Vulnerabilidades de seguridad

Breve descripción:

Un aspecto importante en el desarrollo de “software” es garantizar la seguridad en cada una de las etapas del proceso, incluyendo los despliegues en los distintos ambientes: desarrollo, pruebas y producción. Esto contribuye a la calidad y confiabilidad de las aplicaciones desarrolladas.

Abril 2024

Tabla de contenido

Introducción

Bienvenidos al componente formativo: vulnerabilidades de seguridad.

Cuando se habla de desarrollo de “software”, se deben tener en cuenta varios aspectos para no solo desarrollar pensando en solucionar una necesidad de un cliente, sino también en hacerlo contemplando características que otorgan calidad a los productos desarrollados. La evolución de la tecnología, los medios de comunicación y el acceso a la información han hecho que la seguridad de las aplicaciones se convierta en un aspecto de gran importancia, otorgando confiabilidad a usuarios y clientes al resguardar la información. Por lo tanto, este componente se enfocará en cómo evaluar y diagnosticar este importante aspecto en el desarrollo de “software”.

La gestión de la seguridad en el desarrollo de “software” comprende una serie de etapas que van desde el análisis de requerimientos hasta el despliegue y mantenimiento.

Herramientas como la matriz de control de acceso, estrategias de seguridad perimetral, y el uso de protocolos de comunicación segura son esenciales para fortalecer la defensa contra amenazas externas.

Las pruebas de vulnerabilidad son cruciales para identificar y mitigar riesgos, asegurando que las aplicaciones sean funcionales, seguras y protejan la integridad y confidencialidad de la información.

Este enfoque integral hacia la seguridad es fundamental para desarrollar “software” que sea robusto, confiable y seguro para los usuarios finales.

1. Marco de referencia en gestión de la seguridad

El "software" y la forma en que se accede a las aplicaciones exigen que arquitectos, diseñadores y programadores se centren en la seguridad de estas. Por lo tanto, es importante tener en cuenta que la seguridad no solo implica la configuración de acceso, las redes o los usuarios, sino que debe considerarse durante todo el proceso de desarrollo de las aplicaciones. Esto incluye seguir estándares de programación y adoptar buenas prácticas de desarrollo, como la norma ISO/IEC 27034:2011, COBIT y OWASP.

Figura 1. Ciclo de vida de desarrollo de "software"

Según Norma técnica ISO /IEC 27034-1:2011. El estándar ISO/IEC 27034 proporciona un estándar reconocido internacionalmente para la seguridad de las aplicaciones.

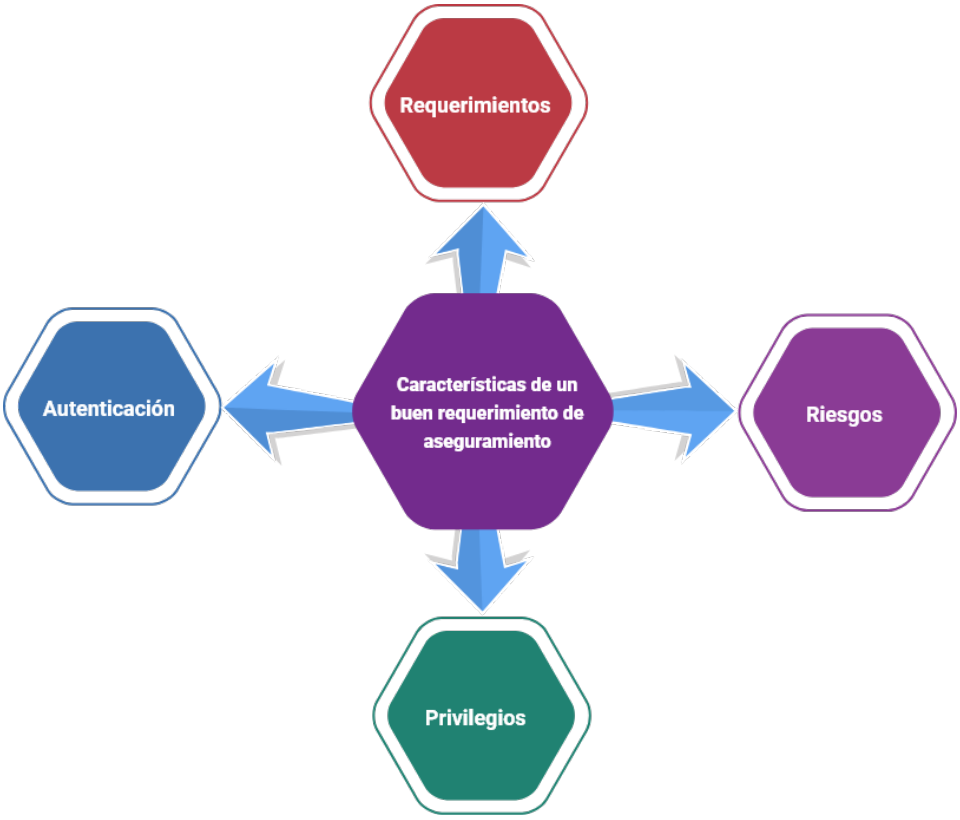
"Tecnología de la información- Técnicas de seguridad-Directrices para la preparación de la tecnología de la información y las comunicaciones para la continuidad del negocio".

Dentro de este marco de referencia se quiere enfocar en algunos aspectos relevantes del aseguramiento desde el desarrollo del "software".

1.1. Seguridad en el análisis de requerimientos

Con respecto a la seguridad en esta etapa del desarrollo, es crucial tener en cuenta las normas y políticas. De esta manera, los desarrolladores sabrán desde el principio qué funcionarios o roles tienen permitido realizar ciertas acciones y cuáles no. Esto facilitará la comprensión de la gestión de usuarios con sus roles y autenticación en las aplicaciones. Se deben evaluar posibles riesgos tales como la comunicación de datos con terceros, políticas de confidencialidad, seguridad de los datos de usuarios que acceden y se registran en la aplicación, y los respaldos de seguridad de la información, entre otros. Además, será posible analizar la estructura para auditar cambios en la información, identificando quién y cuándo se agregaron o modificaron datos. Los requisitos generales a considerar incluyen: autenticación, asignación de roles, aprobación de privilegios y evaluación de riesgos.

Figura 2. Requerimientos de Aseguramiento de calidad



1.2. Seguridad en el proceso de diseño

En la etapa de diseño, es fundamental considerar los procesos y las definiciones de los requisitos de seguridad previamente identificados durante el proceso. Esto incluye, por ejemplo, establecer la periodicidad de las copias de seguridad, el tipo de contraseñas a utilizar (ya sean largas o cortas) y todas sus características, las cuales deberán actualizarse en periodos de tiempo más cortos, además de establecer el cifrado de las comunicaciones y de los datos.

Durante esta etapa, también se deben tener en cuenta las posibles vulnerabilidades que pueden surgir dependiendo de la arquitectura y el diseño de la aplicación. Por ejemplo:

- Evaluar en el diseño los posibles riesgos que tiene una aplicación web.
- Contemplar los riesgos de una aplicación que se ejecutará internamente en una empresa.
- Elegir el diseño y la arquitectura de "software" que se va a implementar.
- Establecer políticas de seguridad para las aplicaciones.

Por lo tanto, es esencial diseñar un modelo de seguridad o de amenazas. Este modelo tiene como objetivo organizar, capturar y analizar los riesgos y vulnerabilidades identificados para tomar decisiones de manera rápida y ejercer un control adecuado, implementando contramedidas de forma efectiva en el proceso.

Para elaborar un modelo de amenazas, es importante tener en cuenta los siguientes pasos:

- Recopilar información esencial sobre las posibles amenazas para construir el modelo.
- Analizar y elaborar el modelo de amenazas utilizando la información recopilada.
- Identificar técnicas y tecnologías para mitigar las amenazas.
- Documentar el modelo de amenazas con claridad, incluyendo la identificación de riesgos, supuestos, y limitaciones.
- Implementar y probar las mitigaciones, y sincronizar el modelo con el diseño, considerando los controles de cambios.

En resumen, en el proceso de diseño, un modelo de seguridad es capaz de identificar las siguientes vulnerabilidades y posibles amenazas, como se muestra a continuación:

Video 1. Análisis, valoración de riesgos y controles de ciberseguridad: vulnerabilidades y amenazas

Enlace de reproducción del video

Síntesis del video: análisis, valoración de riesgos y controles de ciberseguridad: vulnerabilidades y amenazas
El video aborda los conceptos fundamentales de seguridad de la información, centrándose en vulnerabilidades y amenazas. Las vulnerabilidades se definen como

debilidades o fallas de seguridad en sistemas de información, que pueden ser explotadas por acciones no deliberadas o intencionadas, lo que genera riesgos para la seguridad de la información. Por otro lado, las amenazas se refieren a acciones que aprovechan estas vulnerabilidades para comprometer la seguridad de los sistemas, causando impactos adversos. Se mencionan fuentes comunes de amenazas como el "malware", la ingeniería social, las amenazas persistentes avanzadas (APT) y las "botnets". Además, se clasifican las amenazas en distintos tipos, incluyendo desastres naturales, errores y fallos no intencionados, ataques intencionados, entre otros. Finalmente, se resalta la importancia de comprender y protegerse contra estas vulnerabilidades y amenazas para preservar la confidencialidad, integridad y disponibilidad de la información.

En esta etapa, también se identifican requisitos similares a los de la primera fase, que incluyen: acceso a los componentes, administración del sistema, auditoría, gestión de sesiones, registros históricos, manejo de errores y excepciones, y separación de funciones.

1.3. Seguridad en el proceso de codificación

En el proceso de desarrollo de "software", es crucial considerar cómo los desarrolladores modifican y construyen los distintos componentes de las aplicaciones. Por lo tanto, resulta fundamental estandarizar las prácticas de codificación, documentación e identificación de ciertos requisitos, que incluyen:

- Aseguramiento de los ambientes de desarrollo.
- Documentación técnica.

- Codificación segura.
- Seguridad en las comunicaciones.
- Seguridad en ambiente de producción.

En esta etapa, el objetivo es facilitar el trabajo en equipo, evitando reprocesos y pérdida de trabajo. Por ello, es crucial utilizar herramientas que permitan sincronizar el trabajo y guardar la información de forma colaborativa. Además, se recomienda emplear buenas prácticas estandarizadas por organizaciones como OWASP o CERT, las cuales se detallarán más adelante. No obstante, es importante considerar las buenas prácticas para una adecuada codificación, tales como:

- Manejo de excepciones.
- Documentación de líneas o funciones.
- Depuración de código inservible.
- Métodos de nombramiento para las funciones y variables.
- Código legible para mejorar el mantenimiento de las aplicaciones.

1.4. Seguridad en el proceso de pruebas

En la etapa de pruebas, se pueden analizar las vulnerabilidades siguiendo el modelo de amenazas diseñado en la etapa anterior. Las pruebas se centrarán en cada uno de los aspectos del modelo, considerando la configuración de los entornos, la codificación realizada por los desarrolladores y la arquitectura de la aplicación. De esta manera, será posible identificar y corregir vulnerabilidades a tiempo. Una de las técnicas utilizadas para estas pruebas es el Fuzzing, que consiste en enviar datos secuenciales o aleatorios a un "software" o aplicación con el objetivo de detectar

vulnerabilidades no previstas. Además, es fundamental considerar el aseguramiento de la calidad, por lo cual se identifican los siguientes requerimientos:

- **Calidad en control de seguridad**. Es importante que las empresas definan un proceso para el aseguramiento de la calidad del "software". Estos modelos suelen estar basados en el ciclo de desarrollo, puesto que para evitar huecos de seguridad se debe conocer a fondo el proyecto.
- **Inspección de código**. Aplicando la técnica revisión de código se pueden encontrar vulnerabilidades que no son fáciles de identificar haciendo pruebas de caja negra.
- **Gestión de configuraciones**. El conocimiento de la arquitectura de la aplicación web puede revelar información valiosa para un atacante, como los protocolos utilizados, las funcionalidades administrativas, los métodos de cifrado utilizados o el servidor.
- **Caja Negra OWASP**. Presenta una serie de buenas prácticas para realizar pruebas de seguridad en las aplicaciones web e identificar vulnerabilidades que pueden aparecer desde las primeras fases del ciclo de desarrollo.

1.5. Seguridad en el proceso de despliegue y mantenimiento

Una buena práctica consiste en asegurar que los servidores destinados a los despliegues de mantenimiento, desarrollo y producción mantengan configuraciones casi idénticas. La razón por la cual se dice "casi idénticas" es que existen ciertas configuraciones que pueden variar ligeramente debido al acceso a las aplicaciones, pero, en cuanto a características generales, deberían ser iguales. Esto permite que, al

realizar pruebas, las aplicaciones se comporten de manera similar en diferentes entornos.

Los requisitos cruciales a considerar en esta fase incluyen:

Aseguramiento basado en riesgos y pruebas de seguridad, incluyendo pruebas de caja blanca y caja negra.

Además, es necesario configurar la red y gestionar el acceso de manera que solo las personas autorizadas puedan acceder a ella. Es importante tener en cuenta la arquitectura diseñada en etapas anteriores para entender bien los tipos de configuración. Configurar los accesos y la red para despliegues directos en la nube o en un servidor local implica consideraciones diferentes. OWASP también ofrece guías sobre cómo probar estos tipos de aseguramientos.

Entidades de estandarización

Existen entidades responsables de elaborar normativas de nivel técnico, que, con el apoyo de equipos técnicos compuestos por expertos, definen estándares. Estos estándares son técnicas establecidas en documentos publicados que facilitan la creación de un marco de trabajo para abordar problemas comunes en las organizaciones.

A continuación, se listan las principales entidades:

- **ISO - Organización Internacional de Normalización**. La principal actividad es la elaboración de normas técnicas internacionales.

- **ISACA SACA**. Es una organización global sin ánimo de lucro dedicada a fomentar las mejores prácticas y conocimientos en la industria de la tecnología de la información, con reconocimiento y aplicación a nivel mundial.
- **CCITT**. Es el Comité Consultivo Internacional Telegráfico y Telefónico, que se convirtió en ITU-T en 1993, y se dedica a desarrollar recomendaciones para estándares internacionales en comunicaciones telefónicas y telegráficas.
- **NIST**. Es una agencia del Departamento de Comercio de EE. UU. que ofrece un Marco de Ciberseguridad para ayudar a las empresas a comprender, gestionar y mitigar sus riesgos cibernéticos y proteger sus redes y datos.

En la siguiente tabla, se proporciona una perspectiva global de algunas normas que abordan la definición de ciberseguridad.

Tabla 1. Normas relacionadas con la ciberseguridad

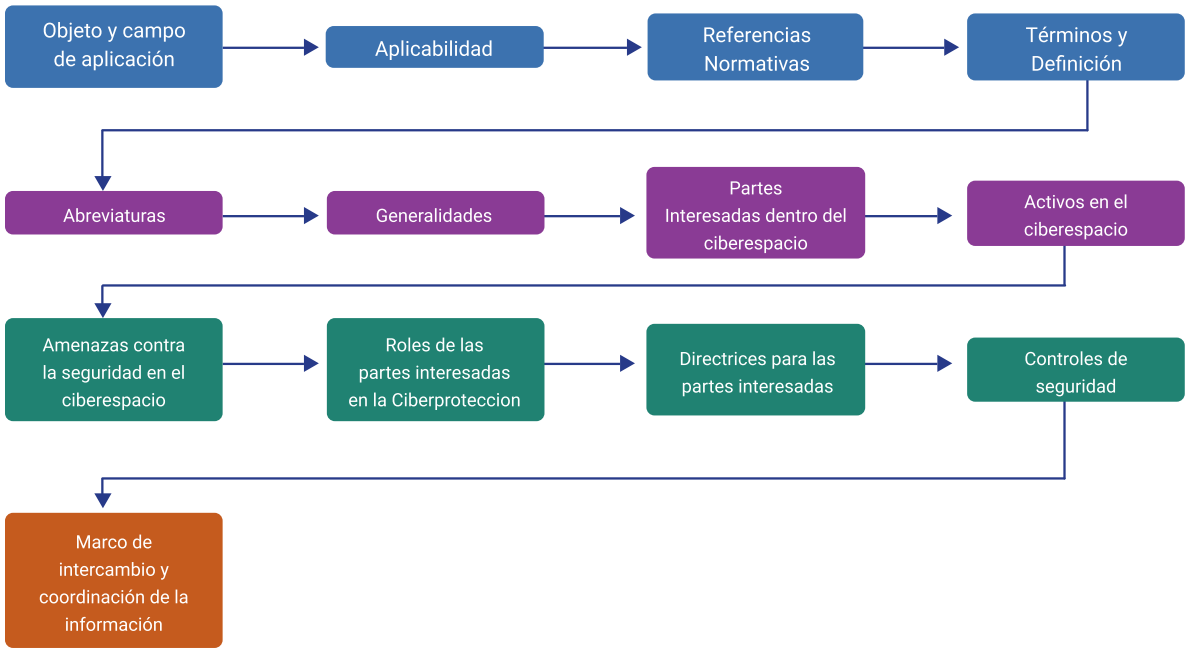
N°	Origen	Documento	Término	Organización	CDI	Intensión	Motivación	Amenazas
01	ISO/IEC JTC1/SC27	27032	Ciberseguridad	ISO	Sí	Solo los activos destinados a internet.	No diferenciación Entre actividades maliciosas o no.	Solo los activos virtuales conectados a internet, sin activos físicos.
02	ISO/IEC JTC1/SC27	27000	Seguridad de la información	ISO	Sí	Cualquier Origen de Riesgo en el Espacio cibernético.	No diferenciación entre malicioso o no intencional.	Cualquier Activo.
03	UIT-T	X.1205	Ciberseguridad	UIT	No	Cualquier Origen de Riesgo en el Espacio cibernético.	No diferenciación entre actividades maliciosas o no.	Cualquier Activo.
04	NIST	SP 800-39	Ciberseguridad	NIST	Sí	Riesgo Originado exclusivamente en el espacio cibernético.	Solo cubre orígenes maliciosos (ataques cibernéticos).	Solo los activos virtuales conectados a internet, sin activos físicos.

N°	Origen	Documento	Término	Organización	CDI	Intensión	Motivación	Amenazas
05	ISACA	Cybersecurity fundamentals	Ciberseguridad	ISACA	Sí	Certificación CSX.	Origen Malicioso.	Activos en el Ciberespacio.

La norma ISO/IEC 27032:2020 "Tecnología de la información - Técnicas de seguridad - Directrices para la ciberseguridad" establece un marco de trabajo diseñado para mejorar el estado de la ciberseguridad. Propone varios puntos estratégicos y técnicos necesarios para esta actividad, así como sus interdependencias con otros dominios de seguridad, incluyendo:

- Seguridad de la información.
- Seguridad en internet.
- Seguridad en redes.
- La protección de infraestructuras críticas de información.

Figura 3. Estructura de la norma ISO/IEC 27032:2020



La norma se enfoca en la seguridad del ciberespacio o cuestiones de ciberseguridad, con un énfasis particular en establecer conexiones entre diferentes brechas de la web. Este documento ofrece una guía técnica para abordar los riesgos comunes de ciberseguridad.

Dado el aumento en la frecuencia y la sofisticación de los ciberataques, se reconoce claramente la necesidad de proteger los recursos y activos. Surge entonces la importante pregunta:

¿Cómo empezar?

Aquí es donde los marcos de referencia, que se han venido desarrollando y adoptando, juegan un papel crucial, ya que proveen información valiosa y útil para el diseño de procesos de control y mitigación de riesgos de ciberseguridad.

Aunque es esencial elegir un marco de referencia y trabajar con él, es importante recordar que son solo una guía y no ofrecen soluciones definitivas. El enfoque en el análisis de riesgos es también crucial; cada marco propone una serie de controles entre los cuales se debe elegir los más aplicables al entorno específico y, si es necesario, realizar adopciones o ajustes de otros marcos de referencia.

Los marcos de referencia más utilizados y desarrollados incluyen propósitos particulares para su adopción y una breve descripción, aunque no se han detallado específicamente aquí.

Los marcos de referencia más utilizados son:

NIST CSF

NIST CSF ("National Institute of Standards and Technology - Cybersecurity Framework") - Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología.

Este marco de trabajo se diseñó para asistir a organizaciones de cualquier tamaño en la identificación, comprensión, gestión y mitigación de riesgos cibernéticos, mejorando la seguridad de sus redes y datos. Ofrece un lenguaje unificado y buenas prácticas basadas en normas de autoridades como ISO, ITU, CIS, y NIST. Clasifica estas prácticas por afinidad y sus recomendaciones enfatizan en la gestión de riesgos cibernéticos como un aspecto crucial en la seguridad organizacional. También busca mejorar la comunicación sobre gestión de riesgos y ciberseguridad entre responsables de seguridad y partes externas.

ISO / IEC 27001: 2013

Creado por la Organización Internacional de Normalización (ISO), este marco de trabajo ha demostrado ser eficaz para empresas de todo tipo y tamaño alrededor del mundo, convirtiéndose en el marco más conocido e implementado internacionalmente. Su enfoque principal reside en la norma ISO 27001, centrada en la protección de la integridad, disponibilidad y confidencialidad de la información. La esencia de esta propuesta se basa en la gestión de riesgos: identificar dónde se encuentran los riesgos y cómo abordarlos de manera metodológica.

COBIT (Objetivos de Control para Información y Tecnologías Relacionadas. En inglés: "Control Objectives for Information and related Technology")

El marco de trabajo COBIT, creado por ISACA, se enfoca en el gobierno de TI con un énfasis en los procesos empresariales, similar a los marcos de NIST e ISO. Utilizado especialmente en el sector público y para el cumplimiento de normativas legales en la gestión de TI, COBIT ofrece un conjunto de mejores prácticas, herramientas de control, supervisión, mapas de auditoría, y técnicas para la implementación y gestión eficaz de las tecnologías de la información.

HITRUST CSF (Health Information Trust Alliance – "Cybersecurity Framework")

Este marco fue desarrollado por la Health Information Trust Alliance (HITRUST), siendo ampliamente utilizado en la industria de la salud de Estados Unidos. HITRUST creó el CSF ("Cybersecurity Framework" - Marco de Ciberseguridad) para identificar elementos clave y posibles riesgos en entidades de salud, abarcando el conjunto de controles más extenso que podría aplicarse a cualquier organización. Es, posiblemente, el marco de trabajo que recibe actualizaciones con mayor frecuencia.

CSA. "Cloud Controls Matrix"

Este marco fue desarrollado por la Cloud Security Alliance (CSA), diseñado específicamente para los proveedores de servicios en la nube. Dado que la estructura del almacenamiento de datos en servicios de nube se enfrenta a riesgos únicos de este entorno, se requieren controles de seguridad especializados para la industria. Este marco proporciona una guía al respecto. La matriz de controles para servicios en la nube se actualiza con frecuencia, haciéndola atractiva para proveedores de servicios IT

en la nube de cualquier tamaño. Además, busca estandarizar las expectativas de seguridad, así como la taxonomía y terminología relacionadas con los servicios en la nube.

2. Matriz de control de acceso

La matriz de control es un documento diseñado para organizar los roles y permisos analizados desde la etapa de desarrollo, específicamente en la fase de requerimientos. Constituye una manera estructurada de definir quién va a realizar qué acciones dentro de la aplicación. Esta herramienta es particularmente útil para empresas grandes que gestionan diversas aplicaciones para llevar a cabo sus operaciones diarias.

Uno de los inconvenientes al desarrollar "software" es realizar pruebas sin considerar adecuadamente el acceso o permisos que cada usuario debe tener, dejando la organización de estos aspectos para la etapa final. Este enfoque puede resultar en reprocesos y en una evaluación insuficiente de la seguridad de la aplicación con respecto al usuario interno. Es crucial reconocer que el usuario interno de la organización representa el primer punto de vulnerabilidad; por tanto, la seguridad interna debe ser considerada un elemento importante dentro del análisis y diseño de las aplicaciones.

A continuación, se muestra un ejemplo de una matriz reducida para ilustrar el enfoque que se debe adoptar y los aspectos que se deben considerar en su implementación:

Figura 4. Matriz de control de acceso

Rol	Gestión de usuarios	Crear cuenta	Actualizar cuenta	Eliminar cuenta	Crear registro	Consultar estado de cuenta
Administrador						
Auxiliar contable						
Operador						

Esta matriz pertenece a una aplicación contable sencilla y muestra los roles de forma vertical en el lado izquierdo, mientras que las funcionalidades se disponen horizontalmente en la parte superior. Ahora procederemos a gestionarla, especificando quién podrá realizar qué acción o quién tendrá acceso a cada una de las funcionalidades. De esta manera, podemos ejercer control sobre la gestión de roles y permisos, determinando el nivel de acceso que cada usuario tiene en la aplicación.

Tabla 2. Gestión de Matriz de control de acceso

Rol	Gestión de usuarios	Crear cuenta	Actualizar cuenta	Eliminar cuenta	Crear registro	Consultar estado de cuenta
Administrador	x	x	x	x	x	x
Auxiliar contable				x	x	x
Operador						x

En la gestión de la matriz, se observa que el administrador podrá realizar todas las funciones, mientras que el auxiliar contable solo podrá ejecutar tareas como crear registros y consultar el estado de las cuentas. Por otro lado, el operador solo tendrá la capacidad de registrar pagos. Es recomendable revisar los accesos mediante la matriz de acceso de forma periódica para garantizar la seguridad y la correcta asignación de permisos.

3. Seguridad perimetral

En el ámbito de la seguridad informática, los sistemas de seguridad perimetral buscan prevenir el acceso no autorizado a la red, así como a los sistemas e información que contiene.

La seguridad perimetral se centra en establecer barreras de protección para prevenir ataques externos, al mismo tiempo que permite identificar actividades legítimas dentro de la propia red. Su objetivo es filtrar, proteger y aislar cualquier actividad desconocida o potencialmente fraudulenta.

Para profundizar en el tema, se invita a revisar el siguiente video:

Video 2. Seguridad perimetral

Enlace de reproducción del video

Síntesis del video: seguridad perimetral
La seguridad perimetral en los sistemas de información es un método utilizado por las empresas para defenderse de ataques cibernéticos antes de que alcancen sus sistemas. Se logra mediante dispositivos que configuran políticas de acceso, instalados entre la red interna y externa de la empresa. Estos sistemas incluyen “firewalls”, VPN, IPS, IDS, “honeypots”, entre otros. Los objetivos principales son soportar ataques externos, detectarlos, alertar sobre ellos, segmentar y asegurar sistemas y servicios, así como filtrar y bloquear tráfico ilegítimo. La protección perimetral es crucial para resguardar la información de la empresa, especialmente en entornos digitales.

4. Protocolos de comunicación segura

Cuando navegamos en internet a través de nuestro navegador preferido, se produce un intercambio de información con las distintas páginas web que visitamos. En muchas ocasiones, se comparte información que el usuario no percibe, mientras que otras veces se trata de información que se comparte de manera consciente, como cuando un usuario se registra o se suscribe.

Internet

Es una red pública a la que accede todo el mundo, y la información compartida puede ser vista por otros usuarios sin que nos demos cuenta.

Por esta razón, es crucial proteger nuestra información mediante protocolos de seguridad.

Los protocolos de comunicación y seguridad en la red

Aseguran que la información se transmita de manera segura en internet.

Están diseñados para impedir que los intrusos accedan a esta información, utilizando para ello diferentes dispositivos, aplicaciones maliciosas o servicios.

Existen diversos tipos de protocolos diseñados para esta protección, los cuales se mencionan a continuación:

Protocolo HTTP. Protocolo de transferencia de hipertexto que consiste en intercambiar información en la internet, es decir se transfiere información por medio de la URL en donde el usuario envía la información y el servidor le responde al usuario mostrando la página que un usuario solicita.

Protocolo FTP. El protocolo FTP funciona similarmente al HTTP, solo que este transfiere archivos por la red, funciona con arquitectura cliente servidor, permite autenticarse al momento de transferir archivos entre el cliente y un servidor de forma remota.

Protocolo SSH. Protocolo "Secure Socket Shell", es un protocolo que permite acceder a la red de forma segura por medio de un terminal remoto, permite autenticarse y encriptar la información entre dos dispositivos que se conectan al internet, es más utilizado para administrar sistemas por acceso remoto.

Protocolo DNS. Protocolo de Sistema de Nombres de Dominio, toma un directorio de dominios y los traduce a direcciones IP, por ejemplo si se escribe la dirección www.sofiaplus, el servidor no lee el nombre sofiaplus.com si no que rastrea la dirección ip correspondiente (192.168.0.1).

Protocolo TCP/IP. Es un protocolo que permite que los ordenadores se comuniquen entre sí de una forma sencilla, intercambiando información en la red, se compone de dos protocolos el TCP y el IP.

5. Pruebas de vulnerabilidad

Se trata de pruebas de "software" realizadas para evaluar los riesgos de seguridad en un "software", con el objetivo de minimizar las posibles amenazas y prevenir futuros ataques cibernéticos que puedan explotar vulnerabilidades en cada sistema instalado.

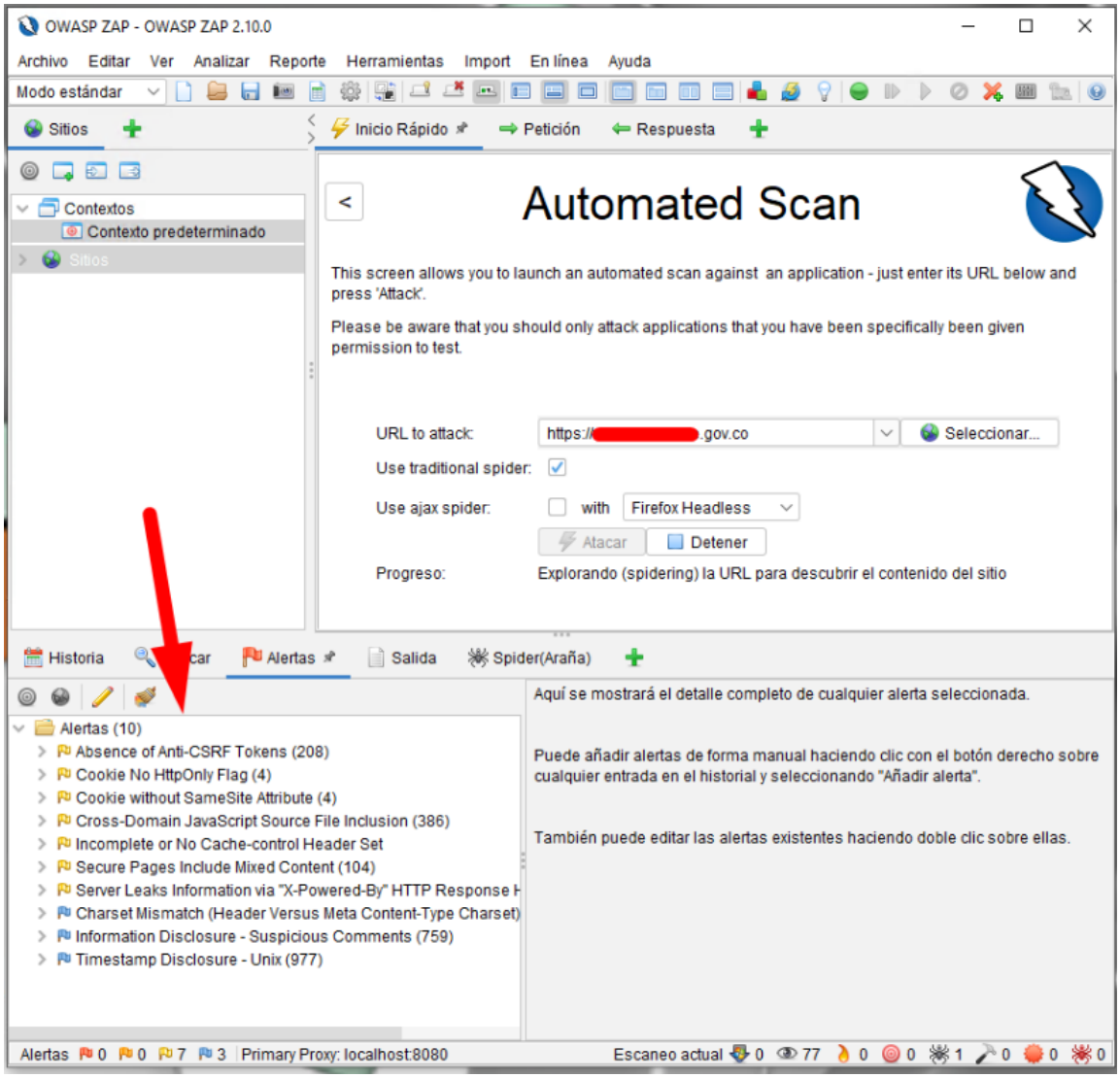
A continuación, se presentará una metodología práctica para identificar vulnerabilidades. Aunque no se sepa cómo explotarlas, es importante ser conscientes de que existen individuos que podrían hacerlo, perjudicando así a nosotros, a nuestros clientes y a sus reputaciones. Por razones de seguridad respecto a las empresas evaluadas, se utilizará como ejemplo el sitio web de una entidad estatal, cuyo nombre y dirección web se mantendrán en reserva. La imagen será editada para no comprometer la reputación de la entidad.

Instalación OWASP ZAP

Para llevar a cabo este proceso, es necesario instalar la aplicación OWASP ZAP en un sistema operativo Windows 10. Para ello, puede descargar el instructivo que le compartimos para este proceso.

Esta herramienta está diseñada para realizar pruebas de vulnerabilidad en aplicaciones y requiere tener instalado el JDK de JAVA como prerrequisito. Una vez instalado el JDK puede continuar descargando el instalador para el sistema operativo indicado.

Figura 5. Ejemplo de prueba



A partir de la prueba presentada, se explicará un poco las vulnerabilidades encontradas:

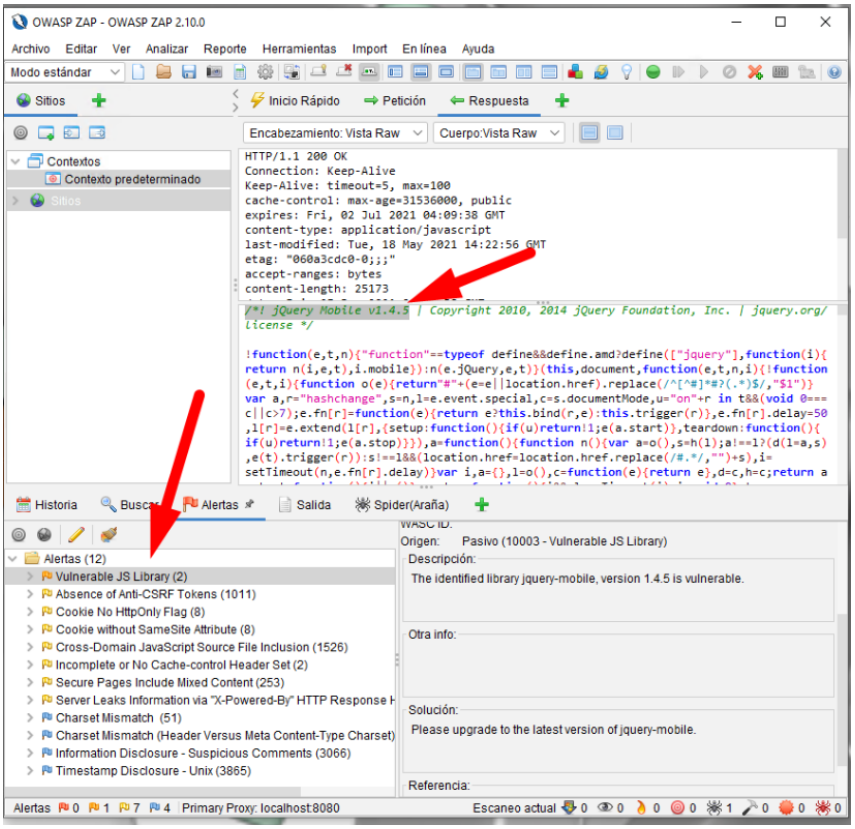
Ausencia de Tokens Anti-CSRF. De acuerdo con el reporte, la página web cuenta con 208 formularios susceptibles a ataques de CSRF. Para solucionar esto, es fundamental entender en qué consiste esta vulnerabilidad. Se puede consultar una guía sobre esta vulnerabilidad en el material complementario. Si utiliza un marco de trabajo

como Laravel, Git, Symphony, etc., busque técnicas específicas de su “framework”; probablemente.

“Cookie” Sin Bandera HttpOnly. Esta vulnerabilidad permite que otras webs puedan acceder a los datos de presencia de usuario o datos de sesión basados en “cookies”. Se puede resolver de varias maneras, siendo quizás la más sencilla agregar una configuración en el servidor.

Examinemos un caso crítico que también es fácilmente explotable.

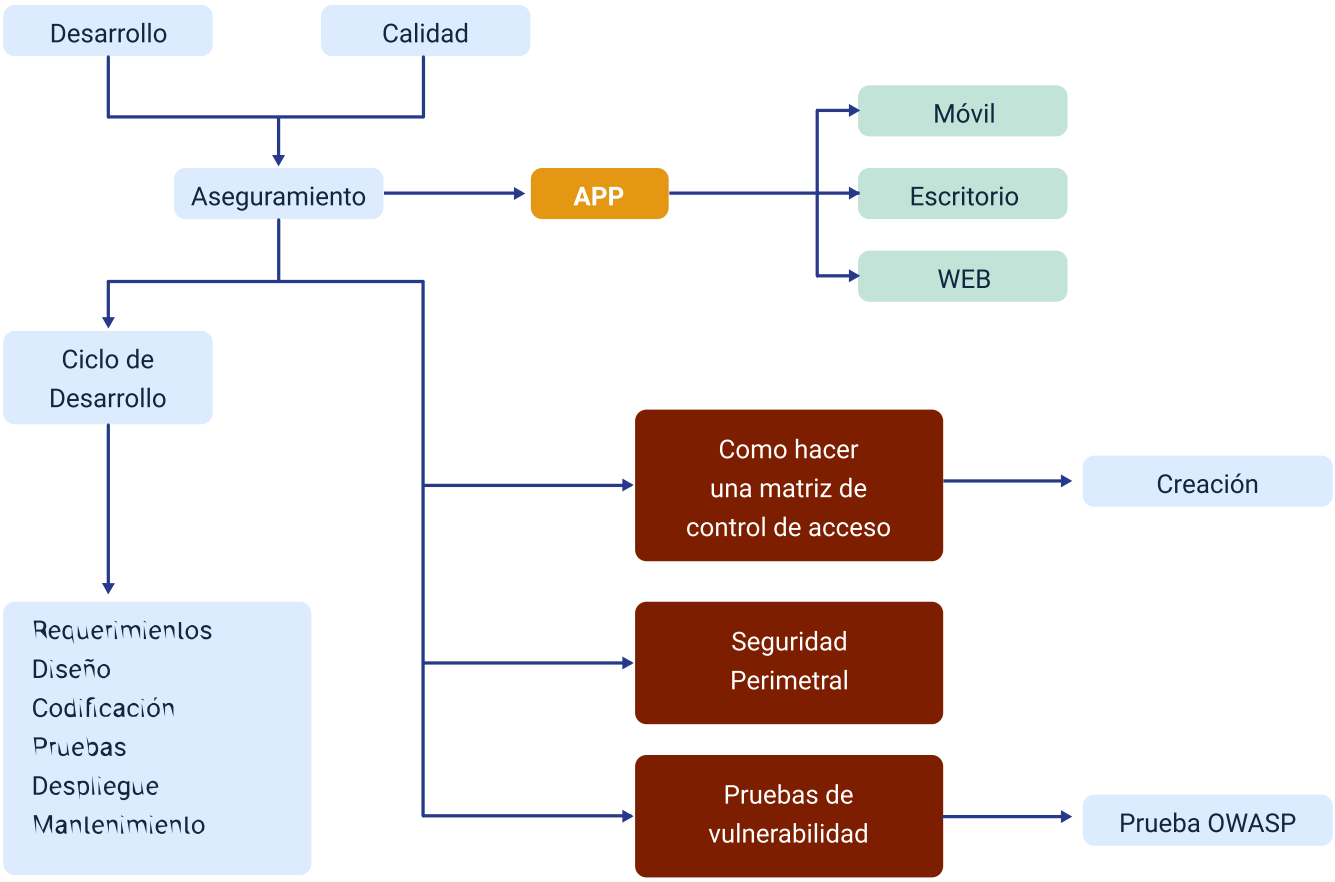
Figura 6. OWASP ZAP 2.10.0



El sitio web está utilizando la librería jQuery Mobile versión 1.4.5, la cual ya ha sido identificada por la comunidad jQuery como vulnerable. Es probable que en los foros de dicha comunidad se discuta cómo se detectó y esto podría indicar cómo

vulnerar este sistema. Sin embargo, la solución propuesta en la imagen es simplemente actualizar la librería a una versión más reciente y segura.

Síntesis


Desarrollo
Calidad
Aseguramiento
APP
Móvil
Escritorio
WEB
Ciclo de Desarrollo
Requerimientos
Diseño
Codificación
Pruebas
Despliegue
Mantenimiento
Como hacer una matriz de control de acceso
Creación
Seguridad Perimetral
Pruebas de vulnerabilidad
Prueba OWASP

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
3.Seguridad perimetral	ComputerHoy.com. (2015). ¿Qué es un firewall o Cortafuegos?	Video de YouTube	https://www.youtube.com/embed/3q2ENiVBAy8
3.Seguridad perimetral	VpnMentor. (2021, Enero 12). VPN Guide for Newbies. Blogpost.	Blog	https://es.vpnmentor.com/blog/que-es-una-vpn-guia-sobre-vpns-para-principiantes/
3.Seguridad perimetral	López, A.(2021). ¿Qué es un Honeypot en ciberseguridad? ¿para qué sirve? Tipos de Honeypots.	Video de YouTube	https://www.youtube.com/embed/SgH9rWB9ivQ
4.Protocolos de comunicación segura	Azuax.C.(2017). Conceptos Fundamentales del protocolo HTTP y HTTPS.	Video de YouTube	https://www.youtube.com/embed/ARmQMSeU9fU
5.Pruebas de vulnerabilidad	Roel.A(2021). Como descargar e instalar Java JDK16 en Windows 10-2021.	Video de YouTube	https://www.youtube.com/watch?v=hCBEavs08as

Glosario

API: una API es un conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar el "software" de las aplicaciones. API significa interfaz de programación de aplicaciones. Las API permiten que sus productos y servicios se comuniquen con otros, sin necesidad de saber cómo están implementados.

Aplicación: es un programa informático diseñado como una herramienta para realizar operaciones o funciones específicas. Generalmente, son diseñadas para facilitar ciertas tareas complejas y hacer más sencilla la experiencia informática de las personas.

Autenticación: es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores. Este proceso implica identificación (decirle al sistema quién es) y autenticación (demostrar que el usuario es quien dice ser).

"Browser": es el término inglés que se utiliza para identificar a un navegador web o navegador de Internet. Consiste en un "software", programa o incluso aplicación, que ofrece al usuario el acceso a la Red.

Delegar: dar [una persona o un organismo] un poder, una función o una responsabilidad a alguien para que los ejerza en su lugar o para obrar en representación suya.

Interfaz: como interfaz designamos, en informática, la conexión física y funcional que se establece entre dos aparatos, dispositivos o sistemas que funcionan independientemente uno del otro. En este sentido, la comunicación entre un ser humano y una computadora se realiza por medio de una interfaz.

Servidor: es un conjunto de computadoras capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Sintaxis: según su definición la sintaxis es la “Parte de la gramática que estudia el modo en que se combinan las palabras y los grupos que estas forman para expresar significados, así como las relaciones que se establecen entre todas esas unidades”

Sitio Web: es un conjunto de páginas web accesibles a través de internet, convenientemente enlazadas y con una finalidad concreta.

Web: conjunto de información que se encuentra en una dirección determinada de internet.

Referencias bibliográficas

Atico34 (2021). Definición de seguridad perimetral informática. Qué es y objetivos. https://protecciondatos-lopd.com/empresas/seguridad-perimetral-informatica/#Definicion_de_seguridad_perimetral

Calder, A. (2018). NIST Cybersecurity Framework: Una guía de bolsillo . IT Governance Publishing Ltd.

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. SISTEMAS (ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS), 119, 4-7.

Firma-e. (2021). ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información?. https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion

Hackmetrix (2021). Matriz de control de accesos: Qué es y cómo hacerla paso a paso. https://blog.hackmetrix.com/matriz-de-accesos/

ISO/IEC. (2020). Tecnologías de la información. Técnicas de seguridad. directrices para ciberseguridad (Num. 27032) https://tienda.icontec.org/gp-tecnologias-de-la-informacion-tecnicas-de-seguridad-directrices-para-ciberseguridad-gtc-iso-iec27032-2020.html

Créditos

Nombre	Cargo	Regional y Centro de Formación
Milady Tatiana Villamil Castellanos	Responsable del Ecosistema	Dirección General
Olga Constanza Bermúdez Jaimes	Responsable de Línea de Producción	Centro de Servicios de Salud - Regional Antioquia
Peter Emerson Pinchao Solis	Experto Temático	Centro Nacional Colombo Alemán - Regional Atlántico
Danny Alejandro Solano Concha	Evaluadora Instruccional	Centro de Servicios de Salud - Regional Antioquia
Paola Alexandra Moya	Evaluadora Instruccional	Centro de Servicios de Salud - Regional Antioquia
Andrés Felipe Herrera Roldán	Diseñador de Contenidos Digitales	Centro de Servicios de Salud - Regional Antioquia
Edwin Sneider Velandia Suárez	Desarrollador Fullstack	Centro de Servicios de Salud - Regional Antioquia
Edgar Mauricio Cortés García	Actividad Didáctica	Centro de Servicios de Salud - Regional Antioquia
Daniela Muñoz Bedoya	Animador y Productor Multimedia	Centro de Servicios de Salud - Regional Antioquia
Laura Gisselle Murcia Pardo	Animador y Productor Multimedia	Centro de Servicios de Salud - Regional Antioquia
Andrés Felipe Guevara Ariza	Locutor	Centro de Servicios de Salud - Regional Antioquia
Margarita Marcela Medrano Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro de Servicios de Salud - Regional Antioquia

Nombre	Cargo	Regional y Centro de Formación
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro de Servicios de Salud - Regional Antioquia
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro de Servicios de Salud - Regional Antioquia
Jaime Hernán Tejada Llano	Validador de Recursos Educativos Digitales	Centro de Servicios de Salud - Regional Antioquia