# Presentación propuesta de proyecto

| | |
|---|---|
| Estado | In progress |
| Fecha Inicio | @21 de septiembre de 2023 |
| Fecha última edición | @1 de noviembre de 2023 20:18 |
| № ID | CAL-35 |

▼ Objetivo

*Realizar pruebas de seguridad y de bases de datos a un sitio web funcional para identificar los posibles ataques informáticos.*

▼ Descripción

*Implementar pruebas de seguridad en redes y bases de datos al sitio web https://www.impetu.com.co/, como resultado se creará un plan de ciberseguridad para evitar ataques informáticos o posibles hackeos*

***PRUEBAS DE REDES***

*Prueba de conectividad:*

*Que el servidor esté accesible desde la red pública y que los puertos necesarios (por ejemplo, el puerto 8069 para Odoo) estén abiertos y respondan a las solicitudes.*

*Verificar que la dirección IP y el nombre de dominio estén configurados correctamente para el sitio web.*

*Prueba de velocidad y rendimiento:*

*herramientas como PageSpeed Insights o GTmetrix para evaluar el rendimiento de la página web, incluyendo la velocidad de carga y las recomendaciones de optimización.*

*Realizar pruebas de carga para determinar cómo responde el sitio web bajo carga pesada utilizando herramientas como Apache JMeter o locust.io para simular múltiples usuarios accediendo al sitio al mismo tiempo.*

*Prueba de seguridad:*

*Realiza análisis de seguridad utilizando herramientas como OWASP ZAP o Nessus para identificar posibles vulnerabilidades en la aplicación web de Odoo.*

*Asegurarse de que todas las actualizaciones de seguridad y parches estén aplicados en el servidor y en la aplicación.*

*Prueba de disponibilidad:*

*Implementar un monitoreo de disponibilidad utilizando herramientas como Pingdom, UptimeRobot o Zabbix para recibir alertas en tiempo real si el sitio web está caído o experimenta problemas de disponibilidad.*

*Pruebas de compatibilidad del navegador:*

*Verificar que el sitio web se muestre y funcione correctamente en varios navegadores web populares, como Chrome, Firefox, Safari e Internet Explorer.*

*Prueba de escalabilidad:*

*Evaluar la capacidad del sitio web para escalar en función de la demanda. Asegurarse de que la infraestructura de alojamiento pueda manejar un aumento en el tráfico sin problemas.*

*Prueba de copias de seguridad y recuperación:*

*Confirmar que se están realizando copias de seguridad regulares de la base de datos y los archivos del sitio web.*

*Verificar que se puede restaurar el sitio web a partir de estas copias de seguridad en caso de fallo.*

*Prueba de DNS: Asegurarse de que la configuración de DNS esté correcta y que el nombre de dominio se resuelva correctamente a la dirección IP del servidor Odoo.*

***PRUEBAS DE BASES DE DATOS***

*Pruebas de Integridad de Datos:*

*Verificar que los datos almacenados en la base de datos estén completos y precisos ejecutando consultas SQL que verifiquen la integridad de datos críticos, como la información del cliente o del producto.*

*Pruebas de Rendimiento de la Base de Datos:*

*Realizar pruebas de rendimiento para asegurarte de que la base de datos esté funcionando de manera eficiente.*

*Medir la velocidad de ejecución de las consultas SQL y asegurarse de que no haya cuellos de botella en la base de datos.*

*Pruebas de Copias de Seguridad y Restauración:*

*Realizar pruebas regulares de copias de seguridad y restauración para asegurarnos de que se pueda recuperar los datos en caso de un fallo inesperado.*

*Verificar que las copias de seguridad sean completas y que se puedan restaurar con éxito.*

*Pruebas de Migración de Datos:*

*Si se realizan actualizaciones de la web o de las extensiones, verificar que las migraciones de datos se realicen correctamente y que no se pierda información durante el proceso.*

*Pruebas de Seguridad de la Base de Datos:*

*Asegurarse de que la base de datos está protegida contra amenazas de seguridad. Esto incluye configurar adecuadamente los permisos de la base de datos y aplicar parches de seguridad.*

*Pruebas de Indexación y Optimización:*

*Comprobar que las tablas de la base de datos estén indexadas correctamente para acelerar las consultas.*

*Realizar análisis de rendimiento para identificar consultas lentas y optimizarlas.*

*Pruebas de Escalabilidad:*

*Evaluar cómo se comporta la base de datos bajo carga pesada, utilizando herramientas de pruebas de estrés de bases de datos para simular un alto volumen de tráfico y verificar que la base de datos pueda escalar adecuadamente.*

*Pruebas de Replicación y Alta Disponibilidad:*

*Si se tiene configurada la replicación de bases de datos o la alta disponibilidad, verificar que estas configuraciones funcionen según lo previsto.*

*Simular la pérdida de un nodo y asegurarse de que el sistema siga funcionando.*

*Pruebas de Recuperación de Desastres:*

*Implementar y probar un plan de recuperación de desastres que incluya la restauración de la base de datos en un entorno de recuperación en caso de un fallo grave.*

*Pruebas de Actualización de la web:*

*Antes de actualizar la web a una versión más reciente, realizar pruebas en un entorno de desarrollo o copia de seguridad para asegurarse de que la base de datos se actualice correctamente y que todas las extensiones y personalizaciones sigan funcionando.*

*Todo el proceso se irá registrando en repositorio de control de versiones de Notion.*

▼ Alcance

*Implementar pruebas exhaustivas de seguridad y rendimiento tanto en la infraestructura de redes como en la base de datos del sitio web https://www.impetu.com.co/. Esto incluye verificar la disponibilidad, velocidad, integridad de datos y seguridad, así como la capacidad de escalabilidad y copias de seguridad. Todas las pruebas se irán documentando en un repositorio de control de versiones en GitHub para garantizar un seguimiento y control efectivo del proceso. El objetivo final es crear un plan de ciberseguridad que proteja el sitio web contra ataques informáticos y asegure su óptimo funcionamiento.*

***FASES DEL PROYECTO***

*El proyecto se desarrolla en tres fases:*

1. *Implementación de las pruebas en el área de redes*
2. *Implementación de las pruebas en el área de bases de datos*
3. *Consolidación de la información que tendrá como resultado un plan de ciberseguridad para evitar ataques informáticos o posibles hackeos; con este plan ayudaremos a mitigar riesgos cibernéticos y a preparar el sitio para un crecimiento sostenible.*

***ALCANCE***

*Con la realización de estas pruebas lograremos:*

- *Mejorar la seguridad: El proyecto ayudaría a identificar y corregir posibles vulnerabilidades en la infraestructura de red y la base de datos, lo que fortalecería la seguridad del sitio web. Esto*

*reduciría el riesgo de ataques informáticos, robos de datos y posibles hackeos.*

- *Generar mayor confianza por parte del Usuario: Un sitio web más seguro y confiable genera confianza entre los usuarios, lo que puede aumentar la retención de clientes y la adquisición de nuevos usuarios.*
- *Mejorar el rendimiento: las pruebas de rendimiento ayudarían a optimizar el tiempo de carga del sitio web y su eficiencia general. Esto mejora la experiencia del usuario, ya que los visitantes obtienen respuestas más rápidas y una navegación más fluida.*
- *Disponibilidad Continua: el monitoreo de disponibilidad garantiza que el sitio esté en funcionamiento la mayor parte del tiempo. Esto es crucial para evitar interrupciones en el servicio que podrían afectar la reputación de la empresa y las ventas.*
- *Escalabilidad Asegurada: evaluar la capacidad de escalabilidad garantiza que el sitio web pueda crecer para manejar un mayor tráfico o demanda, lo que es fundamental para el crecimiento del negocio.*
- *Recuperación rápida de los datos: con las pruebas de copias de seguridad y recuperación aseguramos que en caso de un fallo inesperado, la recuperación de datos sea rápida y eficiente. Esto minimiza el tiempo de inactividad y reduce pérdidas potenciales.*
- *Actualizaciones Seguras: las pruebas antes de las actualizaciones del sitio web garantizan que las nuevas versiones y extensiones se implementen correctamente sin interrupciones ni pérdida de datos.*
- *Documentación y Control: Registrar todo el proceso en un repositorio de control de versiones proporciona una documentación detallada y permite un seguimiento preciso de cambios y mejoras, lo que facilita futuras auditorías y mantenimiento.*

▼ Planificación

*La planificación del proyecto se describe con un cronograma que indica las fechas establecidas por meses y actividades desarrolladas cada uno de los días, con el sistema de control de versiones de Github*

*https://www.notion.so/Cronograma-General-44cddf62367e4e74a5170b7ebb3ad6f8?pvs=4*

*Diagrama de Gantt*

*https://amaloja.atlassian.net/jira/software/projects/PROT/boards/2/timeline?shared=&atlOrigin=eyJpIjoiY2QwNjY2ZGU5NzIwNDIwZGE1NWZlNGM0Y2M1NzFmZDciLCJwIjoiaiJ9*

▼ Medios a utilizar

*https://www.notion.so/Medios-y-software-a-utilizar-f488ad255c644c6d85236fe9dae0ecbf?pvs=4*

▼ Presupuesto

*Para poder realizar un análisis y pruebas más exhaustivas se recomienda a futuro comprar las versiones que sean de pago, ya que traen herramientas adicionales.*

| ***SOFTWARE / HERRAMIENTA*** | ***VERSIÓN/COSTO*** |
|---|---|

| | |
|---|---|
| *PageSpeed Insights* | *Gratis* |
| *JMeter* | *Gratis* |
| *Nessus Essentials / Nessus Expert* | *Gratis / 6.605€ año* |
| *Uptime robot* | *Gratis / 7€ mes* |
| *Kali linux* | *Gratis* |

▼ Título

*Protocolo de ciberseguridad en sitios web*

▼ Ejecución

*El proyecto se desarrolla en tres fases:*

1. *Implementación de las pruebas a nivel de redes*

*https://www.notion.so/Pruebas-de-redes-f8dd96bfe97e4729bf8c9c613226a4cf?pvs=4*

2. *Implementación de las pruebas a nivel de bases de datos*

*https://www.notion.so/Pruebas-a-nivel-de-bases-de-datos-e3f5df3ac034452fbd86094c0b381cdd?pvs=4*

3. *Consolidación de la información que tendrá como resultado un plan de ciberseguridad para evitar ataques informáticos o posibles hackeos; con este plan ayudaremos a mitigar riesgos cibernéticos y a preparar el sitio para un crecimiento sostenible.*

*https://www.notion.so/Protocolo-de-ciberseguridad-en-sitios-web-93494d02a10b42f09f1a0d80c8d215dc?pvs=4*