Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | 1 | "Análisis de Vulnerabilidades y Amenazas"

Análisis de Vulnerabilidades y Amenazas

Ingeniería en Desarrollo de Software

TUTOR: Seguridad Informática I tutor.etica@umi.edu.mx

ALUMNO: Sarahi Jaqueline Gómez Juárez.

FECHA: sábado, 30 de agosto de 2025.

Índice:

Introducción:

En el contexto del colegio ubicado en Veracruz, la seguridad no es un estado sino un proceso que exige atención continua, la vida académica: clases, registros, pagos y expedientes, depende de sistemas que, aunque invisibles, sostienen la operación diaria, cuando esos sistemas fallan o quedan expuestos, el impacto trasciende lo técnico: se interrumpe el aprendizaje, se compromete la confianza y se arriesga información sensible, este trabajo asume, por tanto, que comprender y reducir el riesgo es parte esencial de la misión educativa.

El análisis parte de una premisa central: las **vulnerabilidades** son la base estructural del riesgo y las **amenazas** son los agentes que las explotan, en el plantel conviven debilidades de **almacenamiento** (espacio insuficiente, ausencia de respaldos 3-2-1, falta de cifrado/roles) y de **comunicación** (segmentación nula, Wi-Fi sin controles, firewall deshabilitado, enlace único sin *failover*), sobre ese terreno actúan **amenazas humanas** (ingeniería social, accesos físicos deficientes, uso de contraseñas débiles), **lógicas** (malware/ransomware, software no confiable, saturación/DDoS) y **físicas** (incendio, inundación/sismo, picos eléctricos, falta de alarmas en área financiera).

Para convertir esa realidad en decisiones, se emplea una matriz de cinco columnas: **Activo/Zona o Sistema, Amenaza/Vulnerabilidad, Impacto, Probabilidad y Controles/Medidas** y una escala cualitativa (Impacto: Muy alto/Alto/Medio; Probabilidad: Alta/Media), el enfoque sobre activos críticos (Accesos/Usuarios, Área financiera, Endpoints/Servidores, incluido Servidor 2, BD Oracle, Perímetro/Wi-Fi y Conectividad comercial) permite priorizar acciones con sentido: activar **firewall/EDR** y **hardening** en equipos, controlar **Servidor 2** (inventario y fuentes confiables), asegurar **backups 3-2-1** y

cifrado TDE/RBAC en BD Oracle, implementar **segmentación VLAN** e **IDS/IPS**, fortalecer **Wi-Fi** (WPA3, NAC) y robustecer la **resiliencia física** (detección de incendios, **UPS** y **redundancia de enlace**).

El propósito final es práctico: reducir de manera medible la probabilidad y el impacto de incidentes, proteger la continuidad académica y resguardar la información de la comunidad escolar. La seguridad, entendida así, deja de ser un costo y se vuelve una condición habilitante para enseñar y aprender con confianza.

Descripción:

Análisis de Amenazas y Vulnerabilidades del colegio en Veracruz:

En entornos educativos, la continuidad académica y la protección de datos personales dependen de prácticas básicas de ciberseguridad y de controles físicos elementales. A partir del escenario del colegio en Veracruz, se construyó una matriz de cinco columnas: Activo/Zona o Sistema, Amenaza/Vulnerabilidad, Impacto, Probabilidad y Controles/Medidas, que permite observar con claridad dónde están los riesgos, qué tan graves y probables son, y qué acciones concretas conviene implementar.

El análisis se organizó en dos grandes grupos: **Amenazas** (humanas, lógicas y físicas) y **Vulnerabilidades** (de almacenamiento y de comunicación, para cada caso se identificó la **fuente de origen**, el **activo afectado**, la **descripción** en el escenario, y se estimaron **impacto** y **probabilidad** usando una escala cualitativa (Muy alto, Alto, Medio).

La columna final propone **controles** específicos, factibles y medibles, la prioridad implícita surge de la combinación impacto–probabilidad: eventos con **Muy alto** impacto y **Alta/Media-Alta** probabilidad son críticos.

Amenazas humanas:

Las debilidades del comportamiento del usuario siguen siendo determinantes, en **accesos/usuarios**, la **ingeniería social** (phishing por WhatsApp o correo) presenta **impacto Alto *y* probabilidad Media-Alta*;*** la medida eficaz es una **concientización continua**, simulacros de phishing y **MFA** para reducir el valor de credenciales robadas, en **entradas/área financiera**, el **acceso físico deficiente** (múltiples puertas y registro manual) habilita intrusiones y robo con impacto Alto*;* se recomiendan **torniquetes o biometría, CCTV, credenciales y bitácoras**

digitales, finalmente, el uso de **contraseñas básicas y reutilizadas** en PCs/oficinas eleva la probabilidad de compromiso masivo (Alto–Alta); se mitiga con **política robusta de contraseñas, MFA y gestión centralizada de identidades**.

Amenazas Lógicas:

En el plano técnico, el colegio exhibe una superficie de ataque sobredimensionada, en **endpoints y servidores** se detecta **antivirus gratuito y firewall deshabilitado**, situación que facilita **malware/ransomware** (Muy alto–Alta); el mínimo aceptable es **activar y gestionar firewall**, desplegar **EDR empresarial**, **listas blancas** y **hardening**, en **Servidor 2**, el **software de Internet no confiable** expone a troyanos y puertas traseras (Muy alto–Media-Alta); procede el **inventario y control de software**, uso de **repositorios confiables**, **pruebas en aislamiento** y verificación de **firmas**. Por último, la **saturación/DDoS** del **enlace comercial** (Alto–Media) exige **redundancia**, **QoS**, **telemetría**, e incluso **WAF/IPS** y plan de contingencia.

Amenazas Físicas:

La ubicación y el equipamiento imponen riesgos no técnicos pero decisivos, en **infraestructura/edificio**, la cobertura limitada de **extintores** sitúa el **incendio** en Muy alto–Media; se requiere **detección y supresión**, **simulacros** y **mantenimiento**, la condición de **zona costera** sin sensores eleva **inundación/huracán/sismo** (Muy alto–Media); mitigación: **BCP/DRP**, **UPS/generador**, y **elevación de equipos críticos**, en **sala de equipos/oficinas**, los **picos eléctricos** provocan daños y caídas (Alto–Media); medidas: **UPS, reguladores y mantenimiento eléctrico**, en **área financiera**, la **falta de alarma** facilita sustracción de efectivo/información (Alto–Media); urge **alarma/biometría, CCTV y custodia documental**.

Vulnerabilidades de Almacenamiento:

La práctica operativa revela tres brechas, en **equipos/servidores**, el **espacio insuficiente**

y la **ausencia de gestión de capacidad** elevan fallos y corrupción (Alto–Alta); se recomienda **cuotas, limpieza programada y almacenamiento en red/NAS**, en **BD Oracle/servidores**, la **falta de respaldos 3-2-1 y pruebas de restauración** pone en juego la continuidad (Muy alto–Media-Alta); hay que institucionalizar **backups 3-2-1**, **pruebas periódicas**, **automatización con RMAN** y **política de retención**. Además, en **BD Oracle** sin **cifrado en reposo** ni **roles granulares** se arriesga la confidencialidad (Muy alto–Media); controles: **cifrado TDE**, **RBAC/least-privilege** y **auditoría**.

Vulnerabilidades de Comunicación:

La arquitectura de red demanda segmentación y monitoreo, en **perímetro/red PB**, la **segmentación nula** facilita movimiento lateral (Alto–Alta); procede **VLANs, firewall dedicado y reglas**. En **Wi-Fi de piso superior**, la **ausencia de controles avanzados** dispara el abuso (Alto–Alta); medidas: **WPA3-Enterprise, portal cautivo, NAC y rotación de claves**. En **perímetro/endpoints**, **firewall deshabilitado y sin IDS/IPS** degrada la detección (Muy alto–Alta); activar **firewall**, **IDS/IPS**, **WAF** y monitoreo de eventos. Por último, la **conectividad comercial sin redundancia/failover** (Medio-Alto–Media) exige **enlace secundario, balanceo/failover, QoS** y **telemetría**.

Priorización y Hoja de Ruta:

Convergen como **críticos**: (1) endpoints/servidores sin firewall/EDR; (2) Servidor 2 con software no confiable; (3) BD Oracle sin **backups 3-2-1** ni **cifrado TDE**; (4) red sin segmentación ni **IDS/IPS**; y (5) riesgos físicos de **incendio** y **eventos hidrometeorológicos**. La secuencia recomendada es inmediata en **controles técnicos de base** (firewall/EDR, segmentación, backups y cifrado), en paralelo con **medidas físicas** (detección de incendios, UPS/reguladores) y **programa continuo de capacitación** y **MFA**.

En conclusión la matriz evidencia que los problemas del colegio no se concentran en un único frente, sino que combinan **comportamiento del usuario**, **configuración tecnológica** y **entorno físico**, con acciones puntuales: **políticas de identidad y contraseñas**, **MFA**, **firewall/EDR**, **segmentación VLAN**, **backups 3-2-1 con pruebas**, **cifrado TDE**, **alarma/CCTV**, **detección de incendios**, **UPS** y **redundancia de enlace**, el colegio puede **reducir de forma medible** la probabilidad e impacto de incidentes, sostener la continuidad académica y proteger la información sensible de estudiantes y personal.

Justificación:

El Objetivo de este análisis radica en la necesidad de garantizar la continuidad académica y la protección de la información sensible dentro del colegio en Veracruz. En la actualidad, las instituciones educativas dependen en gran medida de sistemas digitales para la gestión de registros, pagos, comunicación y almacenamiento de datos, lo cual las convierte en objetivos potenciales de amenazas tanto humanas como lógicas y físicas.

Realizar un diagnóstico de vulnerabilidades y amenazas permite no solo identificar los puntos críticos que comprometen la seguridad, sino también establecer medidas preventivas y correctivas que aseguren la integridad, disponibilidad y confidencialidad de la información, sin esta evaluación, la institución corre el riesgo de enfrentar pérdidas económicas, interrupciones en los procesos académicos y daños a la reputación institucional.

Asimismo, la implementación de controles de seguridad fortalece la confianza de estudiantes, docentes y personal administrativo, generando un entorno académico más resiliente y preparado ante incidentes, este análisis no debe considerarse un gasto, sino una inversión estratégica que protege la misión educativa y fomenta una cultura de seguridad informática tanto en la vida académica como en la vida profesional de quienes forman parte de la comunidad escolar.

Desarrollo:

Etapa 1 - Análisis de Vulnerabilidades y Amenazas

Contextualización: Se pretende aplicar mecanismos de seguridad informática a un colegio de educación superior, realizando un análisis de los factores que se describen a continuación tipificando las vulnerabilidades y amenazas.

Escenario principal:

- 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.
- Actualmente tiene 4 escaleras de acceso a planta superior y 1 ascensor principal.
- Presenta una entrada principal 2 laterales y posterior a la cancha principal una salida.
- Los docentes registran su entrada en una libreta y los departamentos utilizan tarjetas de registro.
- El área administrativa financiera no cuenta con una alarma de seguridad para su acceso.
- Se cuenta con 2 extintores Clase A y uno Clase B ubicados en el piso principal.
- Se cuenta con una salida de emergencia.
- No se identifica dispositivo de detección de sismos, u otros fenómenos naturales.
- Se cuenta con un servidor principal (diferente al del centro de cómputo).

Respecto al centro de cómputo presenta la siguiente infraestructura:

- 1 Servicio de internet de 20GB comercial.
- 10 equipos de escritorio.
- 5 laptops.

● 1 servidor espejo.

En los departamentos presenta la siguiente infraestructura:

● 4 equipos por departamento.

● 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.

● Los equipos han estado lentos en el último mes y se están quedando sin espacio de almacenamiento.

Otros detalles:

● Cada equipo cuenta con un usuario y contraseña básicos, por ejemplo:

○ Usuario: Equipo1 ○ Password: 1234abc

● El firewall no se encuentra habilitado.

● El antivirus es nod32 versión gratuita en todos los equipos.

● 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.

● El Servidor cuenta con la base de datos general, este utiliza el software Oracle Database en un sistema operativo Linux, por su parte, 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).

Actividad: De acuerdo al escenario presentado en la contextualización **analizar y realizar una tabla de las posibles fuentes de amenazas y vulnerabilidades (Amenazas: humanas, lógicas y físicas; Vulnerabilidades: almacenamiento y comunicación**

Figura 1

Tabla de Análisis:

Análisis	Amenazas Humanas			Amenazas Lógicas			Amenazas Físicas				Vulnerabilidades de			Vulnerabilidades de Comunicación			
Fuente de Origen	Ingeniería social a docentes/administrativos	Acceso físico deficiente (múltiples entradas, registro manual)	Robo/filtrado o crackeo de credenciales (aprovecha contraseñas débiles o reutilizadas)	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
Activo/Zona o Sistema	Accesos / U	Accesos / Entradas / Área financiera	Usuarios (PCs/aulas/ oficinas)	Endpoints / Servidores	Servidor 2	Perímetro / Conectividad	Infraestructura / Edificio	Infraestructura (zona costera)	Sala de equipos / Oficinas	Área financiera	Equipos / Servidores	BD Oracle / Servidores	BD Oracle	Perímetro / Red planta baja	Red inalámbrica (piso superior)	Perímetro / Endpoints	Conectividad comercial
Descripción en el Escenario	Intentos de phishing y mensajes por WhatsApp/ correo para obtener credenciales o inducir acciones no autorizadas.	Facilita intrusión, robo de dispositivos y sustracción de información sensible.	Contraseñas básicas (p. ej., 1234abc) y la misma por equipo; riesgo de compromiso masivo.	Mayor superficie de ataque con detección insuficiente y ausencia de barreras perimetrales.	Riesgo de troyanos/puertas traseras por software de Internet sin validación.	Único enlace de 20 GB vulnerable a saturación o ataques de denegación de servicio.	Solo 3 extintores con cobertura limitada; riesgo a personas y activos.	Sin sensores/detectores; riesgo de interrupción prolongada y pérdida de equipos.	Daños a hardware, corrupción de datos y caídas de servicio.	Riesgo de sustracción de efectivo/información.	Riesgo de corrupción de datos y fallas por discos al límite.	Riesgo de pérdida de datos ante incidente o ransomware.	Exposición de datos sensibles y abuso de privilegios.	Tráfico sin aislamiento; facilita propagación lateral de ataques.	Riesgo de intrusión y uso no autorizado.	Tráfico no inspeccionado y detección tardía de intrusiones.	Caída o saturación afecta clases, administrativos y sistemas críticos.
Impacto	Alto	Alto	Alto	Muy alto	Muy alto	Alto	Muy alto	Muy alto	Alto	Alto	Alto	Muy alto	Muy alto	Alto	Alto	Muy alto	Medio-Alto
Probabilidad	Media-Alta	Media	Alta	Alta	Media-Alta	Media	Media	Media	Media	Media	Alta	Media-Alta	Media	Alta	Alta	Alta	Media
Controles/Medidas	Capacitación continua, campañas anti-phishing, MFA, alertas tempranas y simulacros.	Control de accesos, torniquetes/ biometría, CCTV, credenciales y bitácoras digitales.	Política de contraseñas robustas, MFA, gestión centralizada de identidades.	Activar y gestionar firewall, EDR/antivirus empresarial, listas blancas y hardening.	Inventario/control de software, repositorios confiables, pruebas/aislamiento y firma/certificación.	Enlace redundante, QoS, telemetría/monitoreo de tráfico, WAF/IPS y plan de contingencia.	Detección y supresión, inspecciones, simulacros, planes de evacuación y mantenimiento.	BCP/DRP, sensores, UPS/generador, elevación de equipos críticos y rutas alternas.	UPS, reguladores, generador, mantenimiento eléctrico y monitoreo.	Alarma/biometría, CCTV, registro de entradas/salidas, custodia documental.	Gestión de capacidad, cuotas, limpieza programada, almacenamiento en red/NAS.	Backups 3-2-1, pruebas de restauración, automatización (RMAN) y política de retención.	Cifrado TDE, RBAC/least-privilege, auditoría y monitoreo de accesos.	VLANs, router/firewall dedicado, reglas de acceso y monitoreo.	WPA3-Enterprise, portal cautivo, NAC, rotación de claves y segmentación.	Activar firewall, IDS/IPS, WAF, listas blancas y monitoreo de eventos.	Enlace secundario, balanceo/failover, QoS y telemetría de red.

Nota: La matriz presenta, en cinco columnas, el **activo/zona**, la **amenaza o vulnerabilidad**, su **impacto**, **probabilidad** y las **medidas de control**, está organizada por bloques:

Amenazas humanas (ingeniería social, accesos físicos deficientes, contraseñas débiles).

En el bloque de amenazas humanas se incluye la debilidad de contraseñas débiles cuando es **explotada por actores** (phishing, fuerza bruta, credential stuffing), para mantener la coherencia con la consigna.

Amenazas lógicas (malware/ransomware por firewall deshabilitado, software no confiable en Servidor 2, riesgo de saturación/DDoS).

Amenazas físicas (incendio, inundación/huracán/sismo, picos eléctricos, falta de alarma en área financiera) y **Vulnerabilidades** de **almacenamiento** (espacio insuficiente, sin respaldos 3-2-1, sin cifrado/roles) y de **comunicación** (sin segmentación, Wi-Fi sin controles, sin IDS/IPS, enlace único sin failover).

Se emplea una escala cualitativa (**Impacto:** Muy alto/Alto/Medio; **Probabilidad:** Alta/Media) aplicada a los activos **Accesos/Usuarios**, **Área financiera**, **Endpoints/Servidores**: incluido **Servidor 2**, **BD Oracle**, **Perímetro/Wi-Fi** y **Conectividad comercial**, de la evaluación surgen como **prioridades**:

1) **activar firewall/EDR y hardening** en todos los equipos;

2) **controlar Servidor 2** (inventario, fuentes confiables, pruebas aisladas);

3) **backups 3-2-1 con pruebas** y **cifrado TDE/RBAC** en BD Oracle;

4) **segmentación VLAN**, **IDS/IPS** y refuerzo de **Wi-Fi** (WPA3, NAC).

5) **MFA y política robusta de contraseñas**.

6) **detección de incendios/UPS** y **redundancia de enlace**.

Con estas acciones se reduce de forma medible la exposición y se protege la continuidad académica.

Conclusión:

El diagnóstico del colegio en Veracruz muestra que las **vulnerabilidades estructurales** en almacenamiento (espacio, respaldos y cifrado) y en comunicación (segmentación, Wi-Fi, perímetro y enlace) son el terreno donde las **amenazas** humanas, lógicas y físicas adquieren mayor impacto y probabilidad. La mitigación efectiva pasa por **controles de base** (activar y gestionar firewall, desplegar EDR y hardening), **gobernanza de identidades** (política de contraseñas y MFA), **higiene de datos** (backups 3-2-1 con pruebas, TDE y RBAC en Oracle), **arquitectura de red segura** (VLAN, IDS/IPS, Wi-Fi con WPA3, NAC) y **resiliencia física** (detección de incendios, UPS/reguladores y redundancia del enlace), implementados con responsables, cronograma y **métricas** de equipos con EDR activo, tasas de restauración exitosa, incidentes de phishing reportados, disponibilidad del enlace, estos controles **reducen de forma medible** la exposición, sostienen la **continuidad académica** y protegen la **información sensible** de la comunidad escolar.

El diagnóstico del colegio en Veracruz confirma que las **vulnerabilidades estructurales** (almacenamiento y comunicación) son el terreno donde las **amenazas** humanas, lógicas y físicas ganan impacto y probabilidad. La mitigación efectiva exige **controles de base** (firewall, EDR, hardening), **gobernanza de identidades** (política de contraseñas y MFA), **higiene de datos** (backups 3-2-1 con pruebas, TDE y RBAC en Oracle), **arquitectura de red segura** (VLAN, IDS/IPS, Wi-Fi con WPA3/NAC) y **resiliencia física** (detección de incendios, UPS y redundancia del enlace), con responsables, cronograma y **métricas** (p. ej., % de equipos con EDR activo, restauraciones exitosas, incidentes de phishing, disponibilidad del enlace), estos controles **reducen de forma medible** la exposición, sostienen la **continuidad académica** y

protegen la **información sensible**.

Beneficios de este conocimiento en la vida cotidiana y laboral

Contraseñas y MFA: crear claves fuertes, usar gestor y activar doble factor en bancos, correo y redes.

Antiphishing: reconocer correos/links falsos, verificar remitentes y dominios antes de hacer clic.

Copias de seguridad personales: aplicar regla **3-2-1** para fotos/documentos y probar la restauración.

Red doméstica más segura: cambiar la clave del router, usar **WPA3/WPA2**, red de invitados y actualizar firmware.

Dispositivos al día: actualizar sistema y apps; mantener **firewall** activo en PC y móvil.

Protección eléctrica básica: usar reguladores/UPS para evitar daños por picos o cortes.

Cultura de seguridad en el trabajo: reportar incidentes, seguir políticas y reducir errores humanos.

Menos interrupciones y costos: menos infecciones, caídas y pérdida de datos → más productividad.

Cumplimiento y reputación: mejores prácticas alineadas a políticas internas y marcos de referencia.

Empleabilidad: base para roles de TI/seguridad y para futuras certificaciones (p. ej., enfoque de riesgos, continuidad de negocio).

En síntesis, lo aprendido no solo fortalece el proyecto: también mejora los hábitos digitales diarios y el desempeño profesional, haciendo más **seguro, confiable y eficiente** cualquier entorno donde participes.

Diferenciar **qué es una amenaza** (evento/actor que causa daño) y **qué es una vulnerabilidad** (debilidad que permite ese daño), así como **su tipo** (humana, lógica, física; almacenamiento o comunicación), aporta ventajas claras en lo cotidiano y en el trabajo:

Priorización inteligente: enfocas primero las combinaciones de alto impacto + alta probabilidad (p. ej., ransomware + endpoints sin firewall/EDR).

Controles adecuados: eliges la medida correcta según el tipo:

Humana → capacitación/MFA/políticas.

Lógica → parches, EDR, listas blancas.

Física → alarmas, CCTV, UPS, detectores.

Almacenamiento → 3-2-1, TDE, RBAC.

Comunicación → VLAN, IDS/IPS, WPA3/NAC.

Uso eficiente de recursos: evitas "parches" generales; inviertes justo donde corta el riesgo (tiempo, presupuesto, personal).

Respuesta a incidentes más rápida: si identificas que es una amenaza lógica explotando una vulnerabilidad de comunicación, sabes a qué equipo y controles escalar.

Prevención vs. contención: al ver la vulnerabilidad raíz (p. ej., contraseñas débiles), aplicas medidas preventivas; ante la amenaza (phishing), refuerzas detección y contención.

Medición clara: puedes asociar métricas por tipo (tasa de restauración de backups, % de equipos con EDR, cobertura de VLAN/IDS, tasa de reportes de phishing).

Cumplimiento y auditorías: mapeas cada control al riesgo que mitiga; facilita evidencias y reduce hallazgos.

Comunicación efectiva: explicas riesgos a docentes/administrativos con ejemplos concretos por tipo, generando adopción real.

Hábitos personales más seguros: distingues si debes mejorar tu *conducta* (no caer en phishing) o tu *configuración* (actualizar, activar 2FA, hacer respaldos).

Empleabilidad: demuestra pensamiento de riesgo maduro (root cause vs. síntoma) valioso en TI, operaciones y gestión.

Ejemplos rápidos de relación (amenaza → vulnerabilidad → control):

Phishing (humana) → **Contraseñas reutilizadas (vuln. humana/identidades) → MFA + gestor de contraseñas + bloqueo por intentos**.

Ransomware (lógica) → **Endpoints sin EDR/Firewall (vuln. comunicación/lógica) → EDR + firewall + listas blancas + backups 3-2-1 probados**.

Corte eléctrico (física) → **Sin UPS (vuln. física/infraestructura) → UPS/reguladores + pruebas de conmutación**.

Intrusión Wi-Fi (lógica) → **Wi-Fi sin controles (vuln. comunicación) → WPA3-Enterprise + NAC + red de invitados + rotación de claves**.

Con esta distinción, las acciones priorizadas (MFA, firewall/EDR, 3-2-1/TDE, VLAN/IDS-IPS, UPS y redundancia de enlace) **reducen riesgo de forma medible** y mejoran tanto la vida diaria digital como el desempeño profesional.

Referencias:

Blog, U. S. S. (2023, julio 15). Análisis de vulnerabilidades. Explora como detectar y solucionar debilidades en tu seguridad. USS. Recuperado el 20 de abril de 2024, https://uss.com.ar/consejos-uss/analisis-de-vulnerabilidades/

Razones para realizar un análisis de vulnerabilidades. (2022, julio 3). Geformasdigital.com. Recuperado el 20 de abril de 2024, https://www.geformasdigital.com/razones-para-realizar-un-analisis-de-vulnerabilidades

Rodríguez, P. (s/f). Análisis de riesgos informáticos y ciberseguridad. Ambit-bst.com. Recuperado el 21 de abril de 2024, de https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

Santana, R. (2023, enero 24). Tipos de análisis de vulnerabilidades, ataques y amenazas. Hillstone Networks. Recuperado el 21 de abril de 2024, https://www.hillstonenet.lat/blog/sin-categorizar/analisis-de-vulnerabilidades-ataques-y-amenazas/

Villanueva, A. (2021, abril 1). ¿Qué es el análisis de vulnerabilidades? - OSTEC. OSTEC | Segurança digital de resultados; OSTEC Business Security. Recuperado el 22 de abril de 2024, https://ostec.blog/es/aprendizaje-descubrimiento/que-es-el-analisis-de-vulnerabilidades/