Universidad Corporativa Coppel | 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: Jessica Hernández Romero tutor.etica@umi.edu.mx

ALUMNO: Sarahi Jaqueline Gómez Juárez.

FECHA: viernes, 05 de agosto de 2025.

Índice:

Introducción:

En esta segunda etapa del proceso del proyecto consiste en trasladar el diagnóstico realizado durante la etapa uno en donde se realizó un análisis de amenazas y vulnerabilidades de la contextualización del caso ahora pasara a un plan de prevención concreto, con controles específicos, medibles y alineados a buenas prácticas de seguridad, por cada amenaza o vulnerabilidad identificada.

Se propone al menos una recomendación que permita reducir su probabilidad de ocurrencia y/o su impacto, asimismo, se especifica la fuente de ataque o intrusión que se busca prevenir.

La finalidad esencial de esta segunda eta es proteger la continuidad académica, la confidencialidad de los datos y la integridad de las operaciones del Colegio de Veracruz, para lograrlo, se han integrado medidas de seguridad en tres niveles: técnicas (como EDR, TDE, VLAN, IDS/IPS, WPA3-Enterprise, NAC), organizacionales (como políticas de contraseñas, autenticación multi- factor, gestión de cambios) y físicas (como detección de incendios, sistemas UPS y control de accesos) entre otros por lo cual es vital entender que la seguridad informática se entiende como el conjunto de políticas, prácticas, técnicas y herramientas orientadas a proteger los sistemas de información, redes y datos frente a accesos no autorizados, alteraciones, pérdidas o daños, su objetivo fundamental es garantizar la confidencialidad, integridad y disponibilidad de la información conocido como el triángulo CIA, así como la autenticidad y trazabilidad de los procesos digitales, en el ámbito académico y organizacional, esto implica aplicar medidas preventivas y correctivas que mitiguen riesgos y fortalezcan la confianza de los usuarios en los sistemas.

La prevención de ataques e intrusiones requiere un enfoque proactivo, esto implica no solo identificar amenazas humanas, lógicas y físicas, sino también analizar vulnerabilidades en el almacenamiento y la comunicación de datos, que podrían ser explotadas por actores internos o externos, al implementar controles como segmentación de red, cifrado de datos, copias de seguridad 3-2-1, monitoreo mediante IDS/IPS y planes de continuidad operativa, se busca garantizar la seguridad integral de la infraestructura tecnológica, asegurando la prestación ininterrumpida de los servicios académicos y administrativos.

Finalmente, adquirir este conocimiento y comprender su aplicación práctica no solo fortalece la protección institucional, sino que también representa una competencia clave en el mundo laboral actual, en un entorno cada vez más digitalizado y globalizado, ya que la capacidad de identificar riesgos y aplicar medidas de seguridad efectivas es fundamental para cualquier profesional comprometido con la transformación digital y la gestión responsable de la información.

Descripción:

Este proyecto tiene como finalidad la identificación de riesgos y el diseño de controles efectivos que permitan mitigar amenazas reales dentro de un entorno académico, la etapa parte de un diagnóstico previo en el que se evaluaron amenazas y vulnerabilidades en el Colegio de Veracruz, con el objetivo de construir un plan de prevención detallado y fundamentado, una de las principales características más relevantes de esta actividad es su enfoque integral y proactivo, la prevención no se limita a reaccionar ante incidentes ocurridos, sino que busca anticiparse a posibles vectores de ataque, evaluando críticamente el entorno y aplicando medidas antes de que los riesgos se materialicen, en este sentido, se adopta una visión holística de la seguridad, que abarca elementos técnicos, organizacionales y físicos, garantizando una cobertura completa ante potenciales intrusiones, entre las cuales acciones clave que se analizan y proponen se encuentran: el fortalecimiento de contraseñas y políticas de acceso, el uso de herramientas como firewalls, EDR, IDS/IPS, la segmentación adecuada de la red,

el cifrado de información, la gestión de respaldos según el esquema 3-2-1, la implementación de planes de continuidad operativa, estas medidas se seleccionan segune el tipo de amenaza identificada, ya sea humana, lógica o física, y se justifican técnicamente, este estos se destaca uno de los elementos más significativos del proyecto es la tabla de análisis, organizada en seis columnas que abordan los siguientes componentes:

El Factor de riesgo que se refiere a cualquier condición que aumente la probabilidad de que una amenaza se materialice o una vulnerabilidad sea explotada, no es una amenaza en sí misma, pero facilita su aparición o amplifica su impacto, los factores pueden ser técnicos (como configuraciones inseguras), humanos (como falta de capacitación) o ambientales (como zonas

vulnerables a desastres).

Ejemplo: Tener software desactualizado es un factor de riesgo que facilita el ingreso de malware.

Amenazas humanas: Derivan de acciones humanas, ya sea por error, negligencia o intencionalidad, incluyen phishing, robo de credenciales, ingeniería social, abuso de privilegios, sabotaje interno y fuga de información, estas amenazas suelen explotar el eslabón más débil: el usuario.

Ejemplo: Un empleado que filtra datos confidenciales o un usuario que cae en un ataque de phishing.

Las amenazas lógicas que afectan la integridad o disponibilidad de los sistemas mediante uso indebido de software, configuraciones erróneas o vulnerabilidades técnicas, incluyen ransomware, malware, software no autorizado o ataques DDoS.

Ejemplo: Un malware que cifra todos los archivos del servidor.

Amenazas físicas: Estás están relacionadas con factores ambientales o estructurales que afectan equipos, servidores o redes, pueden ser incendios, sismos, inundaciones, sobrecargas eléctricas o accesos físicos no autorizados, un ejemplo simple es un corte eléctrico que daña servidores y provoca pérdida de datos.

Vulnerabilidades de almacenamiento: Son debilidades en la protección de datos, como ausencia de respaldos, falta de cifrado o controles de acceso inadecuados.

Ejemplo: Un servidor sin respaldos automáticos que pierde información tras una falla.

Vulnerabilidades de comunicación: Afectan los canales de transmisión de datos, como redes internas, Wi-Fi o enlaces a internet, riesgos comunes incluyen Wi-Fi sin seguridad, redes sin segmentación, firewalls deshabilitados o falta de redundancia.

Ejemplo: Una red Wi-Fi abierta que permite conexiones no autorizadas.

Por último, se identifica la fuente de ataque o intrusión, es decir, el mecanismo específico por el cual se materializa la amenaza puede tratarse de robo de credenciales, ataques SQL, movimientos laterales en red, malware remoto, acceso físico no autorizado, entre otros, reconocer esta fuente es esencial para diseñar controles que mitiguen el vector específico de ataque.

Ejemplo: Un atacante externo que accede a la red interna aprovechando una mala segmentación.

Cada celda de la tabla presenta recomendaciones concretas y justificadas técnicamente, diseñadas para enfrentar amenazas como phishing, ransomware, ataques DDoS, desastres naturales o fallas eléctricas, esto demuestra una capacidad analítica para vincular riesgos con medidas de control efectivas, dentro de una lógica de prevención basada en evidencia.

Otro aspecto destacar es la forma en que este trabajo integra la seguridad informática dentro del ámbito educativo, no solo se busca proteger los activos digitales de la institución, sino también fomentar una cultura de seguridad entre estudiantes, docentes y personal administrativo, la capacitación constante, la concienciación sobre amenazas y el diseño de entornos tecnológicos seguros son parte fundamental de esta estrategia.

Justificación:

El objetivo principal de esta etapa es transformar un diagnóstico teórico en acciones concretas, medibles y priorizadas que reducen de forma real la probabilidad e impacto de incidentes, dentro del contexto académico del Colegio de Veracruz, la continuidad operativa (clases, evaluaciones y servicios) depende de garantizar la **confidencialidad, integridad y disponibilidad** de la información, sin controles preventivos (segmentación, cifrado, respaldos 3-2-1, MFA, IDS/IPS, políticas y controles físicos), las amenazas humanas, lógicas y físicas encuentran terreno fértil en vulnerabilidades de **almacenamiento** y **comunicación**.

Distinguir **amenaza** de **vulnerabilidad** es crítico para invertir bien el esfuerzo: la *amenaza* es el agente o evento dañino potencial (p. ej., phishing, ransomware, incendio), mientras que la *vulnerabilidad* es la debilidad que ese agente podría explotar (p. ej., contraseñas débiles, firewall deshabilitado, falta de respaldo), actuar sin esta distinción lleva a controles mal ubicados, en cambio, un enfoque basado en riesgos (riesgo = amenaza × probabilidad × impacto) permite seleccionar controles de **alto valor** y definir métricas de eficacia (tasas de restauración, reportes de phishing, disponibilidad del enlace, cumplimiento de políticas).

Además, la prevención fortalece la cultura institucional: capacita a usuarios, estandariza procesos y eleva la postura de seguridad, para el estudiantado y el personal, dominar estas prácticas es una **competencia laboral** demandada en la transformación digital, la prevención de ataques no se limita a una acción reactiva, sino que constituye una estrategia proactiva que protege la información y asegura la continuidad operativa en un entorno cada vez más expuesto a riesgos tecnológicos.

Desarrollo:

Etapa 2 - Prevención de Fuentes de Ataques e Intrusión

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 está 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)

Figura 1

Tabla de Recomendaciones:

Análisis	Amenazas Humanas			Amenazas Lógicas			Amenazas Físicas				Vulnerabilidades de Almacenamiento			Vulnerabilidades de Comunicación			
Fuente de Riesgo	Ingeniería social (phishing en correo, WhatsApp, llamadas)	Acceso físico deficiente (entradas abiertas, bitácoras manuales fáciles de falsificar, poca supervisión).	Fuga de información confidencial por personal interno	Malware/Ransomware por antivirus gratuito y firewall deshabilitado	Software no confiable descargado en Servidor 2	Saturación/DDoS al enlace comercial	Incendio	Inundación / Huracán / Sismo	Cortes y picos eléctricos	Sin alarma de seguridad en acceso	Espacio insuficiente y falta de gestión de capacidad	Sin respaldos 3-2-1 ni retención probada	Sin cifrado en reposo ni control granular de roles	Segmentación nula (planta baja directa a módem)	Wi-Fi sin controles avanzados	Firewall deshabilitado y sin IDS/IPS	Único enlace sin redundancia/failover
Recomendaciones	RB3:Q3autorizados. Sin perder de vista el Implementar filtros antispam que bloqueen mensajes sospechosos antes de llegar a los usuarios.	Instalar sistemas de control de acceso con credenciales, biometría o códigos QR, de igual manera el Incorporar cámaras de videovigilancia con grabación continua y almacenamiento mínimo de 30 días, por lo cual es de suma importancia reemplazar las bitácoras manuales por un registro digital de entradas y salidas.	Establecer acuerdos de confidencialidad (NDA) para todo el personal que maneje información sensible, siendo determinante la Implementación del monitoreo de accesos a bases de datos y carpetas críticas para detectar actividades inusuales, aplicando el principio de privilegios mínimos, de modo que cada empleado solo tenga acceso a lo estrictamente necesario.	Sustituir el antivirus gratuito por una solución de seguridad empresarial con actualizaciones automáticas, configurando y manteniendo activo el firewall en todos los equipos y servidores asegurando el Implementar un sistema EDR (Endpoint Detection & Response) para detectar y contener amenazas avanzadas.	Se restringira la descarga e instalación de software en servidores únicamente al personal de TI autorizado para ello se usar listas blancas de aplicaciones (Application Whitelisting) para asegurar que solo se ejecuten programas confiables, ellos mismo monitorizaran el servidor con un SIEM (Security Information and Event Management) para detectar actividades sospechosas en tiempo real.	Se contratara un enlace redundante con failover automático para asegurar continuidad del servicio, por lo cual es vital configurar QoS (Quality of Service) para priorizar tráfico académico y administrativo, eligiendo un proveedor con protección avanzada contra DDoS	Instalan más detectores de humo y alarmas en las áreas críticas del colegio, así mismo se amplia la cantidad de extintores, asegurando su mantenimiento anual. Se realiza simulacros de evacuación cada dos meses para que la comunidad escolar sepa cómo actuar. También se realizar mantenimiento periódico de las áreas, detectores de humo y extintores.	Se elabora un plan de continuidad (BCP/DRP) con protocolos claros, rutas de evacuación señalizadas y sedes alternas en los cuales se lleva acabo instalando sistemas de drenaje pluvial y protección contra inundaciones en áreas críticas, elevando los servidores y equipos críticos para reducir daños por agua, instalar generadores eléctricos de respaldo y UPS para asegurar la operación en apagones, la contratación de pólizas de seguro contra desastres naturales, realizando simulacros periódicos de evacuación para sismos y huracanes , también se mantienen respaldos digitales fuera de sitio para garantizar la continuidad académica	Instalar UPS y reguladores en equipos sensibles para evitar daños por variaciones de voltaje, realizando pruebas trimestrales de respaldo eléctrico (UPS y generador) para comprobar su correcto funcionamiento, sin perder de viste el ejecutar mantenimiento preventivo de la instalación eléctrica para reducir el riesgo de fallas.	Se instalaran alarmas perimetrales y sensores de movimiento en accesos clave, implementando controles de acceso reforzados como biometría o doble verificación, por lo cual se Incorporan cámaras de vigilancia con monitoreo 24/7 en el área financiera y zonas críticas, manteniendo registro digital de entradas y salidas y custodia documental de accesos.	Se configuran cuotas de almacenamiento por usuario y área, programas de limpieza, que hacen las limpiezas periódicas de archivos temporales y duplicados, a su vez se implementan un sistema centralizado (NAS) que emita alertas cuando se alcance el límite de capacidad	Se implementa la estrategia de respaldos 3-2-1 (tres copias, dos medios, una fuera del sitio), a su vez se realizan pruebas mensuales de restauración para asegurar la integridad de los datos, complementando con el almacenamiento en la nube cifrado con políticas de retención definidas.	Se activa el cifrado TDE en la base de datos, así mismo se aplica el RBAC (control de accesos basado en roles) con privilegios mínimos, configurando auditoría y alertas para detectar accesos inusuales.	Se implementan VLANs que separan las distintas áreas del colegio, a su vez se configura un firewall perimetral con reglas de acceso personalizadas, sin dejar de monitorear el tráfico con IDS/IPS para detectar anomalías y posibles intrusiones.	Se configura el WPA3-Enterprise con autenticación 802.1X, implementando una NAC (Network Access Control) para validar los dispositivos conectados, por lo cual es vital establecer una red exclusiva para invitados mediante portal cautivo, así mismo se realiza la rotación periódica de claves y aplicando la segmentación.	Se activa el firewall en todos los equipos y servidores, de igual manera se instala un IDS/IPS perimetral para detectar intrusiones en tiempo real, complementando con un WAF (Web Application Firewall) para proteger las aplicaciones web contra ataques comunes como SQLi o XSS.	Se contrata un segundo enlace con balanceo de carga y failover automático, estableciendo SLA (acuerdos de nivel de servicio) con el proveedor de internet para garantizar disponibilidad mínima, verifico con el monitoreo de la red de forma continua con telemetría y alertas automáticas.
Fuente de ataque e intrusión	**Phishing / Ingeniería social**	**Intrusión física por personas no autorizadas, robo de equipos, manipulación directa de servidores o acceso a información sensible.**	**Abuso de privilegios, fuga de información, manipulación o borrado de datos sensibles por personal interno.**	**Descarga de malware, ejecución de ransomware, acceso remoto no autorizado y cifrado malicioso de archivos.**	**Instalación de malware, backdoors o exploits que comprometan la disponibilidad y la integridad del servidor.**	**Ataques de denegación de servicio distribuido (DDoS), interrupción de red y caída de los servicios institucionales.**	**Incendio en áreas críticas que provoque pérdida de equipos, interrupción académica y daños a la infraestructura.**	**Desastres naturales (inundaciones, huracanes, sismos) que provoquen interrupción prolongada, pérdida de equipos y afectación directa a la infraestructura escolar.**	**Cortes eléctricos prolongados, sobrecargas o variaciones de voltaje que interrumpan clases, dañen servidores y ocasionen pérdida de datos.**	**Intrusión física por terceros o personal interno, robo de documentos sensibles, manipulación de servidores y sustracción de recursos materiales.**	**Interrupción de servicios por falta de espacio, pérdida de información crítica, corrupción de archivos y fallos en respaldos automáticos.**	**Fallos en servidores o bases de datos, ataques de ransomware o borrado accidental de información que impidan la recuperación oportuna de datos.**	**Robo, manipulación o fuga de datos confidenciales mediante accesos indebidos o explotación de vulnerabilidades en bases de datos.**	**Movimiento lateral / intrusión interna**	**Robo de credenciales, sniffing de tráfico, acceso no autorizado a la red interna y propagación de malware desde dispositivos no validados.**	**Ataques de inyección SQL, cross-site scripting (XSS), accesos no autorizados e intrusiones externas que comprometan la disponibilidad y confidencialidad de los sistemas.**	**Caída del servicio por saturación, fallas del proveedor o ataques DDoS que afecten la continuidad académica y administrativa.**

Nota: La presente matriz integra el análisis de **amenazas humanas, lógicas y físicas**, así como de **vulnerabilidades de almacenamiento y comunicación** detectadas en el entorno escolar, para cada caso se identificó la **fuente de riesgo**, se propusieron **recomendaciones específicas de mitigación** y se vinculó la posible **fuente de ataque o intrusión** que se previene, este instrumento permite visualizar de manera clara la relación entre riesgo, control y amenaza, sirviendo como base para la toma de decisiones y la implementación de medidas de seguridad que garanticen la **protección de la información** y la **continuidad académica**.

Conclusión:

En esta etapa comprendimos que la prevención de ataques e intrusiones en el ámbito académico requiere un enfoque integral que combine medidas técnicas, organizacionales y físicas, se identificaron amenazas humanas, lógicas y físicas, así como vulnerabilidades en almacenamiento y comunicación que representan riesgos críticos para la continuidad de las operaciones y la protección de la información.

El análisis realizado permitió proponer controles específicos como segmentación de red, uso de firewalls, cifrado de datos, gestión de respaldos bajo el esquema 3-2-1, políticas de acceso robustas, autenticación multifactor y planes de continuidad operativa, estas recomendaciones, además de reducir la probabilidad e impacto de los incidentes, promueven una cultura de seguridad que fortalece la confianza de los usuarios en los sistemas, hay que tener en cuenta que la seguridad informática no debe entenderse únicamente como una respuesta reactiva, sino como una estrategia proactiva que protege los recursos institucionales y asegura la disponibilidad, integridad y confidencialidad de la información.

El aplicar estas medidas no solo salvaguarda el entorno educativo, sino que también prepara a los futuros profesionales para enfrentar con responsabilidad y eficacia los desafíos de un mundo digital cada vez más complejo y vulnerable, en donde es necesario la prevención de fuentes de ataques e intrusión, porque representa una práctica esencial no solo en el ámbito académico y organizacional, sino también en la vida cotidiana y profesional, ya que al identificar amenazas y vulnerabilidades, y proponer medidas técnicas, organizacionales y físicas para mitigarlas, se fortalece la seguridad de la información y se asegura la continuidad de las operaciones.

En la vida cotidiana, aplicar estos conocimientos nos ayuda a proteger datos personales como contraseñas, cuentas bancarias, historiales médicos y archivos digitales frente a fraudes, robos de identidad o pérdidas irreparables, al sumar estos hábitos como lo es el uso de contraseñas seguras, el respaldo periódico de la información o la navegación en redes confiables brinda mayor tranquilidad y confianza en el uso de la tecnología.

En el ámbito laboral, la implementación de estrategias de prevención se traduce en mayor productividad y resiliencia organizacional, pues permite a las empresas evitar pérdidas económicas, proteger su reputación y garantizar la confianza de clientes y socios, además, quienes adquieren estas competencias se convierten en profesionales más competitivos, capaces de aportar valor en un mercado donde la ciberseguridad es un requisito indispensable para la transformación digital.

En conclusión, la prevención de ataques e intrusiones no es solo un conjunto de medidas técnicas, sino una cultura de seguridad que aporta beneficios directos al día a día de las personas y al desempeño profesional, asegurando la protección de la información y preparando a los individuos y organizaciones para enfrentar los desafíos de un mundo digital en constante evolución.

Referencias:

10 consejos para proteger la información de instituciones educativas. (2014, 8 julio). https://www.welivesecurity.com/la-es/2014/07/08/10-consejos-proteger-informacion-instituciones-educativas/

Calle, J. P. (2024, 10 octubre). 8 consejos para prevenir ataques informáticos. *8 consejos para prevenir ataques informáticos*. https://www.piranirisk.com/es/blog/8-consejos-para-prevenir-ataques-informaticos

De Ceupe, B. (2023, 30 marzo). Ceupe. *Ceupe*. https://www.ceupe.com/blog/seguridad-informatica-y-proteccion-de-datos.html

De Lourdes León, M. (2025, 24 enero). Tips básicos de seguridad informática que debes conocer | Blog UNITEC. *Universidad UNITEC*. https://blogs.unitec.mx/vida-universitaria/tips-super-basicos-de-seguridad-informatica/

Florentín, B. (2020, 20 marzo). *Seguridad informática*. ConceptoABC. https://conceptoabc.com/seguridad-informatica/

Ibm. (2024, 16 julio). Sistema de prevención de intrusiones. *¿Qué es un sistema de prevención de intrusiones (IPS)?* https://www.ibm.com/mx-es/think/topics/intrusion-prevention-system

Team, A. I. (2021, 26 julio). Tipos de Vulnerabilidades y Amenazas informáticas. *Tipos de Vulnerabilidades y Amenazas informáticas*. https://www.ambit-iberia.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Uss. (2023, 30 junio). *Análisis de vulnerabilidades. Explora como detectar y solucionar debilidades en tu seguridad*. USS Alarmas. https://uss.com.ar/consejos-uss/analisis-de-

vulnerabilidades