Prueba - Documentación y Reportes de Incidentes

Incidente de Seguridad en VPN de Acceso Remoto

Alumno: Bladimir Alejandro Burgos Conejeros

Curso: Seguridad en Redes Informáticas

Fecha: Septiembre 2025

# Requerimiento 1: Reconocimiento y análisis del escenario

Se detectó un acceso no autorizado a un servidor interno desde una IP pública externa a través de la VPN de Acceso Remoto (ASA). Las credenciales de un usuario legítimo fueron utilizadas desde una ubicación inusual, evidenciando un posible robo de credenciales.  
  
Posibles causas:  
- Robo de credenciales vía phishing.  
- Falta de MFA en el acceso VPN.  
- Monitoreo insuficiente de logs del ASA.  
  
Técnicas de ataque:  
- Phishing.  
- Uso indebido de VPN (VPN hijacking).  
- Movimiento lateral tras autenticación.  
  
Brechas de configuración:  
- VPN sin MFA.  
- Sin geobloqueo ni restricción de IPs.  
- Logs sin monitoreo en tiempo real.

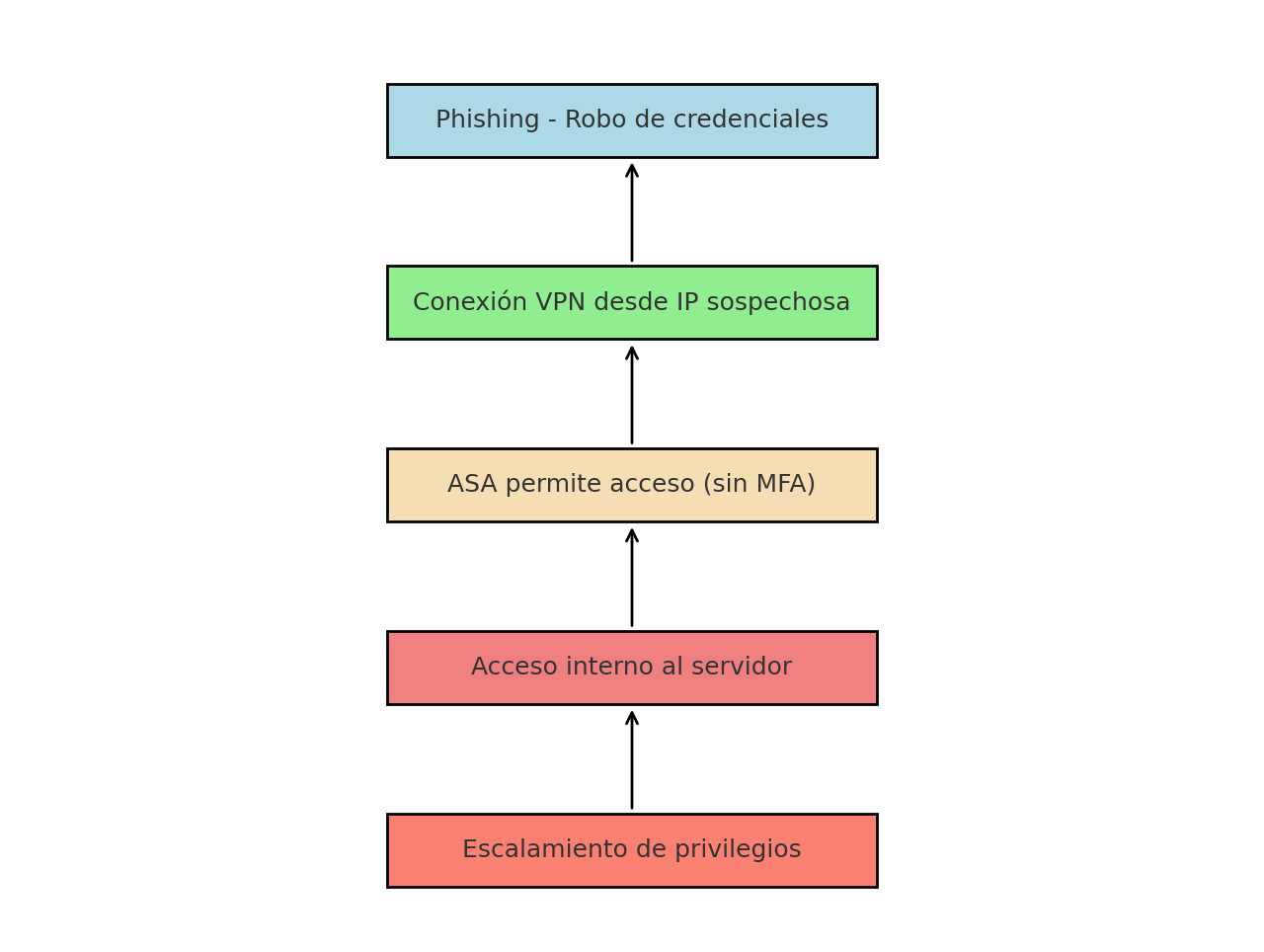
# Requerimiento 2: Políticas fallidas y mejores prácticas

Políticas que fallaron:  
- Acceso remoto sin MFA.  
- Logs de ASA no monitoreados.  
- Sin control de IPs autorizadas.  
- Capacitación insuficiente en phishing.  
  
Mejores prácticas recomendadas:  
- Implementar MFA obligatorio en VPN.  
- Alertas SIEM para accesos desde IPs no habituales.  
- Listas blancas de IPs y geobloqueo.  
- Capacitación en phishing.  
- Monitoreo continuo de logs ASA.

# Requerimiento 3: Causas y consecuencias + Diagrama de flujo

|  |  |  |  |
| --- | --- | --- | --- |
| **Causa** | **Consecuencia** | **Evidencia** | **Control Correctivo** |
| Robo de credenciales (phishing) | Uso no autorizado de VPN | Logs ASA – acceso desde IP inusual | MFA + capacitación |
| Falta de MFA en VPN | Acceso exitoso con usuario/clave | Registro de login sin 2FA | Habilitar MFA |
| Logs no revisados en tiempo real | Tiempo extra para el atacante | No hubo alerta inmediata | SIEM + alertas |
| Falta de restricción geográfica | Conexión desde IP externa | IP origen ≠ rangos corporativos | Geo-bloqueo / lista blanca |

Diagrama de flujo del ataque:



# Requerimiento 4: Informes

## Informe conciso (ejecutivo)

Incidente: Acceso no autorizado a servidor interno vía VPN con credenciales robadas.  
Causa raíz: Robo de credenciales + ausencia de MFA.  
Impacto: Riesgo de fuga de datos.  
Acciones inmediatas:  
- Bloqueo de la cuenta comprometida.  
- Cambio de credenciales.  
- Revisión de accesos en ASA.  
Acciones futuras:  
- Implementar MFA.  
- Reforzar monitoreo con SIEM.  
- Capacitación contra phishing.

## Informe detallado (técnico)

1. Resumen del incidente: Acceso no autorizado a servidor interno desde IP externa vía VPN.  
2. Cronología: robo de credenciales → login desde IP no autorizada → acceso interno → escalamiento de privilegios.  
3. Evidencias: logs ASA con IP sospechosa, registro de login VPN inusual.  
4. Causas y consecuencias: ver tabla incluida.  
5. Brechas detectadas: falta de MFA, ausencia de monitoreo, sin restricción geográfica.  
6. Recomendaciones: MFA, SIEM, geobloqueo, capacitación en phishing.  
7. Plan de seguimiento/post:  
- Responsable: Equipo TI.  
- Acciones inmediatas: bloqueo de cuentas, revisión de logs.  
- Mediano plazo: implementar MFA, reforzar monitoreo.  
- Largo plazo: auditorías semestrales y simulacros de phishing.