Actividad 2 - Análisis de Riesgos en Contextos Reales

Cristóbal Suárez Abad

Seguridad y alta disponibilidad

2º ASIR

Instrucciones

1. **Piensa en un contexto real** (puede ser en casa, en un instituto, en una empresa o en una situación cotidiana con tecnología).
    - Ejemplo: “Uso de la red WiFi en la biblioteca”, “Ordenadores en el aula de informática”, “Servidor web de una empresa”, “Uso de un pendrive en un equipo de oficina”.

Clase de Informática impartida en dependencias del Ayuntamiento.

2. **Rellena la siguiente tabla** analizando tu contexto:

Contexto	**Vulnerabilidades**	**Amenazas**	**Contramedidas**	**Gestión del Riesgo**
Ejemplo: Ordenadores en el aula de informática	Contraseñas débiles en los usuarios, software sin actualizar	Un alumno instala malware, robo de credenciales	Políticas de contraseñas, antivirus actualizado, bloqueos de instalación	Riesgo moderado: se acepta el uso con controles periódicos, pero hay que revisar actualizaciones mensuales

Intenta extenderte más que en este ejemplo

A) Contexto:

Clase de Informática para Principiantes impartida en dependencias del Ayuntamiento.

Vulnerabilidades	Amenazas	Contramedidas	Gestión del Riesgo
1. Configuración de equipos: Para facilitar la clase, los equipos pueden tener permisos de administrador o estar mal configurados (firewalls abiertos, etc), permitiendo la instalación de software no autorizado y aumentando. El software puede ser anticuado (falta de licencias o solo se dispone de hardware obsoleto), pueden faltar actualizaciones y/o no disponer de antivirus. **2. Accesibilidad a elementos físicos:** Los puertos USB y Ethernet están al alcance de los alumnos, sin bloqueo físico. Las dependencias disponen de poco o nulo control de acceso, los equipos no disponen de carcasas con cierres de seguridad o sistemas de anclaje a la mesa.	**1. Amenaza Externa**: - Atacante aprovecha debilidades de sistema y software desactualizado, y mala configuración del firewall para acceder a la red interna del Ayuntamiento a través de un equipo del aula. - Robo de material fuera del horario lectivo. **2. Amenaza Interna**: - Un alumno, sin mala intención, conecta un pendrive infectado con malware que tenía en casa para guardar su trabajo, propagando un virus a la red. - Robo de componentes de los ordenadores durante las clases. - Un alumno, con más conocimientos de la cuenta, intenta acceder a carpetas de red restringidas del Ayuntamiento por curiosidad. - Alumno consigue la contraseña personal de un	**1. Configuración de Equipos:** **-** Perfiles de usuario restringidos: Cada alumno usa un usuario con permisos limitados que impide instalar software o modificar configuraciones críticas. - Creación de cuentas de correo exclusivas para el entorno académico. - Software de control de aula y listas de permiso**:** Herramienta que permite al profesor monitorizar las pantallas y restringir el uso a aplicaciones específicas de la clase (navegador, procesador de texto). - Configuración de equipos de Red: Establecimiento de firewall y de VLAN que “separe” las redes del aula y el Ayuntamiento. También se puede configurar los switches con la desactivación de DTP, establecer seguridad por puertos (solo permitir ciertas	Se intenta evitar el riesgo lo máximo posible, como por ejemplo con el bloque de los puertos, tanto a nivel físico como lógico. Lo más importante es evitar que un atacante pueda aprovechar alguna vulnerabilidad en los equipos del aula para llevar a cabo acciones en la red del Ayuntamiento. Otro punto donde también es importante eliminar el riesgo por completo es en la vulnerabilidad de las cuentas de los alumnos. Por ello es mejor evitar que usen las personales.

3. Falta de concienciación de los usuarios: Los alumnos son principiantes y pueden no reconocer un correo de phishing (otros fraudes de ingeniería social) o los riesgos de conectar un dispositivo USB personal. Tampoco saben de la importancia de usar claves seguras para sus cuentas (email, redes sociales, etc). **4. Red compartida**: La red WiFi o cableada es la misma que usa el personal municipal para otras tareas, sin segmentación.	compañero y le roba su email.	MACs), obligar a usar Ethernet, etc. - Configuración de PCs: uso de software libre (Linux) en vez de propietario. Programar actualizaciones de los equipos y del software. **2. Seguridad Física:** - Bloqueo a nivel de software de puertos USB y Ethernet. - Uso de bloqueadores físicos de puertos USB y Ethernet. - Adquirir, en la medida de los posible, equipos cuyas carcasas tengan agujero para candados. - Instalar una buena cerradura para la puerta del aula.	