Evaluación de Riesgos para el Sistema de la Universidad de California

1. Lista de Inventario de Activos

Categorías de activos:

- **Hardware:**
  - Servidores de bases de datos y almacenamiento en centros de datos.
  - Computadoras personales utilizadas por estudiantes, docentes y personal administrativo.
  - Equipos de red: routers, switches, firewalls.
- **Software:**
  - Sistemas de gestión académica y administrativa (Canvas, sistemas financieros).
  - Herramientas de ciberseguridad (antivirus, sistemas de detección de intrusos).
  - Aplicaciones de investigación científica.
- **Datos:**
  - Registros personales y académicos de estudiantes.
  - Datos de investigación (proyectos científicos, bases de datos sensibles).
  - Información financiera (presupuestos, nóminas, becas).
- **Personal:**
  - Equipo de TI responsable de la infraestructura tecnológica.
  - Docentes e investigadores que generan y gestionan información crítica.
  - Estudiantes y colaboradores externos que acceden a sistemas.

2. Identificación de Amenazas Potenciales

Amenazas externas:

- **Ataques cibernéticos:**
  - Phishing: Engaños para capturar credenciales de usuarios.
  - Ransomware: Bloqueo de sistemas mediante encriptación.
  - Ataques DDoS: Sobrecarga de servidores y pérdida de disponibilidad.
- **Desastres naturales:**
  - Terremotos, incendios o inundaciones que dañen infraestructura crítica.
- **Robo físico:**
  - Sustitución o extracción de dispositivos de centros de datos o campus.

Amenazas internas:

- **Errores humanos:**
  - Configuración incorrecta de sistemas o eliminación accidental de datos.
- **Acceso indebido:**
  - Abuso de privilegios por parte de empleados o estudiantes.
- **Uso no autorizado:**
  - Instalación de software no aprobado o manejo inadecuado de información.

3. Identificación de Vulnerabilidades

Vulnerabilidades detectadas:

- **Hardware:**
  - Ausencia de redundancia en sistemas críticos.
  - Falta de acceso restringido en áreas de servidores.
- **Software:**
  - Aplicaciones sin parches actualizados.
  - Ausencia de autenticación multifactor en sistemas administrativos.
- **Datos:**
  - Bases de datos sin cifrado adecuado.
  - Registro insuficiente de accesos a información sensible.

- **Personal:**
    - Falta de capacitación en ciberseguridad.
    - Políticas de acceso no revisadas periódicamente.

4. Evaluación de Probabilidad e Impacto

Riesgo	Probabilidad	Impacto	Calificación
Acceso no autorizado	Alta	Compromiso crítico	Alto
Malware en sistemas críticos	Media	Interrupción total	Alto
Desastres naturales	Baja	Daño físico	Medio
Contraseñas débiles	Alta	Violación de datos	Alto
Errores humanos	Media	Pérdida operativa	Medio

5. Priorización de Riesgos

1. **Alta prioridad:**
    - Acceso no autorizado.
    - Malware en sistemas críticos.
    - Contraseñas débiles.
2. **Media prioridad:**
    - Errores humanos.
    - Desastres naturales.
3. **Baja prioridad:**
    - Robo físico (cuando el acceso físico está asegurado con controles).

Plan de acción inicial:

1. Implementar autenticación multifactor en todos los sistemas críticos.
2. Realizar simulaciones de incidentes para capacitar al personal.
3. Desarrollar un plan de recuperación ante desastres que cubra sistemas y datos clave.