Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | 2 | Prevención de fuentes de ataques e intrusión

Seguridad Informática I

Ingeniería en Desarrollo de Software

academia global

TUTOR:

ALUMNO: Adriana Esteban López

FECHA: 18 de enero de 2026

Contextualización:

En la actividad 1 se identificaron las diversas amenazas y vulnerabilidades de la universidad y por tal el papel como analista de seguridad es realizar las recomendaciones para estos eventos, por tal es necesario planificar, mejorar o implementar las medidas necesarias para proteger tanto la parte física como la parte de la información, recordando que la información que no esta segura puede ser un factor de riesgo CRÍTICO para cualquier institución.

Actividad:

Con base en la Actividad 1 por cada amenaza o vulnerabilidad encontrada investigar, sustentar y redactar al menos una recomendación para proteger, mejorar o monitorear dichos eventos y con ello evitar las fuentes de ataque e intrusión (por ejemplo: base de datos, DNS, keylogger e ingeniería social, entre otras).

DESARROLLO

Tabla de recomendaciones

	Amenazas Humanas
Factor de Riesgo	El área administrativa financiera no cuenta con una alarma de seguridad para su acceso.
Recomendaciones	Implementación de seguridad electrónica para control de acceso al área física en donde esta el Departamento de Administración Financiera, así mismo la instalación de sensores de movimiento para ser activados una vez que se concluye la jornada laboral, para tener cierta seguridad una vez que todos salen.
Fuente ataque o intrusión	El atacante puede acceder a información sensible, e incluso los recursos monetarios de la Universidad.

	Amenazas Lógicas
Factor de Riesgo	No se cuenta con buena estructura de seguridad en cuanto al uso de usuarios y contraseñas
Recomendaciones	Implementación de Autentificación (Microsoft Authenticator)a través de la gestión usuarios y contraseñas con diferentes parámetros y procesos de renovación periódicos.
Fuente ataque o intrusión	Phishing
Factor de Riesgo	No hay firewall habilitado
Recomendaciones	De acuerdo al sistema que se este utilizando, este debe de ser habilitado conforme a las necesidades del

	mismo sistema, estableciendo que solo el usuario con el perfil de Administrador del Sistema puede hacer cualquier tipo de modificación.
Fuente ataque o intrusión	Malware, Accesos no autorizados, Ataque DDos
Factor de Riesgo	El antivirus es nod32 versión gratuita en todos los equipos.
Recomendaciones	Adquirir la Licencia de funcionamiento comercial, ya que esta garantiza actualizaciones constantes, soporte técnico y mayor uso de herramientas del antivirus que se acoplen a las necesidades de la Universidad.
Fuente ataque o intrusión	Phishing, Exploits
Factor de Riesgo	No se tiene denegado el uso del equipo para actividades personales, por ejemplo, el acceso a redes sociales o el manejo del correo electrónico o whatsapp.
Recomendaciones	Implementación de bloqueas técnicos, restricción de uso de aplicaciones y/o software
Fuente ataque o intrusión	Phishing, Malware
Factor de Riesgo	El Servidor 2 se destina para alojar un sistema de control que descargaron de Internet, y que les ayuda para mantener los registros de los alumnos (se desconoce la fuente de este software).
Recomendaciones	Se considera que la mejor opción es hacer uso de alternativas de código abierto que cuente con plataformas oficinales
Fuente ataque o intrusión	Malware, Troyanos

	Amenazas Físicas
Factor de Riesgo	• La institución educativa se encuentra en Veracruz, cerca de la costa. • Su infraestructura es de 2 pisos con 18 salones, 3 departamentos (Contabilidad y finanzas / Dirección / Desarrollo Académico/, así como un centro de cómputo y una biblioteca. • No se identifica dispositivo de detección de sismos, u otros fenómenos naturales.
Recomendaciones	Implementación de un kit de alerta sísmica que pueden conectarse al sistema de audio de la Universidad. Establecer protocolos de prevención y acción antes, durante y después de algún fenómeno natural
Fuente ataque o intrusión	Fenómenos naturales como huracanes, sismos
Factor de Riesgo	Se cuenta con un servidor principal (diferente al del centro de computo).
Recomendaciones	Debe ser colocado en un área física segura (ambiente controlado).
Fuente ataque o intrusión	Ataque físico y/o robo de información

	Vulnerabilidades de Almacenamiento
Factor de Riesgo	Los equipos han estado lentos en el último mes y se están quedando sin espacio de almacenamiento.
Recomendaciones	Programación periódica de mantenimiento preventivo en los equipos de computo, así como un análisis de

	requerimientos de almacenamiento, para que en caso de ser necesario se realice una expansión de almacenamiento o buscar otras alternativas de almacenamiento (en la nube).
Fuente ataque o intrusión	Ransomware, Malware, Virus
Factor de Riesgo	Servicio de internet de 20GB comercial.
Recomendaciones	Cambiar a Fibra óptica
Fuente ataque o intrusión	Ransomware, phishing

	Vulnerabilidades de Comunicación
Factor de Riesgo	Los equipos de la planta baja se encuentran conectados por cable de manera directa al módem. Los del piso de arriba son portátiles y se conectan vía wifi.
Recomendaciones	Implementar punto de acceso por (Access Point) para garantizar una buena velocidad en la planta alta
Fuente ataque o intrusión	Ataque a diccionario

Se agrega dicha actividad a la plataforma de GitHub a través del siguiente link:

https://github.com/22HADRIA/Seguridad-Inform-tica