**Modelo de seguridad para la gestión de vulnerabilidades en aplicaciones web en el Gobierno Autónomo Departamental de Oruro y sus secretarias basado en el estándar ISO/IEC 27034 y O-ISM3**

**Área**: Seguridad de la información.

**Tema**: Un modelo de seguridad para la gestión de vulnerabilidades en aplicaciones web que contemple lineamientos generales para el diseño de una política de seguridad en aplicación web con estándares internacionales ISO/IEC 27034, y O-ISM3.

**Objeto**: Lineamientos para un modelo de seguridad para la Gobierno Autónomo Departamental de Oruro y sus Secretarias

**INTRODUCCION.**

En el actual panorama tecnológico, donde las aplicaciones web juegan un papel fundamental en la prestación de servicios y en la gestión de información en organizaciones gubernamentales, la seguridad se ha convertido en una preocupación primordial. Es esencial garantizar la protección de los datos sensibles y la integridad de las aplicaciones frente a posibles vulnerabilidades que puedan comprometer la confidencialidad y la disponibilidad de la información.

De acuerdo a Cloudflare Inc. empresa estadounidense que brinda servicios de red de entrega de contenido, ciberseguridad en la nube, mitigación de DDoS y servicios de registros de dominios, publica que los riesgos mas comunes para la seguridad de aplicaciones web enfrentan varios tipos de ataques, siendo los más comunes las vulnerabilidades del día cero, vulnerabilidad desconocidas para los creadores de las aplicaciones web donde no se tiene una solución disponible atendiendo mas de 20.000 casos cada año. También se presentan ataques de Scripting entre sitios (XSS), Inyección de código SQL (SQi), Ataques de denegación de servicio (DoS) y ataques de denegación de servicio distribuido (DDoS), Corrupción de memoria, Abuso de API y API paralelas entre los principales tipos de ataque.

Considerando estos tipos de ataques, el Gobierno Autónomo Departamental de Oruro y sus Secretarías reconocen la necesidad de implementar un modelo de seguridad sólido y efectivo para la gestión de vulnerabilidades en sus aplicaciones web. Para lograr este objetivo, se propone adoptar estándares ISO orientados a la seguridad de la información, reconocidos internacionalmente como marcos de referencia para la seguridad en el desarrollo y la gestión de aplicaciones.

El estándar ISO/IEC 27034 proporciona directrices y mejores prácticas para la aplicación de procesos de seguridad en el ciclo de vida del desarrollo de software, centrándose especialmente en la identificación, el tratamiento y la mitigación de vulnerabilidades. Por otro lado, O-ISM3 es un modelo de madurez de gestión de seguridad de la información que permite evaluar y mejorar los procesos de seguridad en una organización.

A lo largo de este trabajo de investigación, se analizarán los principales desafíos y riesgos asociados a la seguridad en las aplicaciones web del Gobierno Autónomo Departamental de Oruro y sus Secretarías. Se revisarán las mejores prácticas propuestas por estos estándares y se adaptarán a las necesidades y características específicas de estas entidades.

**Antecedentes**

Las instituciones del sector gubernamental cuentan con aplicaciones web que trabajan con información clasificada y que a su vez operan con grandes volúmenes de información; siendo necesario analizar y comprender los desafíos y riesgos asociados a la seguridad de las aplicaciones web utilizadas en este sector. Esto implica examinar las vulnerabilidades comunes en las aplicaciones web, los métodos de explotación utilizados por los atacantes y las consecuencias potenciales de una brecha de seguridad. Motivo por la cual, la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación AGETIC, brinda a las instituciones estatales lineamientos y herramientas para el Gobierno Digital, en cumplimiento al decreto supremo N° 3525 del 4 de abril del 2018 (Decreto Supremo 3525, 2018).

Por otro lado, la tesis doctoral “Técnicas para la optimización del análisis automático de vulnerabilidades en aplicaciones web”, Roman, F, 2018 hace referencia a un estudio de vulnerabilidades en aplicaciones web. En el presente estudio cita que el 55% de los sitios web presentan vulnerabilidades de severidad grave y un 84% de severidad grave.

En Bolivia la tesis de maestría “Modelo de seguridad para el desarrollo de software”, Pachacuti, M., 2020 presenta un modelo de desarrollo basado en normativas, estándares guías y buenas prácticas. Propone actividades para integrar prácticas de seguridad en cada una de las etapas del desarrollo de software con el objetivo de reducir el riego (PACHACUTI, 2020)

**Planteamiento del problema**

La ausencia de un marco de seguridad para la identificación temprana y el manejo adecuado de las vulnerabilidades presentes en las aplicaciones web conlleva un riesgo significativo para la operatividad del gobierno y la protección de los datos personales y financieros de los ciudadanos. Además, la falta de un marco de referencia común dificulta la colaboración y coordinación entre las secretarías, lo que limita la eficacia en la gestión de las vulnerabilidades y la adopción de prácticas de seguridad consistentes.

Considerando la problemática expuesta se plantea el siguiente problema:

¿Cómo reducir las vulnerabilidades de las aplicaciones web implementadas en las entidades gubernamentales del Estado Plurinacional de Bolivia?

**Objetivo General**

Desarrollar un modelo de seguridad para la gestión de vulnerabilidades en aplicaciones web basado en el estándar ISO/IEC 27034 y el marco de referencia O-ISM3.

**Objetivos Específicos**

* Identificar las vulnerabilidades de las aplicaciones web implementadas, identificando su nivel de riesgo.
* Analizar políticas, procedimientos y directrices de seguridad específicas para la gestión de vulnerabilidades en las aplicaciones web, considerando las mejores prácticas definidas en el estándar ISO/IEC 27034 y el marco de referencia O-ISM3.
* Implementar un proceso de monitoreo y seguimiento continuo de las vulnerabilidades en las aplicaciones web, utilizando herramientas y técnicas de escaneo de seguridad, para garantizar una detección temprana y una respuesta eficiente.
* Ejecutar pruebas de penetración y evaluaciones de seguridad en las aplicaciones web, con el fin de validar la efectividad del modelo de seguridad implementado y garantizar la mitigación de las vulnerabilidades identificadas.
* Evaluar la implementación del modelo de seguridad, a fin de identificar áreas de mejora y fortalecer la protección contra posibles brechas de seguridad.

**Justificación**

Las aplicaciones web implementadas desempeñan un papel fundamental en el Gobierno Autónomo Departamental de Oruro y sus Secretarías, ya que facilitan la gestión de información, la comunicación interna y externa, y el acceso a servicios y trámites en línea. Sin embargo, estas aplicaciones también presentan vulnerabilidades que pueden ser explotadas por actores malintencionados, lo que pone en riesgo la integridad, confidencialidad y disponibilidad de la información sensible manejada por la entidad gubernamental.

(Justificación teórica)

Ante este escenario, se hace necesario contar con un modelo de seguridad sólido que permita identificar, evaluar y gestionar de manera efectiva las vulnerabilidades presentes en las aplicaciones web en la entidad. El estándar ISO/IEC 27034 proporciona directrices y mejores prácticas para el desarrollo seguro de aplicaciones, abordando aspectos como la identificación de requisitos de seguridad, el diseño seguro, la implementación y el mantenimiento de aplicaciones web. Por otro lado, el O-ISM3 es un modelo de madurez para la gestión de la seguridad de la información que permite evaluar y mejorar los procesos de seguridad.

(Justificación practica)

La adopción de un modelo de seguridad basado en estos estándares proporcionará una base sólida para fortalecer la seguridad de las aplicaciones web. Esto permitirá mitigar los riesgos asociados a las vulnerabilidades presentes en estas aplicaciones, proteger la información sensible de posibles ataques y garantizar la continuidad de las operaciones gubernamentales.

Por tanto, se quiere brindar una guía práctica y aplicable para la gestión de vulnerabilidades en las aplicaciones web utilizadas por la entidad gubernamental, garantizando así un nivel adecuado de seguridad de la información.

(Justificación metodológica)

La investigación adoptada para este modelo de seguridad, será un combinando de métodos cualitativos y cuantitativos. Esta elección se basa en la necesidad de obtener una comprensión profunda de los aspectos técnicos y de gestión de las vulnerabilidades en las aplicaciones web, así como en la recopilación de datos objetivos y medibles para evaluar la efectividad del modelo propuesto.

La investigación aplicada aborda un problema real y práctico en el ámbito de la seguridad de las aplicaciones web gubernamentales. El objetivo principal de este estudio es desarrollar un modelo de seguridad efectivo para la gestión de vulnerabilidades en estas aplicaciones. Al aplicar los principios y enfoques establecidos en estos estándares reconocidos internacionalmente, se espera que el modelo propuesto sea altamente relevante y útil.

(Justificación social)

Un modelo de seguridad basado en estándares internacionales promueve la protección de la información personal y sensible, prevenir ciberataques, cumplir con regulaciones y estándares, y mejora la confianza de los servicios gubernamentales.

**Alcances y límites**

El modelo abarcará todas las etapas de la gestión de vulnerabilidades en las aplicaciones web implementadas, desde la identificación y evaluación inicial de las vulnerabilidades hasta su mitigación y seguimiento, implicando a los sistemas y plataformas específicas utilizadas en este entorno gubernamental.

El modelo se desarrollará en base a los estándares ISO/IEC 27034 y O-ISM3 utilizando los principios, prácticas y pautas definidas en estos estándares para garantizar la seguridad y la gestión efectiva de las vulnerabilidades en las aplicaciones web.

Se diseñará con el objetivo de ser implementado y aplicado en las aplicaciones web de la entidad gubernamental. Se prestará especial atención a la viabilidad y la aplicabilidad práctica de las medidas propuestas, teniendo en cuenta los recursos disponibles y las restricciones organizativas

Respecto a las limitaciones el éxito del modelo estará condicionado a la voluntad y la capacidad de la institución para adoptar e implementar las medidas propuestas. Si no se cuenta con un compromiso claro y un seguimiento adecuado, la efectividad del modelo puede verse limitada.

En cuanto a las limitaciones tecnológicas y presupuestarias la implementación puede verse limitada por restricciones tecnológicas y presupuestarias. La disponibilidad de recursos técnicos y financieros puede afectar la capacidad para implementar medidas de seguridad avanzadas y adquirir herramientas y tecnologías adecuadas.

A medida que las amenazas cibernéticas evolucionan constantemente, es importante reconocer que el modelo puede volverse obsoleto con el tiempo. Será necesario mantenerlo actualizado y adaptarlo a las nuevas formas de ataque y vulnerabilidades emergentes.

La efectividad del modelo puede depender de la experiencia y el conocimiento técnico de los profesionales encargados de implementarlo. La falta de capacitación y experiencia en la gestión de vulnerabilidades puede limitar la eficacia del modelo.

**MARCO TEORICO**

**ESTADO DEL ARTE**

Es importante de incluir pruebas de seguridad en el proceso de desarrollo. Entre los que se puede destacar:

* "Software Assurance Maturity Model" proyecto de OWASP (Owasp, 2009). OWASP apoyo al desarrollo del modelo de madurez para el aseguramiento del software (SAMM por sus siglas en inglés) desarrollado inicialmente por Pravir Chandra. Actualmente este documento es mantenido y actualizado por el proyecto OpenSAMM que es liderado por el mismo autor, Pravir Chandra. El Modelo de madurez para el aseguramiento del software (SAMM) es un marco abierto para ayudar a las organizaciones a formular e implementar una estrategia para la seguridad del software que se adapte a los riesgos específicos que enfrenta la organización. SAMM cuenta con una flexibilidad para ser utilizado por organizaciones pequeñas, medianas y grandes que utilizan cualquier tipo de desarrollo.
* "Ciclo de vida de desarrollo de la seguridad" por Microsoft (Microsoft, 2018). Integra seguridad en el flujo del ciclo de vida del desarrollo del software. Esta propuesta trata de un proceso de desarrollo de software que ayuda a los desarrolladores a crear un software más seguro y cumplir con los requisitos de cumplimiento de seguridad al tiempo que reduce los costos de desarrollo. La metodología que presenta Microsoft se basa en tres conceptos principales, los cuales son: Formación al personal en temas de seguridad, mejora continua del software y la responsabilidad de tener un plan de detección y respuesta ante incidentes de seguridad.
* "Software Security Design and Testing" por Sami Masalin, (Masalin, 2000). Esta tesis de maestría describe el proceso de pruebas y diseño de seguridad del sistema para el desarrollo seguro. También proporciona una base teórica de seguridad del software y del proceso de desarrollo, da énfasis en estándares de seguridad y análisis de riesgo.
* "Certified Tester Advanced Level Syllabus Security Tester" por la International Software Testing Qualifications Board (ISTQB, 2016). Este plan de estudios provee conceptos básicos de seguridad, plantea la alineación de las actividades de prueba de seguridad con las actividades del ciclo de vida del software. El objetivo de esta guía es capacitar al profesional de control de calidad en temas de seguridad para que este pueda planificar, realizar y evaluar las pruebas de seguridad desde diversas perspectivas.

Al igual que las pruebas de software en general, las pruebas de seguridad no pueden garantizar que un software u organización no esté expuesto a ataques cibernéticos. Los ataques cibernéticos son cada vez más sofisticados y continuamente se van descubriendo nuevas formas de atacar o encontrar vulnerabilidades. Sin embargo, las pruebas de seguridad pueden ayudar a identificar riesgos y evaluar la efectividad de las defensas de seguridad existente en el software. Existen otras actividades para complementar las pruebas de seguridad, como auditorías y revisiones de prácticas de seguridad.

**REFERENCIA TEÓRICA O CONCEPTUAL**

**Desarrollo de software**

Según IBM Research: "El desarrollo de software se refiere a un conjunto de actividades informáticas dedicadas al proceso de creación, diseño, despliegue y soporte de software". (IBM, 2019). Por tanto, el desarrollo de software es un proceso lógico iterative cuyo objetivo es la creación de software. El desarrollo de software incluye subprocesos como recolección de información, diseño de flujos, documentación, pruebas, depuración entre otros, a esto se le denomina ciclo de vida de software o software development life cycle (SDLC).

**Riegos de seguridad**

Los riesgos de seguridad de la información son aquellos que surgen de la pérdida de confidencialidad, integridad o disponibilidad de información o sistemas de información y reflejan los posibles efectos adversos para las operaciones de la organización (es decir, misión, funciones, imagen o reputación), activos de la organización, individuos, otras organizaciones y un país. (NIST 80-30, 2012)

La función de una evaluación de riesgos de seguridad es permitir que una organización comprenda qué áreas y activos pueden estar en riesgo y determinar la magnitud de cada riesgo. Para los evaluadores de seguridad, una evaluación de riesgos de seguridad puede ser una fuente rica de información a partir de la cual se pueden planificar y diseñar pruebas de seguridad. Se puede utilizar una evaluación de riesgos de seguridad para priorizar las pruebas de seguridad, de modo que el mayor nivel de rigor y cobertura de las pruebas se pueda centrar en las áreas con mayor exposición al riesgo.

**Control de calidad de software**

Es la evaluación del software basada en ciertos atributos. La calidad del software se define según el estudio de las características externas e internas del software. La calidad externa se determina según el rendimiento del software en el escenario en tiempo real en el modo operativo y su utilidad para los usuarios. La calidad interna, por otro lado, se centra en los aspectos intrínsecos que dependen de la calidad del código escrito. El usuario se centra más en cómo funciona el software en el nivel externo, pero la calidad en el nivel externo se puede mantener solo si el desarrollador ha escrito un código de buena calidad significativa.

**Seguridad de software**

Es la capacidad del software para mantener la integridad, confiabilidad y disponibilidad de la información. El software siempre tendrá problemas de seguridad. Casi todo software puede ser vulnerado fácilmente. Pero con la seguridad del software y las técnicas relacionadas, es posible que pueda hacer una diferencia en cuanto a la cantidad de errores de seguridad que eventualmente permanecerán en el software.

**PLANTEAMIENTO DE HIPOTESIS**

El diseño de un modelo de seguridad para la gestión de vulnerabilidades en aplicaciones web permite reducir el riesgo de ataques en las aplicaciones implementadas en la Gobierno Autonómica de Oruro y sus Secretarias.

**Variable dependiente**

Efectividad de la gestión de vulnerabilidades en las aplicaciones web.

**Variable independiente**

Modelo de seguridad para gestión de vulnerabilidades.

**Operacionalización de variables**

**Operacionalización de la variable dependiente**

|  |  |  |  |
| --- | --- | --- | --- |
| **Variable** | **Componente** | **Dimensiones** | **Indicadores** |
| **Efectividad de la gestión de vulnerabilidades en las aplicaciones web**.  Disminución de la probabilidad de ocurrencia para la detección, mitigación y prevención de vulnerabilidades en sus aplicaciones web | Detección de vulnerabilidades | Tiempo de resolución de vulnerabilidades | Número de vulnerabilidades detectadas y corregidas |
| Respuesta a vulnerabilidades | Impacto de las vulnerabilidades |
| Monitoreo y seguimiento | Cumplimiento de estándares y regulaciones |
| Detección de vulnerabilidades | Tiempo de detección | Tiempo de respuesta para solucionar vulnerabilidades |
| Evaluación y priorización | Tiempo de evaluación y priorización |
| Planificación de acciones | Tiempo de planificación de acciones |
| Implementación de acciones correctivas | Tiempo de implementación de acciones correctivas |

**Operacionalización de la variable independiente**

|  |  |  |  |
| --- | --- | --- | --- |
| **Variable** | **Componente** | **Dimensiones** | **Indicadores** |
| **Modelo de seguridad para gestión de vulnerabilidades.** | Políticas y marco normativo | Tiempo de respuesta y resolución | Tiempo transcurrido desde la detección de una vulnerabilidad hasta su resolución completa.  Tiempo promedio para corregir y aplicar parches a las vulnerabilidades identificadas |
| Evaluación de riesgos y análisis de vulnerabilidades | Nivel de gravedad e impacto de las vulnerabilidades | Estimación del riesgo asociado a las vulnerabilidades y su impacto en la confidencialidad |
| Pruebas de seguridad | Eficacia de las medidas de mitigación | Porcentaje de vulnerabilidades corregidas con éxito y no reintroducidas posteriormente |
| Gestión de parches y actualizaciones | Cumplimiento normativo y de políticas | Porcentaje de cumplimiento de los requisitos de seguridad definidos en el marco normativo aplicable |
| Respuesta a incidentes y mitigación de vulnerabilidades | Métricas de rendimiento | Número total de vulnerabilidades identificadas y corregidas.  Tiempo medio de resolución de vulnerabilidades.  Frecuencia de pruebas de seguridad realizadas. |

**DISEÑO METODOLOGICO**