

ANÁLISIS DE LA DIMENSIÓN HUMANA DURANTE UN CIBERATAQUE

THE HUMAN DIMENSION DURING A CYBERATTACK

Ricardo Naranjo Faccini

1Skina IT Solutions / Universidad Javeriana

gerencia@skinait.com

<https://orcid.org/0009-0006-1595-4810>

Colombia

Recibido: 17 Mayo 2026 / Revisado: 21 Julio 2026 / Aceptado: 30 Julio 2026 / Publicado: 4 Agosto 2026

Resumen

La gestión de incidentes de ciberseguridad en infraestructuras críticas suele abordarse desde una perspectiva predominantemente técnica, subestimando el impacto de los factores psicosociales y neurocognitivos en los equipos de respuesta. El objetivo de este estudio es analizar las dinámicas operacionales y la toma de decisiones del personal de seguridad de la información durante la atención de un ciberataque de ransomware en una organización multisectorial. Se empleó un enfoque cualitativo mediante un estudio de caso único basado en una entrevista semiestructurada en profundidad aplicada al Chief Information Security Officer (CISO). La evidencia se contrastó con los estándares ISO/IEC 27035 y NIST SP 800-61, así como con la literatura sobre carga cognitiva, fatiga y neurociencia del estrés.

Los hallazgos sugieren que la degradación en el desempeño táctico del equipo no respondió a deficiencias en la competencia técnica, sino al agotamiento prolongado y al estrés agudo, los cuales inhibieron el análisis deliberativo y promovieron el uso de heurísticas automáticas de decisión. La efectividad en la mitigación de ataques de alto impacto exige diseñar protocolos de respuesta que contemplen las limitaciones de la arquitectura cognitiva humana bajo presión, integrando la gestión del estrés y los simulacros operacionales dentro de los planes de continuidad del negocio.

Palabras clave: Ciberseguridad; Gestión de incidentes; Factor humano; Toma de decisiones; Estrés operacional; Estudio de caso.

Abstract

Cybersecurity incident management in critical infrastructures is typically addressed from a predominantly technical perspective, underestimating the impact of psychosocial and neurocognitive factors on response teams. The objective of this study is to analyze the operational dynamics and decision-making processes of information security personnel during the response to a ransomware cyberattack in a multisector organization. A qualitative approach was employed using a single case study based on an in-depth semi-structured interview conducted with the Chief Information Security Officer (CISO). The evidence was benchmarked against the ISO/IEC 27035 and NIST SP 800-61 standards, as well as literature on cognitive load, fatigue, and the neuroscience of stress.

It was identified that the degradation in the team's tactical performance was not due to deficiencies in technical competence, but rather to prolonged exhaustion and acute stress, which inhibited deliberative analysis and promoted the reliance on automatic decision-making heuristics. The effectiveness in mitigating high-impact attacks requires designing response protocols that account for the limitations of human cognitive architecture under pressure, integrating stress management and operational drills into business continuity plans.

Keywords: *Cybersecurity; Incident management; Human factor; Decision-making; Operational stress; Case study*

Introducción

Planteamiento del problema

En el ecosistema de la ciberseguridad contemporánea, la narrativa dominante suele centrarse en la sofisticación de los vectores de ataque, la arquitectura de los sistemas de defensa y la capacidad técnica de respuesta ante incidentes. Sin embargo, existe una brecha crítica en la comprensión de los procesos de seguridad: la invisibilidad de la crisis humana que subyace a la técnica. El problema fundamental radica en que, ante ataques de alta complejidad como el ransomware, las organizaciones tienden a ignorar que las decisiones críticas no son ejecutadas por algoritmos, sino por individuos sometidos a niveles extremos de estrés, fatiga y presión social. Esta omisión del factor humano en la planificación estratégica

debilita la resiliencia institucional, convirtiendo la gestión de crisis en un proceso mecánico que falla al no considerar las dinámicas psicológicas y culturales de los equipos de respuesta.

Relevancia y justificación

La relevancia de este estudio reside en la necesidad de "des-algoritmizar" la ciberseguridad para comprenderla como un fenómeno social e institucional. En América Latina, donde la infraestructura tecnológica a menudo convive con recursos limitados y marcos regulatorios en evolución, la capacidad de los líderes de seguridad para gestionar el capital humano es el factor diferenciador entre la recuperación y el colapso. Justificar una revisión con este enfoque permite a la academia y a la industria reconocer que la soberanía tecnológica y la defensa de activos de información dependen,

en última instancia, de la salud mental del equipo, la efectividad de la comunicación y la solidez de la cultura organizacional.

Tradicionalmente, el "factor humano" en ciberseguridad se ha analizado desde la perspectiva del usuario final como el eslabón vulnerable expuesto a la ingeniería social. Informes de la industria confirman que más de dos tercios de las brechas de seguridad involucran directa o indirectamente la interacción humana, ya sea mediante engaño o configuraciones erróneas (Verizon, 2024). Sin embargo, el marco pionero de Adams y Sasse (1999), que demostró cómo la fricción operativa y la sobrecarga de los controles de seguridad impulsan comportamientos de evasión involuntaria, no se limita a los usuarios finales: aplica con la misma severidad a los propios operadores, analistas y líderes de infraestructura crítica. Cuando los sistemas de gestión de incidentes y las políticas de mitigación imponen cargas cognitivas desmedidas durante una crisis, son los mismos profesionales técnicos quienes se ven forzados a adoptar atajos procedimentales para mantener la continuidad del servicio.

Antecedentes y contexto

Históricamente, la gestión de incidentes se ha fundamentado en estándares internacionales como la ISO/IEC 27035 y NIST SP 800-61, los cuales proporcionan orientaciones operativas indispensables pero se omite la vulnerabilidad de los equipos de respuesta técnica que no responde únicamente a la complejidad del vector de ataque, sino a la degradación de las funciones ejecutivas provocada por el estrés agudo y sostenido cuando las labores se prolongan más allá de la rutina acostumbrada y bajo la presión de saber que la continuidad del negocio depende estrictamente de la respuesta del equipo. La literatura en neurociencia demuestra que el estrés extremo

provoca la inhibición funcional de la corteza prefrontal, trasladando el control conductual hacia estructuras subcorticales primitivas como la amígdala (Arnsten, 2009). En el contexto de la gestión de un ciberataque, esta alteración neurobiológica debilita el pensamiento analítico riguroso, denominado por Kahneman (2011) como "Sistema 2", y fuerza la dependencia en el "Sistema 1", caracterizado por respuestas rápidas, heurísticas e intuitivas. Si a esto se suma la fatiga acumulada, privación de sueño y la presión operacional prolongada, se configuran las condiciones clínicas propicias para el síndrome de burnout (Maslach & Leiter, 2016), manifestado en despersonalización, agotamiento emocional y una drástica reducción en la capacidad de evaluación de riesgos en tiempo real.

Los antecedentes de este estudio se encuentran en la experiencia directa de campo, donde la teoría de la prevención y la detección se enfrenta a la realidad de un ataque de ransomware que paraliza servicios esenciales. Este escenario constituye el laboratorio perfecto para observar cómo las personalidades se transforman bajo tensión y cómo las estructuras familiares y profesionales se entrelazan durante un fin de semana crítico.

Propósito y objetivos

El propósito central de este estudio es documentar y analizar la dimensión humana de la gestión de incidentes a través de la sistematización de una experiencia real. Los objetivos específicos son:

- Identificar los desafíos emocionales y psicológicos que enfrentan los equipos de ciberseguridad durante un ataque de ransomware.

- Analizar la influencia de la cultura organizacional y la comunicación externa en la eficacia de la respuesta técnica.
- Sintetizar lecciones aprendidas que permitan humanizar los protocolos de gestión de incidentes, promoviendo la resiliencia integral en las organizaciones.

Metodología

La presente investigación adopta un enfoque cualitativo con un diseño de estudio de caso único (Yin, 2018), fundamentado en la aplicación de una entrevista semiestructurada en profundidad dirigida al Chief Information Security Officer (CISO) de una organización multisectorial en Colombia. De acuerdo con Stake (1995) y Yin (2018), el estudio de caso único es la estrategia metodológica por excelencia cuando se busca explorar y comprender un fenómeno contemporáneo complejo dentro de su contexto real, especialmente cuando los límites entre el fenómeno (las decisiones bajo estrés del equipo de respuesta) y el contexto (el desarrollo del ciberataque) no son claramente evidentes.

Estrategia de identificación y recolección

La presente revisión no se limita a una búsqueda bibliográfica tradicional, sino que emplea una metodología de sistematización de experiencias y estudio de caso cualitativo. La fuente primaria de información se obtuvo mediante un conversatorio estructurado con un Chief Information Security Officer (CISO) de una organización multisectorial en Colombia. Este encuentro se diseñó como una entrevista técnica semiestructurada, donde se formularon preguntas guía para documentar la cronología, las decisiones técnicas y las respuestas emocionales durante un incidente de ransomware real.

Fuentes y Marco de Referencia para Triangulación

Para contrastar los datos obtenidos en la entrevista con la praxis operativa y los estándares internacionales (triangulación de información), se consultaron fuentes primarias de estandarización como la familia de normas ISO/IEC 27000 (con énfasis en ISO/IEC 27035 para gestión de incidentes) y los marcos de referencia del NIST (Special Publication 800-61).

La base conceptual y metodológica de la revisión se sustenta en la literatura técnica especializada de **Skina IT Solutions**, la cual provee el soporte para el análisis de la Metodología Integral para la Gestión de Riesgos (MIGRI) y la aplicación de Inteligencia Artificial en procesos de seguridad. Se incluyeron artículos fundamentales sobre la protección de activos de información, la taxonomía de amenazas (virus, troyanos, ransomware) y las tácticas avanzadas de defensa. Estas fuentes, junto con su bibliografía asociada, permiten situar el estudio en un marco de ciberseguridad aplicada que trasciende la teoría generalista para enfocarse en la realidad operativa del sector.

La información recopilada fue organizada bajo el modelo de ciclo de vida de activos de información, categorizando las actividades en: preparativas, preventivas, detectivas, reactivas y retrospectivas. Los datos obtenidos del conversatorio fueron contrastados con la literatura técnica para identificar convergencias entre los estándares teóricos y la praxis operativa. Se aplicó una evaluación de calidad basada en la relevancia de las fuentes para el contexto latinoamericano, priorizando aquellas que discuten la autonomía tecnológica y la gestión de infraestructuras críticas. Finalmente, la narrativa se depuró mediante un proceso de

validación con el proponente original (CISO), asegurando que la caricaturización y parodia empleadas no alteraran la veracidad de los hallazgos técnicos y humanos presentados.

Alcance y limitaciones metodológicas

Como es inherente a los diseños cualitativos de caso único, la principal limitación de este estudio radica en la imposibilidad de realizar una generalización estadística de los hallazgos hacia otras organizaciones o entornos informáticos (Yin, 2018; Flick, 2018). Las dinámicas organizacionales, la infraestructura y la intensidad del ciberataque analizado corresponden a un contexto singular.

Consideraciones éticas, anonimización y estrategia narrativa

La recolección de datos primarios se realizó bajo estrictos compromisos de confidencialidad y consentimiento informado con el CISO entrevistado, quien actuó como informante clave autorizado para compartir la experiencia operativa. Dado el nivel de detalle técnico, sectorial y temporal expuesto —el cual podría facilitar la identificación de la organización afectada o generar vulnerabilidades de seguridad de la información—, se estableció un protocolo riguroso de anonimización. En consecuencia, los datos identificadores fueron sustituidos o generalizados sin modificar la secuencia analítica, la duración aproximada del incidente ni los hallazgos relevantes para la investigación y presentados mediante una narrativa dramatizada con tintes de caricaturización. Este recurso cumple una doble función metodológica: actúa como una capa de enmascaramiento ético para proteger la identidad de la institución y sus actores, y funciona como una estrategia pedagógica que

dinamiza la lectura, facilitando la comprensión y previniendo la fatiga cognitiva del lector ante la alta densidad conceptual del análisis técnico.

Desarrollo y discusión

Caso de Estudio: Crisis en una Organización Multisectorial

Para contextualizar el análisis, es imperativo describir el entorno donde se suscitaron los hechos. La organización víctima es un conglomerado empresarial de alta complejidad en Colombia, cuya operación integra sectores críticos y diversos: salud (clínica y droguerías), retail (supermercados), educación (colegios) y turismo (hoteles). Esta heterogeneidad implica una superficie de ataque extensa y una dependencia absoluta de la disponibilidad de datos para la prestación de servicios esenciales.

El incidente ocurrió durante un fin de semana largo (sábado, domingo y lunes festivo), cuando se celebraba el día del padre, un factor estratégico explotado por los atacantes para maximizar el tiempo de intrusión antes de la detección, aprovechando la reducción de personal operativo y la ralentización de las líneas de mando.

Cronología del Incidente: La Dimensión Humana en la Praxis

Para contextualizar el análisis, se presenta la cronología de los hechos documentados durante el conversatorio, los cuales están detallados en el artículo publicado en <https://www.skinait.com/a-Escritos-93>, que sirven como base para esta revisión. El caso describe la respuesta de una CISO ante un ataque de ransomware en una organización multisectorial.

- Viernes, 18:00 h - El Inicio: La crisis comienza al final de la jornada laboral. Se detecta el cifrado de servidores críticos. La respuesta inicial es técnica: aislamiento de redes y confirmación del vector de ataque (Ransomware). Surge el primer impacto humano: la interrupción de la vida personal y el inicio de la fatiga.
- Sábado, 02:00h a 10:00h - La Presión Creciente: El equipo técnico trabaja sin descanso. Aparecen las primeras fricciones con proveedores externos que no responden con la agilidad requerida y aquellos que pretenden aprovecharse de la necesidad apremiante de la organización. La CISO debe gestionar no solo la recuperación de datos, sino la ansiedad de la alta gerencia y la incertidumbre de los empleados.
- Sábado por la tarde - El Clímax del Estrés: Se identifica la magnitud del daño en sectores sensibles (Salud y Educación). La narrativa destaca cómo las personalidades del equipo se transforman: desde el aislamiento defensivo hasta el liderazgo heroico. La relación con los medios se convirtió en una presión adicional.
- Domingo - Recuperación y Agotamiento: Se inicia la restauración de activos desde respaldos seguros. El agotamiento físico es evidente. Las dinámicas familiares de los técnicos entran en conflicto con la responsabilidad profesional, subrayando que la ciberseguridad tiene un costo personal invisible.
- Lunes, 08:00h - Retorno a la "Normalidad": Los servicios básicos se restablecen. Comienza la evaluación de daños y el cierre de brechas. El equipo queda exhausto, evidenciando que la crisis técnica ha terminado, pero la crisis humana requiere un proceso de sanación más largo.

Organización Temática de la Gestión de Incidentes

El análisis se estructura siguiendo el ciclo de vida de la protección de los activos de información que divide las acciones en cinco fases críticas: preparativas, preventivas, detectivas, reactivas y retrospectivas.

1. Fases Preparativas y Preventivas: El Escudo Agrietado y la Trampa de la Rutina

Estas etapas constituyen el cimiento estratégico de la defensa; son el "escudo" que se forja antes de que el primer paquete malicioso toque la red. Bajo la óptica de la metodología **MIGRI** y el estándar **ISO/IEC 27035**, la preparación no es un evento estático, sino un proceso de identificación y valoración de activos que precede al endurecimiento de sistemas (Hardening) y a la gestión de identidades.

- Convergencia Teórica y el Rigor del Diseño: Existe un consenso absoluto entre la literatura de Skina IT Solutions, el NIST y las normas internacionales: una respuesta eficaz es hija directa de una preparación exhaustiva. La teoría dicta que si el diseño preventivo es sólido, el riesgo se mantiene bajo niveles aceptables.
- La Realidad del Terreno: El Factor Humano como Punto de Falla: Sin embargo, el estudio de caso revela una brecha profunda entre el protocolo en papel y la ejecución en la trinchera. En sectores tan demandantes como en esta organización multisectorial, la "dimensión humana" introduce variables que que la técnica no siempre puede predecir: el exceso de confianza y la erosión del rigor por falta de auditorías constantes.

- El Detonante: Fatiga, Rutina y la Autorización de la Crisis: El incidente no fue producto de una falla en el algoritmo, sino de un colapso en la vigilancia humana. La carga de trabajo abrumadora del personal de monitoreo, sumada a una rutina anestesiada por la aparición constante de falsos positivos, creó el escenario perfecto para el desastre. La negligencia se materializó cuando el encargado de verificar las alertas, ignorando la advertencia explícita del sistema automático de detección, autorizó el paso del archivo infectado sin la verificación exhaustiva que exigía el protocolo. Este acto de "ceguera operativa" demuestra que, sin disciplina y gestión del agotamiento, incluso la herramienta de detección más avanzada es inútil frente a un clic humano mal ejecutado.

2. Fases Detectivas y Reactivas: El Caos Operativo y la Contención Selectiva

La detección oportuna, sustentada en un monitoreo de activos robusto, actúa como el puente crítico hacia la fase reactiva. En este escenario, la implementación de inteligencia artificial no es un lujo, sino una necesidad para acelerar el reconocimiento de patrones anómalos de tráfico o cifrado que el ojo humano, nublado por el cansancio, podría omitir.

- La Gestión bajo Presión: Más allá de los Bitsets: Durante el incidente, la fase reactiva trascendió lo meramente técnico (aislamiento de servidores y orquestación de backups). Se transformó en un ejercicio de gestión de crisis donde el estrés actuó como un catalizador químico, alterando las personalidades del equipo y poniendo a prueba la cohesión del liderazgo bajo fuego.
- Divergencia Técnica-Humana y Ruido Externo: Mientras los manuales sugieren una ejecución lineal de los planes de contingencia, la praxis revela que la presión de los medios de comunicación y la incertidumbre de proveedores externos introducen variables de "ruido" que impactan directamente en el tiempo de recuperación técnica.

El Triunfo de la Arquitectura: Segmentación y Resiliencia: No obstante, el caos no fue absoluto. El incidente dejó una lección magistral sobre la importancia de las actividades preventivas: la **segmentación de redes**. Gracias a esta arquitectura, los hoteles —que operaban en un segmento independiente— mantuvieron su normalidad, ajenos al malware que devastaba la casa matriz. Infortunadamente, las **droguerías y supermercados**, al compartir el área administrativa afectada, sufrieron el impacto directo. Por su parte, los **colegios**, protegidos por el paréntesis del fin de semana festivo, regresaron el martes a un entorno ya saneado por el equipo de seguridad, demostrando que una defensa bien estructurada permite salvar órganos vitales mientras se atiende la infección principal.

3. Fase Retrospectiva: El Aprendizaje Estratégico y la Sanación del Equipo

Esta etapa representa la fase menos técnica del ciclo, pero se erige como la más vital para la resiliencia a largo plazo. En la teoría, implica el análisis de causa raíz y la actualización de controles preventivos; en la práctica humana, es el momento de la verdad.

- La Gestión Emocional como Control de Seguridad: El estudio de caso resalta que una retrospectiva profesional no puede limitarse a identificar "qué parche faltaba"

o qué puerto quedó abierto. Es imperativo evaluar cómo respondió el equipo humanamente. Fortalecer la cultura organizacional implica reconocer el desgaste del personal para evitar que las cicatrices del estrés se conviertan en futuras vulnerabilidades.

- El Factor del Outsourcing y la Ética de Mercado: Un hallazgo crítico fue la necesidad de contar con aliados externos antes de que la crisis estalle. El incidente reveló que, aunque se cuente con un equipo disciplinado y competente, existen capacidades especializadas, como la informática forense, que requieren apoyo externo.
- La Oportunidad frente a la Solidaridad: La narrativa expone una realidad dolorosa del ecosistema: en el clímax del ataque, la mayoría de las empresas prestadoras de servicios intentaron aprovecharse de la vulnerabilidad y urgencia de la organización, ofreciendo tarifas desproporcionadas y predatorias. No obstante, el relato destaca un punto de inflexión positivo: el hallazgo de una firma que brindó apoyo con precios razonables y ética profesional. Esta acción no solo resolvió la crisis técnica, sino que cimentó una relación de confianza y gratitud absoluta; hoy, son ellos los aliados estratégicos a quienes la organización acude sin dudar, demostrando que en ciberseguridad, la lealtad se construye en la trinchera.

Análisis del comportamiento del equipo técnico

La evidencia observada en la respuesta operativa del equipo técnico confirma que el deterioro en la toma de decisiones no obedeció a una falta de competencia técnica,

sino que hubo una gran influencia de los efectos neurocognitivos del estrés prolongado descritos por Arnsten (2009). Durante la fase crítica de la emergencia, las decisiones tomadas bajo presión extrema reflejaron un sesgo hacia la heurística del "Sistema 1" (Kahneman, 2011): se privilegiaron acciones inmediatas de contención rápida frente a la verificación metódica de evidencia forense. Este fenómeno valida la necesidad de reinterpretar el principio de Adams y Sasse (1999) en el ámbito de los equipos de respuesta a incidentes: los analistas y el CISO no operaron en un vacío abstracto, sino bajo un agotamiento progresivo, desajustes en la carga de trabajo y afectación en la dinámica del fin de semana, que detonaron síntomas claros de burnout operacional (Maslach & Leiter, 2016).

En consecuencia, reducir la exposición del factor humano en incidentes de alto impacto exige diseñar protocolos de mitigación que contemplen los límites de la arquitectura cognitiva humana en condiciones de fatiga y presión crítica. Para ello, es fundamental preparar formalmente al personal del equipo de respuesta mediante simulacros operacionales y entrenamientos previos que recreen entornos de alta tensión y cansancio acumulado. En este sentido, las brigadas de emergencia institucionales constituyen una plataforma idónea para integrar al equipo técnico en sus ejercicios periódicos de gestión de crisis, fortaleciendo la disciplina procedimental, el autocontrol y la resiliencia operativa antes de que ocurra un evento real.

Comparación y patrones identificados

A continuación, se presenta una tabla de síntesis que relaciona los componentes técnicos con los hallazgos del factor humano derivados del conversatorio:

Tabla 1. Relación entre las fases del ciclo de gestión de incidentes, los componentes técnicos y la dimensión humana identificada

Fase del Ciclo	Componente Técnico (MIGRI/ISO)	Dimensión Humana Identificada
Preparativa	Inventario de activos y valoración de riesgos.	Falsa sensación de seguridad o "fatiga de alertas"
Preparativa	Hardening, cifrado y control de acceso.	Resistencia al cambio en procesos de usuario final.
Detectiva	Monitoreo de logs y detección de ransomware.	Necesidad de intuición técnica frente a falsos positivos.
Reactiva	Contención, erradicación y recuperación.	Toma de decisiones bajo estrés y agotamiento físico.
Retrospectiva	Lecciones aprendidas y mejora de controles.	Sanación de la confianza del equipo y resiliencia.

Limitaciones y Contribuciones

Una limitación recurrente en la literatura es la omisión de las dinámicas familiares y personales del personal de ciberseguridad. El presente estudio contribuye a cerrar esa brecha al demostrar que un ciberataque es, en esencia, una crisis humana que requiere un liderazgo capaz de gestionar tanto el código como las emociones.

Conclusiones

Una limitación recurrente en la literatura es la omisión de las dinámicas familiares y personales del personal de ciberseguridad. El presente estudio contribuye a cerrar esa brecha al demostrar que un ciberataque es, en esencia, una crisis humana que requiere un liderazgo capaz de gestionar tanto el código como las emociones.

Incidencia del Factor Humano en la Respuesta Técnica: El análisis cualitativo del caso demuestra que la eficiencia operacional de un Centro de Respuesta a Incidentes (CSIRT) está condicionada de forma determinante por la capacidad cognitiva de sus operadores. El

estrés agudo y la privación de sueño prolongada inducen fallos de juicio que no obedecen a la falta de idoneidad técnica, sino a la inhibición de la corteza prefrontal y la consecuente transición hacia modelos de decisión basados en heurísticas rápidas (Sistema 1).

Limitaciones de los Marcos Estándar de Gestión de Incidentes: Aunque normativas internacionales como ISO/IEC 27035 y NIST SP 800-61 proveen estructuras procedimentales sólidas para el aislamiento y contención de amenazas, asumen implícitamente un operador en condiciones fisiológicas ideales. La integración de parámetros de rotación de personal, control de la fatiga y gestión de la carga cognitiva resulta indispensable para evitar cuellos de botella informacionales durante una crisis.

Implicaciones para la Preparación Institucional: La resiliencia cibernética organizacional no debe evaluarse exclusivamente en función de la infraestructura tecnológica o el despliegue de herramientas automatizadas. Es preciso implementar programas periódicos de entrenamiento y simulacros en entornos de alta presión, aprovechando estructuras

existentes como las brigadas institucionales de emergencia, que capaciten a los equipos de respuesta para ejecutar procedimientos de contención bajo condiciones de agotamiento severo.

Aporte Metodológico del Caso: La sistematización de este caso único evidencia la utilidad de los enfoques cualitativos para examinar las dimensiones humanas y organizacionales que los reportes puramente cuantitativos u homologaciones técnicas suelen omitir. Los hallazgos ofrecen un modelo explicativo transferible a la planificación estratégica de la seguridad de la información en infraestructuras críticas.

Vacíos de Conocimiento y Limitaciones

A pesar de la robustez de marcos como la ISO/IEC 27035 y el NIST, se observa un vacío significativo en la literatura técnica respecto a protocolos específicos para el manejo del agotamiento psicológico (burnout) y la dinámica familiar de los profesionales de seguridad durante crisis prolongadas. La principal limitación de este estudio radica en la naturaleza cualitativa y parodiada del relato, lo que, si bien facilita la comprensión pedagógica, requiere de una validación cuantitativa posterior para medir el impacto exacto de estas variables humanas en los tiempos de recuperación (RTO) de las organizaciones.

Futuras Líneas de Investigación

Se proponen las siguientes áreas para profundizar el conocimiento en el sector:

- **Automatización Humana:** Investigar cómo la integración de Inteligencia Artificial en la metodología MIGRI puede reducir la carga cognitiva del CISO, permitiéndole

enfocarse en la gestión estratégica y emocional.

- **Soberanía y Psicología:** Estudiar la relación entre el uso de software libre y la generación de confianza técnica en equipos de respuesta latinoamericanos.
- **Protocolos de Resiliencia Humana:** Desarrollar estándares que complementen los controles técnicos con guías de bienestar y gestión de equipos para infraestructuras críticas en situaciones de desastre.

Conflictos de intereses

El autor declara que se desempeña como director y consultor principal de la firma Skina IT Solutions. Las referencias conceptuales y metodológicas derivadas de publicaciones de dicha entidad (como la Metodología Integral para la Gestión de Riesgos - MIGRI) corresponden a la sistematización de la experiencia profesional directa, el desarrollo de herramientas analíticas y la praxis de consultoría del autor en el campo de la ciberseguridad. La firma Skina IT Solutions manifiesta expresamente no tener ningún inconveniente respecto al uso y difusión de los contenidos de su blog corporativo en este artículo. La investigación se desarrolló con independencia académica e imparcialidad en el análisis de los hallazgos cualitativos presentados.

Agradecimientos

El autor expresa su más sincero agradecimiento al Chief Information Security Officer (CISO) que, bajo estricta reserva de identidad, aceptó la invitación para participar en el conversatorio académico que dio origen a este artículo.

Su disposición para compartir una experiencia tan compleja, marcada por el rigor técnico y la vulnerabilidad humana, fue fundamental para enriquecer el proceso de aprendizaje de los estudiantes de la Pontificia Universidad Javeriana.

Este trabajo es un reconocimiento a su generosidad profesional y a su valentía al permitirnos "asomarnos" a la realidad de una crisis de seguridad nacional, recordándonos que detrás de cada protocolo de defensa hay un liderazgo humano comprometido. Si estas líneas llegan a sus manos, reciba este texto como un testimonio de gratitud por su invaluable contribución a la formación de las futuras generaciones de ingenieros y especialistas en ciberseguridad.

Referencias bibliográficas

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40–46. <https://doi.org/10.1145/322796.322806>
- Arnsten, A. F. T. (2009). Stress signalling pathways that impair prefrontal cortex structure and function. *Nature Reviews Neuroscience*, 10(6), 410–422. <https://doi.org/10.1038/nrn2648>
- Denzin, N. K., & Lincoln, Y. S. (Eds.). (2018). *The SAGE handbook of qualitative research* (5th ed.). SAGE Publications.
- Flick, U. (2018). *An introduction to qualitative research* (6th ed.). SAGE Publications.
- International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001). <https://www.iso.org/standard/27001>
- International Organization for Standardization. (2023). *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management* (ISO/IEC Standard No. 27035-1). <https://www.iso.org/standard/27035>
- Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.
- Maslach, C., & Leiter, M. P. (2016). Understanding the burnout experience: Recent research and its implications for psychiatry. *World Psychiatry*, 15(2), 103–111. <https://doi.org/10.1002/wps.20311>
- Naranjo Faccini, R. J. (2024, 21 de marzo). *Cómo proteger los activos de información*. Skina IT Solutions. <https://www.skinait.com/cómo-proteger-los-activos-de-información-Escritos-71/>
- Naranjo Faccini, R. J. (2024, 15 de abril). *IA aplicada en la metodología MIGRI*. Skina IT Solutions. <https://www.skinait.com/ia-aplicada-en-la-metodología-migri-Escritos-104/>
- Naranjo Faccini, R. J. (2024, 10 de mayo). *Metodología Integral para la Gestión de Riesgos (MIGRI)*. Skina IT Solutions. [https://www.skinait.com/metodología-integral-para-la-gestión-de-riesgos-\(migri\)-Escritos-81/](https://www.skinait.com/metodología-integral-para-la-gestión-de-riesgos-(migri)-Escritos-81/)
- Naranjo Faccini, R. J. (2024, 20 de junio). *Ransomware: Exploración, implicaciones y tácticas avanzadas*. Skina IT Solutions. <https://www.skinait.com/ransomware-exploración-implicaciones-y-tácticas-avanzadas-Escritos-80/>
- Naranjo Faccini, R. J. (2024, 15 de agosto). *La dimensión humana durante un ciberataque*. Skina IT Solutions.

-
- <https://www.skinait.com/la-dimensión-humana-durante-un-ciberataque-Escritos-93/>
 - National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.04162018>
 - National Institute of Standards and Technology. (2012). Computer Security Incident Handling Guide (Special Publication 800-61 Revision 2). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-61r2>
 - Stake, R. E. (1995). The art of case study research. SAGE Publications.
 - Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.
 - Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/>