

# **Documento de Alcance y Planificación para Pruebas de Penetración**

## **1. Introducción**

Este documento define el alcance, las reglas de enfrentamiento (RoE) y los requisitos para las pruebas de penetración que se llevarán a cabo en los sistemas y redes del cliente. El objetivo es garantizar que tanto la empresa de ciberseguridad como el cliente tengan una comprensión clara de los términos, límites y expectativas del compromiso.

## **Entrevista con CEO y director de TI**

*CEO: Bienvenido a Nexus Plaza. Lo invitamos a iniciar nuestro compromiso y analizar lo que esperamos de esta auditoría de seguridad. Estamos ansiosos por garantizar que nuestra infraestructura de seguridad cumpla o supere las salvaguardas necesarias. Le pasaré esto a nuestro director de TI para que describa nuestro entorno de red.*

*Director de TI: Como sabe, somos principalmente una empresa minorista en línea. Nuestros sitios de comercio electrónico orientados al cliente se alojan en Amazon, pero todas nuestras comunicaciones, almacenamiento y servicios de TI de envío se manejan internamente. Operamos un centro de datos local en Houston que respalda nuestras instalaciones de fabricación y almacenamiento. Actualmente hay 25 servidores separados en tres clústeres: administración, operaciones y logística. Además, operamos un clúster que brinda soporte para nuestra tienda de Amazon. El acceso remoto a estos sistemas se realiza a través de SSL o IPsec VPN. Usamos dos ISP para conectarnos a Internet, pero uno se usa principalmente para las comunicaciones con Amazon para admitir pedidos en tiempo real, inventario y contacto con clientes.*

*CEO: Recientemente, uno de nuestros competidores sufrió un ataque de ransomware dirigido a su sistema de inventario de producción. Perdieron una cantidad significativa de pedidos de clientes debido a que no podían recoger y enviar el inventario a tiempo. Nos preocupa que nuestros sistemas de depósito y envío puedan tener vulnerabilidades que podrían cerrarnos de manera similar si se produce una infracción. Cuando depende de una entrega rápida a los clientes, cualquier demora es un desastre.*

*Director de TI: Los sistemas que soportan nuestro almacenamiento y envío se encuentran en dos clústeres en el centro de datos: operaciones y logística. El acceso interno a estos sistemas está restringido al personal de administración del almacén, el personal de TI y los empleados de control de inventario. Nuestro sistema de control de inventario es compatible con una base de datos Microsoft SQL Server. Como puede ver en el diagrama, la base de datos SQL se aloja en una SAN separada con conexiones tanto al almacén como a los sistemas de producción. Nuestro negocio depende de nuestro acceso a Amazon; por lo tanto, ninguna prueba debe invadir los clústeres de centros de datos que contienen los datos y el inventario de la tienda de Amazon. Estos se identifican en el diagrama.*

*CEO: Queremos que pruebe los controles de seguridad para garantizar que un atacante que obtenga correctamente el acceso a una cuenta de usuario final y una computadora*

dentro del depósito no pueda obtener acceso de administrador a ninguno de los servidores o tener acceso al inventario de producción base de datos. También queremos asegurarnos de que el software y los sistemas operativos estén actualizados y que no haya vulnerabilidades conocidas en nuestras aplicaciones.

*Director de TI:* le brindaremos acceso interno a través de una VLAN aislada dentro del departamento de TI desde la que podrá realizar las pruebas. Hay un cortafuego con IDS integrado que separa las redes del centro de datos de la LAN corporativa, incluido el departamento de TI. Dentro del centro de datos, cada servidor tiene un cortafuego local habilitado. El DNS interno se proporciona a través de los servicios de Microsoft Active Directory y el DNS externo es un servidor Linux ubicado en una DMZ separada. El acceso externo a los clústeres de operaciones y logística se limita a los empleados que se conectan a través de VPN. No se permite el acceso HTTP a estos clústeres. Los servidores de estos dos clústeres no tienen acceso a Internet, excepto para obtener actualizaciones de software automáticas.

*CEO:* Debido a que los sistemas que queremos que pruebe son sistemas de producción, esperamos limitar al mínimo las interrupciones causadas por las pruebas. Le daremos acceso a un sistema de desarrollo Microsoft SQL Server que está configurado de manera idéntica al sistema de producción con un espejo de la base de datos.

*Director de TI:* Sí, quiero reforzar la necesidad de mantener las interrupciones al mínimo. Le daremos un intervalo de tiempo durante nuestro período de mantenimiento programado normal para realizar pruebas de carga y simulaciones de ataques de denegación de servicio. Nuestro período de mantenimiento programado es entre las 2:00 a. M. Y las 6:00 a. M. Los viernes, sábados y domingos. Se pueden ejecutar otras pruebas no disruptivas durante el horario comercial normal.

*CEO:* Estamos limitando la cantidad de personal de TI que está al tanto de las pruebas. Solo se notificará al personal de TI directamente responsable del monitoreo de las operaciones y los sistemas de logística cuando se realizarán las pruebas. Proporcionaremos una lista de direcciones de correo electrónico del personal de operaciones y depósitos, ya que nos preocupa que la mayoría de los ransomware y las infracciones de datos comiencen con un ataque de ingeniería social exitoso. Los usuarios finales no se darán cuenta de que se están realizando las pruebas. Esperamos que el compromiso comience dos semanas después de la firma del contrato y el acuerdo de confidencialidad. Esperamos el informe final en un plazo de 60 días.

Sus contactos principales para esta interacción son el director de TI, el gerente de depósito y el gerente de operaciones. Programe un informe de actualización semanal y una teleconferencia para informarles sobre el progreso de las pruebas y los resultados intermedios.

# Pruebas de Penetración

Cliente: Nexus Plaza

Fecha de inicio propuesta: [Inserte fecha]

Duración del compromiso: 60 días

## 1. Introducción

A partir de la información proporcionada por Nexus Plaza, identificamos los siguientes puntos clave que influyen en el **alcance del proyecto** y las **reglas de enfrentamiento (RoE)** para las pruebas de penetración:

### 1. Factores que Influyen en el Alcance del Proyecto

#### 1.1. Sistemas y Redes Críticas

- **Incluidos:**
  - **Clústeres de operaciones y logística:** Sistemas de almacenamiento, envío y control de inventario (base de datos SQL Server).
  - **VLAN del departamento de TI:** Punto de acceso interno para las pruebas.
  - **Redes del centro de datos:** Separadas por un cortafuegos con IDS integrado.
  - **DNS interno (Active Directory) y DNS externo (servidor Linux en DMZ).**
  - **Sistemas de desarrollo:** Espejo de la base de datos SQL Server para pruebas no disruptivas.
- **Excluidos:**
  - **Clúster de soporte de Amazon:** Prohibido probar sistemas relacionados con la tienda de Amazon.
  - **Sistemas de producción SQL Server:** Solo se probará el entorno de desarrollo configurado de manera idéntica.
  - **Acceso HTTP externo a clústeres críticos:** No permitido según las políticas del cliente.

#### 1.2. Objetivos del Cliente

- **Prioridades:**
  - Evaluar la posibilidad de que un atacante con acceso a una cuenta de usuario final en el depósito escale privilegios a administrador.
  - Identificar vulnerabilidades en el software, sistemas operativos y aplicaciones.
  - Probar la resistencia contra ataques de ingeniería social (phishing a empleados del almacén y operaciones).
- **Preocupaciones clave:**

- Evitar interrupciones en los sistemas de producción.
- Proteger la integridad del inventario y los datos de pedidos en tiempo real.

### 1.3. Restricciones Operativas

- **Horarios de prueba:**
  - **Pruebas disruptivas** (ej: DoS, pruebas de carga): Solo durante el período de mantenimiento (2:00 a. m. – 6:00 a. m., viernes a domingo).
  - **Pruebas no disruptivas:** Durante horario laboral normal.
- **Acceso limitado:**
  - Solo personal de TI específico estará al tanto de las pruebas.
  - Los empleados finales no deben ser notificados para simular condiciones realistas.

### 1.4. Entorno Técnico

- **Infraestructura:**
    - 25 servidores en clústeres (administración, operaciones, logística, soporte de Amazon).
    - Acceso remoto mediante SSL/IPsec VPN.
    - Dos ISPs: Uno dedicado a comunicaciones con Amazon.
  - **Seguridad existente:**
    - Cortafuegos locales en servidores del centro de datos.
    - Sistemas de operaciones y logística sin acceso a Internet (excepto actualizaciones automáticas).
- 

## 2. Reglas de Enfrentamiento (RoE)

### 2.1. Autorización y Límites Legales

- **Autorización escrita:** Requerida antes de iniciar cualquier prueba.
- **Contrato de confidencialidad (NDA):** Protección de datos sensibles y resultados de las pruebas.
- **Cumplimiento normativo:** Respetar GDPR (protección de datos de clientes) y políticas internas de Nexus Plaza.

### 2.2. Métodos Permitidos

- **Pruebas de vulnerabilidades:**
  - Escaneo de puertos y servicios.
  - Explotación controlada de vulnerabilidades (ej: SQLi, XSS).
  - Simulación de escalada de privilegios desde una cuenta de usuario.
- **Ingeniería social:**
  - Pruebas de phishing dirigido a empleados del almacén y operaciones (usando la lista de correos proporcionada).

- **Pruebas de configuración:**
  - Verificación de parches y actualizaciones en sistemas operativos y software.

## 2.3. Métodos Prohibidos

- **Ataques disruptivos:**
  - Denegación de servicio (DoS/DDoS) fuera de las ventanas de mantenimiento.
  - Manipulación o eliminación de datos en sistemas de producción.
- **Áreas excluidas:**
  - Clústeres de soporte de Amazon.
  - Sistemas de producción SQL Server (solo se prueba el entorno espejo).
  - Redes externas de pedidos en tiempo real con Amazon.

## 2.4. Comunicación y Reportes

- **Contactos principales:**
  - Director de TI, Gerente de Almacén y Gerente de Operaciones.
- **Frecuencia de actualizaciones:**
  - Informes semanales y teleconferencias para revisar el progreso.
- **Gestión de incidentes:**
  - Cualquier impacto no planificado en sistemas de producción debe reportarse inmediatamente.

## 2.5. Seguridad y Ética

- **Privacidad:**
  - No se revelará información sensible fuera del equipo autorizado.
  - Los datos recopilados se eliminarán tras la entrega del informe final.
- **Simulación realista:**
  - Los empleados no serán informados de las pruebas de ingeniería social para mantener la autenticidad.

---

## 3. Consideraciones Adicionales

- **Plazos:**
    - **Inicio:** 2 semanas después de la firma del contrato.
    - **Duración:** 60 días desde el inicio.
    - **Entrega del informe final:** Al finalizar el plazo acordado.
  - **Recursos proporcionados por el cliente:**
    - Acceso a la VLAN aislada del departamento de TI.
    - Lista de direcciones de correo para pruebas de phishing.
    - Entorno de desarrollo SQL Server espejado.
-

## 4. Riesgos y Mitigación

- **Riesgo de interrupción en producción:**
  - Mitigación: Usar el entorno de desarrollo para pruebas críticas y limitar pruebas disruptivas a ventanas de mantenimiento.
- **Falsos positivos en IDS/IPS:**
  - Mitigación: Coordinar con el equipo de TI para filtrar alertas relacionadas con las pruebas.
- **Exposición accidental de datos:**
  - Mitigación: Cifrar todos los informes y comunicaciones.

A partir de la información proporcionada por Nexus Plaza, las **mayores preocupaciones de seguridad** del cliente son las siguientes:

---

### 1. Interrupción de Operaciones Críticas (Ransomware/DoS)

- **Contexto:**

El CEO mencionó que un competidor sufrió un ataque de ransomware que paralizó su sistema de inventario, causando pérdidas significativas.
  - **Preocupación específica:**

Que un ataque similar afecte los sistemas de almacenamiento, envío o control de inventario de Nexus Plaza, interrumpiendo la capacidad de procesar pedidos y cumplir con entregas rápidas.
  - **Impacto:**

Pérdida de ingresos, daño a la reputación y posibles multas por incumplimiento de contratos con clientes.
- 

### 2. Escalada de Privilegios en Sistemas Internos

- **Contexto:**

El cliente quiere asegurarse de que un atacante con acceso a una cuenta de usuario estándar (ej: empleado del almacén) no pueda obtener privilegios de administrador.
  - **Preocupación específica:**

Vulnerabilidades en la configuración de seguridad, permisos excesivos o fallos en la segmentación de redes que permitan movimientos laterales dentro de los clústeres de operaciones y logística.
  - **Impacto:**

Acceso no autorizado a la base de datos de inventario, manipulación de pedidos o sabotaje interno.
-

### 3. Vulnerabilidades en Software y Sistemas Operativos

- **Contexto:**  
El director de TI enfatizó la necesidad de verificar que no existan vulnerabilidades conocidas en aplicaciones, sistemas operativos o la base de datos SQL Server.
    - **Preocupación específica:**  
Parches no aplicados, configuraciones inseguras o servicios expuestos (ej: servicios sin actualizar en los servidores del centro de datos).
    - **Impacto:**  
Explotación de vulnerabilidades para robo de datos o toma de control de sistemas.
- 

### 4. Ataques de Ingeniería Social

- **Contexto:**  
El CEO mencionó que la mayoría de los ransomware comienzan con ataques de ingeniería social.
    - **Preocupación específica:**  
Empleados del almacén u operaciones que caigan en phishing, descarguen archivos maliciosos o revelen credenciales.
    - **Impacto:**  
Inicio de una cadena de compromisos que derive en una brecha mayor.
- 

### 5. Exposición de Datos Sensibles

- **Contexto:**  
La base de datos SQL Server contiene información crítica de inventario y pedidos, alojada en una SAN con conexiones al almacén y producción.
    - **Preocupación específica:**  
Acceso no autorizado a la base de datos (ej: inyecciones SQL) o filtración de datos debido a configuraciones inseguras.
    - **Impacto:**  
Pérdida de información confidencial, incumplimiento del GDPR y daño a la confianza de los clientes.
- 

### 6. Interrupciones en Sistemas de Producción

- **Contexto:**  
El cliente insistió en minimizar las interrupciones durante las pruebas, especialmente en los sistemas de producción.

- **Preocupación específica:**  
Que pruebas invasivas (ej: escaneos agresivos o explotación de vulnerabilidades) afecten la disponibilidad de los sistemas críticos.
  - **Impacto:**  
Parálisis operativa, retrasos en envíos y costos financieros directos.
- 

## 7. Dependencia de Sistemas Externos (Amazon)

- **Contexto:**  
La comunicación con Amazon es vital para el procesamiento de pedidos en tiempo real.
    - **Preocupación específica:**  
Ataques que afecten la conectividad con Amazon (ej: compromiso de la VPN o del ISP dedicado).
    - **Impacto:**  
Interrupción del flujo de pedidos, inventario y atención al cliente.
- 

## 8. Configuraciones Inseguras en Redes Internas

- **Contexto:**  
El director de TI mencionó que los servidores no tienen acceso a Internet (excepto para actualizaciones) y están protegidos por cortafuegos locales.
    - **Preocupación específica:**  
Configuraciones erróneas en el cortafuegos, VLANs mal segmentadas o reglas de IDS/IPS ineficaces.
    - **Impacto:**  
Exposición de sistemas críticos a amenazas internas o externas.
- 

## 9. Reputación y Confianza del Cliente

- **Contexto:**  
Nexus Plaza depende de su imagen como empresa confiable para entregas rápidas.
    - **Preocupación específica:**  
Que una brecha de seguridad se haga pública o cause retrasos visibles para los clientes.
    - **Impacto:**  
Pérdida de participación en el mercado y reputación dañada.
- 

## 10. Cumplimiento Legal y Normativo



- **Contexto:**  
El cliente opera con datos de clientes y transacciones que deben cumplir con regulaciones como el GDPR.
  - **Preocupación específica:**  
Sanciones legales o multas debido a fallos de seguridad que expongan datos personales.

---

## Resumen de Prioridades del Cliente

Preocupación	Ejemplo del Escenario
Interrupción operativa	Ataque de ransomware en sistemas de envío.
Escalada de privilegios	Usuario del almacén accediendo a la base de datos.
Ingeniería social	Phishing a empleados de logística.
Exposición de datos	Filtración de la base de datos SQL.

A partir de la información proporcionada por Nexus Plaza, los **clústeres de servidores, rangos de direcciones de red y aplicaciones específicas** que deben probarse son los siguientes:

---

## 1. Clústeres de Servidores a Probar

### 1.1. Clúster de Operaciones

- **Función:** Respalda los sistemas de almacenamiento y envío.
- **Servicios clave:**
  - Base de datos SQL Server (espejo de desarrollo para pruebas).
  - Sistemas de control de inventario.
  - Aplicaciones de gestión de almacén.
- **Preocupación principal:** Vulnerabilidades que permitan la escalada de privilegios o acceso no autorizado.

### 1.2. Clúster de Logística

- **Función:** Gestiona el control de inventario y producción.
- **Servicios clave:**
  - Base de datos SQL Server (espejo de desarrollo para pruebas).
  - Sistemas de seguimiento de pedidos.
  - Aplicaciones de planificación de envíos.

- **Preocupación principal:** Exposición de datos sensibles o interrupción del flujo de operaciones.

### 1.3. Clúster de Administración

- **Función:** Gestiona la infraestructura interna de TI.
  - **Servicios clave:**
    - Active Directory (gestión de usuarios y permisos).
    - Servidores de correo electrónico.
    - Herramientas de monitoreo y gestión de red.
  - **Preocupación principal:** Configuraciones inseguras que permitan acceso no autorizado.
- 

## 2. Rangos de Direcciones de Red a Probar

### 2.1. Redes del Centro de Datos

- **Clúster de Operaciones:**
  - **Rango de IP:** 172.16.33.0/30 (Administración).
  - **Máscara de subred:** 255.255.255.192.
- **Clúster de Logística:**
  - **Rango de IP:** 172.26.0.0/21.
  - **Máscara de subred:** 255.255.255.0.
- **Clúster de Administración:**
  - **Rango de IP:** 172.24.1.0/24.
  - **Máscara de subred:** 255.255.255.192.

### 2.2. VLANs de la LAN Corporativa

- **VLAN 120 (Administración):**
  - **Rango de IP:** 172.16.1.0.
  - **Máscara de subred:** 255.255.255.0.
- **VLAN 130 (Subred de Tecnología de la Información):**
  - **Rango de IP:** 172.16.4.0.
  - **Máscara de subred:** 255.255.255.0.
- **VLAN 140 (Tecnología de la Información):**
  - **Rango de IP:** 172.16.8.0.
  - **Máscara de subred:** 255.255.255.0.
- **VLAN 150 (Depósito):**
  - **Rango de IP:** 172.16.12.0.
  - **Máscara de subred:** 255.255.255.0.
- **VLAN 160 (Atención al Cliente):**
  - **Rango de IP:** 172.16.16.0.
  - **Máscara de subred:** 255.255.255.0.
- **VLAN 170 (Envío):**
  - **Rango de IP:** 172.16.20.0.

- **Máscara de subred:** 255.255.255.0.

### 2.3. Redes Excluidas

- **Clúster de Soporte de Amazon:**
    - **Rango de IP:** 172.25.0.0/16.
    - **Máscara de subred:** 255.255.252.0.
    - **Motivo:** Prohibido probar sistemas relacionados con la tienda de Amazon.
- 

## 3. Aplicaciones Específicas a Probar

### 3.1. Base de Datos SQL Server

- **Entorno de pruebas:** Espejo de desarrollo proporcionado por el cliente.
- **Objetivo:** Identificar vulnerabilidades como inyecciones SQL, configuraciones inseguras o permisos excesivos.

### 3.2. Active Directory

- **Función:** Gestión de usuarios y permisos.
- **Objetivo:** Verificar que no existan cuentas con privilegios excesivos o configuraciones inseguras.

### 3.3. Aplicaciones de Gestión de Almacén

- **Función:** Control de inventario y seguimiento de pedidos.
- **Objetivo:** Evaluar la seguridad de las interfaces y la integridad de los datos.

### 3.4. VPN (SSL/IPsec)

- **Función:** Acceso remoto a los sistemas internos.
- **Objetivo:** Probar la resistencia contra ataques de fuerza bruta o explotación de vulnerabilidades.

### 3.5. Servidores DNS

- **DNS Interno:** Microsoft Active Directory.
  - **DNS Externo:** Servidor Linux en DMZ.
  - **Objetivo:** Verificar que no existan configuraciones inseguras o vulnerabilidades conocidas.
- 

## 4. Resumen de Áreas de Prueba

Área	Detalles
Clúster de Operaciones	Sistemas de almacenamiento y envío.
Clúster de Logística	Control de inventario y producción.
Clúster de Administración	Active Directory y servidores de gestión.
Base de Datos SQL	Espejo de desarrollo para pruebas no disruptivas.
VLANs Corporativas	VLANs 120-170 (Administración, TI, Depósito, etc.).
Aplicaciones	SQL Server, Active Directory, VPN, DNS.

---

De acuerdo con la información proporcionada por Nexus Plaza, hay ciertos **clústeres de servidores, rangos de direcciones de red y aplicaciones específicas** que **no deben probarse explícitamente**. Estas exclusiones se basan en las preocupaciones del cliente, la criticidad de los sistemas y las restricciones operativas. A continuación, se detallan las áreas excluidas:

---

## 1. Clústeres de Servidores Excluidos

### 1.1. Clúster de Soporte de Amazon

- **Función:** Respalda las comunicaciones con Amazon para pedidos en tiempo real, inventario y atención al cliente.
- **Razón de exclusión:**
  - El cliente ha indicado explícitamente que no se deben probar los sistemas relacionados con la tienda de Amazon.
  - Estos sistemas son críticos para el negocio y cualquier interrupción podría afectar gravemente las operaciones.

---

## 2. Rangos de Direcciones de Red Excluidos

### 2.1. Redes del Clúster de Soporte de Amazon

- **Rango de IP:** 172.25.0.0/16.
- **Máscara de subred:** 255.255.252.0.
- **Razón de exclusión:**

- Estas redes están dedicadas a la comunicación con Amazon y no deben ser perturbadas.

## 2.2. Redes de Producción SQL Server

- **Rango de IP:** No especificado (pero se excluyen los sistemas de producción).
  - **Razón de exclusión:**
    - El cliente ha proporcionado un entorno de desarrollo espejado para pruebas, por lo que los sistemas de producción no deben ser probados directamente.
- 

## 3. Aplicaciones Específicas Excluidas

### 3.1. Sistemas de Producción SQL Server

- **Función:** Base de datos de inventario y pedidos en tiempo real.
- **Razón de exclusión:**
  - El cliente ha proporcionado un entorno de desarrollo espejado para pruebas no disruptivas.
  - Los sistemas de producción son críticos y no deben ser perturbados.

### 3.2. Servicios de Comunicación con Amazon

- **Función:** Procesamiento de pedidos en tiempo real y gestión de inventario con Amazon.
- **Razón de exclusión:**
  - Estos servicios son vitales para el negocio y cualquier interrupción podría causar pérdidas significativas.

### 3.3. Sistemas de Producción de Envíos

- **Función:** Gestión de envíos y logística en tiempo real.
  - **Razón de exclusión:**
    - Pruebas en estos sistemas podrían interrumpir las operaciones diarias y afectar la entrega de pedidos.
- 

## 4. Resumen de Áreas Excluidas

Área	Detalles	Razón de Exclusión
Clúster de Soporte de Amazon	Sistemas de comunicación con Amazon.	Críticos para el negocio; prohibido por el cliente.

<b>Redes de Soporte de Amazon</b>	Rango de IP: 172.25.0.0/16.	Dedicadas a Amazon; no deben ser perturbadas.
<b>Sistemas de Producción SQL</b>	Base de datos de inventario y pedidos.	Se prueba el entorno espejado; producción es crítica.
<b>Servicios de Comunicación</b>	Pedidos en tiempo real con Amazon.	Vitales para el negocio; no deben interrumpirse.
<b>Sistemas de Envíos</b>	Gestión de envíos y logística en tiempo real.	Pruebas podrían afectar operaciones diarias.

---

## 5. Consideraciones Adicionales

- **Entorno de Desarrollo:**  
El cliente ha proporcionado un entorno espejado (desarrollo) para pruebas no disruptivas. Este entorno debe usarse en lugar de los sistemas de producción.
  - **Comunicación con Amazon:**  
Aunque no se probarán directamente, se debe verificar que las configuraciones de red (ej: VPN, cortafuegos) que protegen estas comunicaciones estén seguras.
  - **Minimización de Riesgos:**  
Las pruebas deben diseñarse para evitar cualquier impacto indirecto en los sistemas excluidos.
- 

De acuerdo con la información proporcionada por Nexus Plaza, las **pruebas de penetración se realizarán principalmente en un entorno de prueba**, no en el entorno de producción en vivo. Esto se debe a las preocupaciones del cliente sobre la interrupción de operaciones críticas y la necesidad de mantener la disponibilidad de los sistemas de producción. A continuación, se detalla cómo se manejará este aspecto:

---

## 1. Entorno de Prueba

### 1.1. Base de Datos SQL Server (Espejo de Desarrollo)

- **Descripción:**  
El cliente ha proporcionado un entorno de desarrollo espejado que replica la base de datos SQL Server utilizada en producción.
- **Uso:**
  - Pruebas de vulnerabilidades (ej: inyecciones SQL, configuraciones inseguras).

- Simulación de ataques sin riesgo de afectar los datos reales.
- **Ventajas:**
  - Permite pruebas exhaustivas sin interrumpir las operaciones de producción.
  - Reduce el riesgo de pérdida o corrupción de datos.

## 1.2. VLAN Aislada del Departamento de TI

- **Descripción:**

Una red aislada dentro del departamento de TI que simula el entorno de red del centro de datos.
  - **Uso:**
    - Pruebas de escaneo de puertos y servicios.
    - Simulación de ataques internos (ej: escalada de privilegios).
  - **Ventajas:**
    - Proporciona un entorno controlado para pruebas no disruptivas.
    - Permite evaluar la seguridad de la red sin afectar sistemas críticos.
- 

## 2. Limitaciones en el Entorno de Producción

### 2.1. Pruebas No Invasivas

- **Descripción:**

Algunas pruebas no disruptivas (ej: revisión de configuraciones, verificación de parches) pueden realizarse en el entorno de producción.
- **Condiciones:**
  - Solo durante horario laboral normal.
  - Con supervisión del equipo de TI del cliente.

### 2.2. Pruebas Disruptivas (Solo en Ventanas de Mantenimiento)

- **Descripción:**

Pruebas que podrían afectar la disponibilidad de los sistemas (ej: pruebas de carga, simulaciones de DoS) se realizarán únicamente durante las ventanas de mantenimiento programadas.
  - **Horarios:**
    - Viernes, sábados y domingos, entre las 2:00 a. m. y las 6:00 a. m.
  - **Condiciones:**
    - Coordinación previa con el equipo de TI del cliente.
    - Monitoreo constante para minimizar impactos.
- 

## 3. Resumen de Entornos de Prueba

Entorno	Tipo de Pruebas	Condiciones
Entorno de Prueba	Pruebas de vulnerabilidades, simulaciones de ataques.	Uso exclusivo del entorno espejado y VLAN aislada.
Entorno de Producción	Pruebas no disruptivas (ej: revisión de configuraciones).	Solo durante horario laboral y con supervisión.
Ventanas de Mantenimiento	Pruebas disruptivas (ej: DoS, pruebas de carga).	Viernes a domingo, 2:00 a. m. – 6:00 a. m.

## 4. Consideraciones Adicionales

- **Minimización de Riesgos:**  
Las pruebas en el entorno de producción se limitarán al mínimo necesario para evitar interrupciones.
- **Comunicación con el Cliente:**  
Cualquier prueba en el entorno de producción se coordinará previamente con el equipo de TI del cliente.
- **Enfoque en el Entorno de Prueba:**  
La mayoría de las pruebas se realizarán en el entorno espejado y la VLAN aislada para garantizar la seguridad y disponibilidad de los sistemas de producción.

Sí, las **pruebas de penetración incluirán pruebas de red internas**, ya que el cliente ha expresado preocupaciones específicas sobre la seguridad de sus sistemas internos, como la posibilidad de que un atacante con acceso a una cuenta de usuario estándar pueda escalar privilegios o moverse lateralmente dentro de la red. A continuación, se detalla cómo se obtendrá el acceso y cómo se realizarán estas pruebas:

## 1. Acceso a la Red Interna

### 1.1. VLAN Aislada del Departamento de TI

- **Descripción:**  
El cliente proporcionará acceso a una VLAN aislada dentro del departamento de TI, que simula el entorno de red del centro de datos.
- **Uso:**
  - Pruebas de escaneo de puertos y servicios.



- Simulación de ataques internos (ej: escalada de privilegios, movimientos laterales).
- **Acceso:**
  - Se otorgará acceso remoto a través de una conexión VPN (SSL/IPsec) configurada específicamente para este propósito.
  - El acceso estará limitado a esta VLAN y no permitirá la conexión directa a otros sistemas críticos.

## 1.2. Credenciales de Usuario Estándar

- **Descripción:**

El cliente proporcionará credenciales de usuario estándar (similares a las de un empleado del almacén o logística) para simular un escenario realista de ataque interno.
  - **Uso:**
    - Pruebas de escalada de privilegios desde una cuenta de usuario estándar.
    - Evaluación de la efectividad de los controles de seguridad internos.
  - **Acceso:**
    - Las credenciales se proporcionarán de manera segura (ej: mediante un gestor de contraseñas o cifrado PGP).
- 

## 2. Pruebas de Red Interna

### 2.1. Escaneo de Puertos y Servicios

- **Objetivo:**

Identificar servicios expuestos, puertos abiertos y posibles puntos de entrada.
- **Herramientas:**
  - Nmap, Nessus, OpenVAS.
- **Alcance:**
  - VLAN aislada del departamento de TI.
  - Clústeres de operaciones y logística (acceso limitado).

### 2.2. Movimientos Laterales

- **Objetivo:**

Simular cómo un atacante podría moverse lateralmente dentro de la red después de comprometer una cuenta de usuario estándar.
- **Herramientas:**
  - Mimikatz, BloodHound, CrackMapExec.
- **Alcance:**
  - Evaluación de la segmentación de red y controles de acceso.

### 2.3. Escalada de Privilegios

- **Objetivo:**  
Verificar si un usuario estándar puede obtener privilegios de administrador.
- **Herramientas:**
  - Metasploit, PowerShell Empire.
- **Alcance:**
  - Sistemas dentro de la VLAN aislada y clústeres de operaciones/logística.

## 2.4. Pruebas de Configuración de Red

- **Objetivo:**  
Evaluar la seguridad de las configuraciones de red (ej: cortafuegos, VLANs, IDS/IPS).
  - **Herramientas:**
    - Wireshark, Nessus, manual review.
  - **Alcance:**
    - VLAN aislada y redes del centro de datos.
- 

## 3. Consideraciones de Seguridad

### 3.1. Supervisión del Cliente

- **Descripción:**  
El equipo de TI del cliente supervisará las pruebas en tiempo real para detectar y mitigar cualquier impacto no deseado.
- **Coordinación:**
  - Reuniones diarias o semanales para revisar el progreso y los resultados preliminares.

### 3.2. Minimización de Impactos

- **Descripción:**  
Las pruebas se diseñarán para minimizar el riesgo de interrupciones en los sistemas de producción.
- **Medidas:**
  - Uso de herramientas en modo "solo lectura" cuando sea posible.
  - Limitación de pruebas disruptivas a ventanas de mantenimiento.

### 3.3. Confidencialidad

- **Descripción:**  
Toda la información recopilada durante las pruebas se manejará de manera confidencial.
  - **Medidas:**
    - Cifrado de datos y comunicaciones.
    - Destrucción segura de datos después de la entrega del informe final.
-

## 4. Resumen de Acceso y Pruebas Internas

Acceso	Detalles	Pruebas Relacionadas
VLAN Aislada de TI	Acceso remoto mediante VPN (SSL/IPsec).	Escaneo de puertos, movimientos laterales.
Credenciales de Usuario	Cuenta estándar (simulación de empleado).	Escalada de privilegios, pruebas de configuración.
Supervisión del Cliente	Monitoreo en tiempo real por el equipo de TI.	Coordinación para minimizar impactos.

De acuerdo con la información proporcionada por Nexus Plaza, los **sistemas de cliente/usuario final no están incluidos explícitamente en el alcance de las pruebas de penetración**. Sin embargo, el cliente ha expresado preocupaciones sobre la posibilidad de que un atacante comprometa una cuenta de usuario final (por ejemplo, un empleado del almacén) y utilice ese acceso para moverse lateralmente dentro de la red o escalar privilegios. A continuación, se detalla cómo se abordará este aspecto:

### 1. Enfoque en Usuarios Internos (No Clientes Externos)

- **Contexto:**  
El cliente mencionó que la mayoría de los ransomware y brechas de seguridad comienzan con ataques de ingeniería social dirigidos a empleados internos.
- **Alcance:**
  - **Usuarios finales internos:** Empleados del almacén, logística y operaciones.
  - **Exclusión:** Clientes externos (usuarios de la tienda en línea de Amazon).

## 2. Pruebas de Ingeniería Social

### 2.1. Phishing Dirigido

- **Objetivo:**  
Simular ataques de phishing dirigidos a empleados internos para evaluar su susceptibilidad.
- **Métodos:**
  - Envío de correos electrónicos falsos que imiten comunicaciones legítimas (ej: notificaciones de TI, actualizaciones de sistemas).

- Inclusión de enlaces maliciosos o archivos adjuntos.
- **Credenciales proporcionadas:**
  - El cliente proporcionará una lista de direcciones de correo electrónico de empleados del almacén y operaciones.
- **Limitaciones:**
  - No se incluirán clientes externos ni usuarios de la tienda en línea de Amazon.

## 2.2. Simulación de Ataques de Credenciales

- **Objetivo:**

Evaluar si los empleados revelan credenciales o información sensible.
  - **Métodos:**
    - Páginas de inicio de sesión falsas (simulando el portal de TI o sistemas internos).
    - Llamadas telefónicas simuladas (vishing) para obtener información.
- 

## 3. Escalada de Privilegios desde Cuentas de Usuario Final

### 3.1. Simulación de Acceso Inicial

- **Objetivo:**

Evaluar cómo un atacante podría aprovechar una cuenta de usuario final comprometida.
- **Métodos:**
  - Uso de credenciales proporcionadas por el cliente (simulando una cuenta de empleado del almacén).
  - Pruebas de movimientos laterales y escalada de privilegios dentro de la red.

### 3.2. Evaluación de Controles de Seguridad

- **Objetivo:**

Verificar que los controles de seguridad impidan la escalada de privilegios o el acceso no autorizado.
  - **Métodos:**
    - Uso de herramientas como Mimikatz, BloodHound o Metasploit para simular ataques.
- 

## 4. Consideraciones Éticas y Legales

### 4.1. Autorización del Cliente

- **Descripción:**

Todas las pruebas de ingeniería social y uso de credenciales de usuario final se realizarán con autorización explícita del cliente.

- **Documentación:**
  - Contrato de compromiso y acuerdo de confidencialidad (NDA).

#### 4.2. Minimización de Impactos

- **Descripción:**

Las pruebas se diseñarán para evitar daños o molestias a los empleados.
- **Medidas:**
  - Notificación posterior a los empleados afectados (si es necesario).
  - Capacitación en concienciación de seguridad después de las pruebas.

#### 4.3. Confidencialidad

- **Descripción:**

Los resultados de las pruebas se manejarán de manera confidencial.
- **Medidas:**
  - Cifrado de datos y comunicaciones.
  - Destrucción segura de información sensible después de la entrega del informe final.

---

### 5. Resumen de Pruebas en Usuarios Finales

Prueba	Objetivo	Métodos
Phishing Dirigido	Evaluar susceptibilidad a ataques de phishing.	Correos electrónicos falsos, enlaces maliciosos.
Simulación de Credenciales	Verificar si los empleados revelan información.	Páginas de inicio de sesión falsas, phishing.
Escalada de Privilegios	Evaluar controles de seguridad internos.	Uso de herramientas como Mimikatz, BloodHound.

---

### 6. Exclusión de Clientes Externos

- **Razón:**

El alcance se centra en los sistemas internos y empleados, no en los usuarios de la tienda en línea de Amazon.
- **Impacto:**

Las pruebas no afectarán a los clientes externos ni a la experiencia del usuario en la plataforma de comercio electrónico.

---

Sí, la **ingeniería social está permitida** en el alcance de las pruebas de penetración para Nexus Plaza, pero con **limitaciones específicas** definidas por el cliente. Estas limitaciones están diseñadas para garantizar que las pruebas sean éticas, seguras y no causen daños o molestias innecesarias a los empleados. A continuación, se detalla cómo se abordará la ingeniería social:

---

## 1. Alcance de la Ingeniería Social

### 1.1. Pruebas de Phishing Dirigido

- **Objetivo:**  
Evaluar la susceptibilidad de los empleados a ataques de phishing.
- **Métodos:**
  - Envío de correos electrónicos falsos que imiten comunicaciones legítimas (ej: notificaciones de TI, actualizaciones de sistemas).
  - Inclusión de enlaces maliciosos o archivos adjuntos.
- **Limitaciones:**
  - Solo se dirigirá a empleados específicos (almacén, logística y operaciones).
  - No se incluirán clientes externos ni usuarios de la tienda en línea de Amazon.

### 1.2. Simulación de Ataques de Credenciales

- **Objetivo:**  
Verificar si los empleados revelan credenciales o información sensible.
- **Métodos:**
  - Páginas de inicio de sesión falsas (simulando el portal de TI o sistemas internos).
  - Llamadas telefónicas simuladas (vishing) para obtener información.
- **Limitaciones:**
  - Solo se utilizarán sistemas de prueba proporcionados por el cliente.
  - No se almacenarán ni utilizarán credenciales reales de empleados.

### 1.3. Pruebas de Concienciación

- **Objetivo:**  
Evaluar el nivel de concienciación de los empleados sobre seguridad.
  - **Métodos:**
    - Simulación de intentos de acceso físico a áreas restringidas (si es aprobado por el cliente).
    - Entrega de dispositivos USB maliciosos (simulados) en áreas comunes.
  - **Limitaciones:**
    - Solo en áreas no críticas y con supervisión del cliente.
-

## 2. Limitaciones y Condiciones

### 2.1. Autorización Explícita

- **Descripción:**  
Todas las pruebas de ingeniería social se realizarán con autorización por escrito del cliente.
- **Documentación:**
  - Contrato de compromiso y acuerdo de confidencialidad (NDA).

### 2.2. Empleados Objetivo

- **Descripción:**  
Las pruebas se limitarán a empleados específicos (almacén, logística y operaciones).
- **Exclusión:**
  - No se incluirán clientes externos ni usuarios de la tienda en línea de Amazon.

### 2.3. Minimización de Impactos

- **Descripción:**  
Las pruebas se diseñarán para evitar daños o molestias innecesarias a los empleados.
- **Medidas:**
  - Notificación posterior a los empleados afectados (si es necesario).
  - Capacitación en concienciación de seguridad después de las pruebas.

### 2.4. Confidencialidad

- **Descripción:**  
Los resultados de las pruebas se manejarán de manera confidencial.
- **Medidas:**
  - Cifrado de datos y comunicaciones.
  - Destrucción segura de información sensible después de la entrega del informe final.

---

## 3. Resumen de Pruebas de Ingeniería Social

Prueba	Objetivo	Limitaciones
Phishing Dirigido	Evaluar susceptibilidad a ataques de phishing.	Solo empleados específicos; no clientes externos.
Simulación de Credenciales	Verificar si los empleados revelan información.	Uso de sistemas de prueba; no credenciales reales.

<b>Pruebas de Concienciación</b>	Evaluar concienciación sobre seguridad.	Solo en áreas no críticas y con supervisión.
----------------------------------	---	--

---

## 4. Consideraciones Éticas

- **Transparencia:**  
Los empleados serán informados después de las pruebas (si es necesario) para evitar desconfianza o malestar.
  - **Capacitación:**  
Se proporcionará capacitación en concienciación de seguridad a los empleados afectados para mejorar su resistencia futura.
  - **Protección de Datos:**  
Toda la información recopilada se manejará de acuerdo con las normativas de protección de datos (ej: GDPR).
- 

Sí, las **pruebas de denegación de servicio (DoS)** y otros **ataques disruptivos están permitidos**, pero con **limitaciones estrictas** definidas por el cliente. Estas limitaciones están diseñadas para minimizar el impacto en las operaciones críticas y garantizar que las pruebas no afecten negativamente a los sistemas de producción. A continuación, se detalla cómo se abordarán estas pruebas:

---

## 1. Pruebas Disruptivas Permitidas

### 1.1. Denegación de Servicio (DoS/DDoS)

- **Objetivo:**  
Evaluar la resistencia de los sistemas ante ataques que buscan agotar recursos (ej: ancho de banda, capacidad de procesamiento).
- **Métodos:**
  - Simulación de tráfico malicioso utilizando herramientas como LOIC, Hping o Metasploit.
  - Pruebas de estrés en servidores y aplicaciones.

### 1.2. Pruebas de Carga

- **Objetivo:**  
Verificar cómo los sistemas manejan cargas extremas de tráfico o solicitudes.
- **Métodos:**
  - Uso de herramientas como JMeter, Gatling o Locust.
  - Simulación de picos de tráfico en aplicaciones web o APIs.



### 1.3. Simulación de Ataques de Ransomware

- **Objetivo:**  
Evaluar la capacidad de los sistemas para detectar y mitigar ataques de ransomware.
  - **Métodos:**
    - Uso de herramientas de simulación como Cobalt Strike o scripts personalizados.
    - Pruebas en el entorno de desarrollo espejado (no en producción).
- 

## 2. Limitaciones y Condiciones

### 2.1. Ventanas de Mantenimiento

- **Descripción:**  
Las pruebas disruptivas solo se realizarán durante las ventanas de mantenimiento programadas.
- **Horarios:**
  - Viernes, sábados y domingos, entre las 2:00 a. m. y las 6:00 a. m.
- **Razón:**  
Minimizar el impacto en las operaciones críticas durante el horario laboral.

### 2.2. Entornos de Prueba

- **Descripción:**  
Las pruebas disruptivas se realizarán principalmente en el entorno de desarrollo espejado proporcionado por el cliente.
- **Exclusión:**
  - No se realizarán pruebas disruptivas en los sistemas de producción a menos que sea absolutamente necesario y con autorización explícita.

### 2.3. Supervisión del Cliente

- **Descripción:**  
El equipo de TI del cliente supervisará las pruebas en tiempo real para detectar y mitigar cualquier impacto no deseado.
- **Coordinación:**
  - Reuniones previas para definir los parámetros de las pruebas.
  - Comunicación constante durante las pruebas.

### 2.4. Duración Limitada

- **Descripción:**  
Las pruebas disruptivas tendrán una duración limitada para evitar interrupciones prolongadas.
- **Ejemplo:**
  - Pruebas de DoS: Máximo 30 minutos por sesión.
  - Pruebas de carga: Máximo 1 hora por sesión.

---

### 3. Resumen de Pruebas Disruptivas

Prueba	Objetivo	Limitaciones
Denegación de Servicio (DoS)	Evaluar resistencia ante ataques de agotamiento.	Solo en ventanas de mantenimiento; duración limitada.
Pruebas de Carga	Verificar manejo de cargas extremas.	En entorno de desarrollo; supervisión del cliente.
Simulación de Ransomware	Evaluar detección y mitigación de ransomware.	Solo en entorno de desarrollo espejado.

---

### 4. Consideraciones Adicionales

- **Minimización de Riesgos:**  
Las pruebas se diseñarán para evitar impactos no deseados en los sistemas de producción.
  - **Comunicación con el Cliente:**  
Cualquier prueba disruptiva se coordinará previamente con el equipo de TI del cliente.
  - **Plan de Contingencia:**  
Se establecerá un plan de contingencia para restaurar rápidamente los sistemas en caso de incidentes.
- 

Sí, existen **dispositivos y configuraciones de red** que pueden afectar los resultados de una prueba de penetración, ya sea limitando la visibilidad de vulnerabilidades, bloqueando actividades legítimas de prueba o generando falsos positivos. A continuación, se detallan los dispositivos más comunes que podrían influir en los resultados y cómo se abordarán:

---

#### 1. Dispositivos que Afectan los Resultados

##### 1.1. Cortafuegos (Firewalls)

- **Impacto:**
  - Pueden bloquear el tráfico de escaneo o explotación, limitando la visibilidad de vulnerabilidades.
  - Reglas mal configuradas podrían generar falsos positivos o negativos.

- **Manejo:**
  - Coordinar con el equipo de TI del cliente para desactivar temporalmente reglas restrictivas durante las pruebas.
  - Verificar las configuraciones del cortafuegos para identificar reglas innecesarias o redundantes.

## 1.2. Sistemas de Detección/Prevención de Intrusos (IDS/IPS)

- **Impacto:**
  - Pueden detectar y bloquear actividades de prueba, como escaneos de puertos o intentos de explotación.
  - Generan alertas que podrían interrumpir las pruebas o causar falsos positivos.
- **Manejo:**
  - Desactivar temporalmente el IPS durante las pruebas (si es aprobado por el cliente).
  - Configurar el IDS para ignorar las direcciones IP utilizadas en las pruebas.

## 1.3. Balanceadores de Carga (Load Balancers)

- **Impacto:**
  - Pueden distribuir el tráfico de prueba entre múltiples servidores, dificultando la identificación de vulnerabilidades específicas.
  - Podrían ocultar servidores vulnerables detrás de configuraciones seguras.
- **Manejo:**
  - Coordinar con el equipo de TI para desactivar temporalmente el balanceo de carga durante las pruebas.
  - Realizar pruebas directamente en los servidores individuales.

## 1.4. Proxies y Gateways de Seguridad

- **Impacto:**
  - Pueden filtrar o modificar el tráfico de prueba, limitando la efectividad de las pruebas.
  - Podrían bloquear herramientas de escaneo o explotación.
- **Manejo:**
  - Configurar las herramientas de prueba para evitar el uso del proxy.
  - Realizar pruebas desde dentro de la red (si es posible).

## 1.5. Sistemas de Prevención de Pérdida de Datos (DLP)

- **Impacto:**
  - Pueden bloquear la transferencia de datos sensibles durante las pruebas, limitando la evaluación de vulnerabilidades.
- **Manejo:**
  - Desactivar temporalmente las reglas de DLP durante las pruebas (si es aprobado por el cliente).

## 1.6. Redes Privadas Virtuales (VPN)

- **Impacto:**
  - Pueden limitar el acceso a ciertas áreas de la red, afectando la cobertura de las pruebas.
- **Manejo:**
  - Utilizar credenciales de acceso proporcionadas por el cliente para acceder a redes restringidas.

## 1.7. Sistemas de Detección de Honeypots

- **Impacto:**
    - Pueden generar falsos positivos al simular sistemas vulnerables que no son parte de la infraestructura real.
  - **Manejo:**
    - Identificar y excluir honeypots del alcance de las pruebas.
- 

# 2. Configuraciones que Afectan los Resultados

## 2.1. Segmentación de Red (VLANs)

- **Impacto:**
  - La segmentación puede limitar el movimiento lateral dentro de la red, afectando la evaluación de la postura de seguridad.
- **Manejo:**
  - Verificar las configuraciones de VLAN y ajustar las pruebas para evaluar la efectividad de la segmentación.

## 2.2. Políticas de Control de Acceso (ACL)

- **Impacto:**
  - Las ACL pueden bloquear el tráfico de prueba, limitando la visibilidad de vulnerabilidades.
- **Manejo:**
  - Revisar y ajustar las ACL para permitir el tráfico de prueba (si es aprobado por el cliente).

## 2.3. Cifrado de Tráfico (SSL/TLS)

- **Impacto:**
  - El cifrado puede dificultar la inspección del tráfico y la identificación de vulnerabilidades.
- **Manejo:**
  - Utilizar herramientas que soporten la inspección de tráfico cifrado (ej: Burp Suite, Wireshark con claves SSL).

---

### 3. Resumen de Dispositivos y Configuraciones

Dispositivo/Configuración	Impacto en las Pruebas	Manejo
Cortafuegos	Bloqueo de tráfico de prueba.	Desactivar reglas restrictivas temporalmente.
IDS/IPS	Detección y bloqueo de actividades de prueba.	Desactivar IPS o configurar excepciones.
Balanceadores de Carga	Distribución de tráfico entre servidores.	Desactivar balanceo de carga temporalmente.
Proxies	Filtrado o modificación de tráfico.	Evitar el uso de proxies durante las pruebas.
DLP	Bloqueo de transferencia de datos sensibles.	Desactivar reglas de DLP temporalmente.
VPN	Limitación de acceso a redes restringidas.	Utilizar credenciales de acceso proporcionadas.
Honeypots	Generación de falsos positivos.	Identificar y excluir honeypots.
Segmentación de Red	Limitación del movimiento lateral.	Evaluar la efectividad de la segmentación.
ACL	Bloqueo de tráfico de prueba.	Ajustar ACL para permitir tráfico de prueba.
Cifrado SSL/TLS	Dificultad en la inspección de tráfico.	Usar herramientas con soporte para SSL/TLS.

---

### 4. Consideraciones Adicionales

- **Coordinación con el Cliente:**  
Cualquier ajuste en dispositivos o configuraciones se realizará en coordinación con el equipo de TI del cliente.
  - **Minimización de Impactos:**  
Las modificaciones temporales se revertirán una vez finalizadas las pruebas.
  - **Documentación:**  
Se registrarán todos los cambios realizados para garantizar la transparencia y trazabilidad.
- 

De acuerdo con la información proporcionada por Nexus Plaza, **el acceso inalámbrico no se menciona explícitamente como parte del alcance de las pruebas de penetración**. Sin embargo, si el cliente tiene redes inalámbricas (Wi-Fi) en sus instalaciones, es importante evaluar su seguridad, ya que pueden ser un punto de entrada común para atacantes. A continuación, se detalla cómo se podría abordar este aspecto:

---

## 1. Evaluación del Acceso Inalámbrico

### 1.1. Verificación de la Existencia de Redes Inalámbricas

- **Objetivo:**  
Identificar si Nexus Plaza utiliza redes Wi-Fi en sus instalaciones.
- **Métodos:**
  - Revisión de la documentación proporcionada por el cliente.
  - Escaneo pasivo de redes inalámbricas en las instalaciones (si es aprobado por el cliente).

### 1.2. Pruebas de Seguridad Wi-Fi (Si Aplicable)

- **Objetivo:**  
Evaluar la seguridad de las redes inalámbricas y su configuración.
  - **Métodos:**
    - **Escaneo de redes Wi-Fi:** Identificar puntos de acceso (APs) y redes visibles.
    - **Pruebas de autenticación:** Verificar la fortaleza de los métodos de autenticación (ej: WPA2, WPA3).
    - **Pruebas de cifrado:** Evaluar la robustez del cifrado utilizado (ej: AES, TKIP).
    - **Pruebas de fuerza bruta:** Intentar descifrar contraseñas débiles.
    - **Pruebas de rogue AP:** Detectar puntos de acceso no autorizados.
- 

## 2. Limitaciones y Condiciones

### 2.1. Autorización del Cliente

- **Descripción:**  
Las pruebas de acceso inalámbrico solo se realizarán si el cliente las aprueba explícitamente.
- **Documentación:**
  - Incluir el acceso inalámbrico en el contrato de compromiso y alcance de trabajo.

## 2.2. Minimización de Impactos

- **Descripción:**  
Las pruebas se diseñarán para evitar interrupciones en las operaciones de la red inalámbrica.
- **Medidas:**
  - Realizar pruebas fuera del horario laboral o en ventanas de mantenimiento.
  - Evitar pruebas disruptivas (ej: deautenticación de clientes).

## 2.3. Confidencialidad

- **Descripción:**  
Los resultados de las pruebas se manejarán de manera confidencial.
- **Medidas:**
  - Cifrado de datos y comunicaciones.
  - Destrucción segura de información sensible después de la entrega del informe final.

---

## 3. Resumen de Pruebas de Acceso Inalámbrico

Prueba	Objetivo	Limitaciones
Escaneo de Redes Wi-Fi	Identificar puntos de acceso y redes visibles.	Solo si el cliente aprueba explícitamente.
Pruebas de Autenticación	Verificar la fortaleza de los métodos de autenticación.	Evitar interrupciones en operaciones críticas.
Pruebas de Cifrado	Evaluar la robustez del cifrado utilizado.	Realizar en ventanas de mantenimiento.
Pruebas de Fuerza Bruta	Descifrar contraseñas débiles.	Solo en redes de prueba o con autorización.

#### Detección de Rogue APs

Identificar puntos de acceso no autorizados.

Sin impacto en operaciones.

---

## 4. Consideraciones Adicionales

- **Coordinación con el Cliente:**  
Cualquier prueba de acceso inalámbrico se coordinará previamente con el equipo de TI del cliente.
  - **Plan de Contingencia:**  
Se establecerá un plan de contingencia para restaurar rápidamente la conectividad en caso de incidentes.
  - **Capacitación:**  
Si se identifican vulnerabilidades, se proporcionará capacitación al personal de TI para mejorar la seguridad de las redes inalámbricas.
- 

## 5. Recomendación

Dado que el acceso inalámbrico puede ser un vector de ataque común, se recomienda incluir estas pruebas en el alcance del compromiso, siempre que el cliente lo apruebe. Esto permitirá una evaluación más completa de la postura de seguridad de Nexus Plaza.

---

Sí, los **servicios web están incluidos en el alcance de las pruebas de penetración** para Nexus Plaza, ya que son un componente crítico de su infraestructura, especialmente considerando que Nexus Plaza es una empresa minorista en línea con una fuerte dependencia de aplicaciones web para su comercio electrónico y operaciones internas. A continuación, se detalla cómo se abordarán las pruebas de seguridad en los servicios web:

---

## 1. Servicios Web a Probar

### 1.1. Aplicaciones Web de Comercio Electrónico

- **Descripción:**  
Plataformas web utilizadas por los clientes para realizar compras, consultar inventario y gestionar pedidos.
- **Objetivo:**  
Identificar vulnerabilidades como inyecciones SQL, cross-site scripting (XSS), y fallos de autenticación.
- **Métodos:**



- Escaneo automatizado con herramientas como Burp Suite, OWASP ZAP o Acunetix.
- Pruebas manuales de explotación de vulnerabilidades.

## 1.2. Portales Internos

- **Descripción:**  
Aplicaciones web utilizadas por empleados para gestionar inventario, logística y operaciones.
- **Objetivo:**  
Evaluar la seguridad de las interfaces y la integridad de los datos.
- **Métodos:**
  - Pruebas de autenticación y autorización.
  - Verificación de configuraciones seguras (ej: headers HTTP, cifrado SSL/TLS).

## 1.3. APIs

- **Descripción:**  
Interfaces de programación de aplicaciones (APIs) utilizadas para la comunicación entre sistemas (ej: inventario, envíos).
  - **Objetivo:**  
Identificar vulnerabilidades como inyecciones, autenticación débil o exposición de datos sensibles.
  - **Métodos:**
    - Pruebas de fuzzing con herramientas como Postman o SoapUI.
    - Análisis de respuestas y manejo de errores.
- 

# 2. Tipos de Pruebas en Servicios Web

## 2.1. Pruebas de Vulnerabilidades Comunes

- **Inyecciones SQL:**  
Verificar si es posible manipular consultas a la base de datos.
- **Cross-Site Scripting (XSS):**  
Evaluar si se pueden ejecutar scripts maliciosos en el navegador del usuario.
- **Cross-Site Request Forgery (CSRF):**  
Verificar si es posible realizar acciones no autorizadas en nombre de un usuario autenticado.
- **Fallas de Autenticación y Autorización:**  
Evaluar la robustez de los mecanismos de autenticación y control de acceso.

## 2.2. Pruebas de Configuración

- **Cifrado SSL/TLS:**  
Verificar que los certificados sean válidos y que se utilicen protocolos seguros.

- **Headers de Seguridad:**  
Evaluar la presencia y configuración de headers como Content Security Policy (CSP), X-Content-Type-Options, y Strict-Transport-Security (HSTS).

### 2.3. Pruebas de Carga y Estrés

- **Objetivo:**  
Evaluar cómo los servicios web manejan cargas extremas de tráfico o solicitudes.
  - **Métodos:**
    - Uso de herramientas como JMeter, Gatling o Locust.
    - Simulación de picos de tráfico en aplicaciones web o APIs.
- 

## 3. Limitaciones y Condiciones

### 3.1. Entornos de Prueba

- **Descripción:**  
Las pruebas se realizarán principalmente en el entorno de desarrollo espejado proporcionado por el cliente.
- **Exclusión:**
  - No se realizarán pruebas invasivas en los sistemas de producción a menos que sea absolutamente necesario y con autorización explícita.

### 3.2. Horarios de Prueba

- **Descripción:**  
Las pruebas disruptivas (ej: pruebas de carga) se realizarán durante las ventanas de mantenimiento programadas.
- **Horarios:**
  - Viernes, sábados y domingos, entre las 2:00 a. m. y las 6:00 a. m.

### 3.3. Supervisión del Cliente

- **Descripción:**  
El equipo de TI del cliente supervisará las pruebas en tiempo real para detectar y mitigar cualquier impacto no deseado.
  - **Coordinación:**
    - Reuniones previas para definir los parámetros de las pruebas.
    - Comunicación constante durante las pruebas.
- 

## 4. Resumen de Pruebas en Servicios Web

Prueba	Objetivo	Limitaciones
Inyecciones SQL	Verificar manipulación de consultas a la base de datos.	Solo en entorno de desarrollo espejado.
Cross-Site Scripting (XSS)	Evaluar ejecución de scripts maliciosos.	Pruebas no disruptivas en horario laboral.
Pruebas de Carga	Verificar manejo de cargas extremas.	Solo en ventanas de mantenimiento.
Configuración SSL/TLS	Evaluar robustez del cifrado.	Sin impacto en operaciones críticas.

---

## 5. Consideraciones Adicionales

- **Minimización de Impactos:**  
Las pruebas se diseñarán para evitar interrupciones en los sistemas de producción.
- **Comunicación con el Cliente:**  
Cualquier prueba en servicios web se coordinará previamente con el equipo de TI del cliente.
- **Documentación:**  
Se registrarán todos los cambios realizados para garantizar la transparencia y trazabilidad.

---

De acuerdo con la información proporcionada por Nexus Plaza, **los empleados no serán notificados sobre las pruebas de penetración**, excepto por el personal de TI directamente responsable del monitoreo de los sistemas de operaciones y logística. Esta decisión se tomó para garantizar que las pruebas simulen condiciones realistas y evalúen la efectividad de los controles de seguridad sin sesgos. A continuación, se detalla cómo se manejará este aspecto:

---

### 1. Notificación Limitada a Personal Específico

#### 1.1. Personal de TI Responsable

- **Descripción:**  
Solo el personal de TI directamente responsable del monitoreo de los sistemas de operaciones y logística será notificado sobre las pruebas.

- **Razón:**
  - Permitir la supervisión en tiempo real de las pruebas.
  - Garantizar que cualquier impacto no deseado se detecte y mitigue rápidamente.

## 1.2. Gerentes y Contactos Principales

- **Descripción:**

El director de TI, el gerente de almacén y el gerente de operaciones serán los contactos principales para coordinar y recibir actualizaciones sobre las pruebas.
  - **Razón:**
    - Mantener una comunicación clara y efectiva durante el compromiso.
    - Asegurar que las pruebas se ajusten a los objetivos del cliente.
- 

## 2. Empleados Finales No Notificados

### 2.1. Pruebas de Ingeniería Social

- **Descripción:**

Las pruebas de phishing y otros ataques de ingeniería social se realizarán sin notificar a los empleados finales.
- **Razón:**
  - Evaluar la susceptibilidad real de los empleados a este tipo de ataques.
  - Identificar áreas de mejora en la concienciación sobre seguridad.

### 2.2. Pruebas en Sistemas de Producción

- **Descripción:**

Las pruebas no disruptivas en sistemas de producción se realizarán sin notificar a los empleados finales.
  - **Razón:**
    - Evitar cambios en el comportamiento que puedan afectar los resultados de las pruebas.
- 

## 3. Plazo y Horarios de Pruebas

### 3.1. Plazo General

- **Descripción:**

El compromiso comenzará dos semanas después de la firma del contrato y tendrá una duración de 60 días.
- **Comunicación:**
  - Solo los contactos principales (director de TI, gerentes) conocerán el plazo completo.

### 3.2. Ventanas de Mantenimiento

- **Descripción:**  
Las pruebas disruptivas (ej: DoS, pruebas de carga) se realizarán durante las ventanas de mantenimiento programadas.
  - **Horarios:**
    - Viernes, sábados y domingos, entre las 2:00 a. m. y las 6:00 a. m.
  - **Comunicación:**
    - Solo el personal de TI responsable será notificado sobre estas ventanas.
- 

## 4. Consideraciones Éticas y Legales

### 4.1. Autorización del Cliente

- **Descripción:**  
Todas las pruebas se realizarán con autorización explícita del cliente, documentada en el contrato de compromiso.
- **Documentación:**
  - Incluir detalles sobre la no notificación a empleados finales.

### 4.2. Minimización de Impactos

- **Descripción:**  
Las pruebas se diseñarán para evitar daños o molestias innecesarias a los empleados.
- **Medidas:**
  - Notificación posterior a los empleados afectados (si es necesario).
  - Capacitación en concienciación de seguridad después de las pruebas.

### 4.3. Confidencialidad

- **Descripción:**  
Los resultados de las pruebas se manejarán de manera confidencial.
  - **Medidas:**
    - Cifrado de datos y comunicaciones.
    - Destrucción segura de información sensible después de la entrega del informe final.
- 

## 5. Resumen de Comunicación y Notificación

Grupo	Notificación	Detalles
Personal de TI	Sí	Solo personal responsable de monitoreo.

<b>Gerentes y Contactos</b>	Sí	Director de TI, gerente de almacén y operaciones.
<b>Empleados Finales</b>	No	Pruebas de ingeniería social y sistemas de producción.

## 6. Recomendación

Para garantizar que las pruebas sean éticas y efectivas, se recomienda:

- Capacitación Posterior:**  
 Después de las pruebas, proporcionar capacitación en concienciación de seguridad a los empleados afectados.
- Transparencia Limitada:**  
 Informar a los empleados sobre las pruebas solo si es necesario para mejorar la seguridad a largo plazo.

A continuación, se presenta la **tabla de Elementos de las Reglas para Participar** basada en la transcripción de la entrevista con el CEO y el director de TI de Nexus Plaza, así como en la información de la Hoja de Trabajo del Alcance. Esta tabla define las reglas clave que guiarán las pruebas de penetración.

## Tabla de Elementos de las Reglas para Participar

Elemento	Detalles	Fuente (Entrevista/Hoja de Trabajo)
<b>Autorización</b>	Se requiere autorización por escrito antes de iniciar cualquier prueba.	Entrevista: CEO menciona la necesidad de autorización.
<b>Alcance de Pruebas</b>	- Clústeres de operaciones, logística y administración.	Hoja de Trabajo: Rangos de IP y VLANs definidos.
	- Exclusión de clústeres de soporte de Amazon y sistemas de producción SQL.	Entrevista: Director de TI especifica exclusiones.

<b>Métodos Permitidos</b>	- Pruebas de vulnerabilidades (ej: SQLi, XSS).	Entrevista: CEO y director de TI.
	- Pruebas de ingeniería social (phishing a empleados).	Entrevista: CEO menciona preocupación por phishing.
	- Pruebas de escalada de privilegios.	Entrevista: CEO quiere evaluar controles de acceso.
<b>Métodos Prohibidos</b>	- Ataques de denegación de servicio (DoS/DDoS) en producción.	Entrevista: Director de TI limita pruebas disruptivas.
	- Pruebas en clústeres de soporte de Amazon.	Entrevista: Director de TI especifica exclusiones

## Prueba de Línea de Tiempo

Elemento	Detalles	Fuente (Entrevista/Hoja de Trabajo)
<b>Inicio del Compromiso</b>	2 semanas después de la firma del contrato.	Entrevista: CEO menciona el plazo de inicio.
<b>Duración del Compromiso</b>	60 días desde el inicio.	Entrevista: CEO espera el informe final en 60 días.
<b>Ventanas de Pruebas</b>	- Pruebas disruptivas: Viernes a domingo, 2:00 a. m. – 6:00 a. m.	Entrevista: Director de TI define horarios de mantenimiento.
	- Pruebas no disruptivas: Horario laboral normal.	Entrevista: Director de TI permite pruebas no disruptivas.
<b>Entregables</b>	- Informe de actualización semanal.	Entrevista: CEO solicita informes semanales.
	- Informe final al finalizar los 60 días.	Entrevista: CEO espera el informe final en 60 días.

---

## Explicación de la Línea de Tiempo

1. **Inicio del Compromiso:**
  - Las pruebas comenzarán **2 semanas después de la firma del contrato**, lo que permite tiempo para la planificación y coordinación inicial.
2. **Duración del Compromiso:**
  - El compromiso tendrá una duración total de **60 días**, durante los cuales se realizarán las pruebas y se entregará el informe final.
3. **Ventanas de Pruebas:**
  - **Pruebas disruptivas** (ej: DoS, pruebas de carga) se realizarán únicamente durante las **ventanas de mantenimiento** (viernes a domingo, 2:00 a. m. – 6:00 a. m.).
  - **Pruebas no disruptivas** (ej: escaneos, pruebas de vulnerabilidades) se realizarán durante el **horario laboral normal**, siempre que no afecten las operaciones.
4. **Entregables:**
  - Se proporcionará un **informe de actualización semanal** a los contactos principales (director de TI, gerentes).
  - El **informe final** se entregará al finalizar los **60 días**, resumiendo los hallazgos, riesgos y recomendaciones.

---

### Prueba de Línea de Tiempo:

- Inicio: 2 semanas post-contrato; duración: 60 días.
- Pruebas disruptivas: viernes a domingo (2:00 a. m. – 6:00 a. m.); no disruptivas: horario laboral. Informes semanales y final en 60 días.

### Ubicación de la Prueba:

- Pruebas remotas desde la VLAN aislada del departamento de TI y entorno de desarrollo espejado. Exclusión de sistemas de producción y clústeres de Amazon.

### Ventanas de Tiempo para la Prueba:

- Pruebas disruptivas: viernes a domingo (2:00 a. m. – 6:00 a. m.). Pruebas no disruptivas: horario laboral normal.

### Método de Comunicación Preferido:

- Informes semanales y teleconferencias con el director de TI, gerente de almacén y gerente de operaciones.

### Controles de Seguridad que Podrían Detectar o Evitar las Pruebas:



- Cortafuegos, IDS/IPS, DLP, y sistemas de detección de honeypots. Coordinación con el equipo de TI para ajustar configuraciones durante las pruebas.

#### Manejo de Datos Sensibles:

- Cifrado de datos y comunicaciones; destrucción segura de información sensible tras la entrega del informe final.

¿Siguiente campo? 😊

#### Direcciones IP o Redes de Origen de las Pruebas:

- VLAN aislada del departamento de TI (172.16.33.0/30) y entorno de desarrollo espejado.

Obtener un acuerdo sobre las reglas de enfrentamiento que se aplican a una prueba de penetración o auditoría de seguridad es el primer paso en cualquier compromiso con un cliente. Es importante dedicar tiempo a garantizar que tanto su empresa como el cliente tengan una comprensión clara de los términos y el alcance del trabajo de prueba.

### Documento de Alcance y Planificación para Pruebas de Penetración

Cliente: Nexus Plaza

Fecha de inicio propuesta: [Inserte fecha]

Duración del compromiso: 60 días

#### 1. Introducción

Este documento define el alcance, las reglas de enfrentamiento (RoE) y los requisitos para las pruebas de penetración que se llevarán a cabo en los sistemas y redes de Nexus Plaza. El objetivo es evaluar la seguridad de la infraestructura crítica, identificar vulnerabilidades y garantizar que los sistemas cumplan con los estándares de seguridad necesarios para proteger los datos y operaciones de la empresa

A partir de la información proporcionada por Nexus Plaza, identificamos los siguientes puntos clave que influyen en el alcance del proyecto y las reglas de enfrentamiento (RoE) para las pruebas de penetración:

## **1. Factores que Influyen en el Alcance del Proyecto**

### **1.1. Sistemas y Redes Críticas**

Incluidos:

Clústeres de operaciones y logística: Sistemas de almacenamiento, envío y control de inventario (base de datos SQL Server).

VLAN del departamento de TI: Punto de acceso interno para las pruebas.

Redes del centro de datos: Separadas por un cortafuegos con IDS integrado.

DNS interno (Active Directory) y DNS externo (servidor Linux en DMZ).

Sistemas de desarrollo: Espejo de la base de datos SQL Server para pruebas no disruptivas.

Excluidos:

Clúster de soporte de Amazon: Prohibido probar sistemas relacionados con la tienda de Amazon.

Sistemas de producción SQL Server: Solo se probará el entorno de desarrollo configurado de manera idéntica.

Acceso HTTP externo a clústeres críticos: No permitido según las políticas del cliente.

### **1.2. Objetivos del Cliente**

Prioridades:

Evaluar la posibilidad de que un atacante con acceso a una cuenta de usuario final en el depósito escale privilegios a administrador.

Identificar vulnerabilidades en el software, sistemas operativos y aplicaciones.

Probar la resistencia contra ataques de ingeniería social (phishing a empleados del almacén y operaciones).

Preocupaciones clave:

Evitar interrupciones en los sistemas de producción.

Proteger la integridad del inventario y los datos de pedidos en tiempo real.

### **1.3. Restricciones Operativas**

Horarios de prueba:

Pruebas disruptivas (ej: DoS, pruebas de carga): Solo durante el período de mantenimiento (2:00 a. m. – 6:00 a. m., viernes a domingo).

Pruebas no disruptivas: Durante horario laboral normal.

Acceso limitado:

Solo personal de TI específico estará al tanto de las pruebas.

Los empleados finales no deben ser notificados para simular condiciones realistas.

### **1.4. Entorno Técnico**

Infraestructura:

25 servidores en clústeres (administración, operaciones, logística, soporte de Amazon).

Acceso remoto mediante SSL/IPsec VPN.

Dos ISPs: Uno dedicado a comunicaciones con Amazon.

Seguridad existente:

Cortafuegos locales en servidores del centro de datos.

Sistemas de operaciones y logística sin acceso a Internet (excepto actualizaciones automáticas).

## **2. Reglas de Enfrentamiento (RoE)**

### **2.1. Autorización y Límites Legales**

Autorización escrita: Requerida antes de iniciar cualquier prueba.

Contrato de confidencialidad (NDA): Protección de datos sensibles y resultados de las pruebas.

Cumplimiento normativo: Respetar GDPR (protección de datos de clientes) y políticas internas de Nexus Plaza.

## **2.2. Métodos Permitidos**

Pruebas de vulnerabilidades:

Escaneo de puertos y servicios.

Explotación controlada de vulnerabilidades (ej: SQLi, XSS).

Simulación de escalada de privilegios desde una cuenta de usuario.

Ingeniería social:

Pruebas de phishing dirigido a empleados del almacén y operaciones (usando la lista de correos proporcionada).

Pruebas de configuración:

Verificación de parches y actualizaciones en sistemas operativos y software.

## **2.3. Métodos Prohibidos**

Ataques disruptivos:

Denegación de servicio (DoS/DDoS) fuera de las ventanas de mantenimiento.

Manipulación o eliminación de datos en sistemas de producción.

Áreas excluidas:

Clústeres de soporte de Amazon.

Sistemas de producción SQL Server (solo se prueba el entorno espejo).

Redes externas de pedidos en tiempo real con Amazon.

## **2.4. Comunicación y Reportes**

Contactos principales:

Director de TI, Gerente de Almacén y Gerente de Operaciones.

Frecuencia de actualizaciones:

Informes semanales y teleconferencias para revisar el progreso.

Gestión de incidentes:

Cualquier impacto no planificado en sistemas de producción debe reportarse inmediatamente.

## **2.5. Seguridad y Ética**

Privacidad:

No se revelará información sensible fuera del equipo autorizado.

Los datos recopilados se eliminarán tras la entrega del informe final.

Simulación realista:

Los empleados no serán informados de las pruebas de ingeniería social para mantener la autenticidad.

## **3. Consideraciones Adicionales**

Plazos:

Inicio: 2 semanas después de la firma del contrato.

Duración: 60 días desde el inicio.

Entrega del informe final: Al finalizar el plazo acordado.

Recursos proporcionados por el cliente:

Acceso a la VLAN aislada del departamento de TI.

Lista de direcciones de correo para pruebas de phishing.

Entorno de desarrollo SQL Server espejado.

## **4. Riesgos y Mitigación**

Riesgo de interrupción en producción:

Mitigación: Usar el entorno de desarrollo para pruebas críticas y limitar pruebas disruptivas a ventanas de mantenimiento.

Falsos positivos en IDS/IPS:

Mitigación: Coordinar con el equipo de TI para filtrar alertas relacionadas con las pruebas.

Exposición accidental de datos:

Mitigación: Cifrar todos los informes y comunicaciones.

¿Cuáles son las mayores preocupaciones de seguridad del cliente? (Los ejemplos incluyen la divulgación de información confidencial, la interrupción del procesamiento de producción, la vergüenza debido a la desfiguración del sitio web, etc.)

A partir de la información proporcionada por Nexus Plaza, las mayores preocupaciones de seguridad del cliente son las siguientes:

### **1. Interrupción de Operaciones Críticas (Ransomware/DoS)**

Contexto:

El CEO mencionó que un competidor sufrió un ataque de ransomware que paralizó su sistema de inventario, causando pérdidas significativas.

Preocupación específica:

Que un ataque similar afecte los sistemas de almacenamiento, envío o control de inventario de Nexus Plaza, interrumpiendo la capacidad de procesar pedidos y cumplir con entregas rápidas.

Impacto:

Pérdida de ingresos, daño a la reputación y posibles multas por incumplimiento de contratos con clientes.

### **2. Escalada de Privilegios en Sistemas Internos**

Contexto:

El cliente quiere asegurarse de que un atacante con acceso a una cuenta de usuario estándar (ej: empleado del almacén) no pueda obtener privilegios de administrador.

Preocupación específica:

Vulnerabilidades en la configuración de seguridad, permisos excesivos o fallos en la segmentación de redes que permitan movimientos laterales dentro de los clústeres de operaciones y logística.

Impacto:

Acceso no autorizado a la base de datos de inventario, manipulación de pedidos o sabotaje interno.

### **3. Vulnerabilidades en Software y Sistemas Operativos**

Contexto:

El director de TI enfatizó la necesidad de verificar que no existan vulnerabilidades conocidas en aplicaciones, sistemas operativos o la base de datos SQL Server.

Preocupación específica:

Parches no aplicados, configuraciones inseguras o servicios expuestos (ej: servicios sin actualizar en los servidores del centro de datos).

Impacto:

Explotación de vulnerabilidades para robo de datos o toma de control de sistemas.

#### **4. Ataques de Ingeniería Social**

Contexto:

El CEO mencionó que la mayoría de los ransomware comienzan con ataques de ingeniería social.

Preocupación específica:

Empleados del almacén u operaciones que caigan en phishing, descarguen archivos maliciosos o revelen credenciales.

Impacto:

Inicio de una cadena de compromisos que derive en una brecha mayor.

#### **5. Exposición de Datos Sensibles**

Contexto:

La base de datos SQL Server contiene información crítica de inventario y pedidos, alojada en una SAN con conexiones al almacén y producción.

Preocupación específica:

Acceso no autorizado a la base de datos (ej: inyecciones SQL) o filtración de datos debido a configuraciones inseguras.

Impacto:

Pérdida de información confidencial, incumplimiento del GDPR y daño a la confianza de los clientes.

#### **6. Interrupciones en Sistemas de Producción**

Contexto:

El cliente insistió en minimizar las interrupciones durante las pruebas, especialmente en los sistemas de producción.

Preocupación específica:

Que pruebas invasivas (ej: escaneos agresivos o explotación de vulnerabilidades) afecten la disponibilidad de los sistemas críticos.

Impacto:

Parálisis operativa, retrasos en envíos y costos financieros directos.

#### **7. Dependencia de Sistemas Externos (Amazon)**

Contexto:

La comunicación con Amazon es vital para el procesamiento de pedidos en tiempo real.

Preocupación específica:

Ataques que afecten la conectividad con Amazon (ej: compromiso de la VPN o del ISP dedicado).

Impacto:

Interrupción del flujo de pedidos, inventario y atención al cliente.

## **8. Configuraciones Inseguras en Redes Internas**

Contexto:

El director de TI mencionó que los servidores no tienen acceso a Internet (excepto para actualizaciones) y están protegidos por cortafuegos locales.

Preocupación específica:

Configuraciones erróneas en el cortafuegos, VLANs mal segmentadas o reglas de IDS/IPS ineficaces.

Impacto:

Exposición de sistemas críticos a amenazas internas o externas.

## **9. Reputación y Confianza del Cliente**

Contexto:

Nexus Plaza depende de su imagen como empresa confiable para entregas rápidas.

Preocupación específica:

Que una brecha de seguridad se haga pública o cause retrasos visibles para los clientes.

Impacto:

Pérdida de participación en el mercado y reputación dañada.

## **10. Cumplimiento Legal y Normativo**

Contexto:

El cliente opera con datos de clientes y transacciones que deben cumplir con regulaciones como el GDPR.

Preocupación específica:

Sanciones legales o multas debido a fallos de seguridad que expongan datos personales.

Resumen de Prioridades del Cliente

Preocupación

Ejemplo del Escenario

Interrupción operativa

Ataque de ransomware en sistemas de envío.

Escalada de privilegios

Usuario del almacén accediendo a la base de datos.



Ingeniería social                      Phishing a empleados de logística.

Exposición de datos                  Filtración de la base de datos SQL.

¿Qué clústeres de servidores, rangos de direcciones de red o aplicaciones específicos deben probarse?

A partir de la información proporcionada por Nexus Plaza, los clústeres de servidores, rangos de direcciones de red y aplicaciones específicas que deben probarse son los siguientes:

## **1. Clústeres de Servidores a Probar**

### **1.1. Clúster de Operaciones**

Función: Respalda los sistemas de almacenamiento y envío.

Servicios clave:

Base de datos SQL Server (espejo de desarrollo para pruebas).

Sistemas de control de inventario.

Aplicaciones de gestión de almacén.

Preocupación principal: Vulnerabilidades que permitan la escalada de privilegios o acceso no autorizado.

### **1.2. Clúster de Logística**

Función: Gestiona el control de inventario y producción.

Servicios clave:

Base de datos SQL Server (espejo de desarrollo para pruebas).

Sistemas de seguimiento de pedidos.

Aplicaciones de planificación de envíos.

Preocupación principal: Exposición de datos sensibles o interrupción del flujo de operaciones.

### **1.3. Clúster de Administración**

Función: Gestiona la infraestructura interna de TI.

Servicios clave:

Active Directory (gestión de usuarios y permisos).

Servidores de correo electrónico.

Herramientas de monitoreo y gestión de red.

Preocupación principal: Configuraciones inseguras que permitan acceso no autorizado.

## **2. Rangos de Direcciones de Red a Probar**

### **2.1. Redes del Centro de Datos**

Clúster de Operaciones:

Rango de IP: 172.16.33.0/30 (Administración).

Máscara de subred: 255.255.255.192.

Clúster de Logística:

Rango de IP: 172.26.0.0/21.

Máscara de subred: 255.255.255.0.

Clúster de Administración:

Rango de IP: 172.24.1.0/24.

Máscara de subred: 255.255.255.192.

### **2.2. VLANs de la LAN Corporativa**

VLAN 120 (Administración):

Rango de IP: 172.16.1.0.

Máscara de subred: 255.255.255.0.

VLAN 130 (Subred de Tecnología de la Información):

Rango de IP: 172.16.4.0.

Máscara de subred: 255.255.255.0.

VLAN 140 (Tecnología de la Información):

Rango de IP: 172.16.8.0.

Máscara de subred: 255.255.255.0.

VLAN 150 (Depósito):

Rango de IP: 172.16.12.0.

Máscara de subred: 255.255.255.0.

VLAN 160 (Atención al Cliente):

Rango de IP: 172.16.16.0.

Máscara de subred: 255.255.255.0.

VLAN 170 (Envío):

Rango de IP: 172.16.20.0.

Máscara de subred: 255.255.255.0.

### **2.3. Redes Excluidas**

Clúster de Soporte de Amazon:

Rango de IP: 172.25.0.0/16.

Máscara de subred: 255.255.252.0.

Motivo: Prohibido probar sistemas relacionados con la tienda de Amazon.

## **3. Aplicaciones Específicas a Probar**

### **3.1. Base de Datos SQL Server**

Entorno de pruebas: Espejo de desarrollo proporcionado por el cliente.

Objetivo: Identificar vulnerabilidades como inyecciones SQL, configuraciones inseguras o permisos excesivos.

### **3.2. Active Directory**

Función: Gestión de usuarios y permisos.

Objetivo: Verificar que no existan cuentas con privilegios excesivos o configuraciones inseguras.

### **3.3. Aplicaciones de Gestión de Almacén**

Función: Control de inventario y seguimiento de pedidos.

Objetivo: Evaluar la seguridad de las interfaces y la integridad de los datos.

### **3.4. VPN (SSL/IPsec)**

Función: Acceso remoto a los sistemas internos.

Objetivo: Probar la resistencia contra ataques de fuerza bruta o explotación de vulnerabilidades.

### **3.5. Servidores DNS**

DNS Interno: Microsoft Active Directory.

DNS Externo: Servidor Linux en DMZ.

Objetivo: Verificar que no existan configuraciones inseguras o vulnerabilidades conocidas.

## **4. Resumen de Áreas de Prueba**

Área    Detalles

Clúster de Operaciones      Sistemas de almacenamiento y envío.

Clúster de Logística    Control de inventario y producción.

Clúster de Administración    Active Directory y servidores de gestión.

Base de Datos SQL    Espejo de desarrollo para pruebas no disruptivas.

VLANs Corporativas    VLANs 120-170 (Administración, TI, Depósito, etc.).

Aplicaciones    SQL Server, Active Directory, VPN, DNS.

Este enfoque garantiza que las pruebas se centren en los sistemas y redes críticas, respetando las exclusiones y restricciones definidas por el cliente.

¿Qué clústeres de servidores, rangos de direcciones de red o aplicaciones específicos NO deben probarse explícitamente?

De acuerdo con la información proporcionada por Nexus Plaza, hay ciertos clústeres de servidores, rangos de direcciones de red y aplicaciones específicas que no deben probarse explícitamente. Estas exclusiones se basan en las preocupaciones del cliente, la criticidad de los sistemas y las restricciones operativas. A continuación, se detallan las áreas excluidas:

### **1. Clústeres de Servidores Excluidos**

## **1.1. Clúster de Soporte de Amazon**

Función: Respalda las comunicaciones con Amazon para pedidos en tiempo real, inventario y atención al cliente.

Razón de exclusión:

El cliente ha indicado explícitamente que no se deben probar los sistemas relacionados con la tienda de Amazon.

Estos sistemas son críticos para el negocio y cualquier interrupción podría afectar gravemente las operaciones.

## **2. Rangos de Direcciones de Red Excluidos**

### **2.1. Redes del Clúster de Soporte de Amazon**

Rango de IP: 172.25.0.0/16.

Máscara de subred: 255.255.252.0.

Razón de exclusión:

Estas redes están dedicadas a la comunicación con Amazon y no deben ser perturbadas.

### **2.2. Redes de Producción SQL Server**

Rango de IP: No especificado (pero se excluyen los sistemas de producción).

Razón de exclusión:

El cliente ha proporcionado un entorno de desarrollo espejado para pruebas, por lo que los sistemas de producción no deben ser probados directamente.

## **3. Aplicaciones Específicas Excluidas**

### **3.1. Sistemas de Producción SQL Server**

Función: Base de datos de inventario y pedidos en tiempo real.

Razón de exclusión:

El cliente ha proporcionado un entorno de desarrollo espejado para pruebas no disruptivas.

Los sistemas de producción son críticos y no deben ser perturbados.

### **3.2. Servicios de Comunicación con Amazon**

Función: Procesamiento de pedidos en tiempo real y gestión de inventario con Amazon.

Razón de exclusión:

Estos servicios son vitales para el negocio y cualquier interrupción podría causar pérdidas significativas.

### 3.3. Sistemas de Producción de Envíos

Función: Gestión de envíos y logística en tiempo real.

Razón de exclusión:

Pruebas en estos sistemas podrían interrumpir las operaciones diarias y afectar la entrega de pedidos.

## 4. Resumen de Áreas Excluidas

Área	Detalles	Razón de Exclusión
Clúster de Soporte de Amazon	Sistemas de comunicación con Amazon.	Críticos para el negocio; prohibido por el cliente.
Redes de Soporte de Amazon	Rango de IP: 172.25.0.0/16.	Dedicadas a Amazon; no deben ser perturbadas.
Sistemas de Producción	SQLBase de datos de inventario y pedidos.	Se prueba el entorno espejado; producción es crítica.
Servicios de Comunicación	Pedidos en tiempo real con Amazon.	Vitales para el negocio; no deben interrumpirse.
Sistemas de Envíos	Gestión de envíos y logística en tiempo real.	Pruebas podrían afectar operaciones diarias.

## 5. Consideraciones Adicionales

Entorno de Desarrollo:

El cliente ha proporcionado un entorno espejado (desarrollo) para pruebas no disruptivas. Este entorno debe usarse en lugar de los sistemas de producción.

Comunicación con Amazon:

Aunque no se probarán directamente, se debe verificar que las configuraciones de red (ej: VPN, cortafuegos) que protegen estas comunicaciones estén seguras.

Minimización de Riesgos:

Las pruebas deben diseñarse para evitar cualquier impacto indirecto en los sistemas excluidos.

¿La prueba se realizará en un entorno de producción en vivo o en un entorno de prueba? De acuerdo con la información proporcionada por Nexus Plaza, las pruebas de penetración se realizarán principalmente en un entorno de prueba, no en el entorno de producción en vivo. Esto se debe a las preocupaciones del cliente sobre la interrupción de operaciones críticas y la necesidad de mantener la disponibilidad de los sistemas de producción. A continuación, se detalla cómo se manejará este aspecto:

## **1. Entorno de Prueba**

### **1.1. Base de Datos SQL Server (Espejo de Desarrollo)**

Descripción:

El cliente ha proporcionado un entorno de desarrollo espejado que replica la base de datos SQL Server utilizada en producción.

Uso:

Pruebas de vulnerabilidades (ej: inyecciones SQL, configuraciones inseguras).

Simulación de ataques sin riesgo de afectar los datos reales.

Ventajas:

Permite pruebas exhaustivas sin interrumpir las operaciones de producción.

Reduce el riesgo de pérdida o corrupción de datos.

### **1.2. VLAN Aislada del Departamento de TI**

Descripción:

Una red aislada dentro del departamento de TI que simula el entorno de red del centro de datos.

Uso:

Pruebas de escaneo de puertos y servicios.

Simulación de ataques internos (ej: escalada de privilegios).

Ventajas:

Proporciona un entorno controlado para pruebas no disruptivas.

Permite evaluar la seguridad de la red sin afectar sistemas críticos.

## **2. Limitaciones en el Entorno de Producción**

### **2.1. Pruebas No Invasivas**

Descripción:

Algunas pruebas no disruptivas (ej: revisión de configuraciones, verificación de parches) pueden realizarse en el entorno de producción.

Condiciones:

Solo durante horario laboral normal.

Con supervisión del equipo de TI del cliente.

## 2.2. Pruebas Disruptivas (Solo en Ventanas de Mantenimiento)

Descripción:

Pruebas que podrían afectar la disponibilidad de los sistemas (ej: pruebas de carga, simulaciones de DoS) se realizarán únicamente durante las ventanas de mantenimiento programadas.

Horarios:

Viernes, sábados y domingos, entre las 2:00 a. m. y las 6:00 a. m.

Condiciones:

Coordinación previa con el equipo de TI del cliente.

Monitoreo constante para minimizar impactos.

## 3. Resumen de Entornos de Prueba

Entorno	Tipo de Pruebas	Condiciones
Entorno de Prueba	Pruebas de vulnerabilidades, simulaciones de ataques.	Uso exclusivo del entorno espejado y VLAN aislada.
Entorno de Producción	Pruebas no disruptivas (ej: revisión de configuraciones).	Solo durante horario laboral y con supervisión.
Ventanas de Mantenimiento	Pruebas disruptivas (ej: DoS, pruebas de carga).	Viernes a domingo, 2:00 a. m. – 6:00 a. m.

## 4. Consideraciones Adicionales

Minimización de Riesgos:

Las pruebas en el entorno de producción se limitarán al mínimo necesario para evitar interrupciones.

Comunicación con el Cliente:



Cualquier prueba en el entorno de producción se coordinará previamente con el equipo de TI del cliente.

Enfoque en el Entorno de Prueba:

La mayoría de las pruebas se realizarán en el entorno espejado y la VLAN aislada para garantizar la seguridad y disponibilidad de los sistemas de producción.

¿La prueba de penetración incluirá pruebas de red internas? Si es así, ¿cómo se obtendrá el acceso?

Sí, las pruebas de penetración incluirán pruebas de red internas, ya que el cliente ha expresado preocupaciones específicas sobre la seguridad de sus sistemas internos, como la posibilidad de que un atacante con acceso a una cuenta de usuario estándar pueda escalar privilegios o moverse lateralmente dentro de la red. A continuación, se detalla cómo se obtendrá el acceso y cómo se realizarán estas pruebas:

## **1. Acceso a la Red Interna**

### **1.1. VLAN Aislada del Departamento de TI**

Descripción:

El cliente proporcionará acceso a una VLAN aislada dentro del departamento de TI, que simula el entorno de red del centro de datos.

Uso:

Pruebas de escaneo de puertos y servicios.

Simulación de ataques internos (ej: escalada de privilegios, movimientos laterales).

Acceso:

Se otorgará acceso remoto a través de una conexión VPN (SSL/IPsec) configurada específicamente para este propósito.

El acceso estará limitado a esta VLAN y no permitirá la conexión directa a otros sistemas críticos.

### **1.2. Credenciales de Usuario Estándar**

Descripción:

El cliente proporcionará credenciales de usuario estándar (similares a las de un empleado del almacén o logística) para simular un escenario realista de ataque interno.

Uso:

Pruebas de escalada de privilegios desde una cuenta de usuario estándar.

Evaluación de la efectividad de los controles de seguridad internos.

Acceso:

Las credenciales se proporcionarán de manera segura (ej: mediante un gestor de contraseñas o cifrado PGP).

## **2. Pruebas de Red Interna**

### **2.1. Escaneo de Puertos y Servicios**

Objetivo:

Identificar servicios expuestos, puertos abiertos y posibles puntos de entrada.

Herramientas:

Nmap, Nessus, OpenVAS.

Alcance:

VLAN aislada del departamento de TI.

Clústeres de operaciones y logística (acceso limitado).

### **2.2. Movimientos Laterales**

Objetivo:

Simular cómo un atacante podría moverse lateralmente dentro de la red después de comprometer una cuenta de usuario estándar.

Herramientas:

Mimikatz, BloodHound, CrackMapExec.

Alcance:

Evaluación de la segmentación de red y controles de acceso.

### **2.3. Escalada de Privilegios**

Objetivo:

Verificar si un usuario estándar puede obtener privilegios de administrador.

Herramientas:

Metasploit, PowerShell Empire.

Alcance:

Sistemas dentro de la VLAN aislada y clústeres de operaciones/logística.

## **2.4. Pruebas de Configuración de Red**

Objetivo:

Evaluar la seguridad de las configuraciones de red (ej: cortafuegos, VLANs, IDS/IPS).

Herramientas:

Wireshark, Nessus, manual review.

Alcance:

VLAN aislada y redes del centro de datos.

## **3. Consideraciones de Seguridad**

### **3.1. Supervisión del Cliente**

Descripción:

El equipo de TI del cliente supervisará las pruebas en tiempo real para detectar y mitigar cualquier impacto no deseado.

Coordinación:

Reuniones diarias o semanales para revisar el progreso y los resultados preliminares.

### **3.2. Minimización de Impactos**

Descripción:

Las pruebas se diseñarán para minimizar el riesgo de interrupciones en los sistemas de producción.

Medidas:

Uso de herramientas en modo "solo lectura" cuando sea posible.

Limitación de pruebas disruptivas a ventanas de mantenimiento.

### **3.3. Confidencialidad**

Descripción:

Toda la información recopilada durante las pruebas se manejará de manera confidencial.

Medidas:

Cifrado de datos y comunicaciones.

Destrucción segura de datos después de la entrega del informe final.

## 4. Resumen de Acceso y Pruebas Internas

Acceso                      Detalles                      Pruebas Relacionadas

VLAN Aislada de TI      Acceso remoto mediante VPN (SSL/IPsec). Escaneo de puertos, movimientos laterales.

Credenciales de Usuario      Cuenta estándar (simulación de empleado). Escalada de privilegios, pruebas de configuración.

Supervisión del Cliente      Monitoreo en tiempo real por el equipo de TI.  
Coordinación para minimizar impactos.

¿Los sistemas de cliente / usuario final se incluyen en el alcance? Si es así, ¿cómo se aprovecharán los clientes?

De acuerdo con la información proporcionada por Nexus Plaza, los sistemas de cliente/usuario final no están incluidos explícitamente en el alcance de las pruebas de penetración. Sin embargo, el cliente ha expresado preocupaciones sobre la posibilidad de que un atacante comprometa una cuenta de usuario final (por ejemplo, un empleado del almacén) y utilice ese acceso para moverse lateralmente dentro de la red o escalar privilegios. A continuación, se detalla cómo se abordará este aspecto:

### 1. Enfoque en Usuarios Internos (No Clientes Externos)

Contexto:

El cliente mencionó que la mayoría de los ransomware y brechas de seguridad comienzan con ataques de ingeniería social dirigidos a empleados internos.

Alcance:

Usuarios finales internos: Empleados del almacén, logística y operaciones.

Exclusión: Clientes externos (usuarios de la tienda en línea de Amazon).

## 2. Pruebas de Ingeniería Social

### 2.1. Phishing Dirigido

Objetivo:

Simular ataques de phishing dirigidos a empleados internos para evaluar su susceptibilidad.

Métodos:

Envío de correos electrónicos falsos que imiten comunicaciones legítimas (ej: notificaciones de TI, actualizaciones de sistemas).

Inclusión de enlaces maliciosos o archivos adjuntos.

Credenciales proporcionadas:

El cliente proporcionará una lista de direcciones de correo electrónico de empleados del almacén y operaciones.

Limitaciones:

No se incluirán clientes externos ni usuarios de la tienda en línea de Amazon.

## **2.2. Simulación de Ataques de Credenciales**

Objetivo:

Evaluar si los empleados revelan credenciales o información sensible.

Métodos:

Páginas de inicio de sesión falsas (simulando el portal de TI o sistemas internos).

Llamadas telefónicas simuladas (vishing) para obtener información.

## **3. Escalada de Privilegios desde Cuentas de Usuario Final**

### **3.1. Simulación de Acceso Inicial**

Objetivo:

Evaluar cómo un atacante podría aprovechar una cuenta de usuario final comprometida.

Métodos:

Uso de credenciales proporcionadas por el cliente (simulando una cuenta de empleado del almacén).

Pruebas de movimientos laterales y escalada de privilegios dentro de la red.

### **3.2. Evaluación de Controles de Seguridad**

Objetivo:

Verificar que los controles de seguridad impidan la escalada de privilegios o el acceso no autorizado.

Métodos:

Uso de herramientas como Mimikatz, BloodHound o Metasploit para simular ataques.

## **4. Consideraciones Éticas y Legales**

### **4.1. Autorización del Cliente**

Descripción:

Todas las pruebas de ingeniería social y uso de credenciales de usuario final se realizarán con autorización explícita del cliente.

Documentación:

Contrato de compromiso y acuerdo de confidencialidad (NDA).

#### **4.2. Minimización de Impactos**

Descripción:

Las pruebas se diseñarán para evitar daños o molestias a los empleados.

Medidas:

Notificación posterior a los empleados afectados (si es necesario).

Capacitación en concienciación de seguridad después de las pruebas.

#### **4.3. Confidencialidad**

Descripción:

Los resultados de las pruebas se manejarán de manera confidencial.

Medidas:

Cifrado de datos y comunicaciones.

Dstrucción segura de información sensible después de la entrega del informe final.

### **5. Resumen de Pruebas en Usuarios Finales**

Prueba	Objetivo	Métodos
Phishing Dirigido	Evaluar susceptibilidad a ataques de phishing.	Correos electrónicos falsos, enlaces maliciosos.
Simulación de Credenciales	Verificar si los empleados revelan información.	Páginas de inicio de sesión falsas, vishing.
Escalada de Privilegios	Evaluar controles de seguridad internos.	Uso de herramientas como Mimikatz, BloodHound.

### **6. Exclusión de Clientes Externos**

Razón:

El alcance se centra en los sistemas internos y empleados, no en los usuarios de la tienda en línea de Amazon.

Impacto:

Las pruebas no afectarán a los clientes externos ni a la experiencia del usuario en la plataforma de comercio electrónico.

¿Está permitida la ingeniería social? Si es así, ¿es limitado?

Sí, la ingeniería social está permitida en el alcance de las pruebas de penetración para Nexus Plaza, pero con limitaciones específicas definidas por el cliente. Estas limitaciones están diseñadas para garantizar que las pruebas sean éticas, seguras y no causen daños o molestias innecesarias a los empleados. A continuación, se detalla cómo se abordará la ingeniería social:

## **1. Alcance de la Ingeniería Social**

### **1.1. Pruebas de Phishing Dirigido**

Objetivo:

Evaluar la susceptibilidad de los empleados a ataques de phishing.

Métodos:

Envío de correos electrónicos falsos que imiten comunicaciones legítimas (ej: notificaciones de TI, actualizaciones de sistemas).

Inclusión de enlaces maliciosos o archivos adjuntos.

Limitaciones:

Solo se dirigirá a empleados específicos (almacén, logística y operaciones).

No se incluirán clientes externos ni usuarios de la tienda en línea de Amazon.

### **1.2. Simulación de Ataques de Credenciales**

Objetivo:

Verificar si los empleados revelan credenciales o información sensible.

Métodos:

Páginas de inicio de sesión falsas (simulando el portal de TI o sistemas internos).

Llamadas telefónicas simuladas (vishing) para obtener información.

Limitaciones:

Solo se utilizarán sistemas de prueba proporcionados por el cliente.

No se almacenarán ni utilizarán credenciales reales de empleados.

### **1.3. Pruebas de Concienciación**

Objetivo:

Evaluar el nivel de concienciación de los empleados sobre seguridad.

Métodos:

Simulación de intentos de acceso físico a áreas restringidas (si es aprobado por el cliente).

Entrega de dispositivos USB maliciosos (simulados) en áreas comunes.

Limitaciones:

Solo en áreas no críticas y con supervisión del cliente.

## **2. Limitaciones y Condiciones**

### **2.1. Autorización Explícita**

Descripción:

Todas las pruebas de ingeniería social se realizarán con autorización por escrito del cliente.

Documentación:

Contrato de compromiso y acuerdo de confidencialidad (NDA).

### **2.2. Empleados Objetivo**

Descripción:

Las pruebas se limitarán a empleados específicos (almacén, logística y operaciones).

Exclusión:

No se incluirán clientes externos ni usuarios de la tienda en línea de Amazon.

### **2.3. Minimización de Impactos**

Descripción:

Las pruebas se diseñarán para evitar daños o molestias innecesarias a los empleados.

Medidas:

Notificación posterior a los empleados afectados (si es necesario).

Capacitación en concienciación de seguridad después de las pruebas.

### **2.4. Confidencialidad**

Descripción:



Los resultados de las pruebas se manejarán de manera confidencial.

Medidas:

Cifrado de datos y comunicaciones.

Destrucción segura de información sensible después de la entrega del informe final.

### 3. Resumen de Pruebas de Ingeniería Social

Prueba	Objetivo	Limitaciones
Phishing Dirigido	Evaluar susceptibilidad a ataques de phishing.	Solo empleados específicos; no clientes externos.
Simulación de Credenciales	Verificar si los empleados revelan información.	Uso de sistemas de prueba; no credenciales reales.
Pruebas de Concienciación	Evaluar concienciación sobre seguridad.	Solo en áreas no críticas y con supervisión.

### 4. Consideraciones Éticas

Transparencia:

Los empleados serán informados después de las pruebas (si es necesario) para evitar desconfianza o malestar.

Capacitación:

Se proporcionará capacitación en concienciación de seguridad a los empleados afectados para mejorar su resistencia futura.

Protección de Datos:

Toda la información recopilada se manejará de acuerdo con las normativas de protección de datos (ej: GDPR).

¿Se permiten la denegación de servicio y otros ataques disruptivos? Si es así, ¿hay límites respecto de cuándo se pueden realizar las pruebas disruptivas?

Sí, las pruebas de denegación de servicio (DoS) y otros ataques disruptivos están permitidos, pero con limitaciones estrictas definidas por el cliente. Estas limitaciones están diseñadas para minimizar el impacto en las operaciones críticas y garantizar que las pruebas no afecten negativamente a los sistemas de producción. A continuación, se detalla cómo se abordarán estas pruebas:

#### 1. Pruebas Disruptivas Permitidas

##### 1.1. Denegación de Servicio (DoS/DDoS)

Objetivo:

Evaluar la resistencia de los sistemas ante ataques que buscan agotar recursos (ej: ancho de banda, capacidad de procesamiento).

Métodos:

Simulación de tráfico malicioso utilizando herramientas como LOIC, Hping o Metasploit.

Pruebas de estrés en servidores y aplicaciones.

## **1.2. Pruebas de Carga**

Objetivo:

Verificar cómo los sistemas manejan cargas extremas de tráfico o solicitudes.

Métodos:

Uso de herramientas como JMeter, Gatling o Locust.

Simulación de picos de tráfico en aplicaciones web o APIs.

## **1.3. Simulación de Ataques de Ransomware**

Objetivo:

Evaluar la capacidad de los sistemas para detectar y mitigar ataques de ransomware.

Métodos:

Uso de herramientas de simulación como Cobalt Strike o scripts personalizados.

Pruebas en el entorno de desarrollo espejado (no en producción).

## **2. Limitaciones y Condiciones**

### **2.1. Ventanas de Mantenimiento**

Descripción:

Las pruebas disruptivas solo se realizarán durante las ventanas de mantenimiento programadas.

Horarios:

Viernes, sábados y domingos, entre las 2:00 a. m. y las 6:00 a. m.

Razón:

Minimizar el impacto en las operaciones críticas durante el horario laboral.

### **2.2. Entornos de Prueba**

Descripción:

Las pruebas disruptivas se realizarán principalmente en el entorno de desarrollo espejado proporcionado por el cliente.

Exclusión:

No se realizarán pruebas disruptivas en los sistemas de producción a menos que sea absolutamente necesario y con autorización explícita.

### **2.3. Supervisión del Cliente**

Descripción:

El equipo de TI del cliente supervisará las pruebas en tiempo real para detectar y mitigar cualquier impacto no deseado.

Coordinación:

Reuniones previas para definir los parámetros de las pruebas.

Comunicación constante durante las pruebas.

### **2.4. Duración Limitada**

Descripción:

Las pruebas disruptivas tendrán una duración limitada para evitar interrupciones prolongadas.

Ejemplo:

Pruebas de DoS: Máximo 30 minutos por sesión.

Pruebas de carga: Máximo 1 hora por sesión.

## **3. Resumen de Pruebas Disruptivas**

Prueba	Objetivo	Limitaciones
Denegación de Servicio (DoS)	Evaluar resistencia ante ataques de agotamiento.	Solo en ventanas de mantenimiento; duración limitada.
Pruebas de Carga	Verificar manejo de cargas extremas.	En entorno de desarrollo; supervisión del cliente.
Simulación de Ransomware	Evaluar detección y mitigación de ransomware.	Solo en entorno de desarrollo espejado.

## **4. Consideraciones Adicionales**

Minimización de Riesgos:

Las pruebas se diseñarán para evitar impactos no deseados en los sistemas de producción.

Comunicación con el Cliente:

Cualquier prueba disruptiva se coordinará previamente con el equipo de TI del cliente.

Plan de Contingencia:

Se establecerá un plan de contingencia para restaurar rápidamente los sistemas en caso de incidentes.

¿Existen dispositivos que puedan afectar los resultados de una prueba de penetración? De ser así, ¿cuáles?

Sí, existen dispositivos y configuraciones de red que pueden afectar los resultados de una prueba de penetración, ya sea limitando la visibilidad de vulnerabilidades, bloqueando actividades legítimas de prueba o generando falsos positivos. A continuación, se detallan los dispositivos más comunes que podrían influir en los resultados y cómo se abordarán:

## **1. Dispositivos que Afectan los Resultados**

### **1.1. Cortafuegos (Firewalls)**

Impacto:

Pueden bloquear el tráfico de escaneo o explotación, limitando la visibilidad de vulnerabilidades.

Reglas mal configuradas podrían generar falsos positivos o negativos.

Manejo:

Coordinar con el equipo de TI del cliente para desactivar temporalmente reglas restrictivas durante las pruebas.

Verificar las configuraciones del cortafuegos para identificar reglas innecesarias o redundantes.

### **1.2. Sistemas de Detección/Prevención de Intrusos (IDS/IPS)**

Impacto:

Pueden detectar y bloquear actividades de prueba, como escaneos de puertos o intentos de explotación.

Generan alertas que podrían interrumpir las pruebas o causar falsos positivos.

Manejo:

Desactivar temporalmente el IPS durante las pruebas (si es aprobado por el cliente).

Configurar el IDS para ignorar las direcciones IP utilizadas en las pruebas.

### **1.3. Balanceadores de Carga (Load Balancers)**

Impacto:

Pueden distribuir el tráfico de prueba entre múltiples servidores, dificultando la identificación de vulnerabilidades específicas.

Podrían ocultar servidores vulnerables detrás de configuraciones seguras.

Manejo:

Coordinar con el equipo de TI para desactivar temporalmente el balanceo de carga durante las pruebas.

Realizar pruebas directamente en los servidores individuales.

### **1.4. Proxies y Gateways de Seguridad**

Impacto:

Pueden filtrar o modificar el tráfico de prueba, limitando la efectividad de las pruebas.

Podrían bloquear herramientas de escaneo o explotación.

Manejo:

Configurar las herramientas de prueba para evitar el uso del proxy.

Realizar pruebas desde dentro de la red (si es posible).

### **1.5. Sistemas de Prevención de Pérdida de Datos (DLP)**

Impacto:

Pueden bloquear la transferencia de datos sensibles durante las pruebas, limitando la evaluación de vulnerabilidades.

Manejo:

Desactivar temporalmente las reglas de DLP durante las pruebas (si es aprobado por el cliente).

### **1.6. Redes Privadas Virtuales (VPN)**

Impacto:

Pueden limitar el acceso a ciertas áreas de la red, afectando la cobertura de las pruebas.

Manejo:

Utilizar credenciales de acceso proporcionadas por el cliente para acceder a redes restringidas.

## **1.7. Sistemas de Detección de Honeypots**

Impacto:

Pueden generar falsos positivos al simular sistemas vulnerables que no son parte de la infraestructura real.

Manejo:

Identificar y excluir honeypots del alcance de las pruebas.

## **2. Configuraciones que Afectan los Resultados**

### **2.1. Segmentación de Red (VLANs)**

Impacto:

La segmentación puede limitar el movimiento lateral dentro de la red, afectando la evaluación de la postura de seguridad.

Manejo:

Verificar las configuraciones de VLAN y ajustar las pruebas para evaluar la efectividad de la segmentación.

### **2.2. Políticas de Control de Acceso (ACL)**

Impacto:

Las ACL pueden bloquear el tráfico de prueba, limitando la visibilidad de vulnerabilidades.

Manejo:

Revisar y ajustar las ACL para permitir el tráfico de prueba (si es aprobado por el cliente).

### **2.3. Cifrado de Tráfico (SSL/TLS)**

Impacto:

El cifrado puede dificultar la inspección del tráfico y la identificación de vulnerabilidades.

Manejo:

Utilizar herramientas que soporten la inspección de tráfico cifrado (ej: Burp Suite, Wireshark con claves SSL).

### 3. Resumen de Dispositivos y Configuraciones

Dispositivo/Configuración	Impacto en las Pruebas	Manejo
Cortafuegos	Bloqueo de tráfico de prueba temporalmente.	Desactivar reglas restrictivas
IDS/IPS	Detección y bloqueo de actividades de prueba.	Desactivar IPS o configurar excepciones.
Balanceadores de Carga	Distribución de tráfico entre servidores.	Desactivar balanceo de carga temporalmente.
Proxies	Filtrado o modificación de tráfico.	Evitar el uso de proxies durante las pruebas.
DLP	Bloqueo de transferencia de datos sensibles.	Desactivar reglas de DLP temporalmente.
VPN	Limitación de acceso a redes restringidas.	Utilizar credenciales de acceso proporcionadas.
Honeypots	Generación de falsos positivos.	Identificar y excluir honeypots.
Segmentación de Red	Limitación del movimiento lateral.	Evaluar la efectividad de la segmentación.
ACL	Bloqueo de tráfico de prueba.	Ajustar ACL para permitir tráfico de prueba.
Cifrado SSL/TLS	Dificultad en la inspección de tráfico.	Usar herramientas con soporte para SSL/TLS.

### 4. Consideraciones Adicionales

Coordinación con el Cliente:

Cualquier ajuste en dispositivos o configuraciones se realizará en coordinación con el equipo de TI del cliente.

Minimización de Impactos:

Las modificaciones temporales se revertirán una vez finalizadas las pruebas.

Documentación:

Se registrarán todos los cambios realizados para garantizar la transparencia y trazabilidad.

¿Probar el acceso inalámbrico es parte de este compromiso?

De acuerdo con la información proporcionada por Nexus Plaza, el acceso inalámbrico no se menciona explícitamente como parte del alcance de las pruebas de penetración. Sin embargo, si el cliente tiene redes inalámbricas (Wi-Fi) en sus instalaciones, es importante evaluar su seguridad, ya que pueden ser un punto de entrada común para atacantes. A continuación, se detalla cómo se podría abordar este aspecto:

## **1. Evaluación del Acceso Inalámbrico**

### **1.1. Verificación de la Existencia de Redes Inalámbricas**

Objetivo:

Identificar si Nexus Plaza utiliza redes Wi-Fi en sus instalaciones.

Métodos:

Revisión de la documentación proporcionada por el cliente.

Escaneo pasivo de redes inalámbricas en las instalaciones (si es aprobado por el cliente).

### **1.2. Pruebas de Seguridad Wi-Fi (Si Aplicable)**

Objetivo:

Evaluar la seguridad de las redes inalámbricas y su configuración.

Métodos:

Escaneo de redes Wi-Fi: Identificar puntos de acceso (APs) y redes visibles.

Pruebas de autenticación: Verificar la fortaleza de los métodos de autenticación (ej: WPA2, WPA3).

Pruebas de cifrado: Evaluar la robustez del cifrado utilizado (ej: AES, TKIP).

Pruebas de fuerza bruta: Intentar descifrar contraseñas débiles.

Pruebas de rogue AP: Detectar puntos de acceso no autorizados.

## **2. Limitaciones y Condiciones**

### **2.1. Autorización del Cliente**

Descripción:

Las pruebas de acceso inalámbrico solo se realizarán si el cliente las aprueba explícitamente.

Documentación:



Incluir el acceso inalámbrico en el contrato de compromiso y alcance de trabajo.

## 2.2. Minimización de Impactos

Descripción:

Las pruebas se diseñarán para evitar interrupciones en las operaciones de la red inalámbrica.

Medidas:

Realizar pruebas fuera del horario laboral o en ventanas de mantenimiento.

Evitar pruebas disruptivas (ej: deautenticación de clientes).

## 2.3. Confidencialidad

Descripción:

Los resultados de las pruebas se manejarán de manera confidencial.

Medidas:

Cifrado de datos y comunicaciones.

Destrucción segura de información sensible después de la entrega del informe final.

## 3. Resumen de Pruebas de Acceso Inalámbrico

Prueba	Objetivo	Limitaciones
Escaneo de Redes Wi-Fi	Identificar puntos de acceso y redes visibles.	Solo si el cliente aprueba explícitamente.
Pruebas de Autenticación	Verificar la fortaleza de los métodos de autenticación.	Evitar interrupciones en operaciones críticas.
Pruebas de Cifrado	Evaluar la robustez del cifrado utilizado.	Realizar en ventanas de mantenimiento.
Pruebas de Fuerza Bruta	Descifrar contraseñas débiles.	Solo en redes de prueba o con autorización.
Detección de Rogue APs	Identificar puntos de acceso no autorizados.	Sin impacto en operaciones.

## 4. Consideraciones Adicionales

Coordinación con el Cliente:

Cualquier prueba de acceso inalámbrico se coordinará previamente con el equipo de TI del cliente.

Plan de Contingencia:

Se establecerá un plan de contingencia para restaurar rápidamente la conectividad en caso de incidentes.

Capacitación:

Si se identifican vulnerabilidades, se proporcionará capacitación al personal de TI para mejorar la seguridad de las redes inalámbricas.

## **5. Recomendación**

Dado que el acceso inalámbrico puede ser un vector de ataque común, se recomienda incluir estas pruebas en el alcance del compromiso, siempre que el cliente lo apruebe. Esto permitirá una evaluación más completa de la postura de seguridad de Nexus Plaza.

¿Los servicios web están incluidos en el alcance de las pruebas?

Sí, los servicios web están incluidos en el alcance de las pruebas de penetración para Nexus Plaza, ya que son un componente crítico de su infraestructura, especialmente considerando que Nexus Plaza es una empresa minorista en línea con una fuerte dependencia de aplicaciones web para su comercio electrónico y operaciones internas. A continuación, se detalla cómo se abordarán las pruebas de seguridad en los servicios web:

### **1. Servicios Web a Probar**

#### **1.1. Aplicaciones Web de Comercio Electrónico**

Descripción:

Plataformas web utilizadas por los clientes para realizar compras, consultar inventario y gestionar pedidos.

Objetivo:

Identificar vulnerabilidades como inyecciones SQL, cross-site scripting (XSS), y fallos de autenticación.

Métodos:

Escaneo automatizado con herramientas como Burp Suite, OWASP ZAP o Acunetix.

Pruebas manuales de explotación de vulnerabilidades.

#### **1.2. Portales Internos**

Descripción:

Aplicaciones web utilizadas por empleados para gestionar inventario, logística y operaciones.

Objetivo:

Evaluar la seguridad de las interfaces y la integridad de los datos.

Métodos:

Pruebas de autenticación y autorización.

Verificación de configuraciones seguras (ej: headers HTTP, cifrado SSL/TLS).

### **1.3. APIs**

Descripción:

Interfaces de programación de aplicaciones (APIs) utilizadas para la comunicación entre sistemas (ej: inventario, envíos).

Objetivo:

Identificar vulnerabilidades como inyecciones, autenticación débil o exposición de datos sensibles.

Métodos:

Pruebas de fuzzing con herramientas como Postman o SoapUI.

Análisis de respuestas y manejo de errores.

## **2. Tipos de Pruebas en Servicios Web**

### **2.1. Pruebas de Vulnerabilidades Comunes**

Inyecciones SQL:

Verificar si es posible manipular consultas a la base de datos.

Cross-Site Scripting (XSS):

Evaluar si se pueden ejecutar scripts maliciosos en el navegador del usuario.

Cross-Site Request Forgery (CSRF):

Verificar si es posible realizar acciones no autorizadas en nombre de un usuario autenticado.

Fallas de Autenticación y Autorización:

Evaluar la robustez de los mecanismos de autenticación y control de acceso.

### **2.2. Pruebas de Configuración**

Cifrado SSL/TLS:

Verificar que los certificados sean válidos y que se utilicen protocolos seguros.

Headers de Seguridad:

Evaluar la presencia y configuración de headers como Content Security Policy (CSP), X-Content-Type-Options, y Strict-Transport-Security (HSTS).

### **2.3. Pruebas de Carga y Estrés**

Objetivo:

Evaluar cómo los servicios web manejan cargas extremas de tráfico o solicitudes.

Métodos:

Uso de herramientas como JMeter, Gatling o Locust.

Simulación de picos de tráfico en aplicaciones web o APIs.

## **3. Limitaciones y Condiciones**

### **3.1. Entornos de Prueba**

Descripción:

Las pruebas se realizarán principalmente en el entorno de desarrollo espejado proporcionado por el cliente.

Exclusión:

No se realizarán pruebas invasivas en los sistemas de producción a menos que sea absolutamente necesario y con autorización explícita.

### **3.2. Horarios de Prueba**

Descripción:

Las pruebas disruptivas (ej: pruebas de carga) se realizarán durante las ventanas de mantenimiento programadas.

Horarios:

Viernes, sábados y domingos, entre las 2:00 a. m. y las 6:00 a. m.

### **3.3. Supervisión del Cliente**

Descripción:

El equipo de TI del cliente supervisará las pruebas en tiempo real para detectar y mitigar cualquier impacto no deseado.

Coordinación:

Reuniones previas para definir los parámetros de las pruebas.

Comunicación constante durante las pruebas.

## 4. Resumen de Pruebas en Servicios Web

Prueba	Objetivo	Limitaciones
Inyecciones SQL	Verificar manipulación de consultas a la base de datos.	Solo en entorno de desarrollo espejado.
Cross-Site Scripting (XSS)	Evaluar ejecución de scripts maliciosos.	Pruebas no disruptivas en horario laboral.
Pruebas de Carga	Verificar manejo de cargas extremas.	Solo en ventanas de mantenimiento.
Configuración SSL/TLS	Evaluar robustez del cifrado.	Sin impacto en operaciones críticas.

## 5. Consideraciones Adicionales

### Minimización de Impactos:

Las pruebas se diseñarán para evitar interrupciones en los sistemas de producción.

### Comunicación con el Cliente:

Cualquier prueba en servicios web se coordinará previamente con el equipo de TI del cliente.

### Documentación:

Se registrarán todos los cambios realizados para garantizar la transparencia y trazabilidad.

Este enfoque garantiza que las pruebas en servicios web sean efectivas y seguras, respetando las preocupaciones del cliente sobre la disponibilidad y estabilidad de sus sistemas críticos.

¿Los empleados conocen las pruebas y el plazo en que se realizarán?

De acuerdo con la información proporcionada por Nexus Plaza, los empleados no serán notificados sobre las pruebas de penetración, excepto por el personal de TI directamente responsable del monitoreo de los sistemas de operaciones y logística. Esta decisión se tomó para garantizar que las pruebas simulen condiciones realistas y evalúen la efectividad de los controles de seguridad sin sesgos. A continuación, se detalla cómo se manejará este aspecto:

### 1. Notificación Limitada a Personal Específico

#### 1.1. Personal de TI Responsable

##### Descripción:

Solo el personal de TI directamente responsable del monitoreo de los sistemas de operaciones y logística será notificado sobre las pruebas.

##### Razón:

Permitir la supervisión en tiempo real de las pruebas.

Garantizar que cualquier impacto no deseado se detecte y mitigue rápidamente.

## **1.2. Gerentes y Contactos Principales**

Descripción:

El director de TI, el gerente de almacén y el gerente de operaciones serán los contactos principales para coordinar y recibir actualizaciones sobre las pruebas.

Razón:

Mantener una comunicación clara y efectiva durante el compromiso.

Asegurar que las pruebas se ajusten a los objetivos del cliente.

## **2. Empleados Finales No Notificados**

### **2.1. Pruebas de Ingeniería Social**

Descripción:

Las pruebas de phishing y otros ataques de ingeniería social se realizarán sin notificar a los empleados finales.

Razón:

Evaluar la susceptibilidad real de los empleados a este tipo de ataques.

Identificar áreas de mejora en la concienciación sobre seguridad.

### **2.2. Pruebas en Sistemas de Producción**

Descripción:

Las pruebas no disruptivas en sistemas de producción se realizarán sin notificar a los empleados finales.

Razón:

Evitar cambios en el comportamiento que puedan afectar los resultados de las pruebas.

## **3. Plazo y Horarios de Pruebas**

### **3.1. Plazo General**

Descripción:

El compromiso comenzará dos semanas después de la firma del contrato y tendrá una duración de 60 días.

Comunicación:

Solo los contactos principales (director de TI, gerentes) conocerán el plazo completo.

### **3.2. Ventanas de Mantenimiento**

Descripción:

Las pruebas disruptivas (ej: DoS, pruebas de carga) se realizarán durante las ventanas de mantenimiento programadas.

Horarios:

Viernes, sábados y domingos, entre las 2:00 a. m. y las 6:00 a. m.

Comunicación:

Solo el personal de TI responsable será notificado sobre estas ventanas.

## **4. Consideraciones Éticas y Legales**

### **4.1. Autorización del Cliente**

Descripción:

Todas las pruebas se realizarán con autorización explícita del cliente, documentada en el contrato de compromiso.

Documentación:

Incluir detalles sobre la no notificación a empleados finales.

### **4.2. Minimización de Impactos**

Descripción:

Las pruebas se diseñarán para evitar daños o molestias innecesarias a los empleados.

Medidas:

Notificación posterior a los empleados afectados (si es necesario).

Capacitación en concienciación de seguridad después de las pruebas.

### **4.3. Confidencialidad**

Descripción:

Los resultados de las pruebas se manejarán de manera confidencial.

Medidas:

Cifrado de datos y comunicaciones.

Destrucción segura de información sensible después de la entrega del informe final.

## 5. Resumen de Comunicación y Notificación

Grupo	Notificación	Detalles
Personal de TI	Sí	Solo personal responsable de monitoreo.
Gerentes y Contacto	Sí	Director de TI, gerente de almacén y operaciones.
Empleados Finales	No	Pruebas de ingeniería social y sistemas de producción.

## 6. Recomendación

Para garantizar que las pruebas sean éticas y efectivas, se recomienda:

Capacitación Posterior:

Después de las pruebas, proporcionar capacitación en concienciación de seguridad a los empleados afectados.

Transparencia Limitada:

Informar a los empleados sobre las pruebas solo si es necesario para mejorar la seguridad a largo plazo.

## Explicación de la Línea de Tiempo

*Inicio del Compromiso:*

Las pruebas comenzarán 2 semanas después de la firma del contrato, lo que permite tiempo para la planificación y coordinación inicial.

*Duración del Compromiso:*

El compromiso tendrá una duración total de 60 días, durante los cuales se realizarán las pruebas y se entregará el informe final.

*Ventanas de Pruebas:*

Pruebas disruptivas (ej: DoS, pruebas de carga) se realizarán únicamente durante las ventanas de mantenimiento (viernes a domingo, 2:00 a. m. – 6:00 a. m.).

Pruebas no disruptivas (ej: escaneos, pruebas de vulnerabilidades) se realizarán durante el horario laboral normal, siempre que no afecten las operaciones.

*Entregables:*



Se proporcionará un informe de actualización semanal a los contactos principales (director de TI, gerentes).

El informe final se entregará al finalizar los 60 días, resumiendo los hallazgos, riesgos y recomendaciones.

*Prueba de Línea de Tiempo:*

Inicio: 2 semanas post-contrato; duración: 60 días.

Pruebas disruptivas: viernes a domingo (2:00 a. m. – 6:00 a. m.); no disruptivas: horario laboral. Informes semanales y final en 60 días.

*Ubicación de la Prueba:*

Pruebas remotas desde la VLAN aislada del departamento de TI y entorno de desarrollo espejado. Exclusión de sistemas de producción y clústeres de Amazon.

*Ventanas de tiempo para la prueba (horas del día)*

*Ventanas de Tiempo para la Prueba:*

Pruebas disruptivas: viernes a domingo (2:00 a. m. – 6:00 a. m.). Pruebas no disruptivas: horario laboral normal.

*Método de comunicación preferido*

*Método de Comunicación Preferido:*

Informes semanales y teleconferencias con el director de TI, gerente de almacén y gerente de operaciones.

*Controles de seguridad que potencialmente podrían detectar o evitar las pruebas*

*Controles de Seguridad que Podrían Detectar o Evitar las Pruebas:*

Cortafuegos, IDS/IPS, DLP, y sistemas de detección de honeypots. Coordinación con el equipo de TI para ajustar configuraciones durante las pruebas.

*Manejo de datos sensibles*

*Manejo de Datos Sensibles:*

Cifrado de datos y comunicaciones; destrucción segura de información sensible tras la entrega del informe final.

*Direcciones IP o redes desde las que se originarán las pruebas*

*Direcciones IP o Redes de Origen de las Pruebas:*

VLAN aislada del departamento de TI (172.16.33.0/30) y entorno de desarrollo espejado.

*Tipos de pruebas permitidas o no permitidas*

AI-generated, for reference only