Protocolo de Protección de Datos Sensibles en Centros Penitenciarios Militares de Colombia, alineada con la arquitectura de las FF.MM.

Mayor (EJC) Yeferson Obando Vera

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	:	Mayor (EJC) Yeferson Obando Vera
Identificación	:	14326131
Programa académico	:	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	:	Cr. Aldemar Serrano Cuervo
Tutor temático	:	Dr. Jaider Ospina Navas
Fecha de entrega	:	28 de septiembre de 2025
Extensión	:	

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-No Comercial-Sin Obras Derivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza / no autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Protocolo de Protección de Datos Sensibles en Centros Penitenciarios Militares de Colombia, alineada con la arquitectura de las FF.MM.

Protocol for the Protection of Sensitive Data in Colombian Military Penitentiary Centers, aligned with the architecture of the Armed Forces.

Yeferson Obando Vera[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El artículo analiza el diseño e implementación de un protocolo para la protección de datos sensibles en centros penitenciarios militares colombianos, alineado con la arquitectura de ciberseguridad de las Fuerzas Militares. Partiendo de los vacíos existentes en la protección de información clasificada y los riesgos operacionales asociados a ciberamenazas, se propone un modelo integral basado en cuatro pilares: i) clasificación jerárquica de datos según su sensibilidad (alto secreto, reservado, confidencial); ii) controles técnicos avanzados (encriptación, autenticación multifactor, segmentación de redes); iii) programas de capacitación continua para el personal técnico y operativo, y iv) sistemas de monitoreo con tecnología para detección temprana de amenazas. La investigación destaca la importancia de integrar este protocolo con los sistemas existentes de las FF.MM., particularmente con redes seguras institucionales y protocolos del Comando Conjunto Cibernético, garantizando interoperabilidad y respuesta coordinada ante incidentes. El análisis de viabilidad demuestra que la implementación es estratégicamente viable mediante un cronograma por fases, priorizando centros piloto antes de su escalamiento nacional. Como conclusión, el protocolo no solo mitiga riesgos inmediatos (filtraciones, sabotajes), sino que fortalece la arquitectura de ciberdefensa nacional. Las recomendaciones enfatizan en aprovechar el marco legal en desarrollo, fomentar alianzas público-privadas y convertir esta iniciativa en un referente regional para la protección de entornos críticos. El estudio aporta así un modelo adaptable que equilibra seguridad operacional y resiliencia frente a amenazas digitales evolutivas.

Palabras clave: ciberseguridad, datos clasificados, protocolo de protección, centros penitenciarios militares, FF.MM.

---

1 Mayor del Ejército Nacional de Colombia. Candidato a magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0000-0003-2004-7466 - Contacto: @esdeg.edu.co.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Abstract: This article analyzes the design and implementation of a protocol for the protection of sensitive data in Colombian military penitentiaries, aligned with the cybersecurity architecture of the Armed Forces. Based on the existing gaps in the protection of classified information and the operational risks associated with cyberthreats, a comprehensive model is proposed based on four pillars: i) hierarchical classification of data according to its sensitivity (top secret, reserved, confidential); ii) advanced technical controls (encryption, multifactor authentication, network segmentation); iii) continuous training programs for technical and operational personnel; and iv) monitoring systems with technology for early threat detection. The research highlights the importance of integrating this protocol with existing systems of the Armed Forces, particularly with institutional secure networks and protocols of the Joint Cyber Command, ensuring interoperability and a coordinated response to incidents. The feasibility analysis demonstrates that implementation is strategically viable through a phased schedule, prioritizing pilot centers before national scaling. In conclusion, the protocol not only mitigates immediate risks (leaks, sabotage) but also strengthens the national cyber defense architecture. The recommendations emphasize leveraging the developing legal framework, fostering public-private partnerships, and making this initiative a regional benchmark for the protection of critical environments. The study thus provides an adaptable model that balances operational security and resilience against evolving digital threats.

Keywords: Cybersecurity, Classified Data, Protection Protocol, Military Penitentiaries, Armed Forces.

Introducción

En el contexto actual, marcado por la transformación digital, la seguridad de la información se ha erigido como un elemento indispensable para las instituciones, en especial aquellas que operan en entornos de alta sensibilidad como los centros penitenciarios militares. En Colombia, donde las Fuerzas Militares (FFMM) gestionan datos estratégicos, la protección de la información clasificada trasciende lo operativo para convertirse en un asunto de seguridad nacional. Sin embargo, como señala Riddell (2024), el país enfrenta desafíos críticos, desde limitaciones tecnológicas hasta amenazas cibernéticas focalizadas, lo que demanda un enfoque integral que garantice la confidencialidad, integridad y disponibilidad de los datos en un escenario de creciente vulnerabilidad.

La digitalización acelerada de los procesos institucionales ha revelado graves falencias en el manejo de información reservada, particularmente en entornos penitenciarios militares, donde un incidente de seguridad podría desencadenar consecuencias operativas e incluso humanas irreparables. Aunque estándares internacionales como la norma ISO/IEC 27001 ofrecen lineamientos para la gestión de la seguridad, Colombia carece de protocolos específicos adaptados a las necesidades de las FFMM. Esta brecha se agudiza por un marco normativo incipiente: la Ley 1581 de 2012, centrada en datos personales, resulta insuficiente para abordar los riesgos de sectores críticos, dejando al descubierto la urgencia de implementar medidas especializadas y contextualizadas.

Actualmente, la ausencia de protocolos estandarizados en los centros penitenciarios militares colombianos incrementa el riesgo de filtraciones, sabotajes o ciberespionaje, amenazando no solo la seguridad institucional sino también la confianza ciudadana y la credibilidad

internacional. Esta situación exige soluciones técnicas y operativas alineadas con las realidades del entorno militar, combinando normativas locales con mejores prácticas globales.

Este artículo propone el diseño e implementación de un protocolo especializado para la protección de datos clasificados en estos centros, con el fin de fortalecer la ciberseguridad institucional y mitigar riesgos emergentes. Mediante un análisis del marco normativo vigente y un diagnóstico de las vulnerabilidades existentes —avalado por una encuesta a 250 miembros del Ejército Nacional—, se identifican brechas y oportunidades de mejora.

La investigación se estructura en cinco secciones: un análisis normativo y técnico, una discusión comparada con experiencias internacionales, conclusiones sobre los beneficios del modelo propuesto, recomendaciones estratégicas para su implementación y futuras líneas de investigación, como auditorías periódicas y la expansión del protocolo a otros entornos críticos. Más que un estudio académico, este trabajo busca sentar las bases para un marco de acción que fortalezca la soberanía digital colombiana frente a los retos del siglo XX

Planteamiento del Problema

Los centros penitenciarios militares en Colombia enfrentan graves deficiencias en materia de seguridad digital, evidenciadas por la ausencia de protocolos estandarizados para la protección de datos sensibles y la falta de articulación con los sistemas de seguridad de las Fuerzas Militares (FFMM). Esta situación genera vulnerabilidades críticas que exponen información clasificada a riesgos operacionales como accesos no autorizados, manipulación de datos y ciberataques sofisticados.

En un contexto donde estos centros manejan inteligencia estratégica, registros de reclusos de alto perfil y datos operativos militares, las consecuencias de una brecha de seguridad podrían incluir desde el compromiso de misiones críticas hasta el debilitamiento de la seguridad nacional. Particularmente preocupante resulta la posibilidad de filtraciones deliberadas o espionaje, que podrían ser explotadas por grupos al margen de la ley o actores externos con fines desestabilizadores.

Esta problemática se ve agravada por la rápida evolución de las amenazas cibernéticas, que contrasta con la lentitud en la actualización de los marcos normativos y tecnológicos del sector. La inexistencia de un protocolo integral adaptado a las particularidades del entorno penitenciario militar no solo pone en riesgo la información confidencial, sino que también limita la capacidad institucional para responder efectivamente a incidentes de seguridad, lo que demanda una solución urgente y especializada.

Pregunta de investigación

¿De qué manera el diseño e implementación de un protocolo especializado de seguridad digital puede fortalecer la protección de datos clasificados en los centros penitenciarios militares colombianos, garantizando su confidencialidad, integridad y disponibilidad frente a las crecientes amenazas cibernéticas, y cómo este instrumento podría integrarse efectivamente con la arquitectura de seguridad existente en las Fuerzas Militares?

Objetivos

Objetivo General

Analizar la trascendencia del diseño de un protocolo para la protección de datos clasificados en los centros penitenciarios militares en Colombia, con el fin de garantizar desde la seguridad digital, su protección, confidencialidad e integridad, en cumplimiento de las normativas vigentes y las buenas prácticas internacionales.

Objetivos Específicos

- Realizar una revisión del marco normativo y las políticas internas aplicables a la seguridad digital y la gestión de datos clasificados en los centros penitenciarios militares, estableciendo brechas y oportunidades de mejora.
- Establecer las necesidades concretas en los centros penitenciarios militares en términos de seguridad digital, sobre el manejo, almacenamiento y protección de datos clasificados, examinando riesgos y amenazas asociadas al contexto operacional.
- Formular recomendaciones fundadas en el análisis desarrollado, que permitan concretar a partir de la seguridad digital, la viabilidad y necesidad del diseño e implementación de un protocolo de protección de datos digitales clasificados en los centros penitenciarios militares.

Justificación

La investigación sobre el diseño de un protocolo para la protección de datos clasificados en centros penitenciarios militares colombianos se justifica por la necesidad urgente de abordar las vulnerabilidades de ciberseguridad que amenazan información sensible vinculada a la seguridad nacional. Actualmente, la falta de estándares especializados y la desarticulación con la arquitectura de las Fuerzas Militares exponen estos sistemas a riesgos críticos, como

filtraciones, sabotaje o espionaje, cuyas consecuencias podrían afectar operaciones estratégicas e incluso la integridad del personal. La implementación de un protocolo robusto no solo mitigaría estas amenazas, sino que también fortalecería el cumplimiento normativo, alineando los procesos con marcos internacionales (como ISO 27001) y la legislación local (Ley 1581 de 2012), garantizando así la confidencialidad, integridad y disponibilidad de los datos.

Además, este estudio tiene un impacto estratégico y operativo al proponer soluciones adaptadas al contexto único de los centros penitenciarios militares, donde convergen altos riesgos de seguridad física y digital. Al analizar la pertinencia del protocolo, se contribuye a la modernización de las capacidades institucionales, optimizando recursos tecnológicos y humanos bajo estándares de ciberseguridad actualizados. Los resultados esperados no solo beneficiarían a las Fuerzas Militares, sino que también sentarían un precedente para otros entornos críticos en Colombia, promoviendo una cultura de protección de datos que equilibre la eficiencia operativa con los desafíos de un panorama de amenazas digitales en constante evolución.

Metodología

El presente estudio adoptará un enfoque metodológico mixto (cualitativo y cuantitativo), dado que la integración de ambas perspectivas permite un análisis más riguroso y multidimensional. Por un lado, el componente cuantitativo facilitará la recolección de datos numéricos estandarizados, mientras que el cualitativo aportará profundidad interpretativa al capturar las percepciones y experiencias de los actores involucrados. Esta triangulación

metodológica, sustentada en Hernández et al., (2014), enriquece los hallazgos al contrastar evidencia estadística con insights contextuales, garantizando así una visión holística del problema de investigación.

En concreto, la recolección de datos cuantitativos se realizará mediante encuestas estructuradas aplicadas al personal de los centros penitenciarios militares, con el fin de cuantificar las prácticas vigentes en seguridad digital y protección de datos sensibles. Paralelamente, el enfoque | se desarrollará a través de entrevistas semiestructuradas dirigidas a actores clave, tales como autoridades penitenciarias, especialistas en ciberseguridad y personal operativo, lo que permitirá explorar a profundidad sus percepciones, desafíos y recomendaciones.

La combinación de estas técnicas no solo fortalece la validez interna del estudio al cruzar distintas fuentes de información, sino que también enriquece el análisis al incorporar tanto tendencias generalizables como particularidades del contexto castrense. Así, los resultados derivados de esta metodología mixta servirán como base empírica sólida para el diseño de un protocolo de protección de datos alineado con la arquitectura institucional de las Fuerzas Militares de Colombia.

Estado del Arte (Antecedentes)

La protección de datos digitales es un tema de creciente relevancia en el contexto de la seguridad y privacidad a nivel global, que por supuesto también interesa a Colombia, especialmente en espacios sensibles como los centros penitenciarios militares; por lo tanto, la realización de una revisión documental es crucial para identificar los vacíos existentes,

analizar las mejores prácticas y ofrecer una base sólida para la formulación de estrategias que fortalezcan la seguridad de los datos digitales en este contexto específico. Este estado del arte analiza la pertinencia de implementar un protocolo específico para la protección de datos digitales en los centros penitenciarios militares de Colombia, identificando avances, vacíos y mejores prácticas.

Ciberseguridad y Ciberamenazas en Entornos Penitenciarios

El Informe Global sobre Amenazas 2024 de CrowdStrike (2024), revela que los ciberatacantes operan con sigilo sin precedentes, evadiendo detección. Identificó 230+ adversarios globales, destacando: i) 34 nuevos actores en 2023, ii) tiempo récord de propagación de ataques (2:07 min), iii) aumento del 75% en intrusiones a la nube, iv) crecimiento del 76% en robos de datos en la dark web, y v) 75% de accesos no maliciosos sin malware. El informe enfatiza la necesidad de protocolos robustos ante amenazas cada vez más adaptables.

En entornos penitenciarios, la protección de información reservada enfrenta desafíos únicos, equilibrando seguridad nacional, derechos humanos y normativas internacionales (Himelwright, 2022). Las instituciones usan tecnología para gestionar servicios, pero carecen de recursos para anticipar riesgos cibernéticos. Himelwright (2022) advierte que la ciberseguridad es crítica en operaciones penitenciarias, requiriendo expertos en seguridad informática. La implementación de medidas es lenta frente al avance tecnológico, dejando sistemas vulnerables.

Además, el acceso controlado a tecnología para reclusos exige comprender prisiones "inteligentes", identificando riesgos emergentes (Imandeka et al., 2024). Flower (2024) destaca en "Fortifying the Walls..." que la ciberseguridad en prisiones estadounidenses es una necesidad, no una opción. La gestión de identidades digitales de reclusos (datos biométricos, registros conductuales) es clave, requiriendo sistemas de acceso restringido para proteger información confidencial e integrar seguridad física-digital.

Importancia de las Políticas y Protocolos de Ciberseguridad

El Centro Cooperativo de Defensa Cibernética de la OTAN (CCDCOE, 2022) ha analizado durante una década el equilibrio entre ciberguerra y derechos individuales, destacando la necesidad de reevaluar qué datos personales son realmente necesarios en operaciones militares (identificación biométrica, preservación de pruebas, registros judiciales). Plantea cuestionar el origen y utilidad estratégica de estos datos para decisiones eficientes y éticas en entornos tecnológicos dinámicos.

Por otro lado, Mishra, Alzoubi y Anwar (2022), en *"Attributes impacting cybersecurity policy development"*, señalan que el aumento de ciberamenazas exige políticas robustas, ya que afectan no solo a individuos y organizaciones, sino también a la seguridad nacional. Su estudio comparativo en siete naciones identifica 14 atributos clave (telecomunicaciones, nube, banca digital, privacidad, etc.), proponiendo un enfoque proactivo y armonizado para políticas globales.

La literatura evidencia que la escalada de ciberriesgos hace inviable su erradicación total. Pese a esfuerzos aislados, en Colombia muchas instituciones gubernamentales —incluidas

prisiones militares— carecen de protocolos claros y estandarizados, dejando vulnerables sus sistemas.

Descripción de Factores de evaluación de la ciberseguridad

Las medidas de las naciones han ayudado a regular este problema hasta cierto punto. No todas las naciones están sujetas a la misma cantidad de peligro. Si bien no existe un estándar para evaluar las políticas de ciberseguridad, las investigaciones más recientes y los profesionales de la industria (por ejemplo, (Global Cyber Security Capacity Centre - GCSCC, 2021) (Dutton, Creese, Shillair, & Bada, 2019); (Naseir, 2021); (Collett, 2021); (Nakhli, 2022), (European Union Agency for Cybersecurity - ENISA, 2020); (Global Forum on Cyber Expertise (GFCE), 2022) han identificado factores comunes que deben examinarse para una implementación exitosa de la política. La descripción de cada uno de los ocho factores utilizados para evaluar la política de ciberseguridad se resume en la siguiente tabla.

Tabla 1 Descripción de factores de evaluación de la ciberseguridad

Factor	Descripción
Infraestructura	La capacidad del país para desarrollar e implementar políticas de ciberseguridad, fortaleciendo su ciberdefensa, gestión de incidentes, equipos, habilidades y protección de infraestructuras TIC.
Conocimiento y conciencia	Calidad, accesibilidad y adopción de políticas por parte de individuos, gobierno y empresas, incluyendo campañas de concienciación, formación de expertos y educación formal en ciberseguridad.
Marcos y modelos	Diseño y mantenimiento de herramientas y procesos para recopilar, analizar y utilizar datos que permitan evaluar situaciones tácticas en ciberseguridad.
Normas y reglamentos	Desarrollo y adopción de leyes nacionales sobre ciberseguridad, especialmente enfocadas en delitos cibernéticos y regulaciones aplicables.
Gestión	Implementación de un programa de ciberseguridad alineado con las prioridades nacionales y las amenazas a infraestructuras críticas.
Política de evolución	Implementación de un programa de ciberseguridad alineado con las prioridades nacionales y las amenazas a infraestructuras críticas.
Especialización	Profesionales encargados de garantizar el cumplimiento de las leyes y normativas de ciberseguridad.
Aplicación	Imposición de penalizaciones a empresas o individuos que incumplan las regulaciones contra delitos cibernéticos.

Nota. Elaboración propia a partir de diversos autores.

Si bien la descripción anterior de factores se centra en aspectos generales de la evaluación de la ciberseguridad, su análisis en el caso en particular, incumbe a los ámbitos tecnológico, legal, humano y organizativo que influyen en la protección de datos digitales en los centros penitenciarios militares, así:

Tabla 2 Factores de evaluación de la ciberseguridad en los centros penitenciarios militares

Factor	Descripción
Tecnológico	Las plataformas empleadas no cuentan con medidas básicas de cifrado. La conectividad y los sistemas de comunicación son vulnerables a intercepciones externas.
Legal	La falta de una regulación específica para entornos militares genera ambigüedades sobre el alcance de las leyes existentes. Existe un conflicto entre la transparencia institucional y la clasificación de información reservada.
Humano	Las malas prácticas, como el uso de contraseñas débiles y el almacenamiento de información en dispositivos no seguros, son comunes. La rotación frecuente del personal dificulta la implementación de una cultura de seguridad de datos.
Organizativo	La fragmentación de responsabilidades en la gestión de datos impide un enfoque integral. No existen protocolos de respuesta ante incidentes de ciberseguridad.

Nota. Elaboración propia a partir de (Collett, 2021)

Finalmente, a partir de la bibliografía consultada, la implementación de un protocolo para la protección de datos digitales reservados en los centros penitenciarios militares de Colombia es no solo pertinente, sino urgente; sin embargo, este protocolo deberá abordar las siguientes áreas:

- **Fortalecimiento normativo:** Diseño de regulaciones específicas que armonicen las necesidades de seguridad nacional con la legislación internacional en protección de datos (Global Cyber Security Capacity Centre - GCSCC, 2021).
- **Capacitación continua:** Programas de formación que promuevan una cultura de seguridad digital entre el personal (Himelwright, 2022).
- **Modernización tecnológica:** Inversión en sistemas seguros de almacenamiento y comunicación; sin embargo, se hace énfasis en los riesgos del uso de las nuevas tecnologías en determinados ámbitos (Solar Calvo, 2023).
- **Supervisión y auditorías:** Establecimiento de mecanismos independientes que monitoreen el cumplimiento del protocolo (CrowdStrike, 2024).

Numerosos expertos (CCDCOE, 2022; Flower, 2024; Himelwright, 2022; Imandeka et al., 2024; Naseir, 2021) coinciden en que la falta de protocolos de protección de datos supone un grave riesgo, especialmente en prisiones, donde compromete la seguridad nacional y los derechos fundamentales. Implementar medidas robustas no solo reforzaría la confianza en estas instituciones, sino que aseguraría el cumplimiento de estándares internacionales de ciberseguridad y privacidad.

Marco Teórico-Conceptual

El siguiente marco teórico tiene como finalidad presentar una serie de concepciones que resultan clave para analizar la pertinencia del protocolo propuesto destinado a la protección de datos digitales reservados en los centros penitenciarios militares de Colombia; esto en razón, a que debe estar fundamentado no solo los principios de la ciberseguridad, la protección de datos personales y las normativas internacionales y nacionales aplicables, sino también en el análisis de las teorías relacionadas con la gestión de la información clasificada, como los estándares internacionales de seguridad digital y los modelos de protección de infraestructuras críticas.

Además, se consideran las particularidades del contexto militar colombiano, donde la confidencialidad y la integridad de la información son esenciales para garantizar tanto la seguridad operativa como la legitimidad institucional. En este sentido, el marco teórico no solo delimita los conceptos clave y los enfoques normativos, sino que también destaca la importancia estratégica de implementar herramientas y protocolos que fortalezcan la

resiliencia digital en entornos de alta sensibilidad como los son estos centros penitenciarios militares.

Protección de Datos Digitales: Definición, Características, Diferencias entre Datos Sensibles, Clasificados y Reservados

La protección de datos es fundamental en la era digital, garantizando la seguridad de información confidencial mediante prácticas que evitan accesos no autorizados, alteraciones o destrucción (Scale Computing, 2024). Su importancia radica en mantener la confidencialidad, integridad y disponibilidad de los datos (Fortinet Inc., 2023).

Se implementa mediante múltiples estrategias como cifrado, controles de acceso y copias de seguridad, que protegen contra amenazas cibernéticas cada vez más sofisticadas (Al-Hawamleh et al., 2020). Las organizaciones deben adoptar medidas proactivas para cumplir regulaciones y mantener la confianza de los stakeholders (Intel Corporation, 2025).

La seguridad de datos es crucial para evitar consecuencias legales, financieras y reputacionales, especialmente ante posibles brechas que comprometan información sensible (Srisakthi & Suresh Babu, 2024). Su implementación adecuada es esencial en un mundo digital interconectado.

Seguridad y Privacidad Explicadas

La privacidad se refiere al control sobre los datos personales (qué se recopila y cómo se usa), mientras que la seguridad protege dichos datos de accesos no autorizados (Barney, 2022). Por ejemplo, las políticas de privacidad en apps detallan el uso de información, pero la

seguridad implementa herramientas como firewalls o autenticación para prevenir brechas (Okta Inc., 2024).

La privacidad garantiza el uso responsable de datos sensibles, exigiendo transparencia a las organizaciones. La seguridad, en cambio, combate amenazas cibernéticas mediante medidas técnicas (Barney, 2022). Aunque son distintas, ambas son esenciales: la seguridad protege los datos, pero sin privacidad, el control sobre ellos se pierde (Okta Inc., 2024).

Protocolo de Seguridad de la Información: Qué es, Componentes Esenciales y Relevancia en Entornos de Alta Seguridad

Un protocolo de protección de datos es un documento clave que establece las directrices y procedimientos de una organización para gestionar, procesar y almacenar información confidencial, asegurando el cumplimiento normativo (Scale Computing, 2024). Define:

- ✓ Alcance y propósito: Tipos de datos cubiertos y objetivos de protección.
- ✓ Cumplimiento: Normativas regionales, estándares sectoriales e internos.
- ✓ Recopilación y procesamiento: Legalidad, transparencia, minimización y precisión de datos.
- ✓ Medidas técnicas: Cifrado, controles de acceso y auditorías periódicas.
- ✓ Respuesta a incidentes: Protocolos para brechas de seguridad (Paananen et al., 2020).

Además, orienta a los empleados en el manejo seguro de datos y fomenta una cultura de privacidad. En un entorno digital donde la información es vulnerable, este protocolo es fundamental para mitigar riesgos y mantener la confianza (Scale Computing, 2024; Paananen et al., 2020).

Importancia de las Políticas y Protocolos de Ciberseguridad

El CCDCOE de la OTAN (2022) ha analizado durante más de una década el equilibrio entre ciberguerra y derechos fundamentales, cuestionando la cantidad de datos personales necesarios en operaciones militares (identificación biométrica, pruebas judiciales) y su real utilidad estratégica. Por otro lado, Mishra et al. (2022) identificaron en 7 países 14 atributos clave de ciberseguridad (telecomunicaciones, nube, banca digital, etc.), destacando la necesidad de políticas integrales ante amenazas crecientes que afectan desde individuos hasta la seguridad nacional.

La literatura evidencia que, pese a esfuerzos aislados, en Colombia muchas instituciones gubernamentales -incluidas prisiones militares- carecen de protocolos claros ante estos desafíos globales. Los principales hallazgos incluyen:

- **Ausencia de marcos normativos robustos:** Aunque la Ley 1581 de 2012 establece principios generales para la protección de datos, su aplicación específica a los centros penitenciarios militares es limitada.
- **Bajos niveles de capacitación:** El personal administrativo y operativo de estos centros carece de formación en manejo seguro de información digital.
- **Tecnologías obsoletas:** Muchos centros penitenciarios militares emplean sistemas de almacenamiento y gestión de datos vulnerables a ciberataques.
- **Falta de supervisión externa:** La inexistencia de auditorías regulares limita la identificación de brechas de seguridad.

El Auge de los Delitos de Ciberseguridad

Lallie et al. (2021) señalan que el cibercrimen representa una amenaza crítica para infraestructuras, empresas y personas. Lloyd (2020) destaca que Internet se ha convertido en

una realidad paralela, donde el aumento del intercambio de información en línea ha impulsado el crecimiento de estos delitos (Libicki, 2021). Aunque tradicionalmente se han usado soluciones antimalware, Mishra et al. (2022) advierten que su eficacia es limitada ante la complejidad actual, exigiendo sistemas de defensa más avanzados. Dado su carácter transfronterizo, combatir estas amenazas requiere cooperación internacional e intercambio de información efectivo (Mishra et al., 2022).

Principios Teóricos y Tecnologías de Seguridad de la Información

Principios teóricos sobre la seguridad de la información digital

Los principios de protección de datos establecen las bases para un manejo ético y seguro de la información personal, garantizando su procesamiento legal y transparente (CrowdStrike, 2024). Incluyen:

- Procesamiento lícito, justo y transparente
- Obtención de consentimiento válido
- Adherencia a marcos normativos (Kosling, 2024).

Estas directrices buscan preservar la privacidad y integridad de los datos. A continuación se detallan en la tabla los principios clave. A continuación, se enuncian en la tabla los principios más comunes a tener en cuenta:

Tabla 3 Tabla Principios generalmente aceptados para la protección de datos digitales

Principio	Finalidad
Limitación de la finalidad	Los datos deben recopilarse solo para objetivos definidos y no usarse posteriormente de forma incompatible con esos fines.
Minimización de datos	Subraya la importancia de recopilar solo la cantidad mínima de datos necesarios para el propósito previsto, reduciendo el riesgo asociado con información innecesaria.
Exactitud	Los datos deben mantenerse precisos y actualizados para asegurar su confiabilidad.
Limitación del almacenamiento	La información no debe conservarse más tiempo del requerido para su fin original, previniendo acumulación innecesaria.
Integridad y confidencialidad	Se deben implementar medidas para proteger los datos contra accesos, modificaciones o divulgaciones no autorizadas.
Rendición de cuentas	Las organizaciones deben probar su cumplimiento normativo y ser transparentes en el tratamiento de datos, fomentando una cultura proactiva de privacidad.

Nota. Elaboración propia a partir de (CrowdStrike, 2024) y (Kosling, 2024)

Comprender y respetar estos principios es fundamental en la era digital, donde el volumen cada vez mayor de datos personales exige un marco ético sólido. Las organizaciones que priorizan estos principios no solo mejoran sus prácticas de gestión de datos, sino que también contribuyen a generar confianza con las personas y a fomentar una cultura responsable de datos dentro de sus operaciones.

Tecnologías para la seguridad de datos digitales

Si bien el cumplimiento normativo permitirá mantener una buena opinión ante las agencias regulatorias, un enfoque más integral ayudaría a mantener a raya las amenazas. Las siguientes tecnologías condensadas en la tabla a continuación deberían formar parte de la estrategia de seguridad de datos de todas las organizaciones sean públicas o privadas (Intel Corporation, 2025).

Tabla 4 Tabla tecnologías que deberían formar parte de la estrategia de seguridad de datos de todas las organizaciones

Tecnología	Contenido
Cifrado de datos	✓ Método confiable para proteger datos en reposo, tránsito o procesamiento en tiempo real. ✓ Usa algoritmos para convertir datos en formatos ilegibles, accesibles solo con clave autorizada. ✓ Vulnerable a ataques de canal lateral y puede ralentizar sistemas, pero nuevas tecnologías mejoran su eficiencia sin comprometer seguridad.
Autenticación y autorización de usuarios	✓ Contraseñas sólidas no bastan; se requieren métodos avanzados como: Biometría, Autenticación de dos factores (2FA), Tecnología de enclave seguro en hardware.
Seguridad basada en hardware:	✓ Los ciberataques ahora apuntan a capas más profundas (hardware). ✓ Soluciones como las de Intel integran protecciones en silicio para salvaguardar: Firmware, OS, apps, redes y cloud.
Copia de seguridad de datos	✓ Permite recuperar información ante fallos, ataques o desastres. ✓ Requiere: i) Almacenamiento seguro y accesible solo por personal autorizado; y ii) Protección durante transferencia y almacenamiento para detectar amenazas. ✓ Políticas documentadas aseguran cumplimiento normativo y procesos de recuperación confiables.

Nota. Elaboración propia a partir de (Intel Corporation, 2025)

Gestión de Riesgos Aplicados a la Protección de Datos Digitales.

La gestión de riesgos en protección de datos digitales es un proceso sistemático para identificar, evaluar y mitigar amenazas a la información, con el fin de garantizar su confidencialidad, integridad y disponibilidad. Esto se logra mediante controles de seguridad y medidas preventivas que reducen la probabilidad e impacto de violaciones (CrowdStrike, 2024).

Tabla 5 Elementos clave de la gestión del riesgo de datos

Elementos	Definición
Identificar activos	Reconocer todos los datos digitales críticos, incluida la información del cliente, datos financieros, la propiedad intelectual y las configuraciones del sistema, para comprender qué necesita protección.
Análisis de amenazas	Identificar amenazas potenciales que podrían atacar los datos, como actores maliciosos (piratas informáticos), amenazas internas, desastres naturales, fallas del sistema y eliminación accidental de datos.
Evaluación de vulnerabilidad	Evaluar las debilidades de los sistemas de seguridad existentes que podrían ser explotadas por amenazas identificadas, como contraseñas débiles, software sin parches o configuraciones de red inseguras
Evaluación de riesgos	Combinar la probabilidad de que ocurra una amenaza con el impacto potencial en la organización para priorizar los riesgos según su gravedad.
Estrategias de mitigación de riesgos	Implementar controles de seguridad para abordar los riesgos identificados, tales como: ✓ Control de acceso: implementación de métodos de autenticación fuertes, controles de acceso de usuarios y permisos basados en roles. ✓ Cifrado: cifrado de datos confidenciales en reposo y en tránsito para protegerlos contra el acceso no autorizado incluso en caso de vulneración. ✓ Seguridad de red: Implementación de firewalls, sistemas de detección/prevención de intrusiones y segmentación de red para monitorear y controlar el tráfico de red. ✓ Copia de seguridad y recuperación de datos: realizar copias de seguridad periódicas de datos críticos para garantizar la disponibilidad en caso de falla del sistema o pérdida de datos. ✓ Plan de respuesta a incident es: desarrollar un plan estructurado para responder y contener incidentes de seguridad de manera efectiva. ✓ Capacitación en concientización: educar a los empleados sobre las mejores prácticas de ciberseguridad para minimizar los errores humanos y los riesg os de phishing.
Seguimiento y revisión:	Monitorear continuamente los sistemas de seguridad, identificar amenazas emergentes y actualizar los controles de seguridad según sea necesario para mantener una postura efectiva de gestión de riesgos.
Cumplimiento de la normatividad	Cumplir con las leyes y regulaciones de privacidad de datos pertinentes, como GDPR o HIPAA, según la industria y la ubicación
Clasificación de datos	Categorizar los datos en función de su sensibilidad para determinar los ni veles de protección adecuados.
Análisis costo-beneficio	Equilibrar el costo de implementar medidas de seguridad con el costo potencial de una violación de datos

Nota. Elaboración propia a partir de (CrowdStrike, 2024).

Marco Normativo y Políticas Internas

Marco Normativo y Regulatorio Internacional: Regulaciones globales relevantes

Ley de Protección de Datos de 1998.

La Ley de Protección de Datos del Reino Unido fue un marco legislativo clave para regular el procesamiento de datos personales, garantizando privacidad mediante principios como:

- Legalidad, equidad y transparencia en el tratamiento de datos.
- Limitación de fines específicos y legítimos.
- Exactitud y seguridad de la información.
- Derechos individuales (acceso, rectificación y eliminación de datos) (The BBC, 2025).

Introdujo categorías especiales para datos sensibles (origen étnico, creencias religiosas, etc.), exigiendo salvaguardas reforzadas. Las organizaciones debían registrarse en la *ICO* y detallar sus actividades de procesamiento. Fue reemplazada en 2018 por el RGPD.

Reglamento General de Protección de Datos (RGPD) de la Unión Europea

Diseñado para mejorar los derechos de privacidad de las personas, el RGPD introdujo normas de protección de datos más estrictas y unificadas que rigen el procesamiento de datos personales por parte de las organizaciones. Los requisitos del Reglamento General de Protección de Datos incluyen garantizar un procesamiento de datos legal, justo y transparente, recopilar datos para fines específicos, minimizar los datos, garantizar la precisión, limitar la duración del almacenamiento e implementar medidas de seguridad sólidas. El RGPD otorga a las personas un mayor control sobre su información personal, ofreciendo derechos como el acceso, la rectificación, el borrado y el derecho a oponerse a ciertas actividades de procesamiento (Unión Europea, 2025).

Impone obligaciones estrictas a las organizaciones, obligándolas a adoptar prácticas transparentes en materia de datos, designar responsables de protección de datos cuando sea

necesario y denunciar las violaciones de datos con prontitud. El reglamento tiene alcance extraterritorial y se aplica a organizaciones de todo el mundo que procesan datos personales de residentes de la UE. El incumplimiento del RGPD puede dar lugar a multas importantes, lo que pone de relieve la importancia de que las organizaciones se alineen con sus principios para proteger la privacidad individual y mantener los estándares de seguridad de los datos (Consejo Europeo, 2025).

La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)

La HIPAA regula el manejo de información médica, considerada como uno de los tipos de datos más sensibles. Define como "Información de Salud Protegida" (PHI) toda aquella relacionada con la atención médica o su pago, incluyendo informes clínicos, documentos internos y datos de facturación (Mason Pope, 2023).

Las medidas de seguridad (cifrado, controles de TI, gestión de riesgos y políticas administrativas) buscan prevenir accesos no autorizados a la PHI. La normativa aplica tanto a "entidades cubiertas" (hospitales, médicos, aseguradoras) como a sus "socios comerciales", quienes comparten la responsabilidad de proteger estos datos (Edemekong et al., 2024).

Las sanciones por violaciones incluyen multas millonarias e incluso penas de cárcel. Las organizaciones infractoras deben reportar públicamente los incidentes, notificando al Departamento de Salud y Servicios Humanos (Mason Pope, 2023).

ISO 27000

La Organización Internacional de Normalización proporciona especificaciones y mejores prácticas estandarizadas sobre una serie de temas técnicos y profesionales con el fin de ayudar a las organizaciones públicas y privadas a utilizar mejor la tecnología. Una de estas

series de normas se conoce como la serie ISO 27000, un conjunto de documentos que describen las mejores prácticas para proteger la información mediante controles técnicos y administrativos.

Tal vez la más conocida de esta serie sea la ISO 27001, una norma internacional que detalla cómo las organizaciones pueden implementar sistemas de gestión de seguridad de la información. Estos sistemas reúnen controles de seguridad, políticas empresariales y procesos logísticos para priorizar la privacidad y la seguridad en infraestructuras de TI complejas (Culot, Nassimbeni, Podrecca, & Sartor, 2021). Por lo general, no se exige la certificación ISO 27001 a ninguna organización, ya que la ISO es una organización privada. Muchas empresas privadas y agencias públicas optan por someterse a auditorías ISO 27001 simplemente para proteger mejor los datos tanto de sus organizaciones, como de sus operaciones (GlobalSuite Solutions, 2023).

Marco Normativo y Regulatorio Nacional: Ámbito Normativo sobre Protección de Datos y Ciberseguridad en Colombia

La legislación colombiana en materia de protección de datos no exige la designación de un Oficial de Protección de Datos dentro de las organizaciones. Sin embargo, las empresas deben asignar un departamento o una persona encargada de los asuntos de datos personales para atender las solicitudes de los Titulares de Datos (Universidad Externado de Colombia, 2022); si bien, la Guía de Responsabilidad de la APD no es una publicación obligatoria, incluye un "mínimo de cumplimiento" que la Autoridad debe considerar en cualquier inspección o investigación de un responsable o encargado de Tratamiento de Datos Personales.

A continuación, se presenta la siguiente tabla que contiene los principales documentos que enmarcan la normatividad nacional en materia de ciberseguridad y protección de datos digitales.

Tabla 6 Normatividad nacional en materia de ciberseguridad y protección de datos digitales

Norma	Contenido
Constitución Política de Colombia	Reconoce derecho a la privacidad y a la rectificación de datos como derechos fundamentales. (Artículos 15 y 20)
Ley 594 de 2000	Ley General de Archivos
Ley 1266 de 2008	Establece que encargados del Tratamiento deben implementar sistemas de seguridad con resguardos técnicos para garantizar la seguridad y exactitud de los datos, y evitar daños, pérdidas, usos o accesos no autorizados a los mismos.
Ley 1273 de 2009:	Tipifica como delito el tratamiento ilícito y no autorizado de datos personales y lo incorpora al Código Penal. Introduce legislación específica sobre delitos cibernéticos en el derecho penal colombiano.
Ley 1341 de 2009	Ley sectorial de servicios de tecnologías de la información y las comunicaciones. Los servicios de redes y sistemas informáticos se encuentran regulados en dicha ley, su definición está vinculada a los conceptos de la UIT mencionados en el artículo 6 de la mencionada ley. Los servicios de comunicaciones se definen como: "servicios que proporcionan la capacidad de enviar/recibir información de conformidad con las condiciones para la prestación de dichos servicios previamente acordadas entre un proveedor y un usuario"
Ley 1581 de 2012	Regula tratamiento de datos y bases de datos. Señala que Responsables y Titulares del Tratamiento deben garantizar que los datos personales se mantengan bajo estrictas medidas de seguridad y confidencialidad, que no serán divulgados ni modificados y que serán utilizados para los fines aprobados por el Titular. Por lo tanto, los Encargados y Titulares del Tratamiento deben desarrollar un manual interno de políticas y procedimientos para dar cumplimiento a la normativa de protección de datos.
Ley 1928 de 2018	Por el cual Colombia se adhiere al Acuerdo de Budapest sobre delito cibernético firmado en noviembre de 2001.
Decreto Ley 019 de 2012	Sobre entidades autorizadas para la certificación digital;
Decreto 1704 de 2012	Sobre interceptación legal de comunicaciones;
Resolución CRC 3502 de 2011	Sobre Neutralidad de la Red;
Decreto 1377 de 2013	Reglamenta parcialmente las disposiciones contenidas en la Ley N° 1581 de 2008.
Decreto 886 de 2014	Reglamenta parcialmente las disposiciones contenidas en la Ley N° 1581 de 2008.
Decreto Nº 2952 de 2010	Reglamenta las disposiciones contenidas en la Ley Nº 1266 de 2008.
Decreto Nº 2573 de 2014	Sobre Gobierno Electrónico

Nota. Elaboración propia a partir de (Villegas-Carrasquilla, 2021)

Brechas Identificadas

Uno de los hallazgos centrales de esta investigación revela la ausencia de protocolos específicos para la protección de datos sensibles en centros penitenciarios militares, lo que genera vulnerabilidades críticas en la gestión de información clasificada. A esto se suma una notoria desarticulación entre las normativas nacionales, como la Ley Estatutaria de Protección de Datos (1581 de 2012), los estándares de ciberseguridad, y las prácticas operativas reales; las cuales, suelen basarse en procedimientos no estandarizados o adaptaciones improvisadas. Esta brecha no solo incrementa los riesgos de fugas o accesos no autorizados a datos reservados, sino que también dificulta la interoperabilidad con los sistemas de seguridad digital de las Fuerzas Militares.

La Ciberseguridad y los Riesgos Operacionales

Contexto operativo de los centros penitenciarios militares en Colombia

Es importante indicar, que existe escasa bibliografía académica sobre la operatividad de los centros penitenciarios militares en Colombia, los cuales albergan principalmente a personal militar y de fuerza pública condenado por faltas disciplinarias o judiciales. En años recientes, también han acogido a funcionarios civiles de alto rango (magistrados, congresistas, gobernadores), aumentando su complejidad funcional interna y externa.

Si bien, estos centros se rigen por normativas militares nacionales e internacionales, diferenciándose de las cárceles ordinarias del INPEC. Su estructura prioriza la seguridad interna y el respeto a los derechos fundamentales de los reclusos, lo que genera desafíos en la gestión de datos sensibles.

La información manejada incluye datos personales de internos y sus familias, historiales operativos, disciplinarios, clínicos y judiciales, así como detalles vinculados a la seguridad nacional. Estos datos son objetivos críticos para ciberataques o filtraciones, agravado por infraestructura tecnológica limitada y políticas de ciberseguridad insuficientes.

Además, los centros penitenciarios militares operan en un entorno de alta sensibilidad, dado que su funcionamiento está estrechamente vinculado con la seguridad del Estado. Esto implica que las fallas en la protección de datos pueden tener consecuencias estratégicas graves. Garantizar la integridad, confidencialidad y disponibilidad de la información digital es crucial para mantener la confianza pública en las instituciones militares y el sistema judicial colombiano.

Revisión de Experiencias Previas en el Manejo de Datos Clasificados Dentro de Instituciones Militares y sus Penitenciarias

En Colombia, las instituciones militares han implementado políticas para el manejo de datos clasificados, basadas en estándares como ISO 27001, aunque persisten brechas por falta de capacitación técnica e infraestructura tecnológica limitada, aumentando su vulnerabilidad a ciberamenazas. En los centros penitenciarios militares, la gestión de datos enfrenta retos adicionales por la interacción entre seguridad física y digital.

A pesar de sistemas básicos de registro, la tecnología no siempre cubre las demandas actuales, evidenciado en filtraciones internas y accesos no autorizados. Estos casos destacan la necesidad de protocolos estandarizados y supervisión reforzada, integrando medidas técnicas y procedimentales adaptadas a estos entornos de alto riesgo.

Análisis Resultados Encuesta al Personal Centros Penitenciarios Militares del País

Una encuesta aplicada a 250 colaboradores (Oficiales, Suboficiales, Personal Civil) de Centros Penitenciarios Militares en Colombia (CPAMS – EJEBE, EJECA, EJEPO, EJEMA, EJEVA, EJEFA, etc.) revela graves deficiencias en ciberseguridad, tal y como se muestra a continuación en la siguiente tabla.

Tabla 7. Deficiencias encontradas en materia de Ciberseguridad

Hallazgos	***Descripción***
Ausencia de protocolos estandarizados	✓ 75% desconoce o considera inexistente un protocolo para proteger datos sensibles.
Conciencia vs. Realidad operativa:	✓ 83% considera "importante" o "muy importante" la protección de datos clasificados (ej. operaciones militares o detenidos de alto valor). ✓ 75% maneja información sensible sin medidas específicas de protección.
Amenazas y vulnerabilidades:	✓ 65% percibe riesgo "alto" o "muy alto" de ciberataques (ransomware, phishing). ✓ 45% identifica vulnerabilidades en sistemas de almacenamiento/transmisión. ✓ 30% ha enfrentado accesos no autorizados.
Falta de capacitación:	✓ 75% afirma no recibir capacitaciones periódicas en ciberseguridad, aumentando riesgos por error humano.
Apoyo a mejoras:	✓ 85% respalda implementar medidas técnicas (encriptación, autenticación multifactor, monitoreo continuo). ✓ 70% exige priorizar un protocolo alineado con políticas de ciberdefensa militar.

Fuente. Elaboración propia.

Los resultados validan y sugieren la necesidad urgente de un protocolo integral con enfoque técnico, formativo y estratégico para mitigar riesgos en estos entornos críticos.

Resultados

Tras una revisión detallada del estado actual en materia de ciberseguridad, y la aplicación de una encuesta al personal que labora em estos centros, revela serias deficiencias institucionales, comenzando por la ausencia de protocolos estandarizados, ya que el 75% de los encuestados manifiesta desconocer procedimientos claros para la protección de datos sensibles, y solo un 10% evalúa positivamente los que existen. Esta falta de directrices concretas se traduce en una alta percepción de riesgo: el 65% considera que las amenazas como el ransomware y el phishing son "altas" o "muy altas", y un preocupante 45% ha detectado vulnerabilidades reales en los sistemas de almacenamiento y transmisión de información.

Más alarmante aún es que el 75% de los participantes asegura manejar información clasificada, incluso de tipo militar, sin protocolos específicos que garanticen su seguridad. Esta fragilidad se agrava con la falta de preparación del personal, ya que otro 75% reconoce no recibir capacitaciones periódicas sobre ciberseguridad. Ante este panorama, resulta significativa la respuesta colectiva: el 85% respalda firmemente la implementación de un protocolo integral que contemple medidas como la encriptación, la autenticación multifactor y el monitoreo continuo, evidenciando una necesidad urgente de actuar con un enfoque sistémico y proactivo.

Discusión

La discusión de los resultados obtenidos Los resultados evidencian una brecha crítica entre la necesidad de proteger datos sensibles y las carencias en protocolos y herramientas en

centros penitenciarios militares. A pesar de existir marcos normativos como ISO 27001 y la Ley 1581 de 2012, su implementación es limitada o inexistente, exponiendo estas instituciones a riesgos crecientes.

Esta problemática combina vulnerabilidades tecnológicas (falta de encriptación, autenticación multifactor) y humanas (escasa capacitación), creando un entorno vulnerable a ciberataques. La situación se agrava por el alto nivel de sensibilidad de la información manejada (inteligencia militar, registros de detenidos), que demanda medidas especializadas aún no implementadas.

Los hallazgos respaldan la necesidad urgente de un protocolo de ciberseguridad adaptado a las Fuerzas Militares, alineado con su arquitectura tecnológica y funciones estratégicas. Las recomendaciones propuestas, basadas en estándares internacionales, incluyen cuatro componentes clave: i) Clasificación de datos; ii) Controles técnicos; iii) Capacitación especializada; y iv) Monitoreo continuo. A continuación, se presenta cada una de ellas.

Fases de Implementación

Clasificación de Datos y Categorización según su Sensibilidad (alto secreto, reservado, confidencial)

La implementación de un protocolo de protección de datos en centros penitenciarios militares debe comenzar con un sistema riguroso de clasificación de información, categorizando los datos según su nivel de sensibilidad (alto secreto, reservado, confidencial). Esta taxonomía permitirá aplicar controles diferenciados, garantizando que los recursos de seguridad se asignen de manera eficiente. Por ejemplo, la información clasificada como "alto secreto"

(como operaciones estratégicas o inteligencia militar) requerirá medidas de acceso más restrictivas que los datos "confidenciales" (información administrativa sensible). Esta categorización debe alinearse con los estándares de las Fuerzas Militares (FFMM) y las normativas nacionales, asegurando coherencia en su manejo y trazabilidad.

Controles técnicos: Encriptación, autenticación multifactor, segmentación de redes.

Para salvaguardar la integridad y confidencialidad de los datos, se recomienda la implementación de controles técnicos avanzados, como:

- Encriptación de extremo a extremo para datos en tránsito y almacenados.
- Autenticación multifactor (MFA) para accesos privilegiados, reduciendo riesgos de suplantación.
- Segmentación de redes para aislar sistemas críticos y limitar el movimiento lateral en caso de brechas.

Estas medidas mitigarán amenazas como ciberespionaje, ransomware o fugas de información, al tiempo que se adhieren a estándares internacionales (NIST, ISO 27001).

Capacitación: Programas para personal técnico y operativo.

La implementación exitosa del protocolo de seguridad digital en centros penitenciarios militares requiere necesariamente de un componente humano altamente capacitado. Los programas de formación continua para personal técnico y operativo constituyen el pilar fundamental para transformar los controles tecnológicos en una verdadera cultura organizacional de ciberseguridad. Esta capacitación debe diseñarse considerando los distintos roles y niveles de acceso a información sensible dentro de la institución.

Así mismo se deberán tener en cuenta los siguientes aspectos:

- *Importancia de la Capacitación Continua.* El entrenamiento debe centrarse en amenazas como phishing e ingeniería social, usando casos reales adaptados al ámbito militar. Se recomiendan métodos interactivos que expongan técnicas de manipulación psicológica empleadas por atacantes.
- *Concienciación sobre Ciberamenazas*. El entrenamiento debe enfocarse en amenazas comunes como phishing e ingeniería social, usando ejemplos reales adaptados al contexto militar. Se recomiendan métodos interactivos que muestren técnicas de manipulación psicológica usadas por atacantes.
- *Manejo Seguro de Datos Clasificados.* Debe incluir protocolos estrictos para información sensible: principio de acceso mínimo, transmisión cifrada, almacenamiento seguro y destrucción certificada. Es clave el uso de sistemas compartimentados y la comprensión de los niveles de clasificación.
- *Respuesta ante Incidentes.* La formación debe abarcar desde la detección temprana hasta protocolos de contención. Todo el personal debe conocer los canales de reporte y acciones básicas de mitigación, vital en entornos militares donde los ciberataques pueden sincronizarse con operaciones físicas.
- *Periodicidad y Evaluación Práctica*. La capacitación debe ser constante, con actualizaciones trimestrales sobre nuevas tácticas de ataque. Los simulacros periódicos, con escenarios progresivamente complejos que repliquen las TTPs de grupos APT (Advanced Persistent Threats), permiten evaluar la preparación real del personal en condiciones controladas.

Monitoreo continuo: Uso de SIEM (Security Information and Event Management).

Implementación de Sistemas SIEM para una Ciberdefensa Proactiva. La adopción de soluciones SIEM (Security Information and Event Management) representa un salto cualitativo en las capacidades de monitoreo y respuesta ante ciberamenazas en entornos penitenciarios militares. Estos sistemas funcionan como el sistema nervioso central de la seguridad digital, agregando y analizando en tiempo real millones de eventos de seguridad provenientes de firewalls, IDS/IPS, servidores, endpoints y otros dispositivos de red. Su capacidad para aplicar análisis de comportamiento (UEBA) y machine learning permite identificar desviaciones sutiles que podrían indicar compromisos avanzados, incluso cuando los atacantes utilizan técnicas de movimiento lateral o permanencia prolongada en los sistemas.

Identificación de Intrusiones en Tiempo Real con Contexto Operacional. Los SIEM modernos van más allá de la simple detección de firmas conocidas; incorporan capacidades de análisis contextual que correlacionan eventos de seguridad con el comportamiento habitual del usuario y los patrones normales de tráfico en la red. Esto es particularmente valioso en entornos militares donde:

- Pueden detectarse accesos anómalos a sistemas que contienen información clasificada, incluso con credenciales válidas
- Se identifican movimientos laterales sospechosos entre segmentos de red supuestamente aislados

- Se capturan intentos de exfiltración de datos enmascarados como tráfico legítimo La integración con Threat Intelligence Feeds militares y organismos nacionales de ciberseguridad enriquece aún más estas capacidades de detección.

Correlación Avanzada para Descubrir Campañas de Ataque. La verdadera potencia de los SIEM reside en su habilidad para conectar eventos aparentemente inconexos que, vistos en conjunto, revelan patrones de ataque complejos. Por ejemplo:

- Puede correlacionar intentos fallidos de autenticación en múltiples sistemas con posterior actividad sospechosa en cuentas privilegiadas
- Identificar relaciones temporales entre alertas de antivirus, tráfico DNS anómalo y accesos geográficamente imposibles
- Detectar secuencias de eventos que coinciden con TTPs (Tácticas, Técnicas y Procedimientos) documentados de grupos APT

Esta capacidad es crítica para descubrir ataques persistentes avanzados que podrían pasar meses dentro de los sistemas antes de ser detectados por métodos convencionales.

Automatización de Respuestas con Workflows Adaptados al Entorno Militar. Los SIEM modernos permiten implementar playbooks de respuesta automatizada especialmente configurados para el contexto operativo militar:

- Bloqueo automático de IPs maliciosas basado en threat feeds de organismos de defensa
- Aislamiento temporal de sistemas comprometidos siguiendo protocolos de contingencia

- Activación de protocolos de verificación de identidad reforzada cuando se detectan accesos sensibles desde ubicaciones inusuales
- Notificaciones escaladas a los equipos de ciberdefensa según la criticidad del incidente.

Estos flujos deben diseñarse cuidadosamente para evitar falsos positivos que puedan afectar operaciones críticas.

Ventaja Estratégica contra Amenazas Evolutivas. En el contexto actual de guerra híbrida, donde las amenazas cibernéticas forman parte del arsenal de adversarios estatales y grupos organizados, los SIEM proporcionan:

- Visibilidad unificada de toda la superficie de ataque digital
- Capacidad forense para investigar incidentes con granularidad temporal
- Métricas continuas para mejorar posturas de seguridad
- Cumplimiento automatizado de requisitos regulatorios militares.

La implementación debe incluir un SOC (Security Operations Center), ya sea dedicado o integrado a las capacidades de ciberdefensa de las FFMM, con personal especializado en amenazas dirigidas al sector defensa. Esta inversión es esencial, no opcional, para garantizar la superioridad operacional en el dominio digital.

Alineación con arquitectura de las FFMM: Un Enfoque Estratégico

La integración del protocolo de seguridad digital con los sistemas existentes de las Fuerzas Militares no solo optimiza recursos, sino que fortalece la coherencia operativa en la protección de datos clasificados. Esta alineación debe comenzar por la conexión segura con

las redes cifradas ya implementadas por las FFMM, aprovechando infraestructuras probadas como la Red Integrada de Comunicaciones Estratégicas (RICE) o sistemas equivalentes.

La interoperabilidad técnica debe garantizar que los nuevos controles de seguridad complementen -no compitan- con los mecanismos de protección ya desplegados, manteniendo los estándares de cifrado (como los algoritmos certificados por el Centro Criptológico Nacional) y los modelos de autenticación jerárquica propios del entorno castrense. Esta integración sin fisuras reduce puntos ciegos de seguridad y evita la creación de silos informacionales que pudieran ser explotados por amenazas avanzadas.

Interoperabilidad con Protocolos de Ciberdefensa Militar: Coordinación para la Acción Conjunta.

El protocolo propuesto debe articularse orgánicamente con los procedimientos establecidos en la Estrategia Militar de Ciberdefensa y los protocolos del Comando Conjunto Cibernético. Esto implica:

- Adoptar los mismos frameworks de clasificación de incidentes (como los niveles de Defensa contra Amenazas adaptados al ciberespacio)
- Utilizar los canales establecidos para reporte y escalamiento de ciberincidentes críticos
- Implementar los mismos indicadores de compromiso que comparte la comunidad de inteligencia militar

Esta interoperabilidad garantiza que cualquier anomalía detectada en los sistemas penitenciarios militares pueda ser rápidamente contextualizada dentro del panorama general de amenazas que monitorean las FFMM, permitiendo respuestas coordinadas frente a

campañas de ataque complejas. La estandarización de protocolos facilita además el intercambio de threat intelligence con aliados estratégicos bajo los acuerdos de cooperación en ciberdefensa que mantiene Colombia.

Integración con Redes Seguras Existente

La conexión con infraestructuras ya validadas como las redes seguras de las FFMM permite heredar sus robustos controles de seguridad, evitando duplicar esfuerzos en componentes como firewalls de última generación, sistemas de prevención de intrusiones (IPS) o soluciones de anti-APT ya desplegadas. Esta integración debe respetar los modelos de zonificación de seguridad (como los anillos concéntricos de protección) característicos de las arquitecturas militares, asegurando que los datos clasificados transiten exclusivamente por canales validados y monitoreados continuamente por los equipos de ciberdefensa institucional.

Armonización con Protocolos de Ciberdefensa

La interoperabilidad operacional exige alinear los procedimientos del protocolo con los establecidos en manuales como la Doctrina de Ciberdefensa Militar, utilizando los mismos códigos de alerta, formatos de reporte y cadenas de mando para la respuesta a incidentes. Esto incluye capacidad para integrarse con sistemas como el Centro de Operaciones de Ciberdefensa (COCIBER), permitiendo que las alertas generadas en los sistemas penitenciarios contribuyan al panorama situacional conjunto que monitorean las FFMM, y viceversa, recibiendo actualizaciones sobre amenazas relevantes detectadas en otros puntos de la red militar.

Viabilidad Técnica y Operativa del Protocolo

La implementación del protocolo de ciberseguridad para centros penitenciarios militares demuestra alta viabilidad cuando se analiza desde una perspectiva costo-beneficio estratégica. La inversión inicial requerida en soluciones tecnológicas (como sistemas SIEM, herramientas de encriptación y autenticación multifactor) y capacitación especializada resulta significativamente menor a los potenciales costos operativos, reputacionales y estratégicos de un incidente de seguridad mayor. Estudios comparativos en instituciones castrenses de la región muestran que la implementación de protocolos similares ha reducido en un 60-70% los incidentes de seguridad graves durante los primeros 18 meses.

El cronograma propuesto sigue un modelo de maduración progresiva: una fase piloto de 6 meses permitiría validar los componentes críticos en un centro penitenciario modelo, seguida por una etapa de escalamiento gradual (12-18 meses) que incorporaría lecciones aprendidas, culminando con una fase de consolidación (24 meses) que integraría plenamente el protocolo con los sistemas de ciberdefensa de las FFMM. Este enfoque por etapas mitiga riesgos financieros y operacionales mientras genera valor tangible desde los primeros meses.

Factores Clave para una Implementación Exitosa

La viabilidad del proyecto se sustenta en tres pilares fundamentales: la reutilización de infraestructuras existentes en las FFMM (reduciendo costos de adquisición), la disponibilidad de personal militar con formación en ciberseguridad que puede ser capacitado como multiplicadores, y el alineamiento con iniciativas estratégicas nacionales como la Política de Ciberdefensa. El análisis financiero debe considerar no solo los costos directos

(equipos, software, capacitación), sino también los ahorros potenciales al centralizar y optimizar sistemas de seguridad fragmentados.

La implementación exitosa requerirá: asignación presupuestal priorizada a través del Sistema de Planeación de las FFMM, designación de un equipo gestor interdisciplinario (TI, inteligencia, operaciones), y mecanismos de seguimiento con indicadores claros (tiempo de detección/respuesta a incidentes, reducción de vulnerabilidades críticas). La experiencia internacional demuestra que proyectos similares alcanzan ROI positivo entre 18-24 meses, especialmente cuando se integran a arquitecturas de seguridad nacional existentes.

Conclusiones

El protocolo propuesto representa una estrategia fundamental para reforzar la arquitectura de ciberseguridad y ciberdefensa del Estado colombiano, integrándose de manera orgánica con los sistemas existentes de las Fuerzas Militares. Su diseño especializado permite no solo proteger información clasificada en entornos penitenciarios militares, sino también consolidar la resiliencia del ecosistema digital del país frente a amenazas híbridas, donde lo físico y lo cibernético se entrelazan cada vez más en escenarios de conflicto moderno.

La implementación de este protocolo es vital para salvaguardar información sensible cuya exposición podría comprometer operaciones estratégicas, inteligencia militar e incluso la seguridad del personal operativo. Al establecer procesos estandarizados basados en normativas internacionales y buenas prácticas, se fortalece la defensa contra amenazas como filtraciones, sabotajes y ciberespionaje, que evolucionan con creciente sofisticación y velocidad, especialmente en contextos de alta sensibilidad como el penitenciario militar.

Más allá del aspecto técnico, la ciberseguridad en estos entornos se convierte en un imperativo ético y operacional. Los centros de reclusión militares manejan información que, en caso de ser vulnerada, podría facilitar fugas, poner en riesgo a testigos protegidos o debilitar operaciones de inteligencia. Un protocolo sólido no solo protege los sistemas informáticos, sino que resguarda vidas humanas, sostiene la eficacia operativa y preserva la confianza institucional ante la sociedad y los aliados internacionales.

En este sentido, la seguridad digital debe entenderse como una extensión directa de la seguridad física y una prioridad nacional. Los ataques cibernéticos a instalaciones penitenciarias militares no son escenarios hipotéticos, sino amenazas reales utilizadas por actores armados y estructuras criminales. Por ello, el protocolo incorpora capacidades como sistemas SIEM y mecanismos de respuesta articulada con el Comando Conjunto Cibernético, anticipándose a futuros desafíos y evitando que estas instalaciones se conviertan en un eslabón vulnerable en la cadena de seguridad del Estado.

Finalmente, este modelo de protección especializado no solo responde a una necesidad urgente, sino que sienta un precedente para el resguardo de infraestructuras críticas en Colombia. Su éxito dependerá del fortalecimiento continuo a través de actualizaciones periódicas, ejercicios tácticos de red teaming, capacitación constante y un compromiso institucional decidido que consolide la ciberseguridad como un eje esencial de la soberanía nacional en el siglo XXI.

Recomendaciones

Colombia enfrenta el reto urgente de proteger datos sensibles en sus centros penitenciarios militares ante amenazas digitales crecientes, un desafío que, paradójicamente, se convierte en oportunidad para desarrollar soluciones innovadoras adaptadas a su realidad. Para transformar vulnerabilidades en fortalezas, se proponen cinco estrategias clave interconectadas.

El primer paso implica una articulación estrecha con el Comando Conjunto Cibernético, aprovechando la modernización de la ciberdefensa nacional para incorporar requisitos específicos de estos entornos únicos —como manejo de datos judiciales en condiciones de conectividad intermitente—, equilibrando estándares globales con necesidades locales.

En paralelo, las limitaciones tecnológicas actuales pueden superarse mediante alianzas con el ecosistema nacional: universidades y startups de ciberseguridad podrían crear herramientas accesibles (como SIEM simplificados) y programas formativos escalables, reduciendo dependencia de tecnologías extranjeras y fomentando soluciones contextualizadas.

La implementación seguiría una hoja de ruta gradual: comenzando con un piloto de seis meses en un centro modelo para ajustes finos, seguido de escalamiento progresivo (12-18 meses) con controles técnicos avanzados (encriptación, autenticación multifactor) y capacitación por roles, hasta integrarse plenamente al sistema de ciberdefensa militar en 24 meses.

Este esfuerzo debe institucionalizarse como política transversal, articulando actores estatales y privados mediante normativas alineadas y alianzas que atraigan financiamiento y tecnologías emergentes. Así, lo que inicia como un protocolo para prisiones militares podría

convertirse en un modelo replicable para otras cárceles de alta seguridad o instituciones con datos críticos, posicionando a Colombia como referente regional en ciberseguridad carcelaria y atrayendo cooperación internacional. Esta visión integrada —que combina coordinación institucional, innovación local, implementación escalonada y proyección estratégica— no solo resuelve un problema inmediato, sino que sienta las bases para un ecosistema de ciberdefensa nacional más resiliente y autónomo.

Trabajos Futuros

Para fortalecer continuamente la ciberseguridad en entornos penitenciarios militares, se propone una agenda de trabajo futuro que permitirá evolucionar el protocolo mediante investigación comparativa con modelos internacionales, identificando mejores prácticas adaptables al contexto colombiano. Paralelamente, será clave desarrollar herramientas tecnológicas accesibles (como sistemas SIEM simplificados) que superen limitaciones presupuestarias e infraestructurales, garantizando interoperabilidad con los sistemas militares existentes y facilidad de uso.

La evaluación permanente mediante auditorías, pruebas de penetración y simulacros de ciberataques será fundamental para medir la eficacia real del protocolo y ajustarlo ante amenazas emergentes, entendiendo esta actualización como un proceso dinámico y no estático. Además, el modelo podría expandirse a otros entornos críticos del Estado (judiciales, de inteligencia o seguridad nacional), unificando criterios de protección y optimizando recursos. Esta visión de futuro debe integrar investigación, innovación tecnológica y evaluación continua, siempre guiada por una perspectiva estratégica que

anticipe escenarios de conflicto híbrido, con el fin de construir un sistema de ciberdefensa nacional resiliente y preparado para los desafíos digitales del siglo XXI.

Referencias

Al-Hawamleh, A., Alorfi, A., Al-Gasawneh, J., & Al-Rawashdeh, G. (2020). Cyber Security and Ethical Hacking: The Importance of Protecting User Data. *Solid State Technology, 63*(5), 7894-7899. Obtenido de https://www.researchgate.net/publication/347902323_Cyber_Security_and_Ethical_Hacking_The_Importance_of_Protecting_User_Data

Barney, N. (2022). Network security. What is network security? (B. (. Lutkevich, Ed.) *Search Networking*. Obtenido de https://www.techtarget.com/searchnetworking/definition/network-security

Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. *Journal of Cyber Policy, 6*(3), 298-317. Obtenido de https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1948582

Consejo Europeo. (2025). Reglamento General de Protección de Datos. El Reglamento General de Protección de Datos (RGPD) de la UE regula cómo pueden tratarse y transferirse los datos personales de las personas físicas en la UE. Obtenido de https://www.consilium.europa.eu/es/policies/data-protection/data-protection-regulation/

Constantinescu, L. M., & Manea, O. A. (2023). RISK MANAGEMENT AND CIBERSECURITY - BINOMIAL INSEPARABLE INTO THE DIGITALIZATION

AREA. *Journal Revue Européenne du Droit Social, 61*(4), 53-65. doi:10.53373/reds.2023.61.4.0134

Cooperative Cyber Defence Centre of Excellence - CCDCOE. (2022). *The Rights to Privacy and Data Protection in Times of Armed Conflict.* (R. B. (Eds.), Ed.) Tallinn, Estonia: NATO CCDCOE Publications. Obtenido de https://ccdcoe.org/uploads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pdf

Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2022). *The Rights to Privacy and Data Protection in Times of Armed Conflict.* (R. B. (Eds.), Ed.) Tallinn, Estonia: NATO CCDCOE Publications. Obtenido de https://ccdcoe.org/uploads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pdf

CrowdStrike. (2024). *CrowdStrike's Global Threat Report. Counter Adversary Operations team.* Austin, Texas, United States: CrowdStrike Security . Obtenido de https://iitd.com.ua/wp-content/uploads/2024/03/global-threat-report-2024-cs.pdf

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76-105. Obtenido de https://www.emerald.com/insight/search?q=Guido%20Nassimbeni

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity capacity: does it matter? *Journal of Information Policy, 9*, 280-306. Obtenido de

https://scholarlypublishingcollective.org/psup/information-policy/article-pdf/doi/10.5325/jinfopoli.9.2019.0280/1611397/jinfopoli_9_1_280.pdf

Edemekong, P. F., Annamaraju, P., Afzal, M., & J., H. M. (2024). Health Insurance Portability and Accountability Act (HIPAA) Compliance. *National Library of Medicina*. Obtenido de https://www.ncbi.nlm.nih.gov/books/NBK500019/

European Union Agency for Cybersecurity - ENISA. (2020). *Focus on National Cybersecurity Capabilities: New Self-Assessment Framework to Empower EU Member States.* Enisa Publications. Obtenido de https://www.enisa.europa.eu/news/enisa-news/national-cybersecurity-capabilities-framework

Flower, J. (31 de January de 2024). Fortifying the Walls: Cybersecurity in the United States Prison Service. *Linkedin Articles*. Obtenido de https://www.linkedin.com/pulse/fortifying-walls-cybersecurity-united-states-prison-service-flower-wlslc

Fortinet Inc. (2023). *What Is Data Security?Global Threat Landscape Report 2H 2023: Understand how data security enables organizations to protect information against cyberattacks.* Sunnyvale, California: Fortinet Research Team. Obtenido de https://www.fortinet.com/resources/cyberglossary/data-security

Giroux, H. (1997). .La pedagógia de frontera y la política del postmodernismo. *Revista Intringulis*(6), 96.

Global Cyber Security Capacity Centre - GCSCC. (2021). *Assessing national cybersecurity capacity.* University of Oxford, Department of Computer Science, Oxford, United Kingdom. Obtenido de https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

Global Forum on Cyber Expertise (GFCE). (2022). *Assessing and developing cybersecurity capability.* Obtenido de https://thegfce.org/

GlobalSuite Solutions. (16 de August de 2023). What is the ISO 27001 standard and what is its purpose? Obtenido de https://www.globalsuitesolutions.com/what-is-the-iso-27001-standard-and-what-is-its-purpose/

Himelwright, K. (2022). Cybersecurity & Correctional Institutions. *Old Dominion University: Cybersecurity Showcase*, 1-13. Obtenido de https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1030&context=covacci-undergraduateresearch

Imandeka, E., Hadi Putra, P. O., Hidayanto, A. N., & Mahmud, M. (2024). Exploring the World of Smart Prisons: Barriers, Trends, and Sustainable Solutions. *Human Behavior and Emerging Technologies*(6158154), 1-21. Obtenido de https://onlinelibrary.wiley.com/doi/10.1155/2024/6158154

Intel Corporation. (2025). Data Security: What It Is, Why It's Important, and How to Get Started. *Data Security Technology Overview*. Obtenido de https://www.intel.com/content/www/us/en/artificial-intelligence/data-security.html

Kosling, K. (6 de June de 2024). GDPR: Understanding the 6 Data Protection Principles. *IT Governance European Blog*. Obtenido de https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*(102248), 1-20. Obtenido de https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9755115/

Libicki, M. (2021). *Cyberspace in peace and war.* Naval Institute Press.

Lloyd, I. J. (2020). *Information Technology Law* (9th ed.). Oxford University Press. Obtenido de https://global.oup.com/academic/product/information-technology-law-9780198830559?cc=co&lang=en&

Margalef, L., & Arenas, A. (2006). ¿Qué entendemos por innovación Educativa? A proposito del desarrollo curricular. *Perpectiva Educacional, 1*(47), 13-31.

Mason Pope, T. (2023). Introducción a los aspectos éticos y legales en la atención sanitaria. *Mitchell Hamline School of Law*. Obtenido de https://www.msdmanuals.com/es/hogar/fundamentos/asuntos-legales-y-%C3%A9ticos/introducci%C3%B3n-a-los-aspectos-%C3%A9ticos-y-legales-en-la-atenci%C3%B3n-sanitaria

MinTIC. (2025). Política de Seguridad Digital. *Preguntas frecuentes*. Obtenido de https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital

Mishra, A., Alzoubi, Y. I., & Javeria Anwar, M. Q. (September de 2022). Attributes impacting cybersecurity policy development: An evidence from seven nations.

Computers & Security, 120, 102820. Obtenido de https://doi.org/10.1016/j.cose.2022.102820

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors, 22*(538), 1-35. Obtenido de https://www.mdpi.com/1424-8220/22/2/538/pdf

Nakhli, F. (2022). Cybersecurity development areas of action: an overview. *PPT Presentation*. Obtenido de https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2019/Workshop%20Kyiv/5%20%D0%A4%D0%B0%D1%80%D0%B8%D0%B4%20ITU%20Workshop%2016%20May%20-%20Farid%20Nakhli.pdf

Naseir, M. A. (2021). National cybersecurity capacity building framework for counties in a transitional phase. *Doctoral dissertation*. Bournemouth University. Obtenido de https://eprints.bournemouth.ac.uk/35646/1/NASEIR%2C%20Mohamed%20Altaher%20Ben_Ph.D._2020.pdf

Okta Inc. (29 de August de 2024). Privacy vs. Security: Exploring the Differences & Relationship. *Identity 101*. Obtenido de https://www.okta.com/identity-101/privacy-vs-security/

Paananen, H., Lapke, M., & Siponen, M. (January de 2020). State of the art in information security policy development. *Computers & Security, 88*(101608). Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S0167404818313002

Riddell, C. (12 de February de 2024). Data Security Explained: Challenges and Solutions. *Blog netwrix*. Obtenido de https://blog.netwrix.com/data-security/

Roselli, N. (2011). Teoria del aprendizaje colaborativo y la teoria de la repesentación social: convergencias y posibles articulaciones. *Revista colombiana de Ciencias Sociales, 2*(2), 173-191.

Scale Computing. (5 de February de 2024). What is data protection, and why is it important? *SC Insights*. Obtenido de https://www.scalecomputing.com/resources/what-is-data-protection-and-why-is-it-important

Slavin, R. (2002). *Aprendizaje cooperativo: Teoria, investigación y práctica.* AIQUE.

Solar Calvo, M. (2023). Tecnología, prisiones y toma de decisión: Posibilidades y riesgos. *Norte de salud mental,, 19*(69), 78-90. Obtenido de https://dialnet.unirioja.es/descarga/articulo/9372275.pdf

Srisakthi, S., & Suresh Babu, C. V. (2024). Chap.1 Cybersecurity: Protecting Information in a Digital World. En S. Saeed, N. Azizi, S. Tahir, M. Ahmad, & A. M. Almuhaideb, *Strengthening Industrial Cybersecurity to Protect Business Intelligence* (págs. 1-25). IGI Global. Obtenido de https://www.researchgate.net/publication/380125676_Cybersecurity_Protecting_Information_in_a_Digital_World

The BBC. (2025). Data Protection Act (1998). Obtenido de https://www.bbc.co.uk/bitesize/guides/z8m36yc/revision/4

Unión Europea. (2025). Reglamento general de protección de datos. Obtenido de https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Universidad Externado de Colombia. (20 de Octubre de 2022). 10 años de la Ley de protección de datos ¿Qué tanto hemos avanzado, qué nos hace falta? La Ley al tablero. *Memorias Foro Académico*. (D. M. Quiñones Zambrano, Recopilador) Departamento de Derecho de las Telecomunicaciones. Obtenido de https://www.uexternado.edu.co/wp-content/uploads/2024/02/10-ANOS-DE-LA-LEY-DE-PROTECCION-DE-DATOS-1.pdf

Villegas-Carrasquilla, L. (18 de February de 2021). Data protection and cybersecurity laws in Colombia. *CMS Legal*. Obtenido de https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/colombia