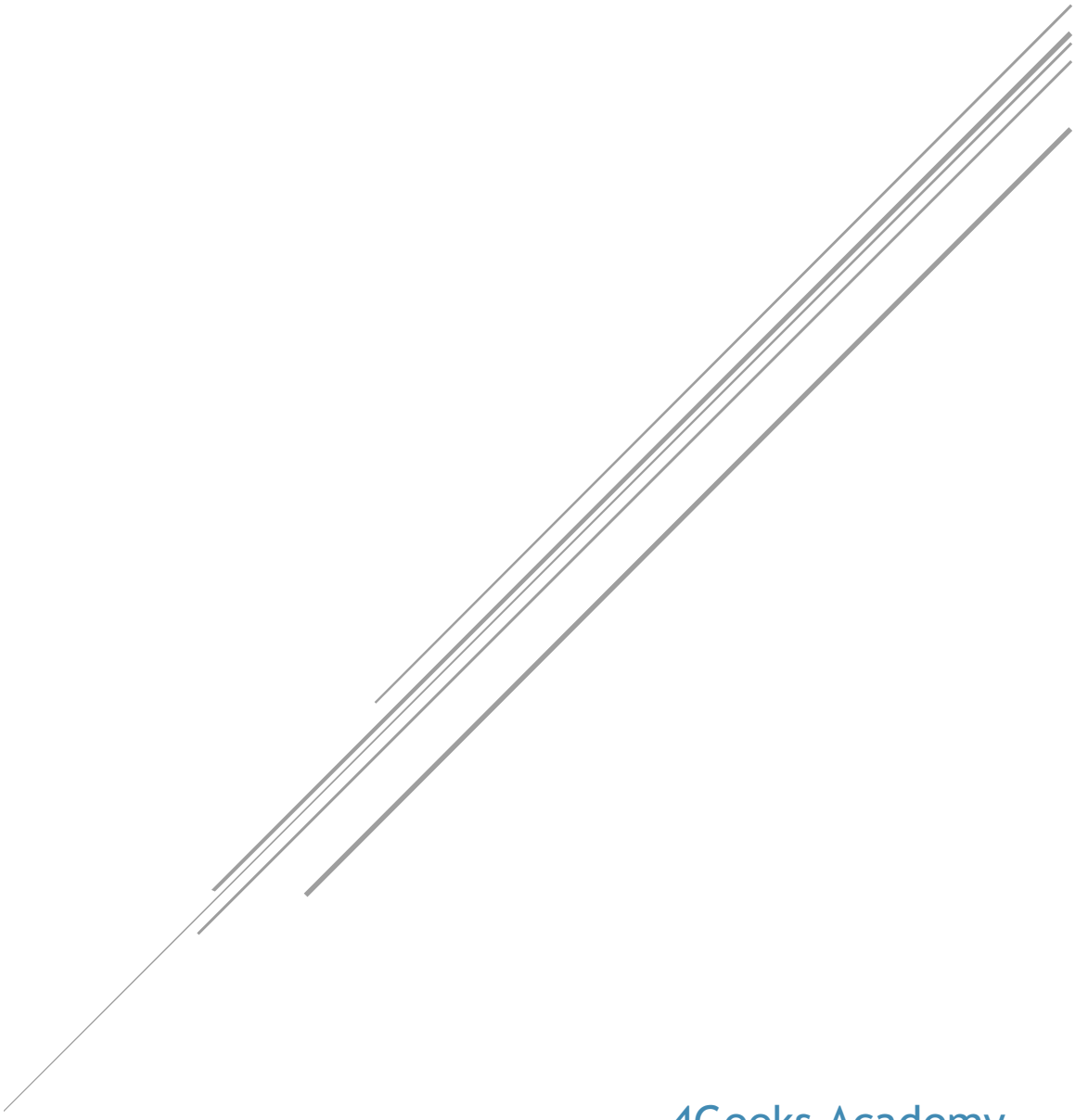
# INFORME DE SGSI Y PLAN DE RESPUESTA A INCIDENTES PARA LEX ABOGADOS & ASOCIADOS

## Proyecto Final: Fase 3



4Geeks Academy
Kevin Pitti

# Indice

1. Introducción .....2
2. Plan de Respuesta a Incidentes .....3
    2.1. Identificación .....3
    2.2. Contención .....4
    2.3. Erradicación .....4
    2.4. Recuperación.....5
3. Respuesta a un Ataque Similar al Hackeo Realizado .....6
4. Mecanismos de Protección de Datos .....7
5. Implementación de un SGSI conforme a la ISO 27001 para
    LEX Abogados & Asociados …….8
    5.1. Análisis de Riesgos .....8
    5.2. Políticas de Seguridad .....10
    5.3. Planes de Acción .....12
6. Conclusión .....16

# 1. Introducción

El presente informe tiene como objetivo presentar un Plan de Respuesta a Incidentes y una propuesta para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001, para la protección de los activos digitales y la información confidencial de LEX Abogados & Asociados.

El enfoque principal es preparar a la organización para identificar, contener, erradicar y recuperar rápidamente de incidentes de seguridad, mientras se asegura la protección continua de la información mediante buenas prácticas y estándares internacionales de seguridad.

# 2. Plan de Respuesta a Incidentes

El Plan de Respuesta a Incidentes es fundamental para gestionar situaciones en las que la seguridad de los sistemas de información se vea comprometida. Este plan se estructura en cuatro fases clave: identificación, contención, erradicación y recuperación.

## 2.1 Identificación

La primera fase es detectar cualquier anomalía o comportamiento sospechoso en los sistemas. Para ello, LEX Abogados & Asociados implementará herramientas como:

- Wazuh: Sistema de detección de intrusos (IDS) que monitorea los logs del sistema y detecta comportamientos inusuales.

- Elasticsearch y Kibana: Junto con Wazuh, estas herramientas permitirán el análisis y la visualización en tiempo real de eventos de seguridad.

Estas herramientas proporcionan alertas en tiempo real y permiten una rápida detección de intrusiones o fallos de seguridad.

## 2.2 Contención

Una vez identificado el incidente, es crucial aislar los sistemas afectados para evitar que el problema se propague a otros recursos. Esta acción puede incluir:

- Firewall de nueva generación: Como pfSense o iptables, para bloquear temporalmente el acceso a los sistemas comprometidos.

- Desactivación de accesos no autorizados: Deshabilitar temporalmente cuentas o servicios comprometidos hasta que se lleve a cabo un análisis forense.

El objetivo es limitar el impacto del incidente mientras se realizan las investigaciones pertinentes.

## 2.3 Erradicación

Después de contener el incidente, se procederá a eliminar cualquier amenaza de los sistemas afectados. Las herramientas recomendadas incluyen:

- ClamAV: Antivirus de código abierto que puede detectar y eliminar malware en sistemas Linux.

- Rkhunter y CHKRootkit: Herramientas para la detección de rootkits en el sistema y eliminación de cualquier tipo de malware que haya comprometido la integridad del sistema.

Además, se llevará a cabo una investigación forense para entender cómo ocurrió el incidente y qué vulnerabilidades fueron explotadas.

## 2.4 Recuperación

Finalmente, se restaurarán los sistemas afectados utilizando copias de seguridad seguras. Las herramientas de respaldo recomendadas son:

- Veeam Backup: Solución de respaldo y recuperación que garantiza que los datos y sistemas se puedan restaurar sin riesgos de infección.

- Bacula: Sistema de respaldo flexible y escalable que asegura que las copias de seguridad estén protegidas y sean recuperables.

Además, se comprobará la integridad de los sistemas restaurados para asegurar que el ataque no haya dejado puertas traseras o vulnerabilidades abiertas.

# 3. Respuesta a un Ataque Similar al Hackeo Realizado

En caso de que se repita un ataque similar al ocurrido, en el cual se aprovecharon vulnerabilidades en servicios como SSH, FTP y WordPress, LEX Abogados & Asociados adoptará las siguientes acciones correctivas:

**Refuerzo de la autenticación:** Implementación de contraseñas más fuertes y autenticación multifactor (MFA) en todos los sistemas críticos utilizando herramientas como Google Authenticator o Authy.

**Desactivación de servicios no esenciales:** Se desactivará el acceso remoto para el usuario root a través de SSH, utilizando configuraciones de seguridad más estrictas en sshd_config.

**Actualización de software:** Utilización de herramientas como OpenVAS o Nessus para realizar escaneos regulares de vulnerabilidades y asegurarse de que todos los sistemas y servicios estén al día con las últimas actualizaciones de seguridad disponibles.

# 4. Mecanismos de Protección de Datos

La protección de los datos confidenciales es una prioridad para LEX Abogados & Asociados. Para garantizar la seguridad de la información, se implementarán los siguientes mecanismos:

**Respaldos periódicos:** Utilización de soluciones como Veeam Backup o Duplicity para realizar copias de seguridad automáticas de los sistemas. Estas copias se almacenarán de manera segura, garantizando que los datos puedan ser recuperados en caso de un incidente.

**Cifrado de datos sensibles:** Implementación de protocolos de cifrado como AES-256 y SSL/TLS para asegurar la protección de los datos tanto cuando están almacenados como cuando se transfieren a través de la red.

**Controles de acceso:** Se establecerán políticas estrictas de acceso a los datos. Herramientas como Okta y LDAP gestionarán los permisos de acceso, asegurando que solo las personas autorizadas puedan acceder a la información sensible. Además, se implementará un sistema de autenticación multifactor (MFA) en todos los sistemas críticos.

# 5. Implementación de un SGSI conforme a la ISO 27001 para LEX Abogados & Asociados

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001 es un proceso fundamental para proteger los activos de información, garantizando que las operaciones de LEX Abogados & Asociados se desarrollen de forma segura y conforme a las mejores prácticas internacionales. A continuación, se desarrolla un SGSI completo para la empresa, alineado con la ISO 27001, utilizando datos ficticios para su implementación.

## 5.1 Análisis de Riesgos

El análisis de riesgos es el primer paso fundamental para implementar un SGSI eficaz. Este análisis identifica, evalúa y prioriza los riesgos de seguridad que podrían afectar los activos de información de la empresa. A continuación, se presentan algunos ejemplos de riesgos identificados en el proceso:

**Activos de Información Clave:**

- Base de datos de clientes (SQL Server): Contiene información personal y confidencial de los clientes.
- Servidor web (Apache2): Alojamiento de la página web de LEX Abogados & Asociados.
- Sistema de correos electrónicos (Microsoft Exchange): Comunicación interna y con clientes.

**Riesgos Identificados:**

- Riesgo de acceso no autorizado a la base de datos de clientes: Un atacante podría obtener acceso a la base de datos debido a contraseñas débiles y a una configuración incorrecta de los controles de acceso.

    - Probabilidad: Alta
    - Impacto: Alto
    - Acción Correctiva: Implementación de autenticación multifactor (MFA) y políticas de contraseñas fuertes.

- Riesgo de Denegación de Servicio (DoS) en el servidor web: Un ataque DoS podría afectar la disponibilidad de los servicios web, impidiendo el acceso a los clientes.

    - Probabilidad: Media
    - Impacto: Alto
    - Acción Correctiva: Implementación de un firewall de aplicaciones web (WAF), como Cloudflare, para mitigar ataques DoS.

- Riesgo de pérdida de datos debido a fallos en el sistema de respaldo: Si los datos no se respaldan adecuadamente, un fallo del sistema podría resultar en la pérdida permanente de información confidencial.
    - Probabilidad: Baja
    - Impacto: Alto
    - Acción Correctiva: Implementación de una política de respaldo regular utilizando Veeam Backup, con copias almacenadas en una ubicación remota.

**Evaluación y Prioridades:**

Los riesgos son evaluados utilizando una escala de probabilidad (Baja, Media, Alta) y un impacto en el negocio (Bajo, Medio, Alto). La prioridad de mitigación se determina por la combinación de estos dos factores. Se han priorizado las acciones correctivas para reducir la exposición a riesgos con alto impacto y alta probabilidad.

## 5.2 Políticas de Seguridad

Las políticas de seguridad son esenciales para guiar el comportamiento y las acciones dentro de la organización en relación con la protección de la información. A continuación, se describen algunas de las principales políticas de seguridad implementadas en LEX Abogados & Asociados:

**Política de Control de Acceso:**

- Autenticación Multifactor (MFA): Todos los accesos a sistemas críticos (bases de datos, servidor web y correos electrónicos) deben requerir la autenticación de dos factores. Se implementarán herramientas como Google Authenticator o Authy para mejorar la seguridad de las cuentas.

- Control de accesos basado en roles (RBAC): Se aplicarán controles de acceso estrictos, limitando el acceso a los sistemas y la información a los usuarios que realmente lo necesiten para realizar su trabajo. Esto se gestionará a través de LDAP y Okta.

**Política de Protección de Datos:**

- Cifrado de Datos Sensibles: Todo dato confidencial, como información personal de los clientes, será cifrado tanto en reposo como en tránsito. Se implementará AES-256 para los datos almacenados y SSL/TLS para la transmisión de datos sensibles.

- Respaldo de Datos: Los datos de clientes y documentos legales serán respaldados periódicamente con Veeam Backup, asegurando que las copias de seguridad estén cifradas y almacenadas en una ubicación remota.

**Política de Respuesta a Incidentes:**

- Plan de Respuesta a Incidentes (PRI): En caso de un incidente de seguridad, como un ataque de ransomware, se activará el plan de respuesta para contener el ataque, erradicar la amenaza y restaurar los sistemas afectados. Este plan estará respaldado por herramientas de monitoreo como Wazuh y Splunk, que alertarán al equipo de seguridad sobre actividades sospechosas.

## 5.3 Planes de Acción

Los planes de acción son una parte fundamental del SGSI, ya que describen las medidas concretas para mitigar los riesgos y asegurar la protección de la información. A continuación, se detallan los planes de acción implementados en LEX Abogados & Asociados:

### Plan de Acción para la Mitigación de Riesgos:

**Riesgo de Acceso No Autorizado a la Base de Datos de Clientes:**

Acción Correctiva: Reforzamiento de la autenticación mediante la implementación de contraseñas más fuertes y la habilitación de autenticación multifactor (MFA) para el acceso a la base de datos de clientes.

Herramienta utilizada: Implementación de Okta para la gestión de autenticación multifactor, lo que añade una capa adicional de seguridad a las cuentas críticas.

Responsable: Departamento de TI, con el soporte del proveedor de bases de datos.

**Riesgo de Ataques de Denegación de Servicio (DoS) en el Servidor Web:**

Acción Correctiva: Implementación de un Firewall de Aplicación Web (WAF), como Cloudflare, para mitigar los riesgos de ataques DoS y asegurar la disponibilidad del servidor web y de la página de LEX Abogados & Asociados.

Configuración de protección DDoS: Ajuste de las reglas del WAF para bloquear ataques distribuidos de denegación de servicio (DDoS) y garantizar la continuidad operativa.

Responsable: Departamento de Seguridad Informática, en colaboración con el proveedor de servicios web.

**Riesgo de Pérdida de Datos por Fallo en el Sistema de Respaldo:**

Acción Correctiva: Implementación de un sistema de respaldo robusto utilizando Veeam Backup, con pruebas regulares de recuperación de datos para asegurar la fiabilidad del proceso de respaldo.

Almacenamiento de Copias de Seguridad: Las copias de seguridad se almacenarán en un entorno remoto para garantizar la protección contra desastres locales.

Responsable: Departamento de Infraestructura, con auditoría anual por el equipo de ciberseguridad.

## Plan de Acción para la Mejora Continua:

### Evaluación Continua de Seguridad:

Acción Correctiva: Realización de escaneos de vulnerabilidades regulares utilizando herramientas como Nessus y OpenVAS. Estos escaneos identificarán vulnerabilidades conocidas y permitirán aplicar las correcciones necesarias antes de que se conviertan en amenazas activas.

Responsable: Departamento de Ciberseguridad y TI.

### Entrenamiento y Sensibilización del Personal:

Acción Correctiva: Capacitación en seguridad informática: Todos los empleados recibirán formación anual en ciberseguridad, enfocándose en la identificación de amenazas como phishing y el manejo adecuado de datos confidenciales. Se utilizarán plataformas como KnowBe4 para realizar simulaciones de ataques de phishing y asegurar que los empleados estén preparados para detectar y evitar amenazas.

Responsable: Departamento de Recursos Humanos, con el soporte del Departamento de Ciberseguridad.

**Monitoreo Continuo y Auditoría de Seguridad:**

Acción Correctiva: Implementación de un sistema de monitoreo continuo con Wazuh para detectar actividades anómalas y generar alertas en tiempo real. Esto incluirá la supervisión de logs de servidores, bases de datos y aplicaciones críticas.

Revisión periódica de auditorías de seguridad: El equipo de ciberseguridad revisará los logs de seguridad y los incidentes previos para identificar patrones y mejorar las políticas de protección.

Responsable: Departamento de Ciberseguridad.

## Plan de Acción para el Cumplimiento Regulatorio:

- Cumplimiento de la Regulación de Protección de Datos:

Acción Correctiva: Revisión y ajuste de políticas de privacidad y protección de datos para garantizar el cumplimiento de las normativas como el Reglamento General de Protección de Datos (GDPR) y otras regulaciones locales de privacidad.

Herramienta utilizada: Implementación de OneTrust para gestionar el cumplimiento de las normativas de protección de datos.

Responsable: Departamento Legal, en colaboración con el Departamento de Ciberseguridad.

# Conclusión

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001 permite a LEX Abogados & Asociados establecer un marco robusto para proteger la información crítica y garantizar que los riesgos de seguridad sean gestionados de manera eficaz. Con el análisis de riesgos, la implementación de políticas de seguridad, y los planes de acción concretos, la organización está preparada para proteger sus activos digitales, responder rápidamente a incidentes de seguridad y mejorar continuamente su postura de ciberseguridad.

Al seguir estas directrices y utilizar herramientas especializadas, como Wazuh, Veeam Backup, Cloudflare, y Okta, LEX Abogados & Asociados fortalecerá su seguridad, protegerá la confidencialidad de la información de sus clientes y minimizará el impacto de las amenazas cibernéticas.