



TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE APIZACO

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA APLICADO A LAS JUNTAS DISTRITALES DEL INSTITUTO NACIONAL ELECTORAL (INE)

TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL

**PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES**

**PRESENTA:
EMMANUEL LUNA HUERTA**

**NOMBRE DEL ASESOR:
CAROLINA ANICA GONZÁLEZ**



APIZACO, TLAX., NOVIEMBRE 2024

Apizaco, Tlaxcala, 22/Agosto/2024

DEPARTAMENTO: División de Estudios Profesionales
ASUNTO: Constancia de Liberación de Residencia Profesional

Por medio de la presente se hace constar que:

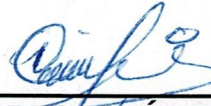
De acuerdo a los documentos que se encuentran en los archivos de esta Institución el: **C. EMMANUEL LUNA HUERTA**, con número de control **19371025** de la carrera de **Ingeniería en Tecnologías de la Información y Comunicaciones**, quien realizó su Residencia Profesional en **INSTITUTO NACIONAL ELECTORAL**, con el desarrollo del proyecto con nombre: **Implementación de un sistema de gestión de seguridad informática aplicado a las juntas distritales del Instituto Nacional Electoral(INE)**, cubriendo un total de 500 horas, durante el periodo comprendido del **06 de febrero de 2024 al 30 de junio de 2024**.

Se extiende la presente para los fines legales que al interesado(a) convengan. Sin otro particular me es grato quedar de usted.

ATENTAMENTE

Excelencia en Educación Tecnológica®
Pensar para Servir, Servir para Triunfar®


CESAR REYNALDO RAMOS GÓMEZ
JEFE DE LA DIVISIÓN DE ESTUDIOS
PROFESIONALES


ELIUT FLORES JIMÉNEZ
COORDINADOR DE LA CARRERA
EN INGENIERÍA EN TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES E
INGENIERÍA INFORMÁTICA

c.p. Interesado (a): **EMMANUEL LUNA HUERTA**,
c.p. Archivo.



Av. Instituto Tecnológico No. 418, San Andrés Ahuashuatepec, Municipio de Tzompantepec,
Tlaxcala, Mex. C.P. 90491 Tel. (241) 4172010 Ext. 104,
e-mail: dep_coordinacion_sistemas@apizaco.tecnm.mx | apizaco.tecnm.mx





TECNOLÓGICO
NACIONAL DE MÉXICO



Instituto Tecnológico de Apizaco
División de Estudios Profesionales

Apizaco, Tlaxcala, 04/noviembre/2024

LUNA HUERTA EMMANUEL.
EGRESADO DE LA CARRERA DE INGENIERÍA
EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.
CON NÚMERO DE CONTROL 19371025.
PRESENTE.

Por este medio, me permito informar a usted que por aprobación de la comisión revisora asignada para valorar el trabajo que mediante la opción TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL cuyo tema es: IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA APLICADO A LAS JUNTAS DISTRITALES DEL INSTITUTO NACIONAL ELECTORAL (INE), conforme a lo establecido en el procedimiento para la obtención del Título Profesional en el Instituto Tecnológico, la División de Estudios Profesionales a mi cargo le otorga la:

AUTORIZACIÓN DE IMPRESIÓN

Debiendo entregar 2 USB del mismo, apropiadamente empastados, a la brevedad, para presentar su Acto de Recepcion Profesional.

Sin otro particular por el momento me despido.

ATENTAMENTE

*Excelencia en Educación Tecnológica-
Pensar para Servir, Servir para Triunfar®*

CÉSAR REYNALDO RAMOS GÓMEZ
JEFE DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES



ccp. Archivo
CRRG/rls



Agradecimientos

Mi más profundo agradecimiento a Dios por haberme permitido llegar hasta este momento, a mis padres **Emiliano Luna Montiel y María Francisca Lidia Huerta Flores** por ser un ejemplo claro de lucha constante, por confiar en mí en todo este proceso y brindarme la oportunidad de estudiar esta carrera y a mis hermanas **Ana y Arely Luna** que siempre me han apoyado para seguir creciendo con su apoyo incondicional como familia.

Mi agradecimiento al Tecnológico Nacional de México, que me brindó la oportunidad de formarme profesionalmente en el Instituto Tecnológico de Apizaco, a los docentes que laboran en dicha Institución, especialmente a la **Mtra. Carolina Anica González** que fue mi asesor interno quien ha fortalecido hasta el final los conocimientos adquiridos durante mi estancia en esta Institución y residencias profesionales.

Al INE, la 01 Junta Distrital Ejecutiva en Tlaxcala, pero principalmente al **Mtro. Andrés Corona Hernández**, al **Lic. Héctor Alejandro Martínez** y el **Arq. Sergio Pluma González** por brindarme la oportunidad y confianza de poder aplicar los conocimientos adquiridos a lo largo de mi carrera.

Finalmente, extendiendo mi agradecimiento a todas las personas que confiaron en mí, a mis amigos y familiares que sin duda alguna han sido partícipes de este logro.

¡Muchas gracias!

Resumen

El proyecto tiene como objetivo principal establecer un Sistema de Gestión de Seguridad Informática (SGSI) en las Juntas Distritales del Instituto Nacional Electoral (INE). Este SGSI abarca la evaluación de riesgos, desarrollo de políticas y procedimientos de seguridad, implementación de controles técnicos y organizativos, así como la preparación para responder a incidentes cibernéticos.

La importancia de este proyecto radica en proteger la integridad, confidencialidad y disponibilidad de la información electoral, asegurando la transparencia, confianza y legitimidad de los procesos electorales. Al aplicar un SGSI sólido y eficiente, se fortalece la ciberseguridad en las Juntas Distritales del INE, mitigando amenazas y vulnerabilidades cibernéticas. Esto contribuye a garantizar los derechos democráticos de los ciudadanos y promueve la integridad del sistema electoral en México.

Índice

Agradecimientos	1
Resumen	2
CAPÍTULO 1: GENERALIDADES DEL PROYECTO	6
1.1 Introducción	6
1.2 Descripción de la empresa u organización y del puesto o área de trabajo del estudiante	6
1.3 Problemas a resolver.....	8
1.4 Objetivos (General y Específicos)	9
1.4.1 Objetivo General.....	9
1.5 Justificación	11
CAPÍTULO 2: MARCO TEÓRICO.....	12
2.1 Seguridad Informática	12
2.1.1 Tipos de seguridad informática	12
2.1.2 Tipos de amenazas en la seguridad informática empresarial	13
2.2 ¿Qué es SSO?	14
2.2.1 ¿Para qué sirve el SSO o Single Sign on?	14
2.3 Sistemas de Gestión de Seguridad Informática (SGSI):	14
2.3.1 ¿Cómo funciona un SGSI?	15
2.3.2 ¿Cuáles son los componentes básicos de un SGSI según la norma ISO/IEC 27001?	15
2.3.3 ¿Cómo implementar un SGSI?	15
2.4 Ciclo de Deming o ciclo PDCA	16
2.4.1 Objetivos del ciclo PDCA.....	17
2.4.2 El ciclo de Deming en un SGSI	17
2.5 Procesos Electorales y Seguridad:	18
2.5.1 Elección Federal	18
2.5.2 Elección Local.....	18
2.6 Normativas y Regulaciones en Seguridad Informática.....	19
2.7 Amenazas y Vulnerabilidades en Entornos Electorales	20
2.7.1 Buenas Prácticas y Estudios de Caso en Seguridad Informática Electoral:	20
2.8 Aplicaciones utilizadas por el INE en los procesos electorales.....	21

2.8.1 Seguimiento de paquetes electorales (SPE)	21
2.8.1.1 ¿Quiénes participan en el SPE?	21
2.8.1.2 ¿Como funciona el SPE?	21
2.8.2 Sistema de Información sobre el desarrollo de la Jornada Electoral (SIJE)	21
2.8.3 Programa de Resultados Electorales Preliminares (PREP)	21
2.8.4 PREP Casilla	22
2.9 Páginas web que utiliza el INE	22
2.9.1 Sitio web Oficial	22
2.7.2 Padrón Electoral y Lista Nominal	23
2.7.3 Plataforma Nacional de Transparencia (PNT):	23
2.7.4 Observadores Electorales	24
CAPÍTULO 3: DESARROLLO	25
3.1 Identificación preliminar de riesgos de seguridad informática	25
3.1.1 Herramientas y comandos para utilizar para la identificación de riesgos y vulnerabilidades	26
3.1.2 Funcionalidad y aplicación a los sitios web del INE	29
3.2 Evaluación detallada de riesgos de seguridad informática	30
3.3 Desarrollo de políticas y procedimientos de seguridad informática	31
3.3.1 Políticas Generales de Seguridad	31
3.3.2 Políticas Específicas de Seguridad:	32
3.3.4 Procedimientos de Control de Acceso	32
3.3.5 Procedimientos de Gestión de Incidentes:	32
3.3.6 Procedimientos de Respaldo y Recuperación:	32
3.4 Implementación de controles técnicos y organizativos para mitigar los riesgos identificados	33
3.5 Capacitación del personal en prácticas de seguridad informática	33
3.5.1 Planificación de la capacitación	34
3.5.2 Implementación de la capacitación	34
3.6 Configuración y despliegue de herramientas de monitoreo de seguridad	34
3.6.1 Planificación	35
3.7 Desarrollo de un Plan de Respuesta ante Incidentes Cibernéticos	35
3.7.1 Que incluye en Plan de Respuesta ante Incidentes Cibernéticos	36

3.8 Desarrollo de un Plan de Recuperación a Incidentes Cibernéticos	36
3.8.1 ¿Cómo funciona el Plan de Recuperación a Incidentes Cibernéticos?	36
3.9 Propuesta de Auditoría de Seguridad Informática para los Sitios	37
CAPÍTULO 4: RESULTADOS.....	38
4.1 Identificación de riesgos y vulnerabilidades	38
4.1.1 Implementación de comandos de Nmap	38
4.1.2 Implementación de la herramienta Owasp Zap	42
4.2 Matriz de Riesgos de Seguridad Informática Identificados y Evaluación	47
4.3 Políticas y Procedimientos de seguridad informática aplicados en la 01 JDE del INE en Tlaxcala	51
4.4 controles técnicos y organizativos para mitigar los riesgos identificados	55
4.5 Propuesta de herramientas para configuración y despliegue el monitoreo de seguridad de los sistemas informáticos del INE	60
4.5.1 Herramientas de Monitoreo Propuestas	60
4.6 Plan de Respuesta ante Incidentes Cibernéticos	61
4.6.1 Objetivo del Plan de Respuesta ante Incidentes	61
4.6.2 Fase 1: Preparación	62
4.6.3 Fase 2: Detección y análisis	62
4.6.4 Fase 3: Contención.....	63
4.6.5 Fase 4: Erradicación.....	63
4.6.6 Fase 5: Recuperación	63
4.7 Plan de Recuperación a Incidentes Cibernéticos.....	64
4.7.1 Fase 1: Preparación para la recuperación	64
4.7.2 Fase 2: Evaluación del Incidente y Análisis de Daños	64
4.7.3 Fase 3: Recuperación de los Sistemas Afectados	65
4.7.4 Fase 4: Verificación de la Integridad y Operatividad	65
4.7.5 Fase 5: Comunicación y Notificación.....	66
4.8 Tablas de Evaluación para la propuesta de Auditoria de Seguridad Informática.....	67
CAPÍTULO 5: CONCLUSIONES.....	70
CAPÍTULO 6: COMPETENCIAS DESARROLLADAS	71
CAPÍTULO 7: FUENTES DE INFORMACIÓN.....	73

CAPÍTULO 1: GENERALIDADES DEL PROYECTO

1.1 Introducción

Este documento describe el trabajo realizado en el proyecto de residencias profesionales de la carrera de Ingeniería en Tecnologías de la Información y Comunicaciones. Este proyecto busca fortalecer la seguridad lógica y las prácticas de seguridad informática en las Juntas Distritales del Instituto Nacional Electoral, mediante la implementación de un Sistema de Gestión de Seguridad Informática (SGSI). Dicho sistema permitirá identificar, evaluar y mitigar los riesgos asociados a la seguridad de la información, así como establecer políticas, procedimientos y controles efectivos para garantizar la protección de los datos electorales.

1.2 Descripción de la empresa u organización y del puesto o área de trabajo del estudiante

Empresa: Instituto Nacional Electoral

Domicilio:

01 Junta Distrital Ejecutiva (JDE)

Calle 5 de febrero, No. 507 Colonia Centro, Apizaco, Tlaxcala

C.P 90300

Tel: (246) 4625299

Nacional: 8004332000

Facebook: INE TLAXCALA

Web: www.ine.mx

Organigrama de la institución



Figura 1: Organigrama de la 01 Junta Distrital Ejecutiva del INE en Tlaxcala (INE, 2024)



Figura 2: Logotipo de la institución (INE, 2024)

INSTITUTO NACIONAL ELECTORAL

El Instituto Nacional Electoral es el organismo público autónomo encargado de organizar las elecciones federales, es decir, la elección de la presidencia de la República, diputadas, diputados, senadoras y senadores que integran el Congreso de la Unión. De igual forma organiza, en coordinación con los organismos electorales de las entidades federativas, las elecciones locales en los estados de la República y la Ciudad de México (INE, 2024).

Misión:

Organizar procesos electorales libres, equitativos y confiables, para garantizar el ejercicio de los derechos político-electorales de la ciudadanía y contribuir al desarrollo de la vida democrática de México (INE, 2024).

Visión:

Ser el organismo electoral nacional autónomo que contribuya a la consolidación de la cultura y convivencia democrática en México, distinguiéndose por ser una institución moderna, transparente y eficiente, en la que la sociedad confíe plenamente para la organización de elecciones equitativas e imparciales (INE, 2024).

Principios Rectores:

- **Certeza**
- **Legalidad**
- **Independencia**
- **Imparcialidad**
- **Máxima Publicidad**
- **Objetividad**

(INE, 2024)

Fines del instituto:

- Contribuir al desarrollo de la vida democrática.
- Preservar el fortalecimiento del régimen de partidos políticos, integrar el Registro Federal de Electores.
- Asegurar a los ciudadanos el ejercicio de sus derechos político-electorales y vigilar el cumplimiento de sus obligaciones, garantizar la celebración periódica y pacífica de las elecciones para renovar a los integrantes de los Poderes Legislativo y Ejecutivo de la Unión, velar por la autenticidad y efectividad del sufragio (INE, 2024).

1.3 Problemas a resolver

En el marco del proyecto se identificaron una serie de problemas y desafíos que requieren atención y solución. Estos problemas están intrínsecamente relacionados con la seguridad

de la información y los sistemas tecnológicos utilizados en los procesos electorales, así como con la integridad, confidencialidad y disponibilidad de los datos electorales.

En primer lugar, se destaca la falta de protección adecuada de la información electoral. Las juntas distritales del INE manejan una gran cantidad de datos sensibles, incluidos registros de votantes, resultados de elecciones y documentos electorales, los cuales son críticos para el funcionamiento de la democracia y el ejercicio libre de los derechos electorales. La ausencia de un Sistema de Gestión de Seguridad Informática (SGSI) efectivo expone esta información a diversos riesgos, como la pérdida, el robo o la manipulación, lo que podría comprometer la integridad y legitimidad de los procesos electorales.

Asimismo, se evidencia una carencia de conciencia y capacitación en seguridad informática entre el personal de las juntas distritales del INE. La falta de conocimientos y habilidades en este ámbito aumenta la probabilidad de que se produzcan prácticas inseguras, como el uso de contraseñas débiles, la descarga de archivos maliciosos o la apertura de correos electrónicos de phishing. Este factor humano constituye una vulnerabilidad significativa que debe ser abordada mediante programas de formación y sensibilización en seguridad informática. Al abordar estos problemas de manera integral, el proyecto busca fortalecer la seguridad informática en el ámbito electoral y garantizar la confianza pública en el proceso democrático en México.

1.4 Objetivos (General y Específicos)

1.4.1 Objetivo General

Desarrollar e implementar un Sistema de Gestión de Seguridad Informática efectivo y adaptado a las necesidades específicas de las Juntas Distritales del INE, con el fin de fortalecer la protección de la información, garantizar la integridad de los procesos electorales y salvaguardar la confianza pública en el sistema electoral.

1.4.2 Objetivos Específicos

- Realizar una evaluación exhaustiva de los riesgos de seguridad informática específicos de la 01 Junta Distrital Ejecutiva en Apizaco Tlaxcala, identificando amenazas potenciales, vulnerabilidades y activos críticos de información.
- Desarrollar e implementar políticas y procedimientos de seguridad informática adaptados a las necesidades y regulaciones locales, incluyendo políticas de acceso, gestión de contraseñas, manejo de datos sensibles.
- Implementar controles técnicos y organizativos para mitigar los riesgos identificados, tales como firewalls, sistemas de detección de intrusiones, encriptación de datos, sistemas de respaldo y recuperación de información.
- Capacitar al personal de la 01 Junta Distrital Ejecutiva en prácticas de seguridad informática, concientizando sobre los riesgos y fomentando comportamientos seguros en el manejo de la información y el uso de sistemas tecnológicos.
- Establecer un sistema de monitoreo continuo de la seguridad informática, con la implementación de herramientas de seguimiento y registro de eventos, así como la definición de indicadores clave de desempeño Key Performance Indicators (KPIs) para evaluar la efectividad de los controles de seguridad.
- Desarrollar un plan de respuesta a incidentes cibernéticos, estableciendo procedimientos claros para detectar, reportar, investigar y mitigar posibles brechas de seguridad, con el objetivo de minimizar el impacto en la integridad y disponibilidad de la información electoral.
- Establecer una planeación y programación de auditorías periódicas de seguridad informática para evaluar el cumplimiento de las políticas y controles establecidos, identificar áreas de mejora y garantizar el cumplimiento de los estándares de seguridad establecidos por el INE y otras regulaciones aplicables.
- Promover la colaboración y coordinación con otras entidades del INE a nivel local, regional y nacional, para compartir buenas prácticas, información sobre amenazas y recursos para fortalecer la seguridad informática en el ámbito electoral.

1.5 Justificación

Salvaguardar la integridad del proceso electoral es fundamental para preservar la democracia. Un sistema de gestión de seguridad informática garantiza que la información electoral crítica no sea comprometida, manipulada o alterada por amenazas cibernéticas.

Las Juntas Distritales Ejecutivas del INE gestionan vastos volúmenes de información sensible relacionada con los procesos electorales, haciéndolas objetivos potenciales para ataques informáticos. Un Sistema de Gestión de Seguridad Informática permite identificar y mitigar proactivamente los riesgos y vulnerabilidades que podrían amenazar la seguridad de los datos electorales. Algunos aspectos por considerar son los siguientes:

- **Cumplimiento normativo y regulatorio:** El INE está sujeto a regulaciones y estándares de seguridad de la información que requieren la implementación de medidas adecuadas para proteger los datos electorales. La adopción de un sistema de gestión de seguridad informática asegura el cumplimiento de estas regulaciones, garantizando que la 01 Junta Distrital Ejecutiva esté en conformidad con las normativas correspondientes.
- **Fortalecimiento de la confianza pública:** La confianza en la integridad y transparencia del proceso electoral es esencial para la estabilidad y legitimidad del sistema democrático. Al implementar un sistema de gestión de seguridad informática efectivo, se muestra el compromiso del INE con la protección de la información electoral, fortaleciendo así la confianza del público en la institución y en el proceso electoral en su conjunto.

CAPÍTULO 2: MARCO TEÓRICO

2.1 Seguridad Informática

La seguridad informática se refiere al conjunto de tecnologías, medidas, procesos y prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado, daños o robos (Hubspot, 2024).

2.1.1 Tipos de seguridad informática

1. Seguridad de red

La seguridad en la red se enfoca en la protección de la red de una empresa u organización, mediante medidas de protección que identifiquen y repelen amenazas externas, hackers, malware y virus. (Hubspot, 2024).

2. Seguridad de datos

Este tipo de seguridad es fundamental, ya que sus acciones se centran en proteger los datos durante el proceso de recopilación y gestión de estos. Así se protege la información de la compañía, como los datos de los clientes, informes financieros y registros de empleados; por supuesto, uno de los pilares de la seguridad informática es la prevención de pérdida de datos. (Hubspot, 2024).

3. Seguridad de aplicaciones

La seguridad informática de las aplicaciones empresariales es sumamente importante para que una organización opere de la mejor manera. Sus acciones se encargan de proteger las aplicaciones que usa una empresa, como el correo electrónico, la mensajería instantánea y los programas personalizados (Hubspot, 2024).

4. Seguridad de la nube

Este tipo de seguridad es más concreto, pero sus acciones abarcan muchas plataformas y software que operan en la nube. Busca la protección de los datos y aplicaciones alojados

en la nube, incluyendo la seguridad de su infraestructura y los datos almacenados en ella (Hubspot, 2024).

5. *Seguridad de la identidad*

Esta tiene que ver con la protección de la identidad digital de los empleados y los clientes, incluyendo el control de acceso y la autenticación de usuarios, incluyendo el SSO (Hubspot, 2024).

2.1.2 Tipos de amenazas en la seguridad informática empresarial

1. *Ataques de phishing*

El phishing es uno de los ataques cibernéticos más utilizados por ciberdelincuentes para obtener información confidencial (números de tarjetas de crédito, contraseñas, nombre de usuario, etc.) de los usuarios en internet.

En este caso, **los atacantes se hacen pasar por una institución verificada** (como por ejemplo una entidad bancaria) o personas de confianza y redactan un correo electrónico con lenguaje formal para solicitar al usuario que ingrese en un link que será muy parecido al de una página oficial de cualquier empresa o banco legítimo. (Delta Protect, 2024).

2. *Ataques de Ransomware*

Ataque de ransomware o secuestro de datos se refiere a un tipo de software malicioso que suele ser utilizado por ciberdelincuentes para **robar información confidencial y mantenerla encriptada bajo un código de acceso** (Delta Protect, 2024).

3. *Malware*

Un malware también se corresponde con un software malicioso que tiene como objetivo **explotar las vulnerabilidades de un sistema informático** para obtener ciertos permisos sin autorización, como, por ejemplo:

- Ejecutar o desinstalar programas
- Acceder a funciones del equipo o sistema en el que está instalado
- Permitir la extracción de información

(Delta Protect, 2024)

4. *Inyección SQL*

En este tipo de ciberataque, el hacker se encarga de **introducir un código SQL (Lenguaje de Consulta Estructurada) corrupto en una página web**, para poder acceder a la información de su base de datos sin necesitar una contraseña.

El lenguaje SQL es utilizado para diseñar y administrar bases de datos y por lo general, para acceder a la información almacenada en ellas, se necesita un usuario y una contraseña específica. (Delta Protect, 2024).

5. *Ataques de denegación de servicios (DDoS)*

Para llevar a cabo el ataque DDoS y burlar la seguridad informática de un sistema, los hackers envían **múltiples solicitudes a un servidor o red con el objetivo de superar la capacidad de respuesta a dichas solicitudes**, cuyo desenlace será el colapso de la red objetivo. (Delta Protect, 2024).

2.2 ¿Qué es SSO?

Es un servicio de autenticación de usuario y sesión que permite a un individuo tener acceso a una o varias aplicaciones. El nombre y la contraseña es el tipo de acceso más común y facilita la administración de varias cuentas (Hubspot, 2024).

2.2.1 ¿Para qué sirve el SSO o Single Sign on?

El SSO hace posible que las funciones transfieran la responsabilidad de autenticar a los usuarios a alguna otra aplicación o servicio. Su objetivo principal es simplificar y mejorar la experiencia del usuario al eliminar la necesidad de recordar y administrar múltiples contraseñas.

Al utilizar el SSO, los usuarios pueden iniciar sesión una vez y acceder a varias aplicaciones y servicios sin tener que volver a autenticarse en cada uno por separado, lo que aumenta la seguridad, al mismo tiempo que simplifica el acceso a sistemas y recursos en línea (Hubspot, 2024).

2.3 Sistemas de Gestión de Seguridad Informática (SGSI):

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas de administración de la información. El término se denomina en inglés “Information Security Management System” (ISMS).

Un SGSI es un conjunto de principios o procedimientos que se utilizan para identificar riesgos y definir los pasos de mitigación de riesgos que deben llevarse a cabo. Éste garantiza que las empresas tomen medidas sistemáticamente para mantener seguros los datos y la información; puede ser cualquier tipo de información, como datos de clientes, procesos internos o detalles de pago (Soluciones de Software OTRS, 2024).

2.3.1 ¿Cómo funciona un SGSI?

Un SGSI está destinado principalmente a la protección de datos o información con el objetivo de mantener la confidencialidad, la integridad y la disponibilidad de esta información.

Por ejemplo, cuando nos referimos a confidencialidad, es fundamental resaltar la necesidad de no revelar la información a personas o entidades no autorizadas. Todo el acceso y el control de los datos y la información deberá estar rigurosamente controlado.

Por otra parte, cuando hablamos de integridad, uno de los aspectos básicos en la información, estamos haciendo alusión a la exactitud de cada uno de los datos. Por este motivo, el tratamiento que se le debe dar a la información debe ser el adecuado, implementando sistemas de calidad que garanticen la transparencia en la información (Delta Protect, 2024).

2.3.2 ¿Cuáles son los componentes básicos de un SGSI según la norma ISO/IEC 27001?

ISO/IEC 27001 es la norma internacional que define cuáles deben ser los componentes de un sistema de gestión de seguridad de la información y cómo deben utilizarse. Los estándares describen las medidas de protección de seguridad de la información que deben considerarse para fines de planeación, llamados controles. A partir de ahí, la norma ISO/IEC 27001 sugiere cómo hacer operativo el sistema y revisar su desempeño a lo largo del tiempo (Soluciones de Software OTRS, 2024).

2.3.3 ¿Cómo implementar un SGSI?

La norma ISO/IEC 27001 es un marco flexible de gestión de la seguridad de la información (GSI) que pueden utilizar empresas de todos los tamaños a medida que examinan las

operaciones, protegen los activos de información y trabajan para mejorar la gestión de la seguridad de la información a través de un SGSI. A un nivel muy alto, los pasos incluyen:

- Crear políticas: una política de seguridad de la información, una declaración de aplicabilidad y un plan de tratamiento de riesgos
- Definir el alcance del SGSI
- Establecer un método para identificar riesgos
- Comenzar a evaluar que riesgos son aplicables a la organización
- Evaluar y definir controles relacionados con estos riesgos
- Documentar y realizar un seguimiento de los esfuerzos de mitigación
- Realizar revisiones y reevaluaciones continuas

(Soluciones de Software OTRS, 2024)

2.4 Ciclo de Deming o ciclo PDCA

Es una metodología de gestión que tiene como objetivo la mejora constante de los procesos consta de cuatro pasos: Planificar (plan), hacer (do), verificar (check) y actuar (act). En la figura de a continuación se muestran las etapas de este ciclo.

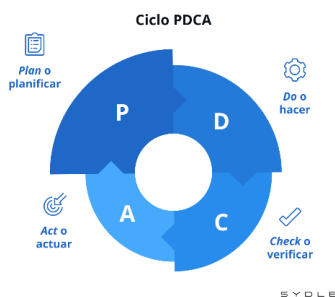


Figura3. Etapas del Ciclo de Deming (sydle,2024)

El concepto PDCA, por tanto, está vinculado a un proceso de mejora continua que debe aplicarse a través de estos cuatro pasos, que se ejecutan de forma cíclica con el objetivo de acelerar y mejorar la calidad de los productos o procesos. (SYDLE , 2024)

2.4.1 Objetivos del ciclo PDCA

Simplificar las rutinas de gestión y facilitar la implementación de cambios positivos.

Para lograrlo, trabaja en función de los siguientes aspectos clave:

- Resolución de problemas: Este ciclo se puede aplicar para resolver cualquier tipo de problema en una empresa o institución, su modelo permite planificar una solución que se verifica continuamente, minimizando al máximo los impactos del problema inicial.
- Toma de decisiones: Esta metodología se basa en información concreta y verificación continua de datos, lo que mejora la toma de decisiones.
- Innovación: El PCDA facilita la organización de nuevas ideas, lo que permite la implementación de soluciones nuevas e innovadoras para problemas cotidianos.
- Flexibilidad y agilidad: A través del PCDA, las empresas pueden adaptarse más rápidamente a los cambios constantes en el mercado, desarrollando un perfil más flexible y dinámico.
- Mejora de la calidad: El PCDA está directamente relacionado con la gestión de la calidad, promoviendo la mejora continua en todos los procesos de la organización. (SYDLE , 2024)

2.4.2 El ciclo de Deming en un SGSI

En el momento de desarrollar e implementar un SGSI, es fundamental tener en cuenta el Ciclo de Deming, que se basa en los siguientes pasos:

✓ Planificar

Esta fase se basa en la creación y el diseño del SGSI. Aquí se debe realizar una completa y detallada evaluación de los riesgos relacionados con la seguridad de la información.

✓ Hacer

En este punto es en donde se lleva a cabo la implementación del SGSI.

✓ Verificar

Este es un periodo que está destinado para la revisión y evaluación del desempeño del programa implementado. Aquí se analiza el impacto y la eficacia del SGSI.

✓ Actuar

Luego de la verificación y la identificación de posibles fallas o de oportunidades para mejorar el rendimiento, en esta fase se realiza cualquier cambio que requiera el SGSI con el objetivo de maximizar su rendimiento (FIRMA-E Consultoria y desarrollo de TI, 2024).

2.5 Procesos Electorales y Seguridad:

Los procesos electorales implican la gestión de una gran cantidad de datos sensibles y críticos, como los registros de votantes, los resultados de las elecciones y la información sobre los candidatos. La seguridad de estos procesos es fundamental para garantizar la transparencia, legitimidad y confianza en los resultados electorales. La seguridad en los procesos electorales abarca aspectos como la protección de la infraestructura tecnológica, la integridad de los datos, la autenticación de los votantes y la prevención de fraudes electorales.

2.5.1 Elección Federal

El Instituto Nacional Electoral es el encargado de organizar las actividades del Proceso Electoral Federal 2023-2024, en el que se elegirán:

- Presidente o presidenta de la República Mexicana: 1 Cargo
- Senadores y Senadoras de la Republica: 128 Cargos
- Diputadas y diputados de la cámara baja: 500 Cargos

Las actividades que desarrolla el INE para la organización del Proceso Electoral Federal derivan del Plan y Calendario aprobado por el Consejo General a través del acuerdo INE/CG441/2023 (INE, 2024).

2.5.2 Elección Local

El INE en coordinación con los Organismos Públicos Locales desarrollarán las actividades para la elección de Gubernaturas, Jefatura de Gobierno de la Ciudad de México, Congresos Locales, Ayuntamientos, Juntas Municipales y Alcaldías. En total se elegirán más de 19 mil cargos; en particular se destaca en los estados de Chiapas, Ciudad de México, Guanajuato,

Jalisco, Morelos, Puebla, Tabasco, Veracruz y Yucatán, la elección para determinar la titularidad de las Gubernaturas.

Para la coordinación de estas actividades, el Consejo General del INE aprobó el acuerdo INE/CG446/2023 por el que se aprobaron el Plan Integral y los Calendarios de coordinación de los Procesos Electorales Locales concurrentes con el Federal 2023-2024 (INE, 2024).

Para las elecciones locales en Tlaxcala se elegirán:

- 25 diputaciones locales
- 60 presidencias municipales
- 60 sindicaturas
- 350 regidurías
- 299 cuarto orden de gobierno

2.6 Normativas y Regulaciones en Seguridad Informática

Existen normativas y regulaciones tanto a nivel nacional como internacional que establecen requisitos y lineamientos para la seguridad informática en organizaciones gubernamentales y electorales. Estas incluyen estándares como ISO 27001, regulaciones específicas para el sector público y leyes de protección de datos personales. Cumplir con estas normativas es fundamental para garantizar la seguridad y confidencialidad de la información electoral y evitar sanciones legales (White Shield, 2024).

1. ISO 27001: La norma ISO 27001 es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). A continuación, se presentan algunos ejemplos de cómo la norma ISO 27001 se aplica en la práctica:
2. Evaluación de riesgos: La norma ISO 27001 requiere que las organizaciones realicen una evaluación de riesgos para identificar las amenazas y vulnerabilidades en su entorno de TI. Con esta evaluación, se pueden establecer medidas de seguridad adecuadas para mitigar los riesgos identificados.
3. Políticas de seguridad: La norma ISO 27001 exige que las organizaciones establezcan políticas de seguridad de la información y que estas sean comunicadas y comprendidas por todos los empleados. Estas políticas deben incluir la gestión de contraseñas, la gestión de acceso, la gestión de incidentes, la gestión de respaldo, entre otras.

4. Control de acceso: La norma ISO 27001 exige que las organizaciones establezcan controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a la información confidencial. Esto incluye la gestión de identidad y acceso, la autenticación multifactor, la gestión de contraseñas, entre otros.
5. Auditoría y monitoreo: La norma ISO 27001 requiere que las organizaciones realicen auditorías periódicas y monitoreen constantemente su SGSI para garantizar que se estén cumpliendo los requisitos y para identificar posibles mejoras.
6. Gestión de incidentes: La norma ISO 27001 exige que las organizaciones establezcan un plan de gestión de incidentes para responder a posibles violaciones de seguridad de la información. Esto incluye la identificación temprana de los incidentes, la respuesta rápida y eficaz, la comunicación a las partes interesadas y la evaluación de los resultados de la respuesta (White Shield, 2024).

2.7 Amenazas y Vulnerabilidades en Entornos Electorales

Los entornos electorales están expuestos a una variedad de amenazas y vulnerabilidades, que van desde ataques cibernéticos sofisticados hasta errores humanos y actividades de interferencia política. Estas amenazas pueden incluir ataques de denegación de servicio (DDoS), intrusiones maliciosas, manipulación de resultados electorales y desinformación en línea. Es importante identificar y mitigar estas amenazas para proteger la integridad y legitimidad de los procesos electorales (Soporte Técnico INE, 2024).

2.7.1 Buenas Prácticas y Estudios de Caso en Seguridad Informática Electoral:

Se pueden estudiar y analizar casos de éxito y buenas prácticas en seguridad informática aplicada a entornos electorales en todo el mundo. Estos estudios de caso pueden proporcionar insights valiosos sobre estrategias efectivas de seguridad, desafíos comunes y lecciones aprendidas. Ejemplos relevantes pueden incluir la implementación de SGSI en organismos electorales de otros países, la respuesta a incidentes de seguridad durante procesos electorales y la aplicación de tecnologías innovadoras para garantizar la integridad de los votos (Soporte Técnico INE, 2024).

2.8 Aplicaciones utilizadas por el INE en los procesos electorales

2.8.1 Seguimiento de paquetes electorales (SPE)

La app de seguimiento de paquetes está diseñada e implementada para dar seguimiento a los paquetes electorales (PE) en las 5 fases de la cadena de custodia (INE, 2024)

2.8.1.1 ¿Quiénes participan en el SPE?

Para darle un correcto seguimiento y validez a los Procesos Electorales, cada una de las Juntas Distritales cuentan con personal debidamente capacitado de los cuales destacan:

- Capacitador(a) Asistente Electoral (CAE)
- Supervisor(a) Electoral (SE)
- Técnico(a) de Voz y Datos (TVyD)
- Auxiliar de consejo
- Vocal de Organización Electoral Distrital (VOED)

2.8.1.2 ¿Como funciona el SPE?

La o el Capacitador Asistente Electoral (CAE) puede escanear los códigos QR o de barras de las etiquetas de los PE o capturar la información manualmente en cada una de sus fases (INE, 2024).

2.8.2 Sistema de Información sobre el desarrollo de la Jornada Electoral (SIJE)

Su objetivo es informar a los órganos competentes del INE sobre el desarrollo de la jornada electoral (INE, 2024).

Por lo que el próximo 2 de junio de 2024 las y los CAEs tendrán que hacer reportes sobre:

- Instalación de las casillas
- Integración de las Mesas Directivas de Casilla (MDC)
- Presencia de las y los representantes de partido político y candidatura independiente
- Incidentes durante la Jornada Electoral

2.8.3 Programa de Resultados Electorales Preliminares (PREP)

¿Qué es el PREP?

Es el mecanismo de información electoral previsto en la ley encargado de proveer los **resultados preliminares y no definitivos, de carácter estrictamente informativo a través**

de la digitalización, captura y publicación de los datos plasmados en las Actas de Escrutinio y Cómputo (AEC) de las casillas que se reciben en los CATD (INE, 2024).

El objetivo del PREP es informar oportunamente bajo los siguientes principios:

- Seguridad
- Transparencia
- Confiabilidad
- Credibilidad
- Integridad

2.8.4 PREP Casilla

PREP Casilla, es una aplicación móvil que permite realizar la toma fotográfica del” Acta PREP” y enviarla al Centro de Recepción de Imágenes y Datos (CRID) para su captura. Dicho proceso facilitará y optimizará la ejecución del Proceso Técnico Operativo (PTO) para la publicación del Programa de Resultados Electorales Preliminares que se llevará a cabo el día de la Jornada Electoral (INE, 2024).

2.9 Páginas web que utiliza el INE

2.9.1 Sitio web Oficial

Este es el portal principal del Instituto, donde se proporciona información institucional, noticias, documentos oficiales, resultados electorales, calendarios electorales y otra información relevante relacionada con el proceso electoral en México.

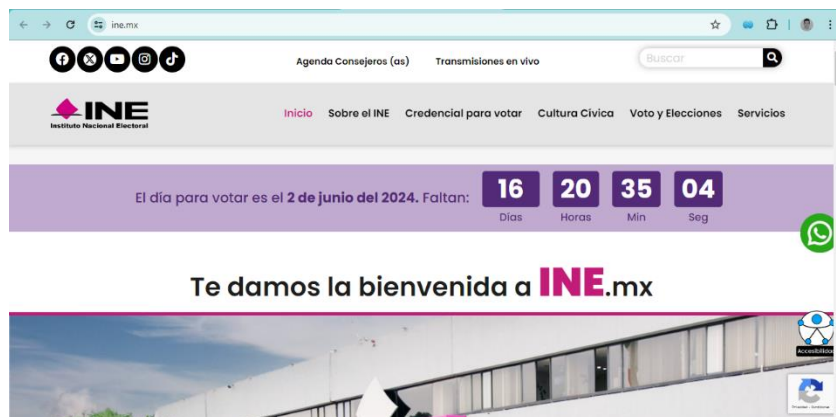


Figura 4: Sitio web oficial del INE (INE, 2024)

2.7.2 Padrón Electoral y Lista Nominal

El INE también proporciona acceso en línea al Padrón Electoral y la Lista Nominal de Electores, donde los ciudadanos pueden verificar su información electoral, como su lugar de votación y su registro en el padrón electoral.



Figura 5: Sitio web Padrón Electoral (INE, 2024)

2.7.3 Plataforma Nacional de Transparencia (PNT):

A través de esta plataforma, el INE proporciona acceso a la información pública relacionada con sus actividades, decisiones y operaciones. Los ciudadanos pueden presentar solicitudes de acceso a la información y consultar documentos públicos en línea.

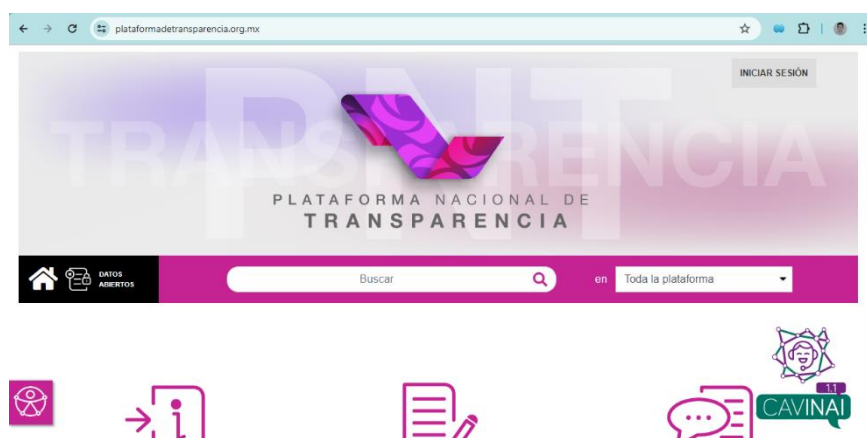


Figura 6: Sitio web Plataforma Nacional de Transparencia (INE, 2024)

2.7.4 Observadores Electorales

Durante los procesos electorales, el INE suele proporcionar información y servicios para observadores electorales nacionales e internacionales a través de una página web dedicada. Esta página puede variar en función de cada proceso electoral, pero generalmente se encuentra en el sitio web del INE



Figura 7: Sitio web Observadores Electorales (INE, 2024)

CAPÍTULO 3: DESARROLLO

3.1 Identificación preliminar de riesgos de seguridad informática

En esta fase dentro de la información recopilada de los sistemas, aplicaciones y sitios web que utiliza la O1 Junta Distrital Ejecutiva (JDE) de Apizaco Tlaxcala, se va a revisar cada una de ellas para así detectar las posibles amenazas que podrían atacar a los sistemas informáticos del INE.

Dentro de esta identificación se detectarán las amenazas que podrían poner en riesgo a los sistemas, para así realizar un plan de mitigación y respuesta ante incidentes cibernéticos y establecer propuestas de solución si se llegaran a presentar dichos incidentes.

Amenazas Internas y accesos no autorizados:

En cada proceso electoral el personal de la Junta Distrital le otorga un dispositivo móvil a sus Capacitadores Asistentes Electorales (CAES), dentro de ese dispositivo vienen instaladas las aplicaciones en las cuales se realizan reportes de la jornada electoral

Las aplicaciones antes mencionadas son (PREP Casilla, SIJE, SPE), estas aplicaciones son monitoreadas desde un servidor interno que está instalado dentro de las instalaciones de la junta distrital, estas aplicaciones están vinculadas por una dirección IP misma que es monitoreada y registrada desde el launcher del dispositivo, este launcher no es modificable y solo administradores pueden realizar cambios dentro del dispositivo. Esto lo hacen con el fin de evitar difundir información personal y falsificación de documentos (INE, 2024).

Accesos permitidos a los CAES para las aplicaciones:

- Iniciar sesión
- Registrar, capturar y enviar información
- Tomar fotografías
- Escanear códigos QR y de barras

Nota: Como las aplicaciones son para uso exclusivo del INE, nadie tiene acceso o autorización de realizar modificaciones que alteren la información de dichos sistemas, ya

que estas mismas aplicaciones son monitoreadas a nivel nacional por personal de soporte técnico de oficinas centrales del INE

Para identificar las posibles amenazas y riesgos, a los sitios web de acceso público se les van a realizar pruebas de vulnerabilidades y seguridad para así clasificar el riesgo de cada una de ellas. Se va a hacer uso de herramientas como NMAP y OWASP ZAP para una detección más precisa y así llevar a cabo una evaluación detallada de cada amenaza detectada y su forma de mitigarla.

3.1.1 Herramientas y comandos para utilizar para la identificación de riesgos y vulnerabilidades

NMAP

Nmap es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando (FreeCodeCamp, 2024).



Figura 8: Logotipo NMAP (Nmap, 2024)

Algunas de las formas que Nmap puede ayudar en el ámbito de los sitios web que utiliza el INE son los siguientes:

1. Descubrimiento de Puertos Abiertos y Servicios:

Escaneo de Puertos: Realizar un escaneo de puertos en los servidores web del INE para identificar qué puertos están abiertos. Esto puede revelar servicios adicionales que se ejecutan en el servidor, aparte del servicio HTTP/HTTPS.

Detección de Servicios y Versiones: Identificar los servicios que se ejecutan en los puertos abiertos y sus versiones específicas. Esto es crucial para detectar servicios desactualizados o vulnerables.

2. Fingerprinting de Sistemas Operativos:

Detección de Sistemas Operativos: Determinar qué sistema operativo se ejecuta en los servidores del INE. Esto puede ayudar a identificar vulnerabilidades específicas del sistema operativo que necesitan ser mitigadas.

3. Identificación de Vulnerabilidades Conocidas:

Nmap Scripting Engine (NSE): Utilizar scripts NSE para buscar vulnerabilidades conocidas en los servicios identificados. Por ejemplo, scripts que detecten versiones obsoletas de software web como Apache, Nginx, o aplicaciones web específicas que podrían estar ejecutándose en los servidores del INE.

4. Evaluación de Seguridad de SSL/TLS:

Escaneo de SSL/TLS: Utilizar scripts NSE para evaluar la configuración de SSL/TLS de los sitios web del INE. Esto incluye la verificación de la fortaleza de los cifrados utilizados, la validez de los certificados digitales y la identificación de posibles configuraciones inseguras.

5. Auditoría de Configuraciones de Seguridad:

Revisión de Configuraciones de Servicios: Auditar las configuraciones de los servicios web y otros servicios relacionados para detectar configuraciones predeterminadas o inseguras que podrían ser explotadas.

6. Mapeo de la Red:

Topología de Red: Realizar un mapeo de la red para obtener una visión clara de la infraestructura del INE. Esto ayuda a identificar otros dispositivos y servicios que interactúan con los servidores web, proporcionando un contexto más amplio de posibles vectores de ataque.

7. Detección de Problemas de Seguridad Comunes:

Scripts NSE para Seguridad Web: Ejecutar scripts NSE específicos para detectar problemas comunes de seguridad en aplicaciones web, como configuraciones inseguras de HTTP headers, problemas con el manejo de cookies, y otras vulnerabilidades web básicas.

OWASP ZAP

OWASP ZAP (Zed Attack Proxy) es una herramienta muy poderosa para identificar vulnerabilidades en aplicaciones web, y puede ser particularmente útil para analizar la seguridad de los sitios web del Instituto Nacional Electoral (INE).

Ventajas de ZAP

- Zap proporciona multiplataforma, funciona en todos los sistemas operativos
- Zap es reutilizable
- Permite generar informes
- Ideal para principiantes

(Academia Seguridad Cero, 2024)



Figura 9: Logotipo de OWASP ZAP (Owasp, 2024)

Funcionamiento General de la herramienta

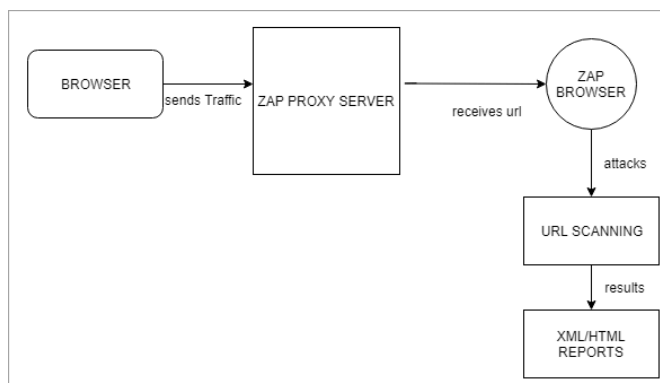


Figura 10: Diagrama de funcionamiento de la herramienta OWASP ZAP (Seguridad cero, 2024)

3.1.2 Funcionalidad y aplicación a los sitios web del INE

1. Escaneo Automatizado de Vulnerabilidades:

Escaneo Pasivo: Al navegar por los sitios web del INE usando OWASP ZAP, la herramienta captura el tráfico y realiza un análisis pasivo para identificar problemas comunes sin enviar solicitudes adicionales. Esto ayuda a detectar vulnerabilidades como la falta de encabezados de seguridad.

Escaneo Activo: ZAP puede realizar un escaneo activo, enviando solicitudes adicionales para detectar una amplia gama de vulnerabilidades, incluyendo inyecciones SQL, XSS (Cross-Site Scripting), y problemas de autenticación (Listopro Community, 2024).

2. Análisis de Contenidos y Funcionalidades Específicas:

Spidering: ZAP puede rastrear automáticamente todos los enlaces y formularios dentro de los sitios web del INE para mapear la estructura completa de la aplicación web. Esto es útil para asegurar que todas las áreas del sitio sean revisadas en busca de vulnerabilidades.

Forced Browsing: Esta función intenta acceder a recursos no referenciados directamente (como archivos y directorios ocultos) para descubrir contenido sensible no destinado al público (Pragma , 2024).

3. Interceptación de Tráfico y Modificación de Solicitudes:

Proxy Intercepting: Al actuar como un proxy, ZAP permite a los usuarios interceptar y modificar las solicitudes y respuestas HTTP en tiempo real. Esto puede ser útil para probar cómo el sitio web del INE maneja datos inesperados o maliciosos.

Manual Testing: Los testers pueden modificar las solicitudes HTTP enviadas por los formularios del sitio web para ver cómo responde la aplicación a entradas no esperadas (Pragma , 2024).

4. Generación de Informes Detallados:

Reportes de Vulnerabilidades: ZAP genera informes detallados que enumeran las vulnerabilidades encontradas, clasificadas por severidad. Esto es esencial para presentar hallazgos a los administradores del INE y para planificar las acciones correctivas.

Historial de Escaneos: Mantener un registro de escaneos permite comparar resultados y verificar si las vulnerabilidades han sido corregidas en futuros análisis (Academia Seguridad Cero, 2024).

3.2 Evaluación detallada de riesgos de seguridad informática

Una vez que se realizó una investigación detallada de los activos críticos relacionados con los sistemas informáticos que utiliza el INE (Servidores web, aplicaciones, sitios web), funcionalidades principales y realizado la identificación de amenazas internas y externas, se va a realizar un escaneo automatizado a los sitios web con la ayuda de la herramienta Owasap Zap, así mismo se hace un escaneo de puertos con el comando **nmap -p 1-65535** y la url del sitio web.

Para realizar la evaluación de riesgos se van a seguir los siguientes pasos:

Evaluación de Impacto:

- Evaluamos el impacto potencial de cada amenaza en función de la criticidad de los activos y la sensibilidad de la información.
- Clasificamos los impactos como alto, medio o bajo.

Evaluación de Probabilidad:

- Determinamos la probabilidad de ocurrencia de cada amenaza, basada en factores históricos, tendencias actuales y características específicas del entorno.
- Clasificamos la probabilidad como alta, media o baja.

Matriz de Riesgos:

- Creamos una matriz de riesgos cruzando la probabilidad y el impacto de cada riesgo identificado.
- Prioriza los riesgos en función de su severidad combinada (impacto y probabilidad).

3.3 Desarrollo de políticas y procedimientos de seguridad informática

El desarrollo de políticas y procedimientos de seguridad informática para los sistemas del Instituto Nacional Electoral (INE) requiere un enfoque estructurado y exhaustivo para asegurar que todas las áreas de seguridad sean cubiertas.

3.3.1 Políticas Generales de Seguridad

- **Política de Seguridad de la Información:** Establecer directrices generales para la protección de la información.
- **Política de Control de Acceso:** Definir cómo se gestionan y controlan los accesos a los sistemas y datos (Docusing, 2024).

3.3.2 Políticas Específicas de Seguridad:

- **Política de Uso Aceptable:** Establecer normas sobre el uso aceptable de los recursos informáticos.
- **Política de Gestión de Incidentes:** Describir los procedimientos para la identificación, respuesta y recuperación ante incidentes de seguridad.
- **Política de Gestión de Cambios:** Definir cómo se gestionan y controlan los cambios en los sistemas informáticos (Docusing, 2024).

3.3.4 Procedimientos de Control de Acceso

Definir los pasos para la creación, modificación y eliminación de cuentas de usuario. Establecer procedimientos para la autenticación y autorización de usuarios (MINTIC COLOMBIA, 2024).

3.3.5 Procedimientos de Gestión de Incidentes:

- Describir los pasos a seguir en caso de un incidente de seguridad, incluyendo la identificación, contención, erradicación, y recuperación.
- Definir los roles y responsabilidades de cada miembro del equipo de respuesta a incidentes (MINTIC COLOMBIA, 2024)

3.3.6 Procedimientos de Respaldo y Recuperación:

- Establecer procedimientos para la realización de copias de seguridad y la recuperación de datos.
- Definir la frecuencia de los respaldos y los métodos de almacenamiento seguro (MINTIC COLOMBIA, 2024).

3.4 Implementación de controles técnicos y organizativos para mitigar los riesgos identificados

Implementar controles técnicos y organizativos para mitigar los riesgos identificados en los sistemas informáticos del Instituto Nacional Electoral (INE) requiere una combinación de medidas de seguridad tecnológica y procedimientos administrativos. Para ello se seguirán los siguientes pasos:

- **Revisar la Evaluación de Riesgos:**
Examina la lista de riesgos identificados y clasificados por su probabilidad e impacto. Prioriza los riesgos que necesitan atención inmediata según su severidad.
- **Selección de controles técnicos:**
Autenticación Multifactor (MFA): Implementa MFA para acceso a sistemas críticos.
Gestión de Identidades y Accesos (IAM): Utiliza sistemas IAM para gestionar cuentas de usuario y privilegios.
- **Cifrado:**
Cifrado de Datos en Reposo: Asegura que los datos almacenados estén cifrados.
Cifrado de Datos en Tránsito: Implementa SSL/TLS para proteger los datos durante la transmisión.
- **Copias de seguridad y recuperación:**
Copias de Seguridad Regulares: Realiza copias de seguridad de datos críticos de forma regular.
Planes de Recuperación ante Desastres: Desarrolla y prueba planes de recuperación para asegurar la continuidad del negocio (IBM, 2024).

3.5 Capacitación del personal en prácticas de seguridad informática

Capacitar al personal en prácticas de seguridad informática es esencial para garantizar que todos los empleados estén equipados con el conocimiento necesario para proteger los sistemas y datos del INE.

3.5.1 Planificación de la capacitación

Para llevar a cabo la capacitación se requiere evaluar las necesidades de cada área para identificar donde el personal necesita información.

Definir los objetivos de la capacitación:

Establecer objetivos claros para la capacitación, como mejorar la conciencia sobre las amenazas de seguridad, enseñar prácticas seguras de manejo de datos, y garantizar el cumplimiento de las políticas de seguridad del INE.

Debemos tener en cuenta los temas a abordar para concientizar al personal sobre la importancia de la seguridad en los sistemas informáticos y evitar robo o pérdida de información y datos personales. Podemos incluir temas como:

- Concienciación sobre phishing y ataques de ingeniería social.
- Uso seguro de contraseñas y autenticación multifactor (MFA).
- Manejo seguro de datos sensibles.
- Políticas de seguridad del INE.
- Procedimientos de gestión de incidentes.
- Seguridad en dispositivos móviles

3.5.2 Implementación de la capacitación

Se programarán sesiones y horarios con el fin de no intervenir en sus labores y asegurar que todos los empleados reciban formación continua.

Se les brindara material de apoyo como diapositivas, videos, etc para que los empleados los puedan consultar después de las sesiones de capacitación.

Implementar un programa de capacitación en seguridad informática efectivo requiere una planificación cuidadosa, ejecución meticulosa y seguimiento continuo. Al capacitar al personal del INE, se fortalece la primera línea de defensa contra amenazas de seguridad, asegurando la protección de los sistemas y datos críticos del instituto.

3.6 Configuración y despliegue de herramientas de monitoreo de seguridad

Configurar y desplegar herramientas de monitoreo de seguridad es un paso crucial para proteger los sistemas informáticos del INE y detectar actividades maliciosas o anómalas en tiempo real.

3.6.1 Planificación

Para ello primeramente debemos definir el objetivo del monitoreo siguiendo los siguientes pasos:

- Determinar qué sistemas, aplicaciones y datos necesitan ser monitoreados.
- Establecer objetivos claros, como detección de intrusiones, monitoreo de cumplimiento, y análisis de tráfico de red.

Una vez definido el objetivo se procede a hacer la elección de la herramienta de monitoreo para hacer el despliegue de los eventos que va a monitorear, para ello existen herramientas como las mencionadas a continuación.

- **Sistemas SIEM (Security Information and Event Management):** Herramientas como Splunk, IBM QRadar o ArcSight que recopilan, correlacionan y analizan eventos de seguridad.
- **Monitoreo de Red:** Herramientas como Nagios, Zabbix o SolarWinds para supervisar el rendimiento y la seguridad de la red.
- **Configuración de entornos de prueba:** configurar un entorno de prueba que simule la infraestructura del INE para realizar pruebas antes del despliegue completo.

Implementar estas herramientas y seguir estos pasos ayudará a crear un entorno de monitoreo de seguridad robusto para los sistemas informáticos del INE, proporcionando una vigilancia constante y una respuesta rápida a cualquier amenaza que pueda surgir (PANDORA FMS, 2024).

3.7 Desarrollo de un Plan de Respuesta ante Incidentes Cibernéticos

Una respuesta ante incidentes (a veces, llamada respuesta ante incidentes de seguridad cibernética) se refiere a los procesos y tecnologías de una organización para detectar y responder a amenazas cibernéticas, violaciones de seguridad o ciberataques. Un plan formal de respuesta a incidentes permite a los equipos de ciberseguridad limitar o prevenir daños. El objetivo de la respuesta a incidentes es prevenir los ataques cibernéticos antes de que ocurran y minimizar el costo y la interrupción del negocio resultante de cualquier ataque cibernético que ocurra (IBM, 2024).

3.7.1 Que incluye en Plan de Respuesta ante Incidentes Cibernéticos

- Las funciones y responsabilidades de cada miembro del Equipo de Respuesta a Incidentes de Seguridad (CSIRT);
- Las soluciones de seguridad (software, hardware y otras tecnologías) que se instalarán en toda la empresa.
- Un plan de continuidad de negocio que describa los procedimientos para restaurar los sistemas y datos críticos afectados lo más rápido posible en caso de una interrupción.
- Una metodología detallada de respuesta a incidentes que establece los pasos específicos que deben tomarse en cada fase del proceso de respuesta a incidentes, y por quién.
- Un plan de comunicaciones para informar a los líderes de la empresa, empleados, clientes e incluso a las autoridades sobre incidentes.
- Instrucciones para documentar y recopilar información y documentar incidentes para revisión a posteriori y (si es necesario) procedimientos legales.

(IBM, 2024).

3.8 Desarrollo de un Plan de Recuperación a Incidentes Cibernéticos

Un Plan de Recuperación a Incidentes Cibernéticos es el procedimiento que ha de seguir la empresa en el caso de que se produzca un incidente grave que afecte a su infraestructura informática. Es decir, se trata de un protocolo en el que se incluyen las acciones a seguir y los recursos necesarios para restaurar los sistemas y los datos de la empresa, para que esta pueda volver a operar con normalidad lo antes posible tras sufrir un desastre, sea este natural, a causa de un error humano o fruto de un ciberataque. (Grupo Atico 34, 2024)

3.8.1 ¿Cómo funciona el Plan de Recuperación a Incidentes Cibernéticos?

El **plan de recuperación de desastres de una empresa funciona**, generalmente, en una serie de fases tras la ocurrencia del desastre:

- Identificación del desastre

- Notificación del desastre al equipo de gestión de desastres (formado, normalmente, por personal del departamento de TI)
- El equipo de gestión de desastres evaluará si es necesario aplicar el DRP
- Aplicación del DRP para poner en marcha las acciones y medidas necesarias para garantizar la continuidad del negocio
- Llevar a cabo las acciones correctivas necesarias para solucionar los problemas derivados del desastre y volver a la normalidad
- Restauración completa de los sistemas y datos

(Grupo Atico 34, 2024).

3.9 Propuesta de Auditoría de Seguridad Informática para los Sitios

La auditoría de seguridad informática es la herramienta principal para poder conocer el estado de seguridad en que se encuentra una empresa en relación con sus sistemas informáticos, de comunicación y acceso a internet. Estas auditorías permiten mejorar los sistemas e incrementar la ciberseguridad, siendo fundamentales para poder garantizar el funcionamiento del negocio y proteger la integridad de la información que manejan. (Ambit bst, 2024).

Ventajas de una auditoría de seguridad informática

Está claro que realizar una auditoría nos va a traer beneficios. Las principales **ventajas que nos ofrece la auditoría informática** son:

- Reducir los riesgos a los que se expone la organización.
- Eliminar las vulnerabilidades que se detectan en el proceso.
- Tomar medidas concretas para garantizar la ciberseguridad.
- Actualizar las políticas de seguridad que toda empresa debe tener.
- Garantizar la seguridad de toda la información que se maneja (empresarial y personal).
- Aumentar la confianza por parte de empleados y clientes. (UNIR FP, 2024).

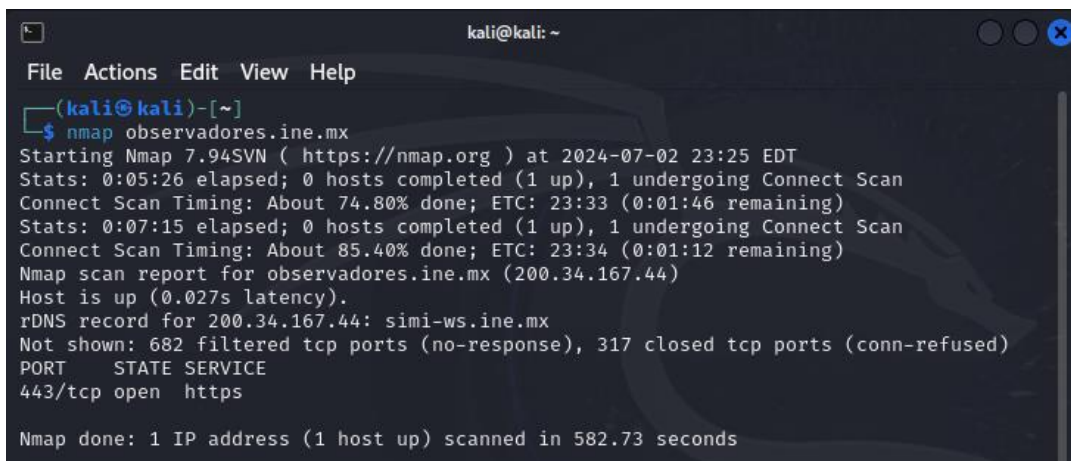
CAPÍTULO 4: RESULTADOS

4.1 Identificación de riesgos y vulnerabilidades

A continuación, se muestran los resultados previos realizados a los sitios web que se utilizan en la 01 Junta Distrital Ejecutiva del INE en Apizaco Tlaxcala, para ello se utilizaron las herramientas de Nmap bajo el entorno de Kali Linux y Owasp Zap ya anteriormente mencionadas.

4.1.1 Implementación de comandos de Nmap

Paso 1: Primeramente, iniciamos con un escaneo básico de los puertos con el siguiente comando: **nmap observadores.ine.mx** y damos Enter para ejecutarlo.



```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nmap observadores.ine.mx
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 23:25 EDT
Stats: 0:05:26 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 74.80% done; ETC: 23:33 (0:01:46 remaining)
Stats: 0:07:15 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 85.40% done; ETC: 23:34 (0:01:12 remaining)
Nmap scan report for observadores.ine.mx (200.34.167.44)
Host is up (0.027s latency).
rDNS record for 200.34.167.44: simi-ws.ine.mx
Not shown: 682 filtered tcp ports (no-response), 317 closed tcp ports (conn-refused)
PORT      STATE SERVICE
443/tcp    open  https
Nmap done: 1 IP address (1 host up) scanned in 582.73 seconds
```

Figura 11: Escaneo básico de puertos con NMAP (Elaboración propia, 2024)

Al ejecutar el comando observamos lo siguiente:

- Dirección IP del host: 200.34.167.44
- Estado del host: Host activo (con una latencia de 0.027 segundos)

Puertos escaneados:

- 682 puertos filtrados (sin respuesta)
- 317 puertos cerrados

Puerto abierto:

- 443/tcp (https) está abierto

Paso 2: Procedemos a hacer un escaneo específico del puerto 443 con el comando **nmap -p 443 observadores.ine.mx**

```
(kali@kali)-[~]
$ nmap -p 443 observadores.ine.mx
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 00:27 EDT
Nmap scan report for observadores.ine.mx (200.34.167.44)
Host is up (0.021s latency).
rDNS record for 200.34.167.44: simi-ws.ine.mx

PORT      STATE SERVICE
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Figura 12: Escaneo específico del puerto 443 con NMAP (Elaboración propia, 2024).

El comando **nmap -p 443 observadores.ine.mx** fue utilizado para verificar el estado del puerto 443 (HTTPS) del dominio observadores.ine.mx. El resultado mostró que el host está activo y que el puerto 443 está abierto, con una latencia muy baja.

Paso3: Con el comando **nmap -sV observadores.ine.mx** obtenemos información sobre los servicios que se están ejecutando en los puertos abiertos.

```
$ nmap -sV observadores.ine.mx
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 23:44 EDT
Nmap scan report for observadores.ine.mx (200.34.167.44)
Host is up (0.024s latency).
rDNS record for 200.34.167.44: simi-ws.ine.mx
Not shown: 845 filtered tcp ports (no-response), 154 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
443/tcp   open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 204.45 seconds
```

Figura 13: Ejecución del comando nmap -sv (Elaboración propia, 2024).

Puertos escaneados

- 845 puertos filtrados (sin respuesta)
- 154 puertos cerrados (conexión rechazada)

Puerto abierto

- **443/tcp** está abierto, pero el servicio aparece como `tcpwrapped`. Esto generalmente significa que el puerto está protegido por un firewall o un sistema de detección de intrusiones, y no se puede determinar con precisión qué servicio está corriendo allí.

El comando `nmap -sV observadores.ine.mx` se utilizó para escanear el dominio `observadores.ine.mx` y detectar la versión de los servicios que se ejecutan en sus puertos. El resultado mostró que el host está activo y que el puerto 443 está abierto, pero protegido (`tcpwrapped`), lo que impide una identificación precisa del servicio. El escaneo también reveló que la mayoría de los puertos están filtrados o cerrados.

Paso 4: Realizamos el escaneo de vulnerabilidades con el comando `sudo nmap --script vuln observadores.ine.mx`. Este comando utilizará una variedad de scripts de NSE para buscar vulnerabilidades comunes en el sitio web.

```

└─$ sudo nmap --script vuln observadores.ine.mx
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 22:16 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:02:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.08% done; ETC: 22:22 (0:03:53 remaining)
Stats: 0:18:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.49% done; ETC: 22:34 (0:00:03 remaining)
Stats: 0:23:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.12% done; ETC: 22:39 (0:00:03 remaining)
Nmap scan report for observadores.ine.mx (200.34.167.44)
Host is up (0.024s latency).
rDNS record for 200.34.167.44: simi-ws.ine.mx
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE
25/tcp    filtered  smtp
443/tcp   open      https
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-2333)
| /index.php source code:

```

Figura 14: Escaneo de vulnerabilidades con NMAP (Elaboración propia, 2024).

```

443/tcp open      https
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-2333)
| /index.php source code:
| <!DOCTYPE html>\x0D
| <html lang="es">\x0D
|   <head> \x0D
|     <meta http-equiv="Content-Type" content="text/html; charset=utf-8">\x0D
|     <meta name="viewport" content="width=device-width, initial-scale=1, maxi
mum-scale=1, user-scalable=no">\x0D
|     <meta http-equiv="X-UA-Compatible" content="IE=Edge">\x0D
|   \x0D
|     <link href="img/faviconINE.ico" rel="shortcut icon">\x0D
|   \x0D
|     <link rel="stylesheet" type="text/css" href="rsc/css/bootstrap.css"> \
x0D
|     <link rel="stylesheet" type="text/css" href="rsc/css/font-awesome.css">\
x0D
|     <link rel='stylesheet' type='text/css' href="rsc/css/error.css" />\x0D
|   \x0D
|     <title>Instituto Nacional Electoral</title>\x0D
|   \x0D
|   </head>\x0D
|   <body>\x0D
|     <div class="row">\x0D
|       <div class="col-md-offset-2 col-md-8">\x0D
|         <section class="cuadroLogin">\x0D
|           <div class="seccion_titulo">\x0D

```

Figura 14.1: Escaneo de vulnerabilidades con NMPAP (Elaboración propia, 2024).

Puertos cerrados: 997 puertos TCP están cerrados (reset).

Puertos específicos detectados:

- 25/tcp (SMTP): El puerto está filtrado.
- 443/tcp (HTTPS): El puerto está abierto.
- 646/tcp (LDP): El puerto está filtrado.

Vulnerabilidades encontradas:

- http-litespeed-sourcecode-download: Se detectó una vulnerabilidad de divulgación de código fuente en el servidor web Litespeed (CVE-2010-2333).
- http-slowloris-check: Se detectó que el servidor web es probablemente vulnerable al ataque de Denegación de Servicio (DoS) Slowloris (CVE-2007-6750).
- http-vuln-cve2010-0738: Se encontró un problema de autenticación no requerida en /jmx-console/.

En resumen, el comando **sudo nmap --script vuln observadores.ine.mx** se utilizó para escanear el dominio **observadores.ine.mx** y detectar los servicios y sus versiones en los puertos abiertos. Se encontraron varias vulnerabilidades, incluyendo la divulgación de código fuente y vulnerabilidades de Denegación de Servicio. Además, se reveló que el puerto 443 (HTTPS) está abierto, mientras que otros puertos están cerrados o filtrados.

4.1.2 Implementación de la herramienta Owasp Zap

Se realizaron escaneos constantes para detectar de manera automática las posibles amenazas y vulnerabilidades que presentan los diferentes sistemas informáticos (Páginas web de acceso público) que son utilizadas por las juntas distritales del INE, esto con el fin de generar reportes de esta y así tener un panorama general de sus vulnerabilidades detectadas y poder realizar su mitigación.

Paso1: Iniciamos el software de Owasp Zap e introducimos la URL del sitio a atacar, posteriormente hacemos click en el botón de “atacar” para que la herramienta inicie el escaneo automatizado.

La herramienta realiza tanto el spidering (exploración del sitio) como el escaneo activo (pruebas de vulnerabilidades) automáticamente.

Nota importante: Configuración del Proxy

- Asegurarse de que el navegador esté configurado para usar el proxy de ZAP (generalmente localhost en el puerto 8080).

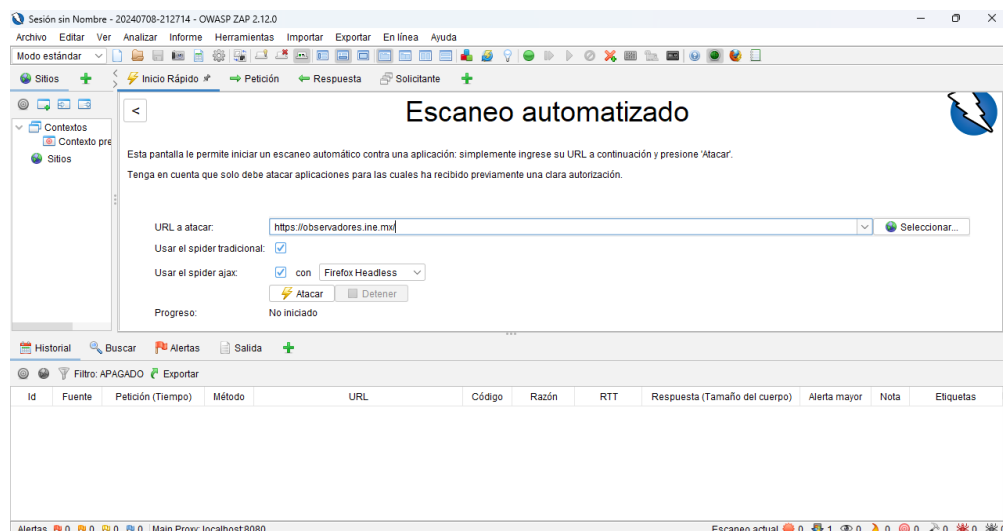


Figura 15: Inicio de la herramienta OWASP ZAP (Elaboración propia, 2024).

Paso 2: Proceso del escaneo automatizado

- Spidering

El spidering rastrea todas las páginas y recursos del sitio web siguiendo enlaces y descubriendo todas las partes de la aplicación web.

- Escaneo activo

Una vez que el spidering se completa, OWASP ZAP realiza un escaneo activo. Este proceso implica enviar diversas solicitudes al servidor y analizar las respuestas para identificar vulnerabilidades.

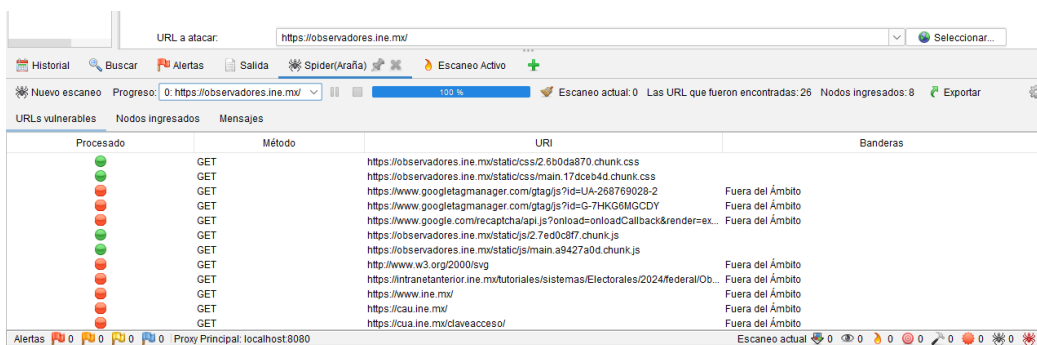


Figura 16: Proceso de spidering con OWASP ZAP (Elaboración propia, 2024).

ID	Petición (Tiempo)	Marca de tiempo Respuesta	Método	URL	Código	Razón	RTT	Tamaño de la Cabecera de Respuesta	Respuesta (Tamaño del cuerpo)
175	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/894695815096...	200	OK	49miliseg...	793bytes	3.445bytes
176	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/364052206944...	200	OK	49miliseg...	793bytes	3.445bytes
178	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/static/42165638...	200	OK	43miliseg...	649bytes	3.445bytes
179	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/static/55303485...	200	OK	39miliseg...	649bytes	3.445bytes
181	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/static/css/1331...	200	OK	32miliseg...	649bytes	3.445bytes
182	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/static/css/5871...	200	OK	34miliseg...	649bytes	3.445bytes
184	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/static/js/544856...	200	OK	33miliseg...	649bytes	3.445bytes
185	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/static/js/400603...	200	OK	31miliseg...	649bytes	3.445bytes
187	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/WEB-INF/web.x...	302	Security R...	28miliseg...	162bytes	0bytes
188	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/WEB-INF/applic...	200	OK	39miliseg...	793bytes	3.445bytes
189	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/WEB-INF/class...	200	OK	30miliseg...	793bytes	3.445bytes
190	10/7/24 9:41:15 p. m.	10/7/24 9:41:15 p. m.	GET	https://observadores.ine.mx/WEB-INF/class...	200	OK	33miliseg...	793bytes	3.445bytes

Figura 17: Proceso de escaneo activo con OWASP ZAP (Elaboración propia, 2024).

Paso 3: Resultados del escaneo

OWASP ZAP proporciona un resumen del escaneo, incluyendo el número total de alertas y su gravedad (baja, media, alta).

Detalles de las vulnerabilidades:

- Vulnerabilidades Críticas:

Detalle sobre vulnerabilidades críticas que podrían permitir a un atacante comprometer el sistema.

- Vulnerabilidades Medias:

Detalle sobre vulnerabilidades de nivel medio que podrían facilitar ataques si se combinan con otras fallas.

- Vulnerabilidades Bajas:

Detalle sobre problemas menores que no representan un riesgo inmediato pero que deben ser corregidos.

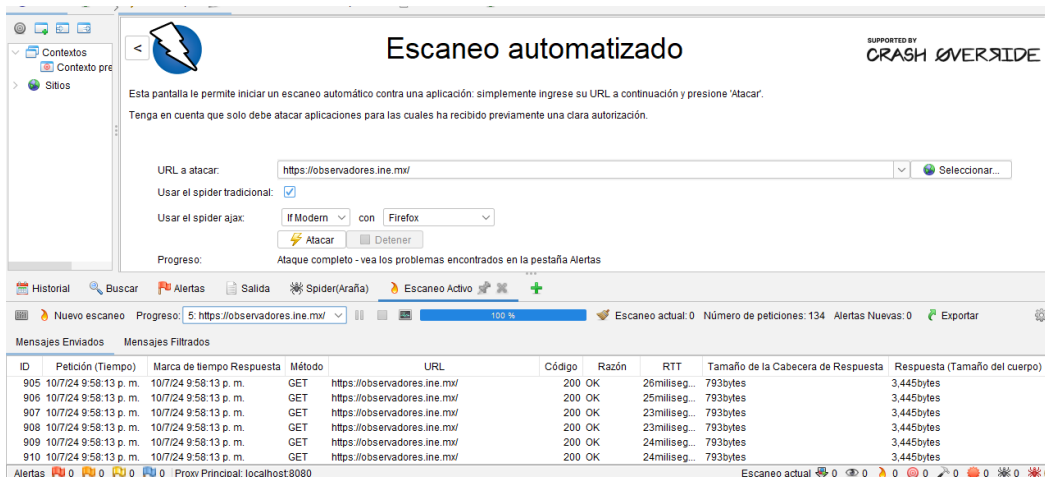


Figura 18: Resultados del escaneo con OWASP ZAP (Elaboración propia, 2024).

OWASP ZAP genera un informe detallado que incluye:

- Descripción de cada vulnerabilidad.
- Gravedad de la vulnerabilidad (baja, media, alta).
- Detalles técnicos de cómo fue encontrada la vulnerabilidad.
- Recomendaciones sobre cómo mitigar la vulnerabilidad.

Nota: Se realizó el mismo proceso con cada uno de los URL de cada sitio web que se ocupa en las juntas distritales del INE.

4.2 Matriz de Riesgos de Seguridad Informática Identificados y Evaluación

A continuación, se muestra una matriz de riesgos de Seguridad Informática identificados que es una propuesta para evaluar la seguridad en los sitios webs y aplicaciones móviles del INE

Esta matriz de riesgos es una herramienta estratégica que nos ayuda a gestionar de manera proactiva los riesgos de seguridad informática, asegurando la protección de sus sistemas y datos, mejorando la eficiencia operativa, y cumpliendo con las normativas aplicables.

Aplicación	Riesgo de Seguridad	Probabilidad	Impacto	Nivel de Riesgo	Medidas de Mitigación
Portal Web Principal (Ine.mx)	SQL Injection	Media	Alta	Alta	Validación y saneamiento de entradas, uso de consultas parametrizadas
	Cross-Site Scripting (XSS)	Alta	Media	Alta	Escapar y validar todas las entradas de usuario, implementar políticas de seguridad de contenido (CSP).
	Ataques DDoS	Alta	Alta	Alta	Implementar soluciones de mitigación DDoS, como el uso de CDN y firewalls de aplicaciones web (WAF).

	Exposición de Datos Sensibles	Baja	Alta	Media	Cifrado de datos en tránsito y en reposo, controles de acceso estrictos.
Portal Web Observadores Electorales (observadores.ine.mx)	SQL Injection	Media	Alta	Alta	Validación y saneamiento de entradas, uso de consultas parametrizadas.
	Cross-Site Scrpiting (XSS)	Alta	Media	Alta	Escapar y validar todas las entradas de usuario, implementar políticas de seguridad de contenido (CSP).
	Exposición de Datos Sensibles	Media	Alta	Alta	Cifrado de datos en tránsito y en reposo, controles de acceso estrictos, revisiones de seguridad de código.
	Ataques DDoS	Alta	Alta	Alta	Implementar soluciones de mitigación DDoS, como el uso de CDN y firewalls de aplicaciones web (WAF).

	Vulnerabilidades de Software	Media	Alta	Alta	Actualizaciones y parches regulares, pruebas de seguridad de aplicaciones (SAST y DAST).
	Fuga de Información Personal	Media	Alta	Alta	Monitoreo y detección de exfiltración, cifrado de datos sensibles, políticas de seguridad de datos estrictas.
Correo Electrónico	Phishing	Alta	Media	Alta	Capacitación de empleados, filtros de correo avanzados, autenticación de correo (DKIM, SPF, DMARC).
	Malware	Media	Alta	Alta	Uso de software antivirus y antimalware, políticas de seguridad de correos, análisis de archivos adjuntos.
	Exfiltración de Datos	Media	Alta	Alta	Monitoreo y detección de exfiltración, cifrado de correos electrónicos sensibles.
Aplicación móvil PREP Casilla	Manipulación de Resultados	Media	Alta	Alta	Revisiones de seguridad de aplicaciones, permisos mínimos necesarios, cifrado de datos.

	Fuga de Información Personal	Media	Alta	Alta	Implementar autenticación y autorización seguras, pruebas de seguridad de API.
Aplicación móvil SIJE	Robo de Identidad	Media	Alta	Alta	
	Manipulación de Resultados	Media	Alta	Alta	
Aplicación móvil SPE	Acceso No Autorizado				
	Fuga de Información Personal				

Tabla 1: Matriz de riesgos de seguridad informática identificados (Elaboración propia, 2024).

4.3 Políticas y Procedimientos de seguridad informática aplicados en la 01 Junta Distrital Ejecutiva (JDE) del INE en Tlaxcala

El INE cuenta con lineamientos y políticas específicas para la gestión y seguridad de los documentos electrónicos, uso de firmas electrónicas avanzadas y la gestión de tecnologías de la información. Dentro de las juntas distritales se implementan una serie de políticas y procedimientos para asegurar la integridad, confidencialidad y disponibilidad de la información y sistemas que maneja estos son esenciales para proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas. A continuación, se describen algunas de las políticas y procedimientos que se toman en cuenta de acuerdo con el código para la prevención de riesgos de seguridad informática y vulnerabilidades en las aplicaciones.

POLÍTICAS Y PROCEDIMIENTOS A IMPLEMENTAR EN LOS SISTEMAS INFORMÁTICOS DE LA 01 JUNTA DISTRITAL EJECUTIVA (JDE) DEL INE EN APIZACO TLAXCALA.

Políticas de Seguridad Informática	Procedimientos
Política de Seguridad de la Información: • Descripción: Define las directrices para proteger la información contra accesos no autorizados, modificaciones no deseadas y amenazas internas y externas. • Fundamento: Se basa en el principio de confidencialidad, integridad y disponibilidad (CIA Triad) de la información,	Procedimiento de Gestión de Accesos: • Descripción: Especifica cómo asignar, revisar y revocar accesos a los sistemas y datos de la organización. • Fundamento: Se basa en principios de control de acceso de la ISO/IEC 27002, que establece la importancia de gestionar los accesos de manera controlada y segura.

que es central en normas como la ISO/IEC 27001. Esta norma es un estándar internacional para la gestión de la seguridad de la información y proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI).	Procedimiento de Copias de Seguridad: • Descripción: Define la frecuencia, el método y la ubicación de las copias de seguridad, así como la verificación de su integridad. • Fundamento: Basado en la ISO/IEC 27031, que trata sobre la preparación y respuesta ante incidentes que pueden afectar la continuidad del negocio, incluyendo la recuperación de datos.
Política de Gestión de Accesos: • Descripción: Regula quién puede acceder a qué información y bajo qué circunstancias, garantizando que solo el personal autorizado tenga acceso a los sistemas críticos. • Fundamento: Se basa en los principios de mínimo privilegio y necesidad de saber, los cuales se derivan de la ISO/IEC 27002, un estándar que complementa la ISO/IEC 27001 y proporciona	Procedimiento de Gestión de Incidentes: • Descripción: Detalla los pasos a seguir desde la detección hasta la resolución de un incidente de seguridad. • Fundamento: Utiliza como guía el NIST SP 800-61, que proporciona un marco para la preparación, detección, análisis, contención, erradicación y recuperación de incidentes.

buenas prácticas para el control de acceso.	
Política de Uso Aceptable: • Descripción: Establece las normas para el uso apropiado de los recursos tecnológicos de la organización, incluyendo redes, sistemas y dispositivos. • Fundamento: Se fundamenta en la necesidad de proteger los activos tecnológicos de la organización contra usos indebidos que puedan comprometer la seguridad. Estas directrices ayudan a prevenir incidentes de seguridad causados por un uso incorrecto o irresponsable de los recursos tecnológicos.	Procedimiento de Gestión de Cambios: • Descripción: Establece cómo evaluar, aprobar y documentar cambios en la infraestructura tecnológica para evitar riesgos de seguridad. • Fundamento: Basado en la ITIL (Information Technology Infrastructure Library) y ISO/IEC 20000, que son marcos para la gestión de servicios de TI, incluyendo la gestión de cambios.
Política de Copias de Seguridad: • Descripción: Establece procedimientos para la realización de copias de seguridad regulares de los datos críticos para garantizar su disponibilidad en caso de pérdida.	

• Fundamento: Se fundamenta en la necesidad de garantizar la disponibilidad y recuperabilidad de la información crítica, un componente esencial de la gestión de la continuidad del negocio y la recuperación ante desastres (ISO/IEC 22301).	
Política de Gestión de Riesgos: • Descripción: Define cómo identificar, evaluar y mitigar los riesgos de seguridad a los que está expuesta la organización. • Fundamento: Basado en la ISO 31000 y la ISO/IEC 27005, que proporcionan un marco para la gestión de riesgos, incluyendo la identificación, evaluación y tratamiento de riesgos.	

Tabla 2: Políticas y procedimientos a implementar (Elaboración propia, 2024).

4.4 Controles técnicos y organizativos para mitigar los riesgos identificados

La siguiente tabla ofrece una visión detallada de los controles técnicos y organizativos necesarios para mitigar los riesgos identificados en las aplicaciones y sistemas del INE. Implementar estos controles contribuirá a fortalecer la seguridad de la información y reducir la probabilidad y el impacto de los riesgos identificados.

CONTROLES TÉCNICOS Y ORGANIZATIVOS A IMPLEMENTAR EN LOS SISTEMAS INFORMÁTICOS DE LA 01 JUNTA DISTRITAL EJECUTIVA (JDE) DEL INE EN APIZACO TLAXCALA.

Aplicación	Riesgo de Seguridad	Controles Técnicos	Controles Organizativos
Portal Web Principal (Ine.mx)	SQL Injection	- Uso de consultas parametrizadas y procedimientos almacenados. - Implementación de WAF. - Pruebas de seguridad regulares (SAST, DAST).	- Capacitación en codificación segura. - Revisión de código y cumplimiento de prácticas seguras.
	Cross-Site Scripting (XSS)	- Implementación de CSP. - Uso de librerías para	- Políticas de gestión de vulnerabilidades. - Capacitación en prevención

		codificación y escape de datos. - Escaneo automatizado de vulnerabilidades XSS.	de XSS y buenas prácticas de desarrollo.
	Ataques DDoS	- Implementación de soluciones DDoS (CDN, WAF). - Monitoreo continuo del tráfico.	- Desarrollo de un plan de respuesta a incidentes DDoS. - Simulacros regulares para evaluar la capacidad de respuesta.
	Exposición de Datos Sensibles	Cifrado de datos en tránsito (TLS) y en reposo. - Implementación de RBAC. - Auditorías y monitoreo de seguridad.	Políticas de gestión y almacenamiento de datos sensibles. - Capacitación en manejo seguro de la información.
Portal Web Observadores Electorales (observadores.ine.mx)	Exposición de Datos Sensibles	Cifrado de datos en tránsito y reposo. - Implementación de controles de	- Políticas claras sobre manejo de datos sensibles. - Capacitación en manejo

		acceso estrictos. - Auditorías de código.	seguro de la información.
	Vulnerabilidad de Software	Actualización y parches regulares. - Pruebas de seguridad regulares (SAST, DAST).	- Gestión de parches y actualizaciones. - Auditorías regulares para asegurar la seguridad del software.
	Fuga de Información Personal	- Monitoreo de exfiltración de datos. - Cifrado de datos sensibles. - Controles de acceso basados en roles.	- Políticas de seguridad de datos. - Capacitación en manejo seguro de la información personal.
Correo Electrónico	Phishing	Implementación de filtros avanzados de correo. - Autenticación de correo electrónico (DKIM, SPF, DMARC).	- Capacitación sobre identificación y reporte de phishing. - Simulacros de ataques de phishing.
	Malware	- Uso de software antivirus y	- Políticas de seguridad de correos.

		antimalware. - Análisis de archivos adjuntos.	- Capacitación en identificación de correos sospechosos.
	Exfiltración de Datos	- Monitoreo continuo de comunicaciones. - Cifrado de correos electrónicos sensibles.	Políticas de manejo seguro de información por correo. - Auditorías regulares.
Aplicación móvil PREP Casilla	Manipulación de Resultados	- Revisiones de seguridad del código y API. - Permisos mínimos necesarios. - Cifrado de datos en tránsito y reposo.	Capacitación en seguridad móvil.
	Fuga de Información Personal	-Implementación de autenticación y autorización seguras. - Pruebas de seguridad de API y monitoreo.	Políticas claras sobre manejo de información personal. - Auditorías de cumplimiento.
Aplicación móvil SIJE	Robo de Identidad	-Implementación de autenticación multifactor(MFA) - Cifrado de	- Capacitación en concientización sobre seguridad.

		datos sensibles. - Monitoreo de actividades.	- Revisiones regulares de seguridad.
	Manipulación de Resultados	- Revisiones de seguridad del código y API. - Permisos mínimos necesarios. - Cifrado de datos en tránsito y reposo.	- Pruebas de penetración y auditorías de seguridad. - Capacitación en seguridad móvil.
Aplicación móvil SPE	Acceso no autorizado	-Implementación de autenticación segura y autorización basada en roles. - Cifrado de datos en tránsito y en reposo.	- Capacitación en seguridad móvil. - Revisiones periódicas de seguridad y auditorías de acceso.

Tabla 3: Controles técnicos y organizativos a implementar (Elaboración propia, 2024).

4.5 Propuesta de herramientas para configuración y despliegue el monitoreo de seguridad de los sistemas informáticos del INE

El propósito de esta propuesta es implementar una solución integral de monitoreo de seguridad para los sistemas informáticos del Instituto Nacional Electoral (INE). La configuración y despliegue de herramientas especializadas permitirá detectar, prevenir y mitigar ciber amenazas en tiempo real, protegiendo la integridad de los sistemas, la información sensible de los ciudadanos y los procesos electorales.

Se cubrirán las siguientes áreas críticas:

- **Sistemas de gestión electoral y bases de datos:** Monitoreo de acceso y protección de datos sensibles de votantes y procesos electorales.
- **Infraestructura de red:** Supervisión de tráfico entrante y saliente, conexiones remotas (VPN), firewalls, routers y switches.
- **Sistemas operativos y servidores:** Monitoreo de la actividad en los servidores del INE, incluyendo sistemas operativos y servicios críticos.
- **Aplicaciones:** Vigilancia de aplicaciones utilizadas para gestionar el padrón electoral y otras plataformas sensibles.
- **Gestión de usuarios y acceso:** Monitoreo de cuentas de usuarios y actividades privilegiadas para prevenir accesos no autorizados.

4.5.1 Herramientas de Monitoreo Propuestas

Para un monitoreo de seguridad efectivo, se propone la implementación de las siguientes herramientas:

1. **SIEM (Security Information and Event Management):**

Herramienta centralizada para recopilar, correlacionar y analizar eventos de seguridad en tiempo real.

Ejemplos: **Splunk, IBM QRadar, Elastic Security (ELK).**

2. **Sistemas de Detección y Prevención de Intrusiones (IDS/IPS):**

Detección de tráfico anómalo en la red y prevención de ataques.

Ejemplos: **Snort, Suricata, Palo Alto Networks.**

3. **Monitoreo de Logs:**

Análisis de registros de servidores, dispositivos de red y aplicaciones para detectar comportamientos sospechosos.

Ejemplo: **Graylog, LogRhythm.**

4. **Firewalls de Nueva Generación (NGFW):**

Monitoreo y protección del tráfico de red a nivel de capa de aplicación, identificando amenazas avanzadas.

Ejemplos: **Cisco ASA, Fortinet FortiGate.**

5. **Endpoint Detection and Response (EDR):**

Monitoreo de dispositivos finales para detectar malware, ataques de día cero y otros comportamientos maliciosos.

Ejemplos: **CrowdStrike Falcon, Microsoft Defender ATP, SentinelOne.**

6. **Sistemas de Monitoreo de Vulnerabilidades:**

Escaneo y evaluación periódica de vulnerabilidades en la infraestructura tecnológica.

Ejemplos: **Nessus, Qualys, OpenVAS.**

4.6 Plan de Respuesta ante Incidentes Cibernéticos

Este plan de respuesta ante incidentes cibernéticos se basa en los riesgos identificados en la matriz de riesgos del INE y en los controles técnicos y organizativos propuestos. El objetivo es definir un procedimiento claro para la identificación, contención, erradicación, recuperación y análisis de los incidentes cibernéticos que puedan afectar las aplicaciones y sistemas del INE.

4.6.1 Objetivo del Plan de Respuesta ante Incidentes

El propósito del plan es minimizar el impacto de los incidentes cibernéticos mediante una respuesta rápida, coordinada y eficaz, restaurar las operaciones afectadas, preservar la confidencialidad, integridad y disponibilidad de los datos y prevenir futuros incidentes similares.

4.6.2 Fase 1: Preparación

- **Formar un equipo de respuesta ante incidentes (CSIRT):** Este equipo debe estar compuesto por personal técnico (seguridad, redes, desarrollo de aplicaciones), legal, recursos humanos, relaciones públicas y gestión de riesgos.
- **Capacitación continua:** Realizar entrenamientos regulares para el equipo de respuesta, simulacros de ataques cibernéticos y sesiones de concientización para el personal sobre los riesgos (phishing, malware, etc.).
- **Herramientas y tecnologías:** Asegurarse de que las herramientas de monitoreo, detección y análisis (SIEM, WAF, DLP, antivirus, IDS/IPS) estén configuradas y actualizadas. Tener listas las soluciones de recuperación y copias de seguridad.

4.6.3 Fase 2: Detección y análisis

Monitoreo activo: Utilizar herramientas como SIEM para detectar actividades anómalas o sospechosas en los sistemas (exfiltración de datos, tráfico anormal, intentos de ataque DDoS, etc.).

Identificación del tipo de incidente: Cuando se detecte una posible brecha de seguridad, el CSIRT debe categorizarla en función de la matriz de riesgos. Ejemplos:

- **Ataque DDoS:** Alta latencia, indisponibilidad de los servicios.
- **SQL Injection o XSS:** Acceso no autorizado a bases de datos, manipulación de páginas web.
- **Phishing o malware:** Acceso no autorizado a correos electrónicos, comportamiento anómalo de usuarios.

Evaluación del impacto: Determinar qué sistemas o datos han sido afectados, la magnitud del incidente, y la potencial pérdida de información (por ejemplo, datos personales, resultados electorales).

4.6.4 Fase 3: Contención

Contención a corto plazo:

- Aislar los sistemas afectados para evitar la propagación del ataque (por ejemplo, desconectar el servidor afectado de la red).
- Implementar listas negras (blacklists) o bloquear direcciones IP sospechosas si se trata de un ataque DDoS.

Contención a largo plazo:

- Implementar parches de seguridad en las aplicaciones y sistemas afectados.
- Reforzar las configuraciones de firewall y los permisos de acceso, evitando nuevas vulnerabilidades.

4.6.5 Fase 4: Erradicación

Eliminación de la amenaza:

- Si es malware, ejecutar herramientas de análisis y desinfección en los sistemas afectados.
- Reparar los códigos vulnerables (SQL Injection, XSS) en aplicaciones web mediante revisiones y parches de seguridad.
- Si la información fue comprometida, asegurarse de revocar accesos y resetear credenciales.

Verificación del sistema: Realizar un análisis exhaustivo para asegurar que no queden restos de la amenaza. Monitorear los sistemas para detectar cualquier actividad residual

4.6.6 Fase 5: Recuperación

Restaurar las operaciones:

- Restaurar el acceso a los sistemas afectados de forma controlada.
- Verificar la integridad de los datos y asegurar que las aplicaciones y servicios estén completamente operativos.
- Utilizar copias de seguridad en caso de pérdida de datos.

Monitoreo post-incidente:

- Incrementar la vigilancia sobre los sistemas afectados para detectar posibles intentos de ataque posteriores.
- Revisar los registros de actividad para asegurarse de que no haya accesos no autorizados después de la recuperación.

4.7 Plan de Recuperación a Incidentes Cibernéticos

El Plan de Recuperación ante Incidentes Cibernéticos tiene como objetivo restaurar las operaciones críticas del INE después de un incidente cibernético, minimizar el impacto en los sistemas afectados y asegurar la continuidad operativa. Este plan se centra en garantizar la confidencialidad, integridad y disponibilidad de los datos y servicios del INE, tomando en cuenta los riesgos previamente identificados.

4.7.1 Fase 1: Preparación para la recuperación

Definir el Equipo de Recuperación: El equipo responsable de la recuperación debe incluir personal de seguridad de la información, administradores de sistemas, desarrolladores, y gerentes de las áreas afectadas.

Planificación de Contingencias:

- Mantener una estrategia clara para respaldos regulares de datos críticos (diarios, semanales, mensuales).
- Definir los RTO (Recovery Time Objective) y RPO (Recovery Point Objective) para cada sistema crítico, indicando el tiempo máximo de recuperación permitido y la pérdida máxima aceptable de datos.

Documentación del Sistema: Asegurar que la documentación de los sistemas, incluyendo las configuraciones y arquitecturas, esté siempre actualizada y accesible.

4.7.2 Fase 2: Evaluación del Incidente y Análisis de Daños

Evaluación de los Sistemas Afectados:

- Revisar qué servicios, sistemas y datos han sido comprometidos durante el incidente.
- Identificar si la integridad de los datos ha sido comprometida (por ejemplo, si se ha realizado manipulación de datos electorales o fuga de información personal).

- Determinar la naturaleza y el origen del ataque para asegurar que el vector de ataque se haya eliminado por completo antes de proceder con la recuperación.

Análisis de Impacto:

- Evaluar el impacto del incidente en las operaciones críticas del INE, como el acceso al portal web, las aplicaciones móviles (PREP Casilla, SIJE, SPE), o la exfiltración de datos a través de correos electrónicos.
- Informar a los directivos y al equipo de comunicaciones para coordinar las acciones de comunicación interna y externa.

4.7.3 Fase 3: Recuperación de los Sistemas Afectados

Restauración desde Copias de Seguridad:

- **Bases de datos y aplicaciones:** Restaurar los datos afectados desde las copias de seguridad más recientes (RPO), priorizando sistemas críticos como el portal web del INE, las aplicaciones móviles (PREP Casilla, SIJE, SPE) y los correos electrónicos.
- **Servidores y redes:** Asegurarse de que los servidores y componentes de red comprometidos sean reparados, parcheados y reinstalados según sea necesario. En caso de un ataque DDoS, asegurar que el tráfico legítimo haya sido restaurado.

Reparación de Vulnerabilidades:

- Asegurar que las vulnerabilidades detectadas durante el incidente hayan sido corregidas, aplicando parches a los sistemas y configurando las medidas de seguridad adecuadas.
- Revisar el código de las aplicaciones web para evitar la recurrencia de SQL Injections, Cross-Site Scripting (XSS), o la exposición de datos sensibles.

Revisión de Permisos y Credenciales:

- Revocar accesos no autorizados y restablecer credenciales comprometidas.
- Implementar autenticación multifactor (MFA) en sistemas sensibles si aún no está configurada.

4.7.4 Fase 4: Verificación de la Integridad y Operatividad

Pruebas de Integridad de Datos:

- Verificar que los datos restaurados desde las copias de seguridad no estén corrompidos y que su integridad sea consistente con los originales.

- Realizar pruebas adicionales de integridad de datos en aplicaciones críticas como el SIJE (Sistema de Información de la Jornada Electoral) para garantizar que los resultados electorales no se hayan visto comprometidos.

Validación de los Sistemas:

- Realizar pruebas de funcionalidad en todos los sistemas y aplicaciones restaurados para asegurar que están operando correctamente.
- Probar las configuraciones de seguridad (firewalls, WAF, autenticaciones) para asegurar que se han implementado las mejoras necesarias.
- Aumentar el monitoreo de la actividad de red en los días posteriores para detectar posibles intentos de reinfección o nuevos ataques.

4.7.5 Fase 5: Comunicación y Notificación

Comunicación Interna:

- Informar a todos los empleados sobre la restauración de los sistemas y las medidas tomadas para garantizar la seguridad de los sistemas del INE.
- Proporcionar información a las áreas afectadas sobre los plazos y procedimientos de recuperación.

Comunicación Externa:

- En incidentes de gran magnitud o cuando haya habido un compromiso de datos sensibles, emitir una notificación pública informando sobre las acciones tomadas y el estado actual del sistema.
- Notificar a los usuarios afectados por la fuga de información (si aplica), según lo exijan las normativas de protección de datos.

Reportes a Autoridades:

- Cumplir con las regulaciones locales (como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares) notificando a las autoridades competentes si ha habido una fuga de datos personales.

4.8 Tablas de Evaluación para la propuesta de Auditoría de Seguridad Informática.

A continuación, propongo una tabla de evaluación para realizar una auditoría de seguridad informática en los sitios web del INE. Esta tabla permite una revisión sistemática de los aspectos más críticos para garantizar la seguridad de las plataformas

EVALUACIÓN DE SEGURIDAD PARA SITIOS WEB

Aspecto a Evaluar	Descripción	Cumple Sí/No/Parcial	Nivel de Riesgo Alto/Medio/Bajo	Observ.
HTTPS/SSL Implementado	Verificar que el sitio web utilice un certificado SSL válido para asegurar la transmisión de datos entre el usuario y el servidor.			
Configuración de Cookies	Verificar que el sitio web utilice un certificado SSL válido para asegurar la transmisión de datos entre el usuario y el servidor.			

Autenticación y Autorización	Comprobar la existencia de mecanismos robustos de autenticación (multi-factor) y autorización para proteger áreas sensibles.			
Control de Sesiones	Revisar el tiempo de expiración de sesiones y la protección contra secuestro de sesión (session hijacking).			
Protección contra Inyección SQL	Verificar que no existan vulnerabilidades de inyección SQL en los formularios y puntos de entrada de datos.			
Protección contra XSS	Revisar si el sitio es vulnerable a ataques de			

	scripting entre sitios (Cross-Site Scripting).			
Política de Contraseñas	Comprobar que las políticas de contraseñas sean seguras (longitud mínima, complejidad, rotación, no reutilización).			

Tabla 4: Auditoría de seguridad informática para los sitios web del INE (Elaboración propia, 2024).

CAPÍTULO 5: CONCLUSIONES

En conclusión, al desarrollar el proyecto “Implementación de un Sistema de Gestión de Seguridad Informática aplicado a las Juntas Distritales del Instituto Nacional Electoral (INE)” me deja buenos aprendizajes puesto a que día a día se manejan grandes volúmenes de datos de datos personales de las personas electoras.

Al aplicar un SGSI en la 01 Junta Distrital del INE en Apizaco Tlaxcala, se fortalece la resiliencia ante incidentes de seguridad, permitiendo una rápida detección, respuesta y recuperación de cualquier amenaza cibernética. Esto asegura la continuidad de los procesos críticos del INE, como la gestión del padrón electoral y los sistemas de votación, que son fundamentales para la democracia del país.

Además, el SGSI permite una mejora continua en los controles de seguridad, adaptándose a las nuevas amenazas y tecnologías, lo que no solo protege la integridad de los sistemas actuales, sino que también prepara al INE para enfrentar futuros desafíos en el ámbito digital. En resumen, este proyecto es esencial para mantener la transparencia, confianza y seguridad de los procesos electorales, garantizando que las Juntas Distritales cuenten con los recursos y capacidades necesarias para operar en un entorno seguro y controlado.

CAPÍTULO 6: COMPETENCIAS DESARROLLADAS

Para llevar a cabo este proyecto se requirió tener una serie de competencias fundamentales para garantizar su éxito y buen desarrollo. A continuación, se describen las competencias adquiridas a lo largo de este proyecto:

- **Protección de Datos Sensibles:** Es fundamental asegurarse que la información estadística y personal recolectada y gestionada por el INE esté protegida contra accesos no autorizados, pérdidas o alteraciones.
- **Cumplimiento Regulatorio:** Debemos tener en cuenta el debido uso y cumplimiento de normativas y leyes relacionadas con la protección de datos y la privacidad, como el Reglamento General de Protección de Datos (GDPR) en Europa o leyes locales de protección de datos.
- **Gestión de Riesgos:** Identifica, evalúa y gestiona los riesgos relacionados con la seguridad de la información nos permite implementar controles adecuados para mitigar posibles amenazas.
- **Análisis de Riesgos y Vulnerabilidades:**
Permite identificar y comprender las amenazas potenciales y debilidades en los sistemas. Esto es fundamental para anticipar problemas y diseñar estrategias para proteger la información y garantizar la estabilidad operativa.
- **Gestión de Proyectos:**
Permite la planificación y ejecución efectiva del SGSI. La gestión de proyectos asegura que todas las tareas se realicen a tiempo y dentro del presupuesto, garantizando la implementación exitosa de las medidas de seguridad.

- **Mejora Continua y Adaptación:**

Permite actualizar y ajustar las prácticas de seguridad en respuesta a nuevas amenazas y tecnologías. La mejora continua asegura que el SGSI se mantenga efectivo y relevante en un entorno tecnológico en constante cambio.

CAPÍTULO 7: FUENTES DE INFORMACIÓN

Academia Seguridad Cero. (2024). Obtenido de

<https://academy.seguridadcero.com.pe/blog/escaneo-vulnerabilidades-autom%C3%A1tico-OWASP-ZAP>

Delta Protect. (2024). Obtenido de

<https://www.deltaprotect.com/blog/amenazas-de-ciberseguridad>

Delta Protect. (2024). Obtenido de <https://www.deltaprotect.com/blog/que-es-sgsi>

Docusing. (2024). Obtenido de <https://www.docuSign.com/es-mx/blog/desarrolladores/politicas-de-seguridad-informatica>

FIRMA-E Consultoria y desarrollo de TI. (2024). Obtenido de

<https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/>

FreeCodeCamp. (2024). Obtenido de

<https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/>

Hubspot. (2024). Obtenido de <https://blog.hubspot.es/website/que-es-seguridad-informatica>

Hubspot. (2024). Obtenido de <https://blog.hubspot.es/website/que-es-sso>

IBM. (2024). Obtenido de <https://www.ibm.com/mx-es/topics/security-controls>

INE. (2024). Obtenido de <https://ine.mx/voto-y-elecciones/elecciones-2024/>

INE. (2024). Obtenido de

<https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/132944/coe-1so-28-03-2022-p04.pdf>

Listopro Community. (2024). Obtenido de

<https://community.listopro.com/owasp-zap-herramienta-de-seguridad-de-aplicaciones-web/#:~:text=Funcionalidades%20y%20Caracter%C3%ADsticas,solicitudes%20y%20respuestas%20HTTP%2FHTTPS.>

MINTIC COLOMBIA. (2024). Obtenido de

https://gobiernodigital.mintic.gov.co/692/articles-150514_G3_Procedimiento_de_Seguridad.pdf

PANDORA FMS. (2024). Obtenido de

<https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/>

Pragma. (2024). Obtenido de <https://www.pragma.co/es/blog/guia-de-uso-de-owasp-zap>

Soluciones de Software OTRS. (2024). Obtenido de

<https://otrs.com/es/casos-de-uso/sgsi/>

SYDLE. (2024). Obtenido de <https://www.sydle.com/es/blog/ciclo-pdca-61ba2a15876cf6271d556be9>

White Shield. (2024). Obtenido de <https://whiteshield.io/blog/normas-de-seguridad-informatica/>