

PRACTICA # 2

NOMBRE: Univ. Delgadillo Quispe Erika Norma

AUXILIAR: Univ. Aldrin Roger Perez Miranda

DOCENTE: M. Sc. Ing. Javier Alexander Duran Miranda

DETERMINAR EL ALCANCE

El análisis de riesgos se centra en la empresa Financiera Oportunidad, dedicada a ofrecer servicios financieros. El alcance incluye la infraestructura tecnológica, el personal del área de TI y los sistemas de información que manejan datos confidenciales de clientes, transacciones y respaldos. El objetivo es identificar y evaluar los riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la información. El Dpto. de seguridad informática en la Financiera Oportunidad.

IDENTIFICAR LOS ACTIVOS

| Tipo de Activo | Descripción |
|-----------------|---|
| Información | *Datos de clientes, transacciones financieras, respaldos de bases de datos. |
| Infraestructura | *Servidores, equipos de red, CPD principal y copias de seguridad. |
| Software | *Sistemas financieros, antivirus, firewall, sistemas operativos Linux. |
| Personal | *Jefe de TI, responsable de redes, practicantes de informática. |
| Servicios | *Acceso remoto (puerto 22), red interna, copias de respaldo, servicio 24/7. |

VALORAR LOS ACTIVOS

| ACTIVO | IMPORTANCIA |
|---|-------------------|
| Dispositivos (Computadoras $D=4+I=4+C=3 \Rightarrow 11$) $\rightarrow 11/3 = 3,66 \rightarrow 4$ | ALTA |
| Software Y Aplicaciones (Sistema institucionales $D=5+I=5+C=5 \Rightarrow 15$) $\rightarrow 15/3 = 5$ (Antivirus y Antimalware $D=3+I=3+C=3 \Rightarrow 9$) $\rightarrow 9/3 = 3$ | MUY ALTA MEDIA |
| Personal (funcionarios $D=4+I=3+C=3 \Rightarrow 10$) $\rightarrow 10/3 = 3,33 \rightarrow 3$ | MEDIA |
| Telecomunicaciones (redes $D=4+I=4+C=4 \Rightarrow 12$) $\rightarrow 12/3 = 4$ | ALTA |

IDENTIFICAR LAS AMANEZAS

| Amenaza | Descripción |
|-----------------------|--|
| Ciberataques externos | *Intentos de acceso no autorizado, ransomware o robo de datos. |
| Errores humanos | *Instalación de software no autorizado o eliminación accidental de archivos. |
| Fallas técnicas | *Daño en servidores o pérdida de energía eléctrica. |
| Desastres naturales | *Incendios o inundaciones que afecten el CPD. |
| Malware / virus | *Infección por uso de antivirus gratuito o no actualizado. |

5. Identificar las Vulnerabilidades

| Vulnerabilidad | Descripción |
|-------------------------------------|--|
| Instalación libre de software | *Posibilidad de introducir programas maliciosos. |
| Bitácoras deshabilitadas | *Impide rastrear incidentes de seguridad. |
| Antivirus gratuito | *Baja capacidad de detección de amenazas avanzadas. |
| Firewall con puerto 22 abierto | *Riesgo de accesos remotos no autorizados. |
| Falta de supervisión a practicantes | *Posibilidad de fuga de información o errores involuntarios. |

EVALUAR RIESGO

Activo: Software y Aplicaciones

| N.º | DESCRIPCION DEL RIESGO | PROBABILIDAD | IMPACTO | | | | RIESGO |
|-----|---|--------------|------------|--------|-----------|-------|--------|
| 1 | Computadoras de usuarios instala cualquier software | 4 | Financiero | Imagen | Operativo | Total | 20 |
| | | | 5 | 5 | 5 | 5 | |
| 2 | Aplicación de antivirus gratuito | 4 | 4 | 4 | 4 | 4 | 16 |

| N.º | DESCRIPCION DE RIESGO | PROBABILIDAD | IMPACTO | ACTIVO |
|-----|---|--------------|---------|-----------------------|
| 1 | Computadoras de usuarios instala cualquier software | 4 | 5 | Software y Aplicación |
| 2 | Aplicación de antivirus gratuito | 4 | 4 | Software y Aplicación |

| | | | | | |
|--------------|--------------|----------|-----------|----------|--------------|
| MUY ALTO (5) | MEDIO | MEDIO | ALTO | 1 | MUY ALTO |
| ALTO (4) | BAJO | MEDIO | ALTO | 2 | MUY ALTO |
| MEDIO (3) | MUY BAJO | BAJO | MEDIO | ALTO | ALTO |
| BAJO (2) | MUY BAJO | BAJO | BAJO | MEDIO | MEDIO |
| MUY BAJO (1) | MUY BAJO | MUY BAJO | MUY BAJO | BAJO | MEDIO |
| | MUY BAJO (1) | BAJO (2) | MEDIO (3) | ALTO (4) | MUY ALTO (5) |

TRATAR EL RIESGOS

| RIESGO | CONTRAMEDIDAS |
|---|---|
| Computadoras de usuarios instala cualquier software | Restringir permisos de instalación solo a TI; bloquear software desconocido |
| Aplicación de antivirus gratuito | implementar soluciones de seguridad pagadas con soporte y actualizaciones |

