ANÁLISIS CRÍTICO DE LA POLÍTICA DE CIBERSEGURIDAD DEL MEP: RETOS Y OPORTUNIDADES PARA SU OPTIMIZACIÓN

Mtr. Ricardo Aguirre Morice
Ministerio de Educación Pública de Costa Rica. Ingeniería Informática, Seguridad de la Información. Ciberseguridad.
ricardoaguirremorice@hotmail.com

RESUMEN

Este artículo evalúa la Política de Ciberseguridad del Ministerio de Educación Pública de Costa Rica (MEP) en relación con estándares internacionales como ISO 27001 y NIST CSF. Se identificaron fortalezas en su alineación con normativas nacionales, pero también brechas en áreas críticas como capacitación, gestión de incidentes y continuidad del negocio. A través de un enfoque comparativo y metodológico, se propone un plan de mejoras para garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

ABSTRACT

This article evaluates the Cybersecurity Policy of Costa Rica's Ministry of Public Education (MEP) in relation to international standards such as ISO 27001 and NIST CSF. Strengths were identified in its alignment with national regulations, but also gaps in critical areas such as training, incident management, and business continuity. Through a comparative and methodological approach, an improvement plan is proposed to ensure the confidentiality, integrity, and availability of institutional information.

Palabras clave: Ciberseguridad, políticas educativas, ISO 27001

INTRODUCCIÓN

El Ministerio de Educación Pública (MEP) de Costa Rica constituye una de las instituciones más extensas del país en términos de estructura administrativa y volumen de información gestionada. Según datos del MEP (2019), cuenta con aproximadamente 88 000 funcionarios públicos, distribuidos entre las oficinas centrales -incluido el despacho de la ministra-, 27 direcciones regionales ubicadas a lo largo del territorio nacional, cerca de 206 circuitos escolares y alrededor de 4825 centros educativos.

A partir de estas cifras, puede inferirse que el MEP es una organización con una alta superficie de exposición y un volumen significativo de datos bajo su gestión. Esta magnitud se incrementa aún más al considerar la población estudiantil. De acuerdo con Sibaja (2024), en el año 2023 se registró una matrícula de 1 123 964 estudiantes. Con base en esta información, se puede extrapolar que el MEP administra datos personales correspondientes al 24,03 % de la población nacional, al sumar tanto al personal funcionario como al estudiantado.

Esto significa que casi una cuarta parte de los datos personales del país se encuentra almacenada en los sistemas del MEP, sin contar los registros históricos acumulados por la institución. Se trata, por tanto, de una cantidad considerable de información concentrada en una sola organización, lo que la convierte en una verdadera mina de oro de datos, susceptible de ser explotada por quienes sepan cómo acceder y utilizar adecuadamente dicha información.

JUSTIFICACIÓN

Con base en los datos presentados con anterioridad, se justifica la necesidad de cuantificar el potencial que posee el MEP y, paralelamente, analizar el riesgo inherente que enfrenta desde una perspectiva estratégica. Costa Rica, como país con un sistema educativo público y obligatorio en los niveles de primaria y secundaria, garantiza que todos los ciudadanos, en algún

 ISSN: 2015-5392

momento de sus vidas, transiten por esta institución mediante sus diversas unidades descentralizadas. Esta característica posiciona a la educación nacional como una infraestructura crítica, dada su función esencial en la formación ciudadana y su alta exposición a riesgos de seguridad.

El MEP, al gestionar información personal sensible -tanto de menores de edad como de administradores de fondos públicos y funcionarios de la institución-, enfrenta riesgos significativos en términos de filtración de datos. Este panorama convierte a la organización en un posible objetivo de interés para actores maliciosos. Por tanto, resulta imperativo integrar elementos de ciberseguridad, ciberinteligencia y seguridad de la información en la estructura primaria del MEP, no solo como una medida de protección, sino también como una estrategia para fortalecer la resiliencia institucional frente a amenazas potenciales. Esta integración tiene como fin mitigar riesgos y garantizar la continuidad operativa, destacando la importancia de incorporar estos componentes dentro de las políticas y estrategias nacionales de protección de infraestructura crítica.

OBJETIVO:

Evaluar la Política de Ciberseguridad del Ministerio de Educación Pública (MEP) y proponer una modificación estructurada que optimice la protección de datos y fortalezca su capacidad de respuesta ante amenazas cibernéticas.

ANTECEDENTES:

Según Moreno (2019), la educación es un derecho de las personas a lo largo de su vida y constituye una responsabilidad del Estado, el cual debe garantizar tanto la alfabetización digital como el uso de las tecnologías de la información y la comunicación en los procesos educativos. Como señala el autor, la educación es la piedra angular de muchas naciones, y uno de los elementos fundamentales que la sostiene es la seguridad. Surge entonces la pregunta: ¿qué tipo de seguridad provee el Estado a las instituciones educativas?

En términos generales, se puede hablar de una seguridad jurídica y física, expresada en medidas como la instalación de alambrado, cercas perimetrales o la presencia de personal capacitado para salvaguardar la integridad de quienes asisten a estos centros. Esta concepción corresponde a una noción de seguridad entendida como “el conjunto de métodos que promueven un entorno seguro y protegido que permite a las personas desarrollar sus actividades cotidianas” (Purpura, 2006, p. 20).

A partir de esta descripción, puede afirmarse que la seguridad es uno de los pilares esenciales para el funcionamiento de cualquier sociedad que aspire a una vida cotidiana estable. Esta idea es respaldada por el filósofo humanista Abraham Maslow, quien en su teoría de la motivación humana sitúa la necesidad de seguridad y protección en el segundo nivel de su jerarquía, justo después de las necesidades fisiológicas básicas . Maslow plantea que el ser humano debe avanzar progresivamente desde la base de dicha pirámide hasta alcanzar la autorrealización.

Fig. 1. Pirámide de Maslow.

Si se considera que las instituciones educativas albergan tanto a personas en proceso de formación como a cientos de profesionales comprometidos con ese fin, resulta evidente que todos los actores deben velar por la seguridad de la comunidad educativa. Sin embargo, esta seguridad no puede limitarse únicamente al ámbito físico o tradicional; también debe extenderse al entorno digital.

[1]La pirámide de Maslow es una teoría psicológica que organiza las necesidades humanas en cinco niveles jerárquicos: fisiológicas (alimento, agua, sueño), de seguridad (protección, estabilidad), sociales (amor, pertenencia), de estima (reconocimiento, respeto) y de autorrealización (desarrollo personal, creatividad). Cada nivel debe satisfacerse parcialmente antes de avanzar al siguiente.

Desde finales del siglo XX, con la expansión del acceso a Internet, se ha producido una creciente digitalización de los espacios educativos. Este fenómeno se ha intensificado en cada década, y cobró especial relevancia tras la pandemia global de COVID-19, la cual sumió al mundo en una interconexión y dependencia aún mayores de las tecnologías digitales. Como consecuencia, aumentó de forma significativa la exposición a los riesgos asociados a este entorno, haciendo urgente una revisión de las estrategias de protección y resiliencia institucional.

La tecnología, en la vida moderna, ha incrementado significativamente los riesgos en materia de seguridad de la información. Los ciberataques -como el robo de datos, el ransomware y el phishing- se han convertido en amenazas constantes que buscan explotar vulnerabilidades en sistemas y redes con el fin de obtener acceso no autorizado a información sensible. La expansión del Internet de las Cosas (IoT) ha agravado esta problemática, ya que muchos dispositivos conectados, a menudo desprotegidos o mal configurados, representan nuevos puntos de entrada para los atacantes. Asimismo, la creciente dependencia de servicios en la nube y de soluciones de almacenamiento digital ha expuesto tanto a empresas como a individuos a fallos de seguridad asociados con accesos indebidos y configuraciones erróneas.

La seguridad de la información también enfrenta un desafío crítico relacionado con el factor humano, el cual continúa siendo una de las principales vulnerabilidades. La falta de concienciación sobre prácticas seguras, el uso de contraseñas débiles y la susceptibilidad a técnicas de ingeniería social son problemáticas recurrentes que facilitan la explotación de datos confidenciales. Paralelamente, la cantidad masiva de información personal almacenada en plataformas digitales ha generado crecientes preocupaciones sobre la privacidad, incluyendo riesgos de seguimiento no autorizado, uso indebido de datos y su comercialización sin consentimiento.

Por todo lo anterior, se hace imprescindible añadir una capa adicional de protección a las ya existentes, especialmente en sectores estratégicos como la educación. Es necesario, incluso, replantear la jerarquía de necesidades de Maslow, incorporando la seguridad de la información como un componente esencial para resguardar la infraestructura crítica del sistema educativo. Proteger los datos de los ciudadanos que acceden a estos servicios es indispensable para la formación integral de quienes construirán el futuro de la nación.

La creación de una cultura de seguridad de la información en la sociedad -y particularmente en los entornos educativos- es fundamental, dada la centralidad de la tecnología en la vida cotidiana y los riesgos emergentes que se presentan en escenarios catastróficos o altamente tecnologizados. En un contexto donde la información personal está digitalizada y la identidad puede ser manipulada o incluso robada, emergen amenazas como el otorgamiento indebido de una identidad a terceros o a humanos digitales. Esto podría derivar en accesos no autorizados a recursos críticos, en decisiones legales erróneas o incluso en la suplantación total de una identidad digital.

En el ámbito educativo, donde los datos de estudiantes y docentes son especialmente vulnerables, la falta de medidas de seguridad incrementa el riesgo de estas amenazas. La posibilidad de clonar o reutilizar una identidad educativa con fines maliciosos -como el fraude académico o el acceso indebido a recursos institucionales- constituye un peligro real.

Una cultura sólida de seguridad de la información también es clave para prevenir el uso indebido de identidades digitales y garantizar la integridad de los datos en una sociedad cada vez más interconectada. Sin una formación adecuada en prácticas seguras, las personas son más susceptibles a ataques sofisticados capaces de usurpar su identidad no solo en redes sociales o plataformas financieras, sino también en entornos digitales avanzados, donde humanos artificiales pueden simular comportamientos, voces o decisiones de individuos reales.

Este tipo de amenazas plantea implicaciones éticas y legales profundas, ya que una identidad comprometida en un entorno digital hiperconectado puede ser utilizada para manipular sistemas, cometer delitos o distorsionar realidades personales y sociales. Por ello, integrar la educación en ciberseguridad desde edades tempranas no solo promueve una ciudadanía más consciente y resiliente, sino que también fortalece la capacidad colectiva de anticiparse y responder ante escenarios críticos, donde las consecuencias de una identidad comprometida podrían ser irreversibles.

ISSN: 2015-5392

Es en este punto donde debe iniciarse el proceso de comprensión de algunos términos clave, con el fin de establecer el contexto en el que se debe actuar desde una etapa previa. Purpura (2006) define la prevención como "métodos de reducción de las posibilidades de que ocurra una pérdida y también los gastos asociados" (p. 21). A partir de esta definición, puede inferirse que la prevención constituye una estrategia orientada a disminuir los posibles efectos adversos de un evento no deseado.

Asimismo, el mismo autor introduce el concepto de prevención de pérdidas, que describe como "una gama más amplia de métodos para proteger a las personas y la propiedad" (p. 20). Este conjunto de métodos integra elementos esenciales, entre ellos la estrategia, entendida como un procedimiento que puede aplicarse de forma metódica para obtener resultados consistentes, sin importar el contexto en el que se implemente. Su finalidad última es salvaguardar los bienes o las personas que se desean proteger.

Es en esta confluencia conceptual donde se vislumbran los marcos internacionales de seguridad de la información como referentes fundamentales para la estructuración de políticas eficaces de protección:

Posicionamiento teórico
Explicación de conceptos clave: Confidencialidad, integridad, disponibilidad.
Resumen de estándares relevantes (ISO 27001, NIST) ISO 27001 y 27002

Las normas ISO/IEC 27001 e ISO/IEC 27002 constituyen pilares fundamentales en la gestión de la seguridad de la información a nivel organizacional. La ISO/IEC 27001 establece un marco integral para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), siendo una norma certificable que define los requisitos esenciales para administrar eficazmente la seguridad informática en cualquier entidad. Su contraparte, la ISO/IEC 27002, actúa como una guía complementaria detallada, ofreciendo directrices específicas y mejores prácticas para la implementación efectiva de los controles de seguridad.

La relevancia de estas normas se manifiesta en diversos aspectos críticos para las organizaciones. En primer lugar, proporcionan una protección robusta frente a filtraciones de datos y ataques cibernéticos mediante un enfoque sistemático de gestión de riesgos. Asimismo, facilitan el cumplimiento de regulaciones legales como el GDPR, HIPAA y PCI-DSS, lo cual resulta esencial en el entorno normativo actual. Las organizaciones que obtienen la certificación ISO/IEC 27001 no solo demuestran un compromiso serio con la seguridad de la información, sino que también adquieren una ventaja competitiva significativa al generar mayor confianza entre clientes y socios estratégicos.

La estructura de estas normas se organiza de forma meticulosa en cuatro categorías principales de controles. Los controles organizacionales, que comprenden 37 elementos, abordan aspectos clave como el establecimiento de políticas de seguridad, la asignación de roles y responsabilidades, la evaluación sistemática de riesgos y el aseguramiento del cumplimiento normativo. Los controles relacionados con las personas, con 8 elementos, se enfocan en aspectos fundamentales como la concienciación en seguridad, la capacitación del personal y la gestión de accesos basada en funciones claramente definidas.

Los controles físicos, integrados por 14 elementos, se centran en la protección tangible de la infraestructura, incluyendo el control de acceso a las instalaciones, la protección de equipos y activos, y la adecuada gestión de residuos y medios de almacenamiento. Por su parte, los controles tecnológicos, compuestos por 34 elementos, constituyen una capa importante de defensa que abarca la protección contra malware, la seguridad en redes y comunicaciones, el cifrado de datos y la gestión de vulnerabilidades.

La implementación de estas normas sigue un proceso estructurado basado en el ciclo de vida del SGSI, que inicia con la definición clara del alcance y los objetivos. Esta fase implica la identificación precisa de los procesos, activos y sistemas que estarán bajo protección, así como el establecimiento de metas medibles y alcanzables. Posteriormente, se desarrolla una evaluación exhaustiva de riesgos, que incluye la clasificación de activos de información, la valoración de amenazas y vulnerabilidades, y la implementación de controles específicos para mitigar los riesgos identificados.

La fase de implementación requiere el desarrollo de políticas y procedimientos formales, la conformación de un equipo competente de respuesta a incidentes y la aplicación de medidas técnicas de protección como el cifrado avanzado, los sistemas de respaldo y los controles de acceso robustos. Este proceso se complementa con auditorías internas periódicas y un compromiso con la mejora continua, que incluye revisiones constantes de cumplimiento y la ejecución de acciones correctivas cuando sea necesario.

Entre las medidas específicas de seguridad se destacan el control de acceso basado en el principio del menor privilegio, la autenticación multifactor, la implementación de firewalls y sistemas de detección de intrusos, así como el uso del cifrado AES-256 para la protección de datos. Asimismo, se subraya la importancia de programas continuos de formación en seguridad informática dirigidos al personal, junto con la adopción de medidas específicas para entornos en la nube, incluyendo plataformas como AWS, Azure y Google Cloud.

Aplicación de ISO/IEC 27001 e ISO/IEC 27002 en centros educativos y oficinas centrales de una organización educativa

La adopción de las normas ISO/IEC 27001 e ISO/IEC 27002 en centros educativos y oficinas administrativas de una organización educativa establece un marco estructurado de seguridad para la protección de la información académica, administrativa y personal de estudiantes, docentes y personal institucional. Esta implementación responde a la necesidad de garantizar la integridad, confidencialidad y disponibilidad de la información, especialmente en un contexto donde la digitalización educativa y el uso de plataformas en la nube son cada vez más frecuentes.

1. Implementación en centros educativos

En los centros educativos, la aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 se enfoca en la protección de los datos de estudiantes y docentes, así como en la seguridad de los sistemas digitales utilizados en el entorno educativo. Las principales medidas a implementar incluyen:

Controles organizacionales:

- Definir políticas de seguridad para el manejo de información sensible, como calificaciones, registros médicos y datos personales de los estudiantes.
- Establecer protocolos para la gestión de incidentes de ciberseguridad, asignando roles y responsabilidades al personal docente y administrativo.
- Implementar un programa de formación en ciberseguridad dirigido a docentes y estudiantes, con el objetivo de fomentar una cultura de protección de datos desde edades tempranas.

Controles de personas:

- Capacitar de forma periódica a docentes y estudiantes en temas como phishing, ingeniería social y buenas prácticas de seguridad digital.
- Gestionar los accesos a plataformas educativas y bases de datos mediante mecanismos de autenticación multifactor (MFA) y privilegios basados en roles.

Controles físicos:

- Garantizar que los dispositivos ubicados en laboratorios de cómputo y aulas virtuales cuenten con medidas de acceso restringido, a fin de evitar usos no autorizados.
- Implementar medidas de seguridad en las redes Wi-Fi institucionales para prevenir accesos indebidos y ataques de intermediario (Man-in-the-Middle, MITM).

Controles tecnológicos:

- Aplicar mecanismos de cifrado a las bases de datos académicas para proteger la información sensible.
- Implementar firewalls y sistemas de detección de intrusos para evitar accesos no autorizados a la red institucional.
- Asegurar que todos los dispositivos conectados a la red educativa cuenten con protección contra malware y se mantengan actualizados frente a vulnerabilidades.

ISSN: 2015-5392

2. Implementación en oficinas centrales de la organización educativa

Las oficinas centrales de una organización educativa tienen un enfoque predominantemente administrativo y estratégico, lo que exige controles más estrictos para la protección de la información institucional. La aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en este entorno incluye:

Controles organizacionales:

- Implementar políticas de seguridad para la gestión de datos en plataformas como ERP, LMS y sistemas de nómina.
- Cumplir con las leyes de protección de datos, como el GDPR o la normativa local, para evitar sanciones legales.
- Establecer un comité de seguridad encargado de supervisar el cumplimiento del SGSI y promover su mejora continua.

Controles relacionados con las personas:

- Aplicar programas de concienciación en ciberseguridad dirigidos al personal administrativo, con énfasis en la prevención de fraudes y filtraciones de información.
- Definir políticas de acceso a documentos administrativos sensibles, asegurando que solo el personal autorizado pueda consultarlos.

Controles físicos:

- Implementar medidas de seguridad en servidores y centros de datos para evitar accesos no autorizados.
- Utilizar sistemas de videovigilancia y control de acceso con credenciales biométricas.

Controles tecnológicos:

- Aplicar cifrado AES-256 en documentos críticos, como contratos, registros financieros y planes estratégicos.
- Realizar auditorías de seguridad periódicas para identificar y corregir vulnerabilidades en la infraestructura digital.

Aplicación del marco NIST en el entorno educativo

El National Institute of Standards and Technology (NIST), organismo del Departamento de Comercio de los Estados Unidos, desarrolla estándares, directrices y buenas prácticas para diversos sectores. En el contexto de la seguridad de la información, se recomienda la aplicación de las guías NIST SP 800-53 (controles de seguridad para sistemas de información) y NIST SP 800-30 (análisis de riesgos).

La aplicación adaptada de la NIST 800-53 requiere un enfoque detallado. Se inicia con la gestión de riesgos, que incluye la adopción del Risk Management Framework (RMF), el cual promueve un enfoque sistemático para evaluar y mitigar amenazas. Dentro de este marco, la evaluación de riesgos (RA) permite identificar activos críticos y analizar las vulnerabilidades asociadas.

La NIST 800-53 propone 20 familias de controles y destaca varios de ellos como fundamentales para una política de seguridad eficaz:

- Control de acceso (AC): Debe implementarse la autenticación multifactor (MFA) en todos los entornos donde se requiera autenticación, siendo de uso obligatorio. Además, se deben controlar los privilegios y accesos mediante una gestión basada en roles, así como realizar supervisión y auditoría del acceso a información crítica, asegurando que únicamente los usuarios autorizados puedan acceder a ella.
- Gestión de identidad y autenticación (IA): Es esencial el uso de contraseñas seguras y autenticación robusta, junto con la implementación de una infraestructura de clave pública (PKI). Asimismo, se debe restringir el acceso a usuarios no autorizados, especialmente en oficinas centrales y regionales.
- Monitoreo, auditoría y rendición de cuentas (AU): Es de suma importancia registrar y auditar los eventos de seguridad críticos, implementar un sistema de gestión de información y eventos de seguridad (SIEM) para una respuesta inmediata ante incidentes, y garantizar la notificación y mitigación oportuna. La estructura institucional requiere segmentación por regiones, con controles auditables y supervisión de eventos. Para ello, deben crearse puestos de vigilancia regional o establecer una red nacional que permita la vigilancia centralizada.
- Protección de la integridad del sistema y la información (SI): Se recomienda el uso de soluciones antimalware, la prevención de ejecución de código malicioso, el monitoreo de la integridad de archivos críticos y la segmentación de redes para reducir el impacto de posibles ataques. En este apartado, se hace evidente la necesidad de una homogenización organizacional mediante una política que estandarice el uso de software institucional, con el fin de coordinar la prevención y erradicación de amenazas.

- Respuesta a incidentes (IR): Es fundamental desarrollar un plan de respuesta a incidentes, realizar simulacros regulares y asegurar una comunicación efectiva, así como una rápida recuperación de los sistemas afectados. Este punto requiere entrenamiento y capacitación del personal a nivel nacional sobre cómo actuar y comunicarse adecuadamente frente a eventos adversos, especialmente porque muchos incidentes deben ser atendidos por el MICITT.
- Seguridad en la cadena de suministro (SR): La evaluación de proveedores y terceros desde una perspectiva de seguridad, la implementación de controles para la protección de datos en la cadena de suministro, y la verificación de software y hardware para evitar ataques de tipo "puerta trasera" son pasos esenciales. En este punto, debe fortalecerse la aplicación de la Ley 8968 para proteger a los clientes internos y externos, evitando la filtración de información. Además, se debe proteger la cadena de suministro, particularmente en el caso del MEP, que contrata múltiples servicios a proveedores. Toda junta administrativa o entidad que maneje fondos públicos debe regirse por la Ley 9986, Ley General de Contratación Pública.
- Protección de datos y privacidad (PT): Se debe aplicar cifrado tanto en datos en reposo como en tránsito, utilizar controles que minimicen la exposición de información personal e implementar medidas de privacidad desde el diseño, con el objetivo de preservar la confidencialidad e integridad de los datos. Es trascendental fortalecer la conciencia institucional sobre la Ley 8968 y el tratamiento de datos personales, especialmente en lo relativo a expedientes del personal, información financiera de becas y comedores escolares, datos médicos, adecuaciones curriculares y casos de alta dotación. Además, se recomienda estandarizar, mediante un acuerdo institucional, que todo dispositivo adquirido cuente con cifrado y funciones biométricas de fábrica.

Implementación de una política de seguridad

Para una política de seguridad eficaz, se deben establecer normas de acceso basadas en roles y niveles de seguridad, desarrollar planes de respuesta a incidentes con procedimientos claros, ofrecer capacitación continua en ciberseguridad para sensibilizar y formar al personal, y mantener un sistema de monitoreo y auditoría constante para revisar registros (logs), controlar el acceso a los datos y detectar posibles anomalías. Asimismo, es esencial que todos los proveedores y contratistas cumplan con los estándares de seguridad establecidos.

Análisis de riesgos: NIST 800-30 y marco normativo costarricense

Otro elemento fundamental es el análisis de riesgos, donde entra en juego la guía NIST 800-30. No obstante, en el contexto costarricense, debe considerarse la Ley Nacional de Emergencias y Prevención del Riesgo Nº 8488, así como normativa complementaria relevante, con el objetivo de unificar criterios que permitan establecer un enfoque coherente en la construcción de un entorno digital seguro.

La seguridad de la información en centros educativos y oficinas administrativas constituye un pilar esencial para garantizar la integridad, confidencialidad y disponibilidad de los datos. El documento NIST 800-30 proporciona un marco sólido para la evaluación de riesgos en sistemas de información, lo que permite la implementación de controles efectivos para prevenir incidentes de ciberseguridad. A su vez, documentos clave como la Política Nacional de Gestión del Riesgo 2016–2030, el Plan Nacional de Gestión del Riesgo 2021–2025 y la Estrategia de Gestión del Riesgo de Desastres en el Sector Educativo 2022–2026 subrayan la necesidad de fortalecer la resiliencia digital en las instituciones educativas y administrativas del país.

Se presentan así los principales elementos aplicables en materia de seguridad de la información y ciberseguridad en entornos educativos, con el fin de garantizar la protección de datos, la continuidad de los servicios institucionales y la consolidación de una cultura de seguridad digital.

1. Gestión de riesgos en la seguridad de la información

La NIST 800-30 enfatiza la importancia de la gestión de riesgos como punto de partida para cualquier estrategia de ciberseguridad. En los ámbitos educativo y administrativo, esto implica:

- Identificación de activos críticos: Sistemas de gestión del aprendizaje (LMS), bases de datos de estudiantes y docentes, plataformas de comunicación interna y externa, servidores de documentos y redes institucionales.

ISSN: 2015-5392

- Análisis de amenazas: Desde ataques de phishing y malware, hasta suplantación de identidad y accesos no autorizados a datos sensibles.
- Evaluación de vulnerabilidades: Infraestructura desactualizada, contraseñas débiles, falta de segmentación de redes y ausencia de autenticación multifactor.
- Determinación del impacto potencial: Un ciberataque puede comprometer registros académicos, exponer datos personales y paralizar sistemas administrativos esenciales.
- Estrategias de mitigación: Implementación de cifrado, realización de copias de seguridad periódicas y monitoreo en tiempo real de amenazas.

2. Protección de infraestructura crítica en entornos educativos

Los centros educativos y oficinas administrativas manejan grandes volúmenes de información sensible, por lo que es esencial contar con una infraestructura tecnológica segura y resiliente. Se recomienda lo siguiente:

- Segmentación de redes: Separar las redes académicas, administrativas y de acceso público para evitar intrusiones no autorizadas.
- Cifrado de datos: Proteger las bases de datos mediante algoritmos de cifrado robustos que resguarden la información confidencial.
- Uso de firewalls y sistemas de prevención/detección de intrusiones (IPS/IDS): Controlar y monitorear el tráfico de red para detectar y bloquear actividades sospechosas.
- Autenticación multifactor (MFA): Reforzar el acceso a plataformas digitales mediante la utilización de credenciales adicionales.
- Actualización y parcheo de sistemas: Mantener el software y el hardware al día para prevenir la explotación de vulnerabilidades.

3. Concienciación y capacitación en ciberseguridad

Uno de los eslabones más débiles en la seguridad de la información es el factor humano. Por ello, es fundamental fomentar una cultura de ciberseguridad en la comunidad educativa y administrativa mediante:

- Capacitaciones regulares: Sensibilizar a docentes, estudiantes y personal administrativo sobre amenazas como phishing, ingeniería social y malware.
- Políticas de uso responsable de dispositivos y redes: Establecer normativas claras para el uso adecuado de dispositivos personales en entornos institucionales.
- Ejercicios de simulación de ataques: Realizar pruebas de phishing y simulacros de respuesta ante incidentes para evaluar la preparación de los usuarios.
- Gestión de accesos y permisos: Aplicar el principio de mínimo privilegio, limitando el acceso a información sensible únicamente a usuarios autorizados.

4. Planes de continuidad y respuesta ante incidentes

Documentos clave de gestión del riesgo en Costa Rica, como el Plan Nacional de Gestión del Riesgo 2021–2025, destacan la importancia de contar con estrategias de respuesta y recuperación ante incidentes de seguridad informática. Para ello, se deben establecer:

- Planes de respuesta ante incidentes: Procedimientos estructurados para identificar, contener, erradicar y recuperar los sistemas afectados por ciberataques.
- Copias de seguridad periódicas: Implementación de backups en servidores físicos y en la nube, con políticas claras de recuperación.
- Centros de operaciones de seguridad (SOC): Monitoreo en tiempo real de eventos de ciberseguridad para detectar y mitigar ataques de manera proactiva.
- Simulacros de ciberataques y desastres tecnológicos: Evaluar la capacidad de respuesta de la institución frente a eventos críticos.

ANÁLISIS: POLÍTICA DE CIBERSEGURIDAD DEL MEP

Este proceso pretende generar debate y concienciar sobre los elementos débiles o ausentes en la política de ciberseguridad y seguridad de la información del MEP. Con el fin de facilitar su comprensión y sistematizar la información, esta se ha condensado de la siguiente manera:

Categoría	Debilidad o Inconsistencia	Impacto Potencial
Inconsistencias Técnicas	Falta de especificidad en la implementación de medidas técnicas	Implementaciones ineficaces que dejan vulnerabilidades abiertas
Inconsistencias Técnicas	Ausencia de un enfoque basado en riesgos	No hay un método claro para evaluar y mitigar amenazas
Inconsistencias Técnicas	No se integra con estándares internacionales como ISO 27001 o NIST	Falta de alineación con estándares globales, lo que reduce la efectividad
Inconsistencias Técnicas	Autenticación multifactor (MFA) opcional en lugar de obligatoria	Mayor riesgo de accesos no autorizados a sistemas críticos
Inconsistencias Técnicas	No se menciona el cifrado de extremo a extremo para comunicaciones y almacenamiento	Mayor exposición a ataques de intercepción y robo de datos
Gestión y Cumplimiento	No se especifican sanciones claras en caso de incumplimiento	Falta de disuasión y cumplimiento deficiente de la política
Gestión y Cumplimiento	Falta de monitoreo continuo y respuesta a incidentes en tiempo real	Las amenazas pueden no detectarse a tiempo, aumentando el daño
Gestión y Cumplimiento	No se detallan mecanismos de auditoría y control de cumplimiento	Falta de supervisión efectiva que permita verificar el cumplimiento
Gestión y Cumplimiento	No hay un plan de continuidad del negocio ni recuperación ante desastres	Institución vulnerable a interrupciones prolongadas por ataques
Gestión y Cumplimiento	Falta de requerimientos estrictos de seguridad en la contratación de terceros	Proveedores pueden representar una puerta de entrada a ataques
Operativos y educativos	Capacitación insuficiente en ciberseguridad para funcionarios	Usuarios mal preparados pueden ser el punto débil en la seguridad
Operativos y educativos	No hay estrategias concretas contra ataques de ingeniería social (phishing)	Mayor exposición a fraudes y engaños dirigidos a funcionarios
Operativos y educativos	No se establecen controles claros para el uso de dispositivos personales (BYOD)	Riesgo de filtración de datos por falta de control sobre dispositivos externos
Operativos y educativos	Definición ambigua de responsabilidades entre distintas direcciones del MEP	Dificultad en la aplicación de la política por falta de claridad en roles
Operativos y educativos	No se establece un proceso de actualización periódica de la política	Riesgo de que la política quede obsoleta frente a nuevas amenazas

Fuente de elaboración propia

ISSN: 2015-5392

1. Ausencia de especificidad técnica

Por lo expresado anteriormente, se puede afirmar que la política presenta vacíos significativos en la implementación técnica de seguridad. Aunque se mencionan herramientas fundamentales como firewalls e IDS/IPS, no se establecen parámetros específicos para su implementación efectiva. La ausencia de estándares mínimos y protocolos de actualización compromete la solidez del sistema de seguridad.

Impacto

Esta falta de especificidad técnica puede derivar en:

- Implementaciones inconsistentes entre departamentos.
- Dificultad para evaluar el cumplimiento de las medidas de seguridad.
- Vulnerabilidades potenciales debido a la inexistencia de estándares claros.

Recomendaciones de mejora

- Es necesario desarrollar un anexo técnico que especifique:
- Estándares mínimos para las configuraciones de seguridad.
- Protocolos detallados de implementación y mantenimiento.
- Integración con marcos de referencia internacionales como ISO/IEC 27001 y NIST.

2. GESTIÓN DE RIESGOS Y CUMPLIMIENTO

La política carece de una metodología estructurada para la gestión de riesgos y no establece mecanismos claros de cumplimiento ni de rendición de cuentas (accountability). La falta de sanciones específicas y de procesos de auditoría debilita su capacidad de aplicación.

Impacto

Estas carencias generan:

- Dificultad para priorizar recursos y esfuerzos en materia de seguridad.
- Ambigüedad en cuanto a las consecuencias por incumplimiento.
- Imposibilidad de medir eficazmente el nivel de seguridad.

Recomendaciones de mejora

Se recomienda incorporar:

- Una metodología detallada de evaluación y gestión de riesgos.
- Un régimen de sanciones específico y gradual.
- Procedimientos de auditoría con plazos y métricas claramente definidos.

3. Respuesta a incidentes y continuidad operativa

La política no contempla de forma adecuada la gestión de incidentes ni la continuidad operativa. Se carece de un framework integral para el manejo de crisis y la recuperación ante desastres.

Impacto

Esta omisión puede traducirse en:

- Respuestas desorganizadas frente a incidentes de seguridad.
- Tiempos de recuperación prolongados.
- Pérdida potencial de datos críticos.

Recomendaciones de mejora

Es imprescindible desarrollar:

- Un plan detallado de respuesta ante incidentes.
- Protocolos de continuidad del negocio con asignación clara de roles.
- Procedimientos de recuperación ante desastres con tiempos objetivos definidos.

4. Factor humano y capacitación

La política subestima el papel del factor humano en la seguridad de la información. La ausencia de programas estructurados de capacitación y concienciación representa un riesgo considerable.

Impacto

Estas deficiencias pueden provocar:

- Mayor exposición a ataques de ingeniería social.
- Comportamientos inseguros por parte del personal.
- Incidentes de seguridad derivados del error humano.

Recomendaciones de mejora

Es esencial implementar:

- Programas obligatorios de capacitación con evaluaciones periódicas.
- Simulacros regulares de ataques de phishing.
- Políticas claras sobre el uso de dispositivos personales.

5. Falta de control sobre los datos personales

En años anteriores, se han presentado incidentes relacionados con el manejo de datos personales en el MEP. Parte de esta situación se ve reflejada en las omisiones y debilidades de la política actual

Problema identificado	Impacto potencial
Falta de aplicación de la Ley 8968 en la política de ciberseguridad	Riesgo legal y posibles sanciones por incumplimiento de la legislación de protección de datos
No se establecen mecanismos claros para la recolección, tratamiento y almacenamiento de datos personales	Vulnerabilidad ante filtraciones y mal uso de información personal
No se garantiza el derecho a la autodeterminación informativa conforme a la Ley 8968	Falta de transparencia y confianza en el manejo de información de estudiantes y funcionarios
No se definen procesos de consentimiento informado para el tratamiento de datos	Riesgo de demandas o denuncias por uso indebido de datos personales
No se especifican medidas de seguridad para la protección de datos personales	Mayor exposición a ataques y fugas de información sensible
No se aborda el derecho de acceso, rectificación y eliminación de datos personales	Usuarios sin herramientas para corregir o eliminar sus datos de sistemas del MEP
No se establecen lineamientos sobre la transferencia de datos a terceros	Riesgo de transferencia inadecuada de datos a empresas o terceros sin control
No se menciona la anonimización de datos como una práctica obligatoria	Exposición innecesaria de información sensible que podría ser usada de manera malintencionada
No se prevén sanciones o medidas disciplinarias por incumplimiento en la protección de datos	Ausencia de consecuencias fomenta el incumplimiento de buenas prácticas en protección de datos
No se especifica un ente responsable de velar por el cumplimiento de la Ley 8968 dentro del MEP	No hay un equipo o departamento específico que garantice la correcta aplicación de la normativa

ISSN: 2015-5392

La política actual presenta graves omisiones en relación con el cumplimiento de la Ley 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales. No se establecen mecanismos fundamentales para garantizar la protección de los datos ni se designan responsables claros para su implementación.

1. Impacto legal

La falta de alineación con la Ley 8968 expone al MEP a:

- Sanciones legales y administrativas.
- Vulnerabilidad ante demandas por el mal manejo de datos.
- Incumplimiento de obligaciones constitucionales en materia de autodeterminación informativa.

Recomendaciones normativas

Es necesario implementar:

- Un marco específico de cumplimiento de la Ley 8968.
- La designación de un oficial de protección de datos.
- Procedimientos claros para el ejercicio de derechos ARCO.

2. Gestión de datos personales

La política carece de procedimientos específicos para:

- La recolección y el tratamiento de datos personales.
- Procesos de consentimiento informado.
- Mecanismos de anonimización de información sensible.

Impacto operativo

Estas carencias resultan en:

- Riesgo de filtración de información personal.
- Falta de transparencia en el manejo de datos.
- Vulnerabilidad ante usos no autorizados de información.

Recomendaciones de mejora

Debe establecerse:

- Protocolos detallados para la recolección y tratamiento de datos.
- Sistemas formales de consentimiento informado.
- Procedimientos obligatorios de anonimización.

3. Derechos de las personas titulares de datos

La política no contempla adecuadamente:

- Mecanismos para ejercer derechos ARCO.
- Procedimientos de rectificación de datos.
- Protocolos de eliminación de información personal.

Impacto en los usuarios

Esta omisión afecta:

- La capacidad de las personas usuarias para controlar su información.
- La transparencia en el tratamiento de los datos.
- La confianza en los sistemas del MEP.

Recomendaciones de implementación

Es necesario desarrollar:

- Plataformas para el acceso y gestión de datos personales.
- Procedimientos claros de rectificación y actualización.
- Sistemas eficaces de eliminación de información.

4. Transferencia y seguridad de los datos

La política no establece:

- Lineamientos para la transferencia de datos a terceros.
- Requisitos de seguridad específicos para la información personal.
- Controles efectivos sobre el acceso a datos sensibles.

Impacto en la seguridad

Estas carencias generan:

- Riesgos en la transferencia indebida de datos.
- Accesos no autorizados a información confidencial.
- Exposición innecesaria de datos sensibles.

Recomendaciones de seguridad

Debe implementarse:

- Protocolos para la transferencia segura de datos.
- Controles de acceso granulares y auditables.
- Sistemas de monitoreo y auditoría continua.

5. Responsabilidad y cumplimiento

La política carece de:

- Asignación clara de responsabilidades.
- Sanciones específicas por incumplimiento.
- Mecanismos de supervisión y control efectivos.

Impacto institucional

Esta situación se traduce en:

- Falta de responsabilidad concreta.
- Dificultad para implementar medidas correctivas.
- Riesgo de incumplimiento sistemático.

Recomendaciones estructurales

Es fundamental establecer:

- Un comité institucional de protección de datos.
- Un régimen sancionatorio específico.
- Un sistema regular de auditoría y supervisión.

CONCLUSIONES

La política de ciberseguridad del MEP se presenta como un documento carente de sentido práctico, cuya estructura refleja una profunda desconexión entre su propósito declarado y la realidad de la gestión de la seguridad de la información. Aunque en su redacción se incluyen principios generales y terminología técnica propia del ámbito, la ausencia de lineamientos concretos, mecanismos de control y estrategias efectivas de implementación la convierten en un instrumento vacío, destinado más a cumplir con un requisito burocrático que a ofrecer una guía real para la protección de la información y de la infraestructura tecnológica de la institución.

Desde una perspectiva crítica, resulta evidente que este documento no solo carece de coherencia interna, sino que también incurre en una omisión grave respecto al cumplimiento de marcos normativos fundamentales, como la Ley 8968. La recolección, tratamiento, almacenamiento y eliminación de datos personales no están regulados de forma adecuada, lo que deja a estudiantes y funcionarios expuestos a un manejo arbitrario y potencialmente riesgoso de su información. La ausencia de medidas concretas de anonimización, transparencia en la gestión de datos y mecanismos de fiscalización eficaces abre la puerta a vulneraciones de derechos fundamentales, sin un protocolo claro de prevención o mitigación.

Una política de ciberseguridad sin ciberseguridad

El documento falla en cumplir con su propósito central: proteger la información y garantizar la resiliencia tecnológica del MEP. No se identifican mecanismos concretos para la detección, respuesta y recuperación ante incidentes de seguridad. No existe un sistema de monitoreo continuo ni una estrategia clara de auditoría, lo que deja a la institución en un estado de vulnerabilidad permanente. Más allá de un enunciado de intenciones, la falta de procedimientos operativos convierte esta política en un texto sin impacto real en la prevención de ciberataques.

Las experiencias recientes de ataques a instituciones gubernamentales en Costa Rica han demostrado la fragilidad de las infraestructuras digitales y la urgente necesidad de contar con estrategias robustas y bien definidas. No obstante, esta política ignora esas lecciones y no establece medidas concretas para evitar que eventos como los sufridos por el Ministerio de Hacienda, la Caja Costarricense de Seguro Social (CCSS) y otras entidades públicas se repitan. La omisión de controles estrictos de acceso, la falta de un plan detallado de continuidad del negocio y la inexistencia de protocolos ante ciberataques refuerzan la percepción de que este documento no representa un esfuerzo serio por fortalecer la seguridad institucional.

El peligro de convertirse en un documento burocrático

Más allá de sus deficiencias técnicas, la mayor amenaza que representa esta política es su destino previsible: convertirse en un documento de referencia que nadie consulta ni aplica; un archivo más en la maraña burocrática, incapaz de generar cambios reales en la cultura organizacional. La ausencia de sanciones por incumplimiento y de mecanismos efectivos de rendición de cuentas fomenta una cultura de indiferencia, donde la ciberseguridad se reduce a un formalismo sin impacto.

Finalmente, el documento omite un componente esencial: la formación y concienciación de las personas usuarias. Sin una estrategia clara y sostenida de educación en ciberseguridad, cualquier esfuerzo técnico resulta insuficiente. La protección de la información no depende únicamente de herramientas digitales, sino del comportamiento de quienes las utilizan. La falta de programas de formación robustos, continuos y obligatorios evidencia una visión limitada, que deja tanto al personal como al estudiantado sin la preparación necesaria para identificar y mitigar amenazas reales.

ISSN: 2015-5392

Hacia una revisión urgente y una transformación real

La falta de sustancia y aplicabilidad de esta política no solo representa un riesgo institucional, sino que también evidencia una preocupante falta de compromiso con la protección de la información y la seguridad digital de la comunidad educativa. Es imperativo replantear este documento desde una perspectiva que priorice la acción, la eficacia y la adaptabilidad a las amenazas emergentes. Para lograrlo, se deben considerar los siguientes aspectos fundamentales:

Aplicación efectiva de la Ley 8968: Se deben establecer mecanismos de cumplimiento claros para la protección de datos personales, garantizando el derecho de autodeterminación informativa de los estudiantes y funcionarios.

Implementación de medidas de seguridad obligatorias: La autenticación multifactor debe ser un requisito en todos los sistemas críticos, y el cifrado de extremo a extremo debe ser un estándar mínimo.

Monitoreo continuo y respuesta a incidentes: Es necesario establecer un centro de operaciones de seguridad (SOC) que permita la detección y mitigación temprana de amenazas.

Sanciones claras por incumplimiento: El documento debe incluir penalizaciones para quienes no sigan las normativas establecidas, evitando así la impunidad y la negligencia en la gestión de la seguridad.

Educación y cultura de ciberseguridad: Sin una estrategia de capacitación real, la política seguirá siendo ineficaz. Es necesario invertir en formación continua para toda la comunidad educativa.

Auditorías y revisiones periódicas: Se deben establecer mecanismos de auditoría interna y externa para garantizar que las medidas de seguridad sean efectivas y actualizadas ante nuevas amenazas.

La seguridad de la información no es un tema opcional ni secundario; es una necesidad urgente en un mundo cada vez más digitalizado y expuesto a riesgos tecnológicos de gran impacto. La inacción en este campo no solo compromete la integridad de los datos institucionales, sino que también pone en peligro la confianza en el sistema educativo y la seguridad de miles de estudiantes y funcionarios. Es momento de que el MEP deje de lado las políticas vacías y adopte un enfoque serio, técnico y aplicable en la gestión de la ciberseguridad.

REFERENCIAS

Ministerio de Educación Pública. (2019). *Acerca del MEP*. https://dgth.mep.go.cr/sobre-el-mep/

Moreno Guerra, C. B. (2019). Seguridad de la información para instituciones educativas a tercer nivel basado en la ISO/IEC 27001. *Revista Caribeña de Ciencias Sociales*. https://www.eumed.net/rev/caribe/2019/07/seguridad-informacion.html

Purpura, P. (2006). *Manual de capacitación para personal de seguridad*. Thomson Learning.

Sibaja, D. (2024, 26 de febrero). MEP cerró 180 escuelas en los últimos 10 años. *Teletica*. https://www.teletica.com/calle-7/mep-cerro-180-escuelas-en-los-ultimos-10-anos_352595