# Laboratorio #13: Escaneo de vulnerabilidades

**Juliana Torres Aarón**

## Objetivos del Laboratorio:

El objetivo de este taller es que los participantes adquieran habilidades prácticas en el uso de herramientas de escaneo de vulnerabilidades, identifiquen debilidades en sistemas informáticos y comprendan las medidas necesarias para mitigar los riesgos.

| Caso | Activos | Amenazas | Vulnerabilidad | Impactos | Probabilidad | Niveles de Riesgo | Medidas de tratamiento |
|---|---|---|---|---|---|---|---|
| 1 | Sistema academico web, Credenciales de acceso de los usuarios | Phishing | 1. Ausencia de autenticación en dos pasos, 2. Ausencia de capacitación en ciberseguridad | Medio | Alto | Alto | Implementar 2FA en el sistema académico. |
| 2 | Archivos clínicos, copia de seguridad | Ransomware | 1. Software antivirus caducado, 2. Falta de respaldo actualizado | Alto | Alto | Alto | 1. Actualizar el antivirus, 2. segmentar la red |
| 3 | Cámaras de seguridad, Fiemware | Acceso no autorizado | 1. Firmware desactualizado, 2. falta de gestión de contraseña | Alto | Medio | Alto | 1. Actualizar firmware de cámaras a versiones seguras, 2. Cambiar inmediatamente todas las contraseñas por defecto |
| 4 | Bases de datos con información personal, Reputación institucional | Acceso no autorizado | 1. Sin registros de logs ni auditorías, 2. Acceso sin control de privilegios | Alto | Alto | Alto | 1. Acceso sin control de privilegios, 2. Clasificar la información según sensibilidad. |
| 5 | Sitio web institucional, Infraestructura de servidor web | DoS | 1. Falta de protección DoS, 2. Monitoreo en tiempo real ausente | Alto | Alto | Alto | 1. Implementar firewall de aplicaciones web (WAF) y protección DoS, 2. Definir roles de monitoreo y respuesta inmediata. |