CASO PRÁCTICO

En el análisis de riesgos se deben responder las preguntas:
¿A qué riesgos en la seguridad informática está expuesta la Universidad?

1. **Accesos no autorizados:**

- Los estudiantes pueden tener contraseñas débiles y desactivado el sistema de autenticación, de esta manera los atacantes pueden obtenerlas mediante sitios web inseguros y programas maliciosos.
- Las personas no autorizadas pueden entrar al sistema de manera física si la universidad no cuenta con medidas de seguridad, tales como cámaras y controles de acceso.

2. Riesgo de virus y malware:

- Los estudiantes pueden conectar dispositivos como discos duros externos y unidades USB que contengan malware y virus a las computadoras de la universidad afectando la integridad y confidencialidad de los usuarios además de que puede propagarse como un virus de gusano hacia las demás máquinas y de esta manera ya no solo afectará a los usuarios sino a la universidad.
-

3. Pérdida de datos:

- En algún momento puede haber un desastre natural que perjudique los datos de los servidores ya que son discos rígidos, disquetes, etc. que tiene la universidad.
- Errores cometidos por los estudiantes, cómo realizar un formateo del sistema por una tarea a realizar de manera rápida y sin escuchar al profesor.
- Los robos de hardware que puede haber con las computadoras como (mouse, algún cable, teclado, disco duro, etc.) además de los notebooks perjudican a la universidad ya sea con la información, seguridad u inactividad de la computadora.
-

4. Interrupción del servicio:

- Si en algún momento hay fallos en el suministro de energía claro está que un UPS 12 KVA no bastaría para alimentar a los 20 servidores de red que están en uso esto causaría una afectación al hardware de los servidores perjudicando su ralentización de los sistemas que estén con el servidor.
-

5. Discos rígidos:

- En este riesgo sería el uso excesivo sin cuidado(golpes)o también el uso en una temperatura ya sea muy alta o baja.
-

6. Copias de seguridad:

- Los backups que se realizan en los disquetes pueden estar hechos de manera incorrecta debido a su desuso en la actualidad, lo cual generaría ausencia de recuperación de datos, en algunos casos que hasta esta sea permanente.
-

7. Utilización de programas crackeados:

- La universidad al tener diversos programas o utilitarios entre ellos (Office, Autocad, Corel Draw, Netscape) podría tener problemas legales por utilizar dichos programas crackeados (sin licencia original).

¿Qué probabilidad hay de que se produzca un incidente de seguridad para cada uno de los riesgos encontrados?

Nivel de impacto / Urgencia	Alto	Medio	Bajo
Acceso no autorizado	5	4	4
Riesgo de virus y malware	5	4	2
Pérdida de datos	5	4	2
Interrupción del servicio	4	2	2
Discos rígidos	5	4	2
Copias de seguridad	6	5	4
Utilización de programas crackeados	6	5	4

¿Qué nos arriesgamos a perder en caso de ocurrir cada uno de los riesgos?

- Se pueden perder los datos de las personas que integran la Universidad, los cuales pueden ser muy confidenciales.
- Al querer solucionar alguno de los riesgos se pierde tiempo en las clases o procesos que se quieran realizar al utilizar los servicios.
- Hacer uso indebido de los accesos no autorizados al sistema, donde se pueden tener problemas al dañar el nombre de la institución, además de tener problemas legales.
- La universidad podría ser víctima de un ataque informático que dañe o interrumpa los sistemas y servicios informáticos, lo que podría afectar el funcionamiento normal de la universidad y causar daños económicos y de reputación.
- La pérdida de hardware, como computadoras y dispositivos de red, podría resultar en una interrupción del trabajo de la universidad y la pérdida de información valiosa.

INTEGRANTES:
- Montalvan Pintado Edilsa
- Mayanga Pupuche Anthony
- Neyra Quesquen Renzo