

Artículo Académico • Investigación Original

DOI: <https://doi.org/10.67827/2ne9ky26>

Cultura de seguridad y gestión de riesgos ISO/IEC 27001 en la Dirección Nacional de Migraciones

Security Culture and ISO/IEC 27001 Risk Management at the National Directorate of Migration

✉ **Alicia Raquel Fornerón Llano**,  mail: alicform@gmail.com

✉ **Perla Candia**,  mail: perla.candia@gmail.com

*Programa Académico – Maestría en Auditoría en Informática
Instituto Superior Vía Pro Desarrollo, Asunción, Paraguay*

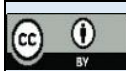
Recibido: 30/05/2025

Aceptado: 30/06/2026

Publicado: 31/08/2026

Cómo citar este artículo:

Fornerón Llano, A. R. & Candia, P. (2026). Cultura de seguridad y gestión de riesgos ISO/IEC 27001 en la Dirección Nacional de Migraciones. *VIACONCIENCIA*, 1(2), 185-203.
DOI: <https://doi.org/10.67827/2ne9ky26>



Esta obra está bajo una Licencia Creative Commons Atribución-No Comercial 4.0 Internacional © 2026
Instituto Superior Vía Pro Desarrollo. Todos los derechos reservados.

RESUMEN

El presente estudio analiza la relación entre la gestión de riesgos de tecnologías de la información (TI) y la cultura de seguridad de la información en la Dirección Nacional de Migraciones (DNM) del Paraguay, con el propósito de diseñar un plan de gestión de riesgos fundamentado en la norma ISO/IEC 27001 que fortalezca las prácticas de protección de los datos migratorios. El diseño metodológico adoptado fue mixto, de tipo secuencial con preponderancia cuantitativa y alcance descriptivo: se aplicó una encuesta a una muestra probabilística de 219 funcionarios de una población de 512, se entrevistó a cinco altos directivos y se examinaron las políticas institucionales mediante una lista de cotejo alineada a la norma. Los resultados revelan una brecha entre la conciencia y la práctica: aunque el 75,2 % de los funcionarios conoce las políticas de seguridad y el 91,7 % considera muy importante cumplirlas, el 83,5 % no recibió capacitación formal en los últimos doce meses, solo el 53,2 % encuentra claras dichas políticas y el 44 % desconoce el procedimiento de reporte de incidentes. Sobre esa base se identificaron diez riesgos prioritarios asociados al factor humano mediante el método MOSLER, tres de nivel crítico, y se asignaron responsabilidades con la matriz RACI.

Se concluye que la combinación de ISO/IEC 27001, MOSLER y RACI proporciona un modelo estructurado y replicable para consolidar la cultura de seguridad en instituciones públicas paraguayas.

Palabras clave: seguridad de la información; gestión de riesgos; cultura organizacional; tecnologías de la información; ciberseguridad; Paraguay

Abstract

This study analyzes the relationship between information technology (IT) risk management and information security culture at the National Directorate of Migration (DNM) of Paraguay, with the purpose of designing a risk management plan based on the ISO/IEC 27001 standard to strengthen the protection of migration data. The methodological design was mixed, sequential with quantitative predominance and descriptive scope: a survey was applied to a probabilistic sample of 219 officials out of a population of 512, five senior managers were interviewed, and institutional policies were examined through a checklist aligned with the standard. The results reveal a gap between awareness and practice: although 75.2 % of officials are aware of the security policies and 91.7 % consider compliance very important, 83.5 % received no formal training in the last twelve months, only 53.2 % find those policies clear, and 44 % do not know the incident reporting procedure. On this basis, ten priority risks associated with the human factor were identified through the MOSLER method, three of them critical, and responsibilities were assigned using the RACI matrix. It is concluded that the combination of ISO/IEC 27001, MOSLER and RACI provides a structured and replicable model to consolidate the security culture in Paraguayan public institutions.

Keywords: information security; risk management; organizational culture; information technology; cybersecurity; Paraguay

1. INTRODUCCIÓN

En la era digital, la seguridad de la información constituye un pilar de la continuidad operativa de las organizaciones, en particular de las instituciones gubernamentales que administran cotidianamente datos sensibles. El incremento sostenido de amenazas como el ransomware, el phishing y los accesos no autorizados ha impulsado la adopción de estándares internacionales de gestión, entre los que destaca la norma ISO/IEC 27001, que establece los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI) orientado a preservar la confidencialidad, la integridad y la disponibilidad de los activos (ISO/IEC, 2022).

No obstante, la evidencia regional indica que la eficacia de estos marcos depende menos de los controles tecnológicos que del comportamiento de las personas que los operan.

En América Latina y el Caribe los avances son desiguales. El reporte conjunto del Banco Interamericano de Desarrollo y la Organización de los Estados Americanos (BID y OEA, 2020) señala que, al momento de su publicación, solo 12 de los 32 países analizados contaban con estrategias nacionales de ciberseguridad, menos del 30 % disponía de marcos legales robustos y la región presentaba un déficit estimado de 600.000 profesionales del área. El mismo informe advierte que los usuarios suelen ser conscientes de los riesgos, pero no actúan en consecuencia en sus prácticas cotidianas, lo que sitúa a la cultura de seguridad como una dimensión crítica de la madurez cibernética nacional.

El Paraguay ha construido de manera progresiva un andamiaje normativo en la materia: el Plan Nacional de Ciberseguridad (Decreto N.º 7052, 2017), el modelo de gobernanza de la seguridad de la información en el Estado (Resolución MITIC N.º 733, 2019) y el Plan Nacional TIC 2022–2030 (Decreto N.º 8942, 2023). Sin embargo, el Informe de Ciberseguridad del equipo nacional de respuesta a incidentes documenta que la falta de formación estructurada del funcionariado sigue siendo un desafío recurrente en las instituciones públicas (CERT-PY, 2022), diagnóstico coincidente con el plan estratégico sectorial de defensa (Secretaría Permanente del Consejo de Defensa Nacional, 2024).

En ese contexto se sitúa la Dirección Nacional de Migraciones (DNM), organismo rector del régimen migratorio conforme a la Ley N.º 6984 (2022), que procesa grandes volúmenes de datos personales de connacionales y extranjeros en su oficina central, oficinas regionales y puestos de control. Al inicio del estudio la institución no contaba con un plan estructurado de gestión de riesgos de TI ni con un programa sostenido de concientización, y se habían observado fallas recurrentes en los controles de acceso, prácticas inseguras en el manejo de contraseñas y baja participación del personal en capacitaciones. Estas debilidades incrementan la exposición a incidentes capaces de comprometer la confidencialidad, la integridad y la disponibilidad de información crítica para el control migratorio y la confianza ciudadana.

Pese a ese andamiaje normativo y a la evidencia regional disponible, la literatura no registra diagnósticos integrales de la cultura de seguridad de la información ni planes de gestión de riesgos de TI centrados en el factor humano para organismos públicos paraguayos que administran datos personales masivos; ese vacío de conocimiento es el que aborda el presente estudio. La investigación respondió a la siguiente pregunta general: ¿cómo el diseño de una estrategia de gestión de riesgos de TI bajo el marco de ISO/IEC 27001 puede fortalecer la cultura de seguridad en la DNM? El objetivo general consistió en diseñar dicha estrategia, y los

objetivos específicos fueron: (a) revisar las políticas institucionales vigentes vinculadas con la cultura de seguridad; (b) identificar la cultura de seguridad existente entre los funcionarios; y (c) elaborar el plan de gestión de riesgos aplicando la matriz RACI y el método MOSLER. Como supuesto de trabajo se planteó que el diseño de una estrategia de gestión de riesgos de TI bajo el marco de ISO/IEC 27001 contribuiría a mejorar significativamente la cultura de seguridad institucional.

2. MARCO TEÓRICO

2.1. Seguridad de la información y la norma ISO/IEC 27001

La seguridad de la información comprende el conjunto de medidas técnicas, organizativas y humanas destinadas a proteger los activos de información frente a amenazas que afecten su confidencialidad, integridad o disponibilidad. La norma ISO/IEC 27001, en su tercera edición, especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI, e incorpora en su Anexo A un catálogo de controles agrupados en las dimensiones organizacional, de personas, física y tecnológica (ISO/IEC, 2022). Su estructura de alto nivel exige comprender el contexto de la organización, demostrar liderazgo, planificar el tratamiento de riesgos, proveer recursos y competencias, operar los controles y evaluar el desempeño, ciclo que convierte a la gestión de riesgos en el núcleo del sistema. La revisión sistemática de Culot et al. (2021) confirma la consolidación de la norma como estándar de referencia en seguridad de la información, con una agenda de investigación aún abierta sobre sus efectos organizacionales, mientras que la evidencia empírica reciente asocia su certificación con mejoras verificables de desempeño (Podrecca et al., 2022).

La adopción de la norma en organizaciones públicas ha sido documentada como una vía para ordenar la protección de la información y armonizarla con buenas prácticas internacionales. Burgos Salazar y Campos (2008) propusieron tempranamente un modelo de seguridad para tecnologías de la información y comunicación (TIC) articulado sobre estándares de la familia ISO, mientras que Paillacho Arias (2015) desarrolló, para entidades gubernamentales, un proceso de gestión del riesgo basado en ISO/IEC 27005 cuya fortaleza radica en combinar controles técnicos con la socialización de los riesgos entre los niveles estratégicos y operativos.

2.2. Gestión de riesgos de tecnologías de la información

La gestión de riesgos de TI es un proceso iterativo y permanente: cada cambio organizacional, regulatorio o tecnológico conlleva riesgos y oportunidades, y la organización debe anticiparse a ellos para minimizar la probabilidad de eventos no deseados (ISACA, 2009). En la literatura latinoamericana, el modelo MOGRIT de Vanegas Devia y Pardo (2014) armoniza normas y marcos como ISO/IEC 27005, ISO/IEC 31010, COBIT, ITIL, CRAMM y MAGERIT en una metodología integradora para identificar, analizar y tratar riesgos de TI; aunque fue concebido para micro, pequeñas y medianas empresas, sus principios de planificación, evaluación y mejora continua resultan trasladables a instituciones públicas. En el plano de la gobernanza, Calder y Watkins (2020) subrayan que la implementación de marcos como ISO/IEC 27001 exige el compromiso verificable de la alta dirección y la asignación explícita de responsabilidades.

Para la valoración de riesgos, el método MOSLER ofrece un procedimiento estructurado en fases de definición, análisis, evaluación y clasificación que pondera el impacto y la probabilidad de cada amenaza a fin de priorizar su tratamiento. De manera complementaria, la matriz RACI distribuye los roles de responsable de la ejecución (R), aprobador (A), consultado (C) e informado (I) sobre cada acción de mitigación, lo que favorece la rendición de cuentas y evita vacíos de responsabilidad en la operación del SGSI.

2.3. Cultura de seguridad de la información y factor humano

La cultura organizacional es el patrón de supuestos básicos compartidos que un grupo desarrolla al resolver sus problemas de adaptación externa e integración interna (Schein, 2010); proyectada al dominio de la seguridad, comprende los valores, creencias, actitudes y prácticas que orientan el comportamiento de los empleados frente a la protección de la información. Cano (2015) propone los imaginarios sociales como herramienta sistémico-social para transformar esa cultura, y posteriormente formula un modelo de madurez que advierte que una cultura de seguridad efectiva no depende únicamente de la existencia de normativas, sino de su socialización y del compromiso visible de la alta dirección (Cano, 2016). En la misma línea, Hernández Otálora (2019) documenta que la formación continua es el vehículo principal para convertir las políticas en hábitos, y el Instituto Nacional de Ciberseguridad de España destaca que desarrollar cultura de seguridad requiere programas sostenidos de concientización y no acciones aisladas (INCIBE, 2022). En el plano internacional, la revisión sistemática de Uchendu et al. (2021) identifica el apoyo de la alta dirección, la política de seguridad y la formación continua como los factores más determinantes para construir y sostener una cultura

de ciberseguridad, y advierte que pocos marcos han sido evaluados en escenarios organizacionales reales, lo que acentúa el valor de las aplicaciones situadas.

La evidencia empírica en instituciones públicas latinoamericanas respalda este enfoque. Romero Romero et al. (2022), en un estudio cuantitativo descriptivo aplicado a una entidad pública mexicana con un universo de 400 empleados, identificaron como fortalezas el sentido de pertenencia hacia la protección de la información y la percepción de programas efectivos de concientización, sobre un marco de referencia basado en ISO/IEC 27001 y COBIT. Estos antecedentes delimitan la brecha que aborda el presente estudio: la ausencia de diagnósticos integrales de cultura de seguridad y de planes de gestión de riesgos centrados en el factor humano —la denominada capa 8— en organismos públicos paraguayos que administran datos personales masivos.

3. METODOLOGÍA

El estudio adoptó un enfoque mixto con diseño secuencial de preponderancia cuantitativa (CUAN-cual), en el entendido de que los métodos mixtos permiten complementar la precisión de la medición numérica con la profundidad interpretativa de los datos cualitativos (Hernández-Sampieri y Mendoza Torres, 2018). El alcance fue descriptivo, dado que se caracterizó el manejo de la información por parte de los funcionarios en su entorno natural, sin manipulación de variables, siguiendo el proceder sistemático del método científico (Arias, 2012). La variable independiente fue la cultura de la seguridad y la variable dependiente el plan de gestión de riesgos de TI.

La población estuvo compuesta por 512 funcionarios de la DNM distribuidos en la oficina central de Asunción, las oficinas regionales y los puestos de control. Para la encuesta se calculó una muestra probabilística aleatoria simple de 219 personas, con un nivel de confianza del 95 % y un margen de error del 5 %, mediante la fórmula clásica de tamaño muestral para poblaciones finitas. Para las entrevistas se empleó una muestra por conveniencia de cinco altos directivos: los responsables de Tecnología de la Información y Comunicación, Movimiento Migratorio, Expediciones, Gestión y Monitoreo Migratorio y Administración. La Tabla 1 resume los parámetros del diseño muestral.

Se utilizaron tres técnicas complementarias. Primero, una encuesta con cuestionario de preguntas cerradas, administrada mediante formulario electrónico, orientada a medir el conocimiento, las prácticas y las percepciones de los funcionarios sobre la seguridad de la información. Segundo, entrevistas semiestructuradas con cuestionario de preguntas abiertas a los cinco directivos, organizadas en torno a los tres objetivos específicos. Tercero, análisis

documental de las políticas y procedimientos institucionales mediante una lista de cotejo construida sobre las cláusulas de la norma ISO/IEC 27001: contexto de la organización, liderazgo, planificación, apoyo, operación y evaluación del desempeño. En cuanto a la validez de los instrumentos, los ítems del cuestionario y de las guías de entrevista se derivaron de los controles de la norma ISO/IEC 27001 y de la literatura sobre cultura de seguridad, y su pertinencia y claridad fueron revisadas por la tutoría metodológica del programa de posgrado, lo que aporta evidencia de validez de contenido; no se aplicó una prueba piloto ni se estimaron coeficientes de consistencia interna, aspecto que se declara entre las limitaciones del estudio.

Tabla 1

Parámetros del diseño muestral de la encuesta

Parámetro	Símbolo	Valor
Tamaño de la población	N	512
Nivel de confianza (95 %)	Z	1,96
Variabilidad positiva	p	0,5
Variabilidad negativa	q	0,5
Precisión o error admitido	E	0,05
Tamaño de la muestra	n	219

Nota. Elaboración propia a partir de Fornerón Llano (2025), con base en la fórmula clásica de tamaño muestral para poblaciones finitas.

El análisis de los datos cuantitativos fue descriptivo, con distribución de frecuencias porcentuales por ítem. Los datos cualitativos se sometieron a análisis temático, para identificar patrones recurrentes en el discurso directivo, y a análisis de contenido, para contrastar los documentos institucionales con los requisitos normativos. Los resultados de las tres fuentes se triangularon para fundamentar el plan de gestión de riesgos. En materia ética, la participación fue voluntaria y anónima en las encuestas, y las entrevistas se realizaron con consentimiento de los directivos, resguardando la confidencialidad de la información institucional sensible. El estudio se desarrolló con conocimiento y autorización institucional para la aplicación de los instrumentos y, por tratarse de una investigación de percepción sin intervenciones clínicas ni tratamiento de datos sensibles de salud, no requirió el dictamen de un comité de ética. Entre las limitaciones se reconocen la circunscripción del estudio a una única institución, el carácter autorreportado de las prácticas medidas, la ausencia de validación psicométrica del cuestionario y el hecho de que el impacto real del plan solo podrá evidenciarse en el mediano plazo, tras su implementación.

4. RESULTADOS

4.1. Conocimiento, prácticas y percepciones de los funcionarios

La Tabla 2 sintetiza la distribución de respuestas de los 219 funcionarios encuestados en los principales indicadores del cuestionario. El perfil de la muestra reprodujo la estructura institucional: la mayor proporción de participantes pertenecía a la Dirección General de Movimiento Migratorio, seguida de las direcciones generales de Extranjeros y de Administración y Finanzas, la Dirección de Tecnología de la Información y Comunicación y la Dirección de Gestión de Talento Humano.

Tabla 2

Distribución porcentual de respuestas de la encuesta sobre cultura de seguridad de la información (n = 219)

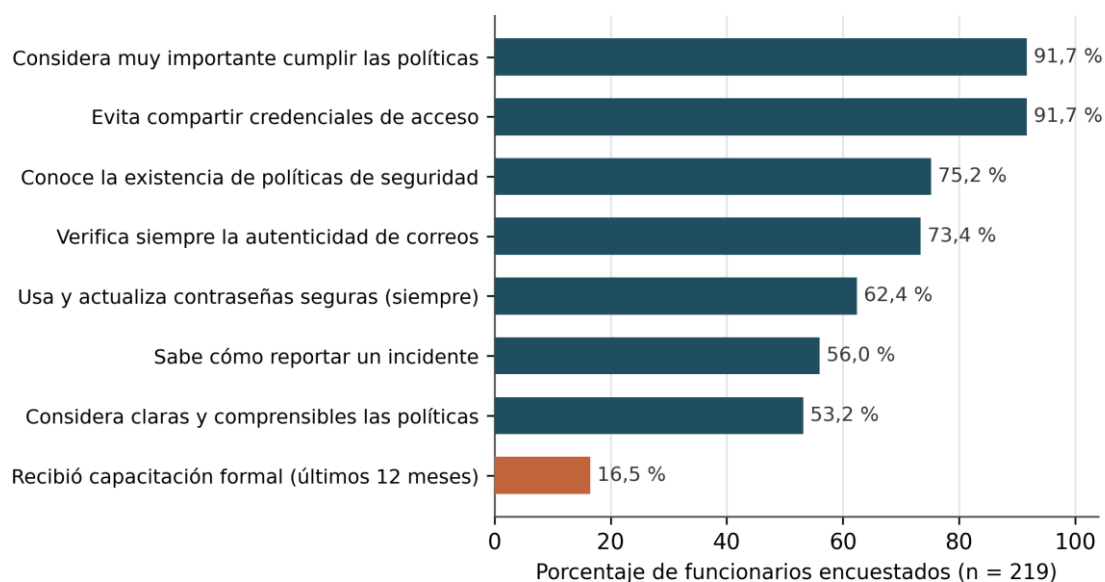
Indicador	Categoría de respuesta	%
Conocimiento de la existencia de políticas de seguridad	Sí / No está seguro / No	75,2 / 15,6 / 9,2
Capacitación formal recibida en los últimos 12 meses	Sí / No	16,5 / 83,5
Percepción de claridad de las políticas	Sí / No está seguro / No	53,2 / 37,6 / 9,2
Uso y actualización de contraseñas seguras	Siempre / Ocasionalmente o nunca	62,4 / 37,6
Evita compartir credenciales de acceso	Sí / No	91,7 / 8,3
Verificación de autenticidad de correos electrónicos	Siempre / A veces / Nunca	73,4 / 22,0 / 4,6
Importancia atribuida al cumplimiento de las políticas	Muy importante / Algo o poco importante	91,7 / 8,3
Percepción de compromiso del personal	Sí / Solo algunos / No	60,6 / 34,9 / 4,5
Percepción de apoyo institucional (recursos y formación)	Sí / No / No está seguro	52,3 / 24,8 / 22,9
Calificación de la cultura de seguridad institucional	Muy buena / Buena / Regular / Mala	27,5 / 26,6 / 38,6 / 7,3
Efectividad percibida de las capacitaciones	Muy efectivas / Efectivas / Poco / No efectivas	38,5 / 32,1 / 22,0 / 7,3
Promoción institucional de la seguridad	Frecuente / Ocasional / No se promueve	39,4 / 46,8 / 13,8
Conocimiento del procedimiento de reporte de incidentes	Sí / No	56,0 / 44,0
Ha reportado alguna vez un incidente	Sí / No	30,3 / 69,7
Calificación de la respuesta al incidente reportado	Muy buena / Buena / Regular / Mala	50,0 / 17,4 / 21,7 / 10,9
Mejora prioritaria sugerida	Capacitación / Compromiso directivo / Recursos / Otras	65,1 / 13,8 / 13,8 / 7,3

Nota. Elaboración propia a partir de Fornerón Llano (2025). Los porcentajes de categorías no rotuladas en los gráficos originales se obtuvieron por complemento aritmético; en dos ítems se informan categorías combinadas por no disponerse del desglose exacto.

Los datos configuran una paradoja entre conciencia y práctica. Tres de cada cuatro funcionarios (75,2 %) conocen la existencia de políticas de seguridad y una proporción casi unánime (91,7 %) considera muy importante cumplirlas; sin embargo, el 83,5 % declara no haber recibido capacitación formal en el último año, apenas algo más de la mitad (53,2 %) encuentra claras y comprensibles esas políticas y el 37,6 % expresa dudas sobre su contenido. Las prácticas de autoprotección muestran el mismo contraste: mientras el 91,7 % evita compartir credenciales, solo el 62,4 % utiliza y actualiza siempre contraseñas seguras y el 73,4 % verifica sistemáticamente la autenticidad de los correos electrónicos, de modo que porciones relevantes del funcionariado permanecen expuestas al phishing y a la ingeniería social. Aunque el alcance descriptivo no contempló contrastes inferenciales, la lectura conjunta de los indicadores agregados sugiere asociaciones plausibles entre el déficit formativo y las demás brechas —en particular, la coexistencia del 83,5 % sin capacitación con el 44 % que desconoce el procedimiento de reporte y con el 46,8 % que percibe una promoción apenas ocasional de la seguridad—, cuya verificación mediante análisis bivariados de los microdatos se propone como línea de profundización. La Figura 1 resume estos indicadores.

Figura 1

Indicadores de conocimiento y prácticas declaradas de seguridad de la información (n = 219)



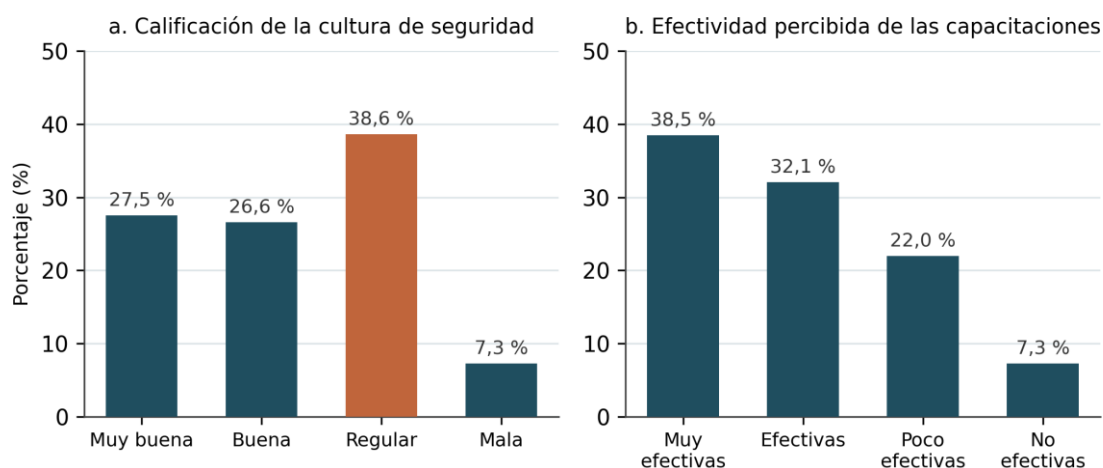
Nota. Elaboración propia a partir de los datos de la encuesta de Fornerón Llano (2025). En terracota se destaca el indicador crítico de capacitación.

La valoración global de la cultura institucional resulta moderada: la categoría más frecuente fue regular (38,6 %), seguida de muy buena (27,5 %) y buena (26,6 %), con un 7,3 %

que la califica de mala (Figura 2a). Las capacitaciones, cuando existieron, fueron bien valoradas —el 70,6 % las consideró muy efectivas o efectivas (Figura 2b)—, lo que indica que el problema no reside en la calidad de la formación sino en su cobertura y frecuencia. De manera consistente, el 46,8 % percibe que la seguridad se promueve solo ocasionalmente y el 13,8 % que no se promueve en absoluto.

Figura 2

Calificación de la cultura de seguridad y efectividad percibida de las capacitaciones



Nota. Elaboración propia a partir de los datos de la encuesta de Fornerón Llano (2025).

El eslabón más débil se localiza en la gestión de incidentes: el 44 % de los encuestados desconoce cómo reportar un problema de seguridad y el 69,7 % nunca ha reportado uno. Entre quienes sí lo hicieron, la mitad calificó la respuesta institucional como muy buena, aunque un tercio la consideró regular o mala, lo que sugiere protocolos de respuesta no uniformes. Finalmente, consultados por la mejora prioritaria, el 65,1 % señaló el refuerzo de las capacitaciones y la concientización del personal, por encima del compromiso de la alta gerencia (13,8 %) y de la mejora de los recursos tecnológicos (13,8 %): el propio funcionariado identifica la formación como la palanca principal de cambio.

4.2. Perspectiva directiva y análisis documental

Las entrevistas confirmaron que la institución cuenta con dos políticas vigentes desde 2023 —la Política de Seguridad de la Información y la Política de Copias de Seguridad y Restauración de la Información—, consideradas alineadas con las necesidades operativas, aunque los propios directivos admitieron la conveniencia de evaluarlas periódicamente frente a la evolución de los riesgos. El análisis temático reveló tres patrones convergentes: (a) un involucramiento directivo alto pero heterogéneo entre áreas, con mayor adhesión a las normas

allí donde la jefatura supervisa y promueve activamente su cumplimiento; (b) una oferta de capacitación limitada en frecuencia y alcance, sin un plan estructurado y continuo de formación; y (c) la ausencia de mecanismos sistemáticos de promoción de la seguridad, reconocida de manera explícita por el responsable del área tecnológica, quien señaló la necesidad de implementar acciones de concientización para todo el personal.

La lista de cotejo aplicada sobre las cláusulas de ISO/IEC 27001 arrojó un cumplimiento asimétrico. Como fortalezas se constataron el compromiso de la alta dirección, la existencia de roles definidos con una política de seguridad aprobada y comunicada, la implementación de controles de acceso y la realización de auditorías internas.

Como brechas críticas se identificaron: la falta de definición de los requisitos internos y externos que afectan la seguridad (contexto de la organización); la ausencia de un proceso documentado de gestión de riesgos y de un plan de tratamiento (planificación); la insuficiencia de recursos, capacitación y documentación accesible (apoyo); la carencia de procedimientos formalizados de gestión de incidentes (operación); y la inexistencia de indicadores de desempeño y de revisiones periódicas del sistema (evaluación del desempeño).

Al contrastar estos hallazgos con la Resolución MITIC N.º 733 (2019), que exige un área de seguridad de la información independiente, transversal y con reporte directo a la máxima autoridad institucional, se evidenció una brecha estructural entre el mandato normativo nacional y su aplicación efectiva en la DNM.

4.3. Plan de gestión de riesgos: matriz MOSLER e integración RACI

Sobre la base del diagnóstico triangulado se diseñó el plan de gestión de riesgos, cuyo alcance abarca los activos críticos de información de la DNM —infraestructura tecnológica, software y sistemas, datos sensibles, usuarios y procesos— con énfasis en el factor humano o capa 8. La aplicación del método MOSLER permitió identificar y clasificar diez riesgos prioritarios según su impacto y probabilidad de ocurrencia, tres de ellos de nivel crítico: el uso de contraseñas débiles, el phishing y la ingeniería social, y la falta de capacitación en seguridad (Tabla 3, Figura 3).

Tabla 3

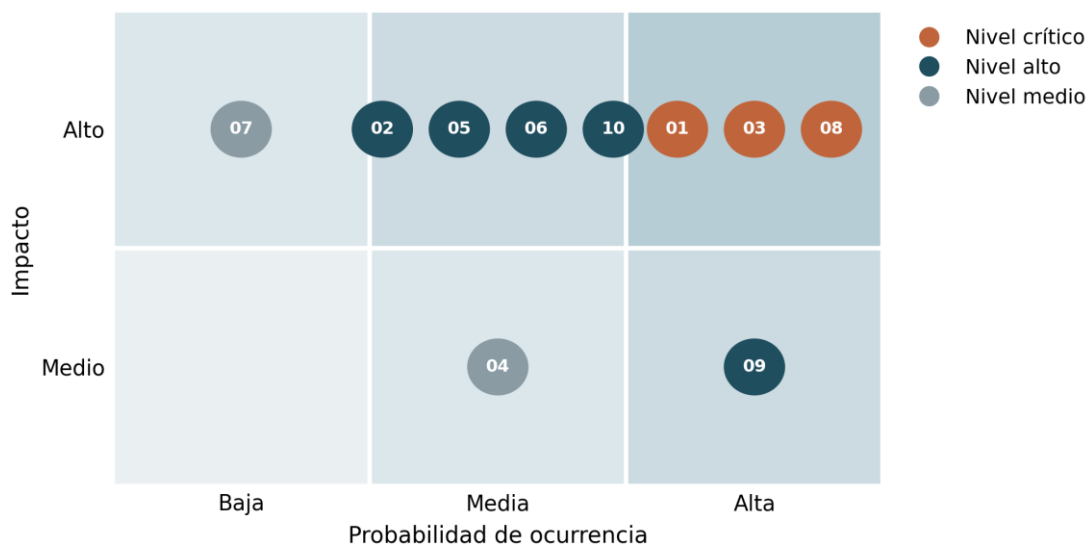
Matriz de identificación de riesgos del factor humano según el método MOSLER

ID	Riesgo identificado	Impacto	Probabilidad	Nivel	Medida de mitigación principal
R-01	Uso de contraseñas débiles	Alto	Alta	Crítico	Autenticación multifactor y contraseñas robustas
R-02	Compartición de credenciales	Alto	Media	Alto	Capacitación y monitoreo de uso indebido
R-03	Phishing e ingeniería social	Alto	Alta	Crítico	Simulacros de phishing y formación en detección
R-04	Uso de dispositivos no autorizados	Medio	Media	Medio	Políticas de control de acceso y restricción
R-05	Acceso a información sin justificación	Alto	Media	Alto	Principio de mínimo privilegio y auditoría de accesos
R-06	Instalación de software no autorizado	Alto	Media	Alto	Restricción de permisos y listas blancas
R-07	Pérdida o robo de dispositivos	Alto	Baja	Medio	Cifrado y procedimientos de respuesta a pérdida
R-08	Falta de capacitación en seguridad	Alto	Alta	Crítico	Programa de capacitación continua con evaluaciones
R-09	Uso indebido del correo institucional	Medio	Alta	Alto	Filtrado de contenido y clasificación de la información
R-10	Configuración incorrecta de permisos	Alto	Media	Alto	Revisión periódica y segmentación de privilegios

Nota. Elaboración propia a partir de la matriz MOSLER de Fornerón Llano (2025).

Figura 3

Mapa de calor de los riesgos identificados según impacto y probabilidad de ocurrencia



Nota. Elaboración propia a partir de la matriz MOSLER de Fornerón Llano (2025). Los números corresponden a los identificadores de riesgo de la Tabla 3.

La integración con la matriz RACI asignó responsabilidades uniformes para el tratamiento de los diez riesgos, con una única variación en el rol consultado del riesgo de capacitación, que incorpora a la gestión del talento humano (Tabla 4). Esta delimitación de funciones fortalece la rendición de cuentas y operacionaliza el requisito de liderazgo y asignación de roles de la norma.

Tabla 4

Asignación de responsabilidades del plan según la matriz RACI

Rol RACI	Actor institucional	Alcance
Responsable (R)	Área de Tecnología de la Información	Ejecución de las medidas de mitigación (R-01 a R-10)
Aprobador (A)	Departamento de Seguridad Informática	Aprobación de medidas y políticas (R-01 a R-10)
Consultado (C)	Auditoría Interna; Gestión de Talento Humano	Auditoría en R-01 a R-07, R-09 y R-10; talento humano en R-08
Informado (I)	Funcionarios de la institución	Comunicación de todas las medidas (R-01 a R-10)

Nota. Elaboración propia a partir de la matriz RACI de Fornerón Llano (2025).

El plan se estructura en cuatro fases: (1) identificación de riesgos, mediante entrevistas, encuestas, revisión de auditorías previas, análisis de configuraciones e inventario de activos; (2) evaluación y priorización, con el desarrollo de políticas y procedimientos, la programación de capacitaciones diferenciadas por perfil, la incorporación de herramientas de control — cortafuegos, gestión de eventos e información de seguridad (SIEM), antivirus corporativo y autenticación multifactor— y un cronograma anual de simulacros de ingeniería social; (3) implementación de las medidas de mitigación, con formalización documental aprobada por la alta dirección y despliegues con pruebas piloto; y (4) monitoreo y mejora continua, con auditorías internas alineadas a ISO/IEC 27001, gestión formal de incidentes, revisión semestral del plan y evaluaciones periódicas de la cultura de seguridad.

El cronograma de implementación abarca nueve meses, de julio a marzo, y el presupuesto estimado asciende a 363.900.000 guaraníes, cuyos componentes principales son las herramientas de seguridad informática (109.500.000), la consultoría especializada (73.000.000), las auditorías internas (58.400.000), los traslados del equipo de implementación

a ciudades clave (50.000.000), las capacitaciones al personal (36.500.000), los simulacros de seguridad (21.900.000) y el material de difusión (14.600.000).

5. DISCUSIÓN

El hallazgo central del estudio es la brecha entre conciencia y práctica: un funcionariado que valora casi unánimemente la seguridad de la información (91,7 %) pero que en su gran mayoría no recibe formación (83,5 % sin capacitación en doce meses) y que en proporciones relevantes desconoce los procedimientos operativos básicos, como el reporte de incidentes (44 %). Este patrón replica, a escala institucional, la observación regional del reporte BID y OEA (2020) según la cual los usuarios son conscientes de los riesgos pero no actúan en consecuencia, y coincide con el diagnóstico nacional sobre la falta de formación estructurada en las instituciones públicas (CERT-PY, 2022). La convergencia de la evidencia cuantitativa, las entrevistas y la lista de cotejo otorga solidez al diagnóstico: las tres fuentes apuntan a que la debilidad no reside en la ausencia de políticas —que existen y están aprobadas desde 2023— sino en su socialización, comprensión y traducción en hábitos.

Esta interpretación es consistente con el marco teórico. Cano (2016) sostiene que la cultura de seguridad no se decreta mediante normativas, sino que se construye a través de su apropiación colectiva y del compromiso observable de la dirección; el estudio verificó empíricamente esa tesis al constatar que las áreas con jefaturas activamente involucradas presentan mayor adhesión a las normas. Del mismo modo, la alta valoración de las capacitaciones existentes (70,6 % las considera efectivas o muy efectivas) junto con su escasa cobertura confirma el planteamiento de Hernández Otálora (2019) e INCIBE (2022): el problema paraguayo no es la calidad de la formación disponible sino su discontinuidad. Resulta significativo que el propio personal identifique la capacitación como la mejora prioritaria (65,1 %), por encima de la inversión tecnológica, lo que legitima internamente un plan centrado en la capa 8.

En el plano metodológico, la combinación de MOSLER y RACI bajo el paraguas de ISO/IEC 27001 mostró complementariedad con los modelos previos de la literatura. Frente al proceso de Paillacho Arias (2015), centrado en la matriz de riesgo inicial y la socialización, la propuesta añade la asignación explícita de responsabilidades por riesgo; frente a MOGRIT (Vanegas Devia y Pardo, 2014), concebido como armonización de estándares para pequeñas organizaciones, aporta una aplicación situada en una entidad pública con despliegue territorial. La concentración de los riesgos críticos en el factor humano —contraseñas débiles, phishing y déficit formativo— respalda además la decisión de diseño de priorizar controles de personas

sobre controles exclusivamente tecnológicos, en línea con el énfasis del Anexo A de la norma en la dimensión de personas (ISO/IEC, 2022) y con las buenas prácticas de gobernanza descritas por Calder y Watkins (2020).

Los resultados poseen implicaciones prácticas inmediatas para la administración pública paraguaya. La brecha detectada respecto de la Resolución MITIC N.º 733 (2019) —la ausencia de un área de seguridad independiente y transversal— indica que el fortalecimiento cultural debe acompañarse de ajustes de estructura organizacional, no solo de programas formativos.

Entre las limitaciones, debe reiterarse que los hallazgos corresponden a una única institución y a prácticas autorreportadas, que la muestra cualitativa se limitó a cinco directivos y que el efecto del plan sobre la cultura solo podrá medirse tras su implementación; futuras investigaciones deberían explorar análisis bivariados e inferenciales sobre los microdatos de la encuesta, aplicar mediciones longitudinales de madurez cultural, incorporar métricas conductuales objetivas —por ejemplo, tasas de clic en simulacros de phishing— y extender el diseño a otras entidades del Estado para evaluar su replicabilidad.

6. CONCLUSIONES

Respecto del objetivo general, el diseño de la estrategia de gestión de riesgos de TI basada en ISO/IEC 27001 permitió establecer un enfoque estructurado para fortalecer la cultura de seguridad en la DNM, articulando la identificación, evaluación y mitigación de riesgos con la concientización y capacitación del personal como condición de sostenibilidad. La respuesta a la pregunta de investigación es afirmativa en el plano del diseño: una estrategia de gestión de riesgos anclada en la norma, focalizada en el factor humano y con responsabilidades explícitas, ofrece el andamiaje necesario para transformar políticas formales en prácticas cotidianas.

En relación con el primer objetivo específico, el análisis documental estableció que la institución dispone de normativas y procedimientos de seguridad, pero con brechas de aplicación y actualización: no están definidos los requisitos del contexto, no existe un proceso documentado de gestión de riesgos ni procedimientos formales de gestión de incidentes, y no se monitorean indicadores de desempeño, carencias que además distancian a la institución del modelo de gobernanza estatal vigente.

En cuanto al segundo objetivo, la encuesta evidenció niveles heterogéneos de conocimiento y práctica: una valoración casi unánime de la importancia de la seguridad convive con un déficit formativo masivo, comprensión parcial de las políticas y desconocimiento extendido de los canales de reporte, de donde se concluye que la cultura de seguridad aún no está arraigada de manera homogénea en todos los niveles.

Con relación al tercer objetivo, la aplicación conjunta del método MOSLER y la matriz RACI produjo un plan operativo con diez riesgos priorizados —tres críticos, todos vinculados al comportamiento humano—, medidas de mitigación específicas, responsabilidades delimitadas, cronograma de nueve meses y presupuesto estimado.

El aporte científico original del estudio es doble: constituye el primer diagnóstico integral y triangulado de la cultura de seguridad de la información en el organismo migratorio paraguayo, y formaliza un modelo replicable —ISO/IEC 27001 como marco, MOSLER como método de valoración y RACI como instrumento de gobernanza— transferible a otras instituciones públicas de similar escala. El supuesto de trabajo resulta plausible a la luz del diseño logrado, si bien su confirmación definitiva exigirá evaluar la madurez cultural tras la implementación.

Se recomienda a la institución asegurar el compromiso visible de la alta dirección, presupuestar la formación continua, formalizar los procedimientos de gestión de incidentes mediante resolución de la máxima autoridad, adecuar sus normativas al plan nacional de ciberseguridad vigente y establecer indicadores de desempeño que permitan la mejora continua del sistema.

REFERENCIAS BIBLIOGRÁFICAS

- Arias, F. G. (2012). *El proyecto de investigación: introducción a la metodología científica* (6.^a ed.). Editorial Episteme.
- Banco Interamericano de Desarrollo y Organización de los Estados Americanos. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*. BID; OEA. <https://doi.org/10.18235/0002513>
- Burgos Salazar, J., y Campos, P. G. (2008). Modelo para seguridad de la información en TIC. *CEUR Workshop Proceedings*, 488, 234–253. <https://ceur-ws.org/Vol-488/paper13.pdf>
- Calder, A., y Watkins, S. (2020). *IT governance: An international guide to data security and ISO 27001/ISO 27002* (7.^a ed.). Kogan Page.
- Cano, J. (2015). *Imaginarios sociales: una herramienta sistémico-social para transformar una cultura organizacional de seguridad de la información* [Ponencia académica]. ResearchGate. <https://www.researchgate.net/publication/282769507>
- Cano, J. (2016). *Modelo de madurez de cultura organizacional de seguridad de la información: una visión desde el pensamiento sistémico-cibernético*. En *Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información (RECSI)* (pp. 24–29). Universitat de les Illes Balears. <http://recsi16.uib.es/wp-content/uploads/2016/10/ACTAS-RECSI-2016.pdf>
- CERT-PY. (2022). *Informe de Ciberseguridad en Paraguay 2022*. Ministerio de Tecnologías de la Información y Comunicación. <https://www.cert.gov.py/wp-content/uploads/2024/01/Informe-Ciberseguridad-Paraguay-2022.pdf>
- Culot, G., Nassimbeni, G., Podrecca, M., y 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. <https://doi.org/10.1108/TQM-09-2020-0202>
- Decreto N.º 7052. (2017). *Por el cual se aprueba el Plan Nacional de Ciberseguridad y se integra la Comisión Nacional de Ciberseguridad*. Presidencia de la República del Paraguay. <https://www.cert.gov.py/wp-content/uploads/2022/07/Decreto-N%C2%B0-7052-17.pdf>
- Decreto N.º 8942. (2023). *Por el cual se aprueba el Plan Nacional TIC Paraguay 2022–2030*. Presidencia de la República del Paraguay. <https://www.cert.gov.py/wp-content/uploads/2023/08/Plan-Nacional-TIC.pdf>

- Fornerón Llano, A. R. (2025). *Diseño de un plan de gestión de riesgos de TI basado en ISO 27001 para el fortalecimiento de la cultura de seguridad en la Dirección Nacional de Migraciones. Año 2024* [Tesis de maestría, Instituto Superior Vía Pro Desarrollo].
- Hernández Otálora, S. J. (2019). *Cultura en seguridad de la información* [Trabajo de grado, Universidad Piloto de Colombia]. Repositorio Institucional. <http://repository.unipiloto.edu.co/handle/20.500.12277/6436>
- Hernández-Sampieri, R., y Mendoza Torres, C. P. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Interamericana.
- Instituto Nacional de Ciberseguridad. (2022). *Desarrollar cultura en seguridad*. INCIBE. <https://www.incibe.es/empresas/que-te-interesa/develop-culture-in-security>
- ISACA. (2009). *The Risk IT Framework*. ISACA.
- ISO/IEC. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (3.^a ed.). International Organization for Standardization. <https://www.iso.org/standard/27001>
- Ley N.º 6984. (2022). *De Migraciones*. Biblioteca y Archivo Central del Congreso Nacional. <https://www.bacn.gov.py/leyes-paraguayas/10973/ley-n-6984-de-migraciones>
- Paillacho Arias, S. M. (2015). *Modelo de un proceso de la gestión del riesgo de la seguridad de la información en entidades gubernamentales* [Tesis de maestría, Escuela Politécnica Nacional]. Repositorio Digital EPN. <http://bibdigital.epn.edu.ec/handle/15000/10653>
- Podrecca, M., Culot, G., Nassimbeni, G., y Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, 142, 103744. <https://doi.org/10.1016/j.compind.2022.103744>
- Resolución MITIC N.º 733. (2019). *Por la cual se aprueba el modelo de gobernanza de seguridad de la información en el Estado*. Ministerio de Tecnologías de la Información y Comunicación. https://www.cert.gov.py/wp-content/uploads/2022/07/RESOLUCION_MITIC_N_733-2019_-_Modelo_de_Gobernanza-1.pdf
- Romero Romero, A., Gasca Leyva, M. E., García Palmas, M. A., y Hernández Suárez, A. (2022). Aplicación de buenas prácticas, un camino hacia la cultura de la seguridad informática en las instituciones públicas. *Revista Electrónica sobre Tecnología, Educación y Sociedad*, 9(18). <https://www.ctes.org.mx/index.php/ctes/article/view/794>
- Schein, E. H. (2010). *Organizational culture and leadership* (4.^a ed.). Jossey-Bass.

- Secretaría Permanente del Consejo de Defensa Nacional. (2024). *Seguridad para el Desarrollo: Plan Estratégico 2023–2028*. Ministerio de Defensa Nacional del Paraguay. <https://mdn.gov.py/wp-content/uploads/2024/11/Plan-Seguridad-para-el-Desarrollo-2023-2028.pdf>
- Uchendu, B., Nurse, J. R. C., Bada, M., y Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, 102387. <https://doi.org/10.1016/j.cose.2021.102387>
- Vanegas Devia, G. A., y Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT. *Sistemas & Telemática*, 12(30), 35–48. <https://www.redalyc.org/pdf/4115/411534000003.pdf>