

INSTITUCIÓN EDUCATIVA SAN JOAQUÍN

ÁREA DE TECNOLOGÍA E INFORMÁTICA

DOCENTE: EDUIN KAMMERE KAMMERER



EL IMPACTO DE LAS REDES SOCIALES EN ADOLESCENTES EL RESGUARDO DE LA PRIVACIDAD

DESCRIPCIÓN BREVE

En la última década, y de manera exponencial tras la crisis sanitaria global, el ámbito educativo ha experimentado una transición disruptiva hacia la digitalización.

Grados: 6-7

PRESENTADO POR:

NIÑO NIÑO YULIANIS MARGARITA

OLAYA AMARIS LUIS CARLOS

ORTEGA MATRONES GABRIELA SOFIA

PIÑANGO PEREZ YORMARY VALENTINA

ROSADO BERMUDEZ DORIANNY SOFIA

TABLA DE CONTENIDO

| | |
|---|----|
| 1. <u>INTRODUCCIÓN</u> | 3 |
| 1.1 CONTEXTUALIZACION DEL ENTORNO DIGITAL EDUCATIVO..... | 3 |
| 1.2 JUSTIFICACIÓN DEL INFORME..... | 3 |
| 1.3 OBJETIVOS DEL INFORME..... | 3 |
| 1.4 ALCALCE..... | 4 |
| 2. <u>LOS TRES PILARES DE LA SEGURIDAD INFORMÁTICA (TRÍADA CIA)</u> | 4 |
| 2.1 CONFIDENCIALIDAD: EL RESGUARDO DE LA PRIVACIDAD..... | 4 |
| 2.2 INTEGRIDAD: LA VERACIDAD DE LA INFORMACIÓN ACADÉMICA..... | 5 |
| 2.3 DISPONIBILIDAD: LA CONTINUIDAD DEL PROCESO DE APRENDIZAJE..... | 5 |
| 3. <u>RIESGOS Y AMENAZAS ACTUALES EN EL SECTOR EDUCATIVO</u> | 6 |
| 3.1 AMENAZAS TÉCNICAS Y DE INFRAESTRUCTURA..... | 6 |
| 3.2 INGENIERIA SOCIAL Y FACTOR HUMANO..... | 7 |
| 3.3 RIESGOS EN LA CONVIVENCIA Y SEGURIDAD DE LOS MENORES..... | 7 |
| 4. <u>MEDIDAS DE PREVENCIÓN Y PROTOCOLOS DE ACTUACIÓN</u> | 8 |
| 4.1 MEDIDAS DE INFRAESTRUCTURA Y CONTROL TÉCNICO..... | 8 |
| 4.2 MEDIDAS ORGANIZATIVAS Y DE GOBERNANZAS..... | 8 |
| 4.3 CAPACITACIÓN Y CONCIENCIACIÓN (EL FACTOR HUMANO)..... | 9 |
| 5. <u>LA INTELIGENCIA ARTIFICIAL EN LA CIBERSEGURIDAD ESCOLAR</u> | 10 |
| 5.1 LA IA COMO HERRAMIENTA DE DEFENSA..... | 10 |
| 5.2 DESAFÍOS Y RIESGOS DE LA IA GENERATIVA..... | 10 |
| 6. <u>MARCO LEGAL Y PROTECCIÓN DE DATOS</u> | 11 |
| 7. <u>CONCLUSIONES</u> | 12 |
| 8. <u>BIBLIOGRAFIA</u> | 13 |

INTRODUCCIÓN

1.1. Contextualización del Entorno Digital Educativo

En la última década, y de manera exponencial tras la crisis sanitaria global, el ámbito educativo ha experimentado una transición disruptiva hacia la digitalización. La integración de plataformas de aprendizaje en línea (LMS), el uso de dispositivos personales en el aula (*Bring Your Own Device - BYOD*) y el almacenamiento de datos en la nube han redefinido el concepto de "aula". Sin embargo, esta apertura tecnológica ha expandido la superficie de ataque, convirtiendo a las instituciones educativas en objetivos primarios para los ciberdelincuentes debido a la vulnerabilidad intrínseca de los usuarios menores de edad y la posesión de bases de datos masivas con información sensible.

1.2. Justificación del Informe

La ciberseguridad en el aula ya no puede ser considerada una función secundaria del departamento de sistemas; es un componente crítico de la seguridad física y emocional del alumnado. El robo de identidad, el secuestro de datos institucionales (ransomware) y el acoso digital no solo comprometen la operatividad de los centros, sino que tienen repercusiones legales, financieras y psicológicas profundas. Este informe surge de la necesidad de establecer un marco de referencia que equilibre la libertad pedagógica con protocolos de protección técnica y educativa robustos.

1.3. Objetivos del Informe

El presente documento tiene como propósito fundamental:

- **Analizar el panorama actual de amenazas:** Identificar los vectores de ataque más comunes que afectan a centros educativos en el presente año.
- **Evaluar la vulnerabilidad del factor humano:** Comprender cómo la falta de concienciación digital en docentes y alumnos facilita la ingeniería social.
- **Establecer directrices preventivas:** Proponer un conjunto de medidas técnicas y normativas alineadas con los estándares internacionales de protección de datos.

- **Fomentar la cultura de la ciberseguridad:** Promover que la seguridad digital sea un eje transversal en el currículo académico y no solo una respuesta ante incidentes.

1.4. Alcance

Este análisis abarca desde la infraestructura de red física del centro educativo hasta el comportamiento digital de los usuarios en entornos híbridos, proporcionando una visión integral que facilite a los directivos y docentes la toma de decisiones informadas en materia de seguridad de la información.

2. LOS TRES PILARES DE LA SEGURIDAD INFORMÁTICA (TRÍADA CIA)

La seguridad de la información en el ámbito educativo no se limita a la instalación de un antivirus; se fundamenta en un modelo de equilibrio conocido como la **Tríada CIA** (por sus siglas en inglés: *Confidentiality, Integrity, Availability*). La ruptura de cualquiera de estos pilares compromete la estabilidad institucional y la seguridad del alumnado.

2.1. Confidencialidad: El Resguardo de la Privacidad

La confidencialidad garantiza que los datos sensibles sean accesibles únicamente para las personas debidamente autorizadas. En el aula, este pilar es crítico debido al manejo de información de menores de edad.

- **Aplicación Práctica:** Implementación de sistemas de **Control de Acceso Basado en Roles (RBAC)**. Por ejemplo, un docente debe visualizar las calificaciones de su grupo, pero no el historial médico de un alumno de otro curso; un estudiante no debe tener acceso a las actas de evaluación de sus compañeros.
- **Riesgos Asociados:** El acceso no autorizado a través de credenciales débiles o el robo de dispositivos físicos (laptops de docentes) que contengan bases de datos sin cifrar.
- **Herramienta de Control:** Uso de **Cifrado de Extremo a Extremo** y protocolos de autenticación robustos (MFA).

2.2. Integridad: La Veracidad de la Información Académica

La integridad asegura que la información se mantenga exacta, completa y libre de alteraciones no autorizadas, ya sean accidentales o malintencionadas. Un sistema educativo sin integridad pierde su validez legal y pedagógica.

- **Aplicación Práctica:** Garantizar que las actas de notas, los registros de asistencia y los certificados de grado no puedan ser modificados por estudiantes o agentes externos. Esto se logra mediante **Registros de Auditoría (Logs)** que permiten rastrear quién hizo qué cambio y en qué momento.
- **Riesgos Asociados:** Inyección de código malicioso en las bases de datos de la escuela o manipulación de archivos mediante el acceso a cuentas con privilegios de administrador mal gestionadas.
- **Herramienta de Control:** Implementación de **Firmas Digitales** y funciones *hash* para verificar que un documento no ha sido alterado desde su creación.

2.3. Disponibilidad: La Continuidad del Proceso de Aprendizaje

De nada sirve tener datos seguros y exactos si los usuarios no pueden acceder a ellos cuando los necesitan. La disponibilidad garantiza que los servicios educativos (plataformas como Moodle, Classroom o bases de datos de investigación) operen sin interrupciones.

- **Aplicación Práctica:** Asegurar que durante la semana de exámenes finales o periodos de inscripción, los servidores soporten la carga de tráfico y no sufran caídas que impidan el cumplimiento del calendario académico.
- **Riesgos Asociados:** Ataques de **Denegación de Servicio Distribuido (DDoS)**, fallos en el suministro eléctrico del centro de datos o ataques de *Ransomware* que cifran los servidores de la institución, dejando al colegio inoperativo durante días o semanas.

- **Herramienta de Control:** Estrategias de **Redundancia de Datos**, uso de balanceadores de carga y, fundamentalmente, una política estricta de **Backups (Copias de Seguridad)** alojadas fuera de la red principal.

3. RIESGOS Y AMENAZAS ACTUALES EN EL SECTOR EDUCATIVO

El sector educativo se ha consolidado como uno de los objetivos más rentables para el cibercrimen organizado. La combinación de infraestructuras tecnológicas a veces obsoletas, una cultura de ciberseguridad aún en desarrollo y la posesión de datos personales de menores crea un escenario de alto riesgo.

3.1. Amenazas Técnicas y de Infraestructura

Estas amenazas buscan vulnerar los sistemas informáticos del centro para obtener un beneficio económico o causar interrupción operativa.

- **Ransomware de Doble Extorsión:** Ya no se trata solo de cifrar los datos y pedir un rescate. Los atacantes ahora exhuman información sensible (expedientes psicopedagógicos o financieros) y amenazan con publicarlos si no se paga. Esto pone a las instituciones en un dilema legal y ético devastador.
- **Ataques de Denegación de Servicio (DDoS):** Inundar los servidores del colegio con tráfico falso para colapsar las plataformas de exámenes virtuales o inscripciones. En ocasiones, estos ataques son ejecutados de forma amateur por los mismos estudiantes usando herramientas de bajo costo.
- **Shadow IT (Tecnología en la Sombra):** El uso de aplicaciones, extensiones de navegador o software no autorizado por parte de docentes y alumnos que introducen vulnerabilidades no monitoreadas por el equipo de IT del centro.
- **Vulnerabilidades en el IoT Escolar:** Cámaras de seguridad, pizarras inteligentes y sistemas de climatización conectados que, si no están debidamente segmentados de la red principal, sirven como puerta de entrada para intrusos.

3.2. Ingeniería Social y Factor Humano

El eslabón más débil sigue siendo el usuario. Los atacantes explotan la confianza y la falta de formación digital.

- **Phishing Dirigido (Spear Phishing):** Correos electrónicos que suplantando la identidad de la dirección del centro o de plataformas oficiales (como Microsoft 365 o Google Workspace) para robar credenciales de acceso de profesores con privilegios de administrador.
- **Business Email Compromise (BEC):** Fraudes financieros donde el atacante intercepta comunicaciones de tesorería del colegio para desviar pagos de matrículas o proveedores a cuentas fraudulentas.

3.3. Riesgos en la Convivencia y Seguridad de los Menores

Más allá de los bits y bytes, existen amenazas que afectan directamente la integridad emocional y física del alumnado.

- **Ciberacoso Dinámico:** El acoso ya no termina al salir del aula; se extiende 24/7 a través de grupos de mensajería y redes sociales, utilizando herramientas de Inteligencia Artificial para crear *deepfakes* (imágenes o videos falsos) con el fin de humillar a compañeros o docentes.
- **Grooming y Suplantación de Identidad:** Delincuentes que se hacen pasar por estudiantes de la misma edad en juegos en línea o redes educativas para ganarse la confianza de los menores y obtener material sensible o encuentros físicos.
- **Desinformación y "Fake News":** La incapacidad de los estudiantes para distinguir fuentes fiables facilita la propagación de campañas de desinformación que pueden alterar el clima de convivencia escolar o promover retos virales peligrosos (*challenges*).

4. MEDIDAS DE PREVENCIÓN Y PROTOCOLOS DE ACTUACIÓN

La ciberseguridad efectiva no depende de una sola herramienta, sino de una estrategia multicapa que combine tecnología robusta con usuarios formados. A continuación, se detallan las medidas esenciales para blindar el entorno educativo.

4.1. Medidas de Infraestructura y Control Técnico

Son las barreras tecnológicas que la institución debe implementar para mitigar ataques automatizados y fugas de datos.

- **Segmentación de Redes (VLANs):** Es crítico separar la red de administración (donde están las notas y finanzas) de la red Wi-Fi para estudiantes y de la red de invitados. Esto evita que un malware en el móvil de un alumno salte a los servidores centrales.
- **Autenticación de Doble Factor (2FA/MFA):** Implementar obligatoriamente el segundo factor de autenticación para docentes y administrativos. El 99% de los ataques de robo de cuentas se detienen con esta medida simple.
- **Gestión de Parches y Actualizaciones:** Automatizar la actualización de sistemas operativos y software educativo. Las vulnerabilidades no corregidas (*exploits*) son la puerta de entrada más común para el ransomware.
- **Filtrado de Contenido y DNS Seguro:** Utilizar soluciones de seguridad en la nube que bloqueen automáticamente el acceso a sitios web de phishing, contenido para adultos o descargas ilegales desde la red del colegio.

4.2. Medidas Organizativas y de Gobernanza

Se refieren a las reglas del juego. Sin políticas claras, la tecnología no es suficiente.

- **Política de Uso Aceptable (PUA):** Un documento que alumnos, padres y docentes deben firmar, donde se establecen las normas de comportamiento digital, la propiedad de los datos y las consecuencias de un mal uso de los recursos del centro.

- **Plan de Respuesta ante Incidentes (PRI):** Establecer un protocolo de "Qué hacer si...". ¿A quién se avisa si se detecta un hackeo? ¿Cómo se aíslan los equipos infectados? La rapidez de respuesta determina la magnitud del daño.
- **Copias de Seguridad Bajo la Regla 3-2-1:** Mantener **3** copias de los datos, en **2** soportes diferentes (ej. nube y disco físico) y **1** de ellas fuera de la red principal (offline) para que no sea alcanzada por un virus.

4.3. Capacitación y Concienciación (El Factor Humano)

La educación es la mejor defensa. Un usuario que duda antes de hacer clic es más efectivo que cualquier firewall.

- **Alfabetización Digital Crítica:** Integrar en el currículo talleres sobre cómo identificar noticias falsas (*fake news*), cómo crear contraseñas seguras (usando frases en lugar de palabras simples) y los riesgos de la sobreexposición en redes sociales (*oversharing*).
- **Simulacros de Phishing:** Realizar pruebas controladas enviando correos falsos a los docentes para evaluar su capacidad de detección y reforzar la formación en aquellos que caigan en la trampa.
- **Cultura de Denuncia sin Castigo:** Fomentar un ambiente donde el alumno se sienta seguro reportando si ha sido víctima de un engaño o si ha cometido un error técnico, sin miedo a represalias inmediatas, para poder actuar a tiempo.

5. LA INTELIGENCIA ARTIFICIAL EN LA CIBERSEGURIDAD ESCOLAR

La integración de la IA en las aulas presenta una dualidad: es una herramienta de protección avanzada y, simultáneamente, un vector que sofisticada las amenazas existentes.

5.1. La IA como Herramienta de Defensa (Blue Teaming)

- **Detección de Anomalías en Tiempo Real:** Los sistemas de seguridad modernos usan aprendizaje automático (*Machine Learning*) para identificar comportamientos inusuales en la red del colegio (ej. un inicio de sesión de un docente a las 3:00 a.m. desde otro país) y bloquearlo automáticamente.
- **Sistemas de Tutoría Segura:** Implementación de *chatbots* educativos que filtran lenguaje inapropiado, detectan signos de depresión o acoso en las interacciones y protegen la privacidad de los datos del menor.

5.2. Desafíos y Riesgos de la IA Generativa

- **Deepfakes y Suplantación:** La facilidad para clonar voces o rostros mediante IA permite crear campañas de acoso altamente realistas o engañar a administrativos mediante llamadas que simulan ser del director solicitando transferencias de fondos.
- **Privacidad de los Prompts:** Los estudiantes suelen introducir datos personales o tareas completas en IAs públicas (como ChatGPT). Estas herramientas pueden almacenar dicha información, alimentando modelos de terceros y vulnerando la privacidad del alumno.

6. MARCO LEGAL Y PROTECCIÓN DE DATOS (COMPLIANCE)

El cumplimiento normativo no es opcional; es la base legal que protege a la institución ante demandas y sanciones.

- **Reglamento General de Protección de Datos (RGPD) / Leyes Locales:** Las escuelas manejan datos de "categoría especial" (menores, salud, religión). El centro debe contar con un **Delegado de Protección de Datos (DPD)** y realizar Evaluaciones de Impacto de Privacidad antes de adoptar nuevas apps.
- **Consentimiento Informado:** Se debe obtener autorización explícita de los tutores legales para el uso de biometría (huella dactilar para comedor), publicación de fotos en redes sociales y uso de plataformas en la nube.
- **Derecho a la Desconexión Digital:** Normativas recientes protegen el derecho de docentes y alumnos a no ser contactados por medios digitales fuera del horario lectivo, reduciendo el estrés y la exposición a riesgos fuera de control.

7. CONCLUSIONES

1. **Cultura sobre Tecnología:** La ciberseguridad no es un producto que se compra, sino un proceso continuo. El factor humano (docentes, alumnos y padres) es la primera y más importante línea de defensa.
2. **Enfoque Proactivo:** Las instituciones deben pasar de una postura reactiva (arreglar cuando algo falla) a una proactiva, realizando auditorías periódicas y simulacros de incidentes.
3. **Responsabilidad Compartida:** La seguridad del menor en el entorno digital es un esfuerzo tripartito entre la escuela, la familia y el Estado. La alfabetización digital debe ser una asignatura transversal en todas las etapas educativas.
4. **Adaptabilidad:** Ante la evolución de la IA, el marco de ciberseguridad escolar debe ser flexible y actualizarse anualmente para enfrentar amenazas que aún no conocemos.

8. BIBLIOGRAFÍA

Recuperado de: [Ciberseguridad en la Educación - Informe 2025](#)

Recuperado de: [Guía de Protección de Datos en Centros Educativos](#)

Recuperado de: [Manual de Ciberseguridad para Docentes](#)