TRABAJO DE GRADO
Opción Seminario-Diplomado.

Gestión de Ciberseguridad en Entornos Organizacionales Modernos

Corporación Universitaria Remington.
Faculta de Ingeniería
Ingeniería de Sistemas

Fernando Jose Benavides Contreras

Jorge Mauricio Sepúlveda Castaño
Opción de Trabajo de grado Seminario.
2026

Dedicatoria

Dedico este logro a mi familia. Ustedes han sido el soporte inamovible, gracias por creer en mi formación profesional incluso en las noches más largas de estudio. Este proyecto no es solo el cierre de un ciclo académico, sino el resultado del esfuerzo compartido.

Agradecimientos

Con gratitud y satisfacción terminamos este proceso académico del cual le hacemos un reconocimiento a la Corporación Universitaria Remington**,** institución que nos acompañó en nuestra formación donde nos brindó todas las herramientas y la orientación, extendemos un reconocimiento a los docentes e ingenieros que hicieron parte de este proceso académico, su experiencia y dedicación fueron fundamentales para fortalecer nuestra comprensión sobre la ingeniería, la gestión de la tecnología y la ciberseguridad

Contenido

Resumen

Dentro del ámbito tecnológico del 2026, la protección digital pasó a ser un soporte estratégico fundamental para que las organizaciones se mantengan firmes, superando su función como mera responsabilidad del área de informática. Los negocios se topan con un ambiente de peligros más avanzado gracias a la incorporación de sistemas basados en la nube, el empleo de inteligencia artificial para acometer ataques específicos y el crecimiento del teletrabajo. Manejar la ciberseguridad demanda una visión completa que incorpore la mentalidad de la gente, acatar las normas legales y manejar preventivamente los peligros.

Este informe técnico propone estrategias para la gestión de la seguridad digital. Se presenta un marco conceptual que aborda tendencias y estándares actuales, como el modelo Zero Trust. Se detalla la implementación de controles de seguridad en escenarios reales y se comparan los resultados con las mejores prácticas.

Finalmente, se ofrecen conclusiones y referencias bibliográficas.

Palabras clave

Ciberseguridad, Outsourcing, software, NIST, Vulnerabilidades.

Marco conceptual y contextual

El manejo de la ciberseguridad se define como un conjunto procesos, controles y políticas que una organización implementa para mantener protegido sus sistemas y redes, en la actualidad, ya no solo basta con una defensa perimetral si no de un ciclo interminable de identificación, protección, respuesta y recuperación ante las amenazas (NIST, 2024)

Al contratar servicios de tecnología externos, las organizaciones pueden delegar el manejo de sus sistemas a otros, buscando ahorrar dinero y conseguir especialistas, pero esto genera nuevos retos ante amenazas y problemas de protección como indica ISACA (2025).

Evaluar los peligros asociados a colaboradores y asociados es lo que hace la administración de riesgos de terceros (TPRM), y es clave en la seguridad digital, puesto que muchas fallas de seguridad vienen de debilidades en la cadena de suministro, de acuerdo con IBM (2025). El concepto de confianza nula exige confirmar siempre a las personas y aparatos. El cambio digital provocó que en Colombia aumentara un 20% el uso de esquemas de subcontratación en ciberseguridad, lo que recalca la importancia de tener procedimientos seguros y seguir las leyes para garantizar que el trabajo siga sin interrupciones.

Ciberseguridad

Es la practica de proteger redes, equipos, aplicaciones, sistemas críticos y posibles amenazas cibernéticas, las organizaciones modernas tienes ahora la responsabilidad de proteger los datos y los sistemas para mantener la confianza de sus clientes y cumplir con las normativas. Así se evitarán interrupciones en sus operaciones

Principios fundamentales de la ciberseguridad

Cualquier estrategia de ciberseguridad moderna en una organización debe basarse en los cuatro pilares.

Confidencialidad: Solo el personal autorizado puede acceder a la información, así se protege de la divulgación no autorizada y ayuda a la seguridad y privacidad de los datos.

Integridad: Se asegura de prevenir las modificaciones no autorizadas, de moto que se pueda confiar que los datos van a seguir siendo precisos.

Disponibilidad: Se asegura que los datos y los sistemas van a estar listos para usarse, cuando la empresa o los usuarios lo necesitan.

Resiliencia operativa: Es la fuerza de la empresa para resistir un ataque. También para aguantarlo y luego volver a operaciones. No preguntamos si nos van a atacar. Preguntamos cuándo y qué tan rápido nos vamos a

recuperar (NIST, 2024).

Gestión de riesgos

Manejar los riesgos de la ciberseguridad es un proceso donde se trata de identificar, evaluar y priorizar qué amenazas y vulnerabilidades pueden dañar los sistemas de información. Se evalúan y se mitigan al tiempo que la organización pueda cumplir sus objetivos. En una organización el peligro cambia todo el tiempo. Según ISACA (2025) dice que manejar peligros no es algo de una vez al año, sino monitoreos constantes.

Estándares y marcos de referencia

- **ISO/IEC 27001:** Esta norma define el modo central para manejar la seguridad de la información (SGSI). Permite fijar reglas claras. También define que hace qué dentro de la organización.

- **NIST Cybersecurity Framework (CSF) 2. 0:**

  Este modelo se organiza en partes que ayudan a tener mejor comunicación mejor entre el equipo técnico y los directivos. Estas partes son: Gobernar, identificar, proteger, detectar, responder y recuperar (NIST, 2024). Es un modelo flexible. Esto se adapta muy bien a organizaciones que usan servicios de nube y outsourcing

Contexto del informe

Este informe se basa en referencia a una pyme del sector de servicios logísticos y distribución digital que cuenta con 30 colaboradores, donde su infraestructura es hibrida, operan con bases de datos locales y servicios en la nube (SaaS) para la gestión de ventas e inventario, el uso de VPNs para el personal de ventas y soporte técnico (tercerizado) son los puntos más críticos, donde nos permite usar los controles de Zero Trush.

Desarrollo e implementación del aprendizaje

En esta sección del documento técnico, se detalla cómo se llevaron a cabo en la práctica los temas de seguridad informática vistos durante proceso académico. El trabajo se centró en reforzar la plataforma digital de una empresa de ejemplo, usando medidas de seguridad basadas en el estándar NIST CSF 2. 0 y la regulación ISO 27001.

Ejecución del Diagnóstico y Aplicación de Controles

Lo primero que se hizo fue revisar fallos de seguridad y hacer un inventario de los recursos. Se descubrió que el mayor riesgo estaba en el acceso de gente externa y del personal que trabaja a distancia. Para solucionar esto, se aplicó un esquema de Seguridad de Confianza Cero.

- **Implementación técnica:** Se configuró la Autenticación de Múltiples Factores para todos los sistemas en la nube y las entradas a la red privada virtual. También,

se instaló un programa de Detección y Respuesta en los Dispositivos (EDR) para vigilar al instante cualquier intento de correr software dañino.

- **Gestión administrativa**

  Se revisaron los compromisos de calidad con las empresas externas, añadiendo condiciones sobre quién es responsable si hay fugas de información, siguiendo la Ley 1581 de 2012.

  Monitoreo y respuesta de incidentes

  Se creó un sistema de observación continua con un panel centralizado para todas las alarmas de seguridad. Mientras se hacía esto, se llevaron a cabo simulacros de ataque controlados para comprobar qué tan bien funcionaban las nuevas estrategias de defensa.

Metodología

Para llevar a cabo este informe se empleó un enfoque que era tanto descriptivo como analítico, organizado en tres fases distintas:

- Se examinaron las normas mundiales y las previsiones de riesgos.
- Se diseño una estrategia de fortalecimiento y gestión para solucionar las amenazas halladas
- Se utilizaron encuestas y evaluaciones alineadas con el sistema NIST para determinar cómo estaba la protección en la empresa en este momento.

- Diseño de modelo integral de gestión de ciberseguridad alineado con ISO/IEC 27001, NIST CSF, COBIT 2019 e ISO 22301.

- Integración de los aprendizajes adquiridos en el seminario académico.

Diagnóstico Situacional

Aplicamos las funciones principales del marco NIST para avaluar nuestra seguridad.

Gobernar e Identificar: Encontramos huecos en

el listado de aparatos móviles y de Internet que se conecta a la red corporativa

Proteger y detectar: La compañía dispone de defensas cortafuegos sencillas, pero le falta un método más fuerte para manejar quién tiene acceso.

Responder y recuperar: Las maneras de reaccionar son poco estructuradas y se apoyan en lo que sabe el técnico disponible en ese momento.

Análisis de riesgos

Matriz de riesgos

Activo de Información	Riesgo / Amenaza	Probabilidad	Impacto	Nivel de Riesgo	Control / Salvaguarda Sugerida
Bases de Datos	Fuga de datos por acceso no autorizado	Media	Muy Alto	**Crítico**	Cifrado de datos en reposo y MFA (Autenticación multifactor).

Infraestructura Cloud	Denegación de servicio (DDoS)	Baja	Alto	**Alto**	Implementación de WAF y balanceadores de carga con mitigación.
Talento Humano	Ingeniería Social / Phishing	Alta	Medio	**Alto**	Plan de concienciación y pruebas de phishing controlado.
Endpoints (Equipos)	Ataque de Malware / Ransomware	Media	Muy Alto	**Crítico**	EDR (Endpoint Detection and Response) y backups aislados.
APIs de Terceros	Interrupción de servicios externos	Media	Medio	**Medio**	Acuerdos de Nivel de Servicio (SLA) y planes de redundancia.

Fuente: Mintic, gia para la gestión y clasificación de riesgos de seguridad de la información.

Matriz FODA

Categoría	Factores Positivos	Factores Negativos
Factores Internos	**FORTALEZAS (F)**	**DEBILIDADES (D)**
	1. Adopción del marco NIST CSF 2.0 para la respuesta ante	1. Brecha de competencias técnicas en el personal no especializado.

	incidentes.	
	2. Políticas de control de acceso.	2. Fragmentación de la visibilidad de activos en entornos híbridos (Cloud/On-premise).
	3. Infraestructura con soporte para segmentación de red y cifrado de datos.	3. Procesos de actualización de parches (Patch Management) con alta latencia.
Factores Externos	**OPORTUNIDADES (O)**	**AMENAZAS (A)**
	1. Cumplimiento de la **Ley 1581 de 2012** para mejorar la confianza del cliente.	1. Sofisticación de ataques de Ransomware.
	2. Integración de herramientas de IA Predictiva para detección de anomalías.	2. Aumento de ataques a la cadena de suministro y proveedores de servicios.
	3. Disponibilidad de servicios de seguridad gestionada.	3. Explotación de vulnerabilidades de "Día Cero" en software crítico.

Fuente: Mintic, gia para la gestión y clasificación de riesgos de seguridad de la información.

Modelo de Gestión de Ciberseguridad Propuesto

Se sugiere un plan completo que se fundamenta en la idea de Ciberdefensa Participativa:

Gobernanza Establecer un grupo para asuntos de seguridad informática y revisar las normas sobre cómo usar apropiadamente los recursos.

Controles técnicos: Poner en práctica la Arquitectura de Confianza Cero (ZTA), obligando a confirmar cada ingreso sin importar dónde se origine. Instalar software de detección y respuesta en los equipos finales (EDR).

Controles organizacionales: Realizar entrenamientos cada seis meses para el personal sobre protección digital y simulacros de fallos.

Respuesta rápida: Formar un grupo interno para atender emergencias (CSIRT) con guías de actuación fijas para cada clase de peligro descubierto.

Ilustraciones y tablas

1- Comparativa de madurez en ciberseguridad (Antes vs. Después)

Categoría NIST	Estado Inicial (Nivel 1-2)	Estado Post-Implementación (Nivel 4)	Herramienta/Control Aplicado
Identificar	Inventario manual y desactualizado.	Inventario automatizado de activos.	Scan de red y gestión de parches.
Proteger	Solo antivirus básico y firewall.	MFA, EDR y cifrado de datos.	Azure AD / SentinelOne.
Detectar	Dependencia de reportes de usuario.	Monitoreo 24/7 de anomalías.	SIEM (Gestión de eventos).
Responder	Sin manual de incidentes claro.	Equipo de respuesta y manuales.	CSIRT interno y Playbooks.
Recuperar	Backups manuales esporádicos.	Backups automatizados e inmutables.	Almacenamiento en nube fría.

Conclusiones

Tras concluir este documento técnico sobre cómo manejar la seguridad en redes de hoy, se ven estas conclusiones:

- **La seguridad digital es clave:** Se vio que la seguridad en línea no es solo trabajo de TI. Es una parte vital del plan de negocios. Para el 2026, qué tan bien se recupera una empresa depende de su poder para ver y parar riesgos en línea. Esto debe pasar antes de que afecten las operaciones en la organización

- **Efectividad de los marcos de referencia:** Usar la guía NIST CSF 2. 0 y la regla ISO 27001 fue muy útil. Ayudó a hacer una defensa con varios niveles. Pasar de solo reaccionar a actuar antes redujo mucho el tiempo para ver peligros. Esto muestra que el orden interno importa tanto

como la herramienta.

Gestión crítica de terceros (Outsourcing): Un gran descubrimiento fue el riesgo que crean las uniones con socios de externos. Se concluye que la seguridad de hoy solo funciona si se llevan los controles internos a toda la red de entrega. Se debe asegurar el cumplimiento legal (Ley 1581) y técnico en todo sitio de unión.

Factor humano y tecnología Aunque hay herramientas nuevas como EDR y Confianza Cero, la persona sigue siendo el punto fácil de atacar. Por eso, entrenar siempre y hacer una cultura de seguridad es la mejor inversión. Esto previene muchos problemas.

Preparación para el futuro: El análisis realizado deja ver que los peligros cambian con el mal uso de la IA. Esto fuerza a las empresas a mejorar siempre (Ciclo PHVA). La seguridad en redes no es un final. Es seguir cambiando con la tecnología.

Referencias bibliográficas

- **Amazon Web Services.** (2026). *¿Qué es la ciberseguridad?* https://aws.amazon.com/es/what-is/cybersecurity/
- **Almeida, R.** (2022). *ISO 27001 Information Security Management Systems*. ResearchGate. https://www.researchgate.net/publication/367166657_ISO_27001_Information_Security_Management_Systems
- **Club CISO - AEC.** (2026). *Diagnóstico y gestión de riesgos de la ciberseguridad.* https://club-ciso.aec.es/diagnostico-y-gestion-de-riesgos-de-la-ciberseguridad/
- **ENISA (Agencia de la Unión Europea para la Ciberseguridad).** (2025). *Threat Landscape 2025: Strategic Analysis of Cyber Threats.* https://www.enisa.europa.edu/publications
- **Fortinet.** (206). *¿Qué es la ciberseguridad?* https://www.fortinet.com/lat/resources/cyberglossary/what-is-cybersecurity
- **IBM.** (2026). *¿Qué es la gestión de riesgos cibernéticos?* https://www.ibm.com/mx-es/think/topics/cyber-risk-management

- **IBM Security.** (2025). *Cost of a Data Breach Report 2025: Analysis of Supply Chain Vulnerabilities.* https://www.ibm.com/reports/data-breach
- **International Organization for Standardization.** (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO. https://www.iso.org/standard/27001
- **ISACA.** (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA. http://www.isaca.org/resources/cobit
- **ITU (Unión Internacional de Telecomunicaciones).** (2024). *Global Cybersecurity Index 2024: Strengthening digital trust in the age of AI*. https://www.itu.int/gci
- **Ministerio de Tecnologías de la Información y las Comunicaciones.** (2022). *Guía de estándares de talento digital*. https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
- **Microsoft.** (s.f.). *Zero Trust: Una estrategia de seguridad moderna*. https://www.microsoft.com/es-co/security/business/zero-trust

- **National Institute of Standards and Technology (NIST).** (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
- **NQA.** (2019). *Guía de implantación ISO 22301: Gestión de la Continuidad de Negocio*. https://www.nqa.com/medialibraries/NQA/NQA-MediaLibrary/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-deimplantacion.pdf
- **UPK Latam.** (s.f.). *Seguridad en la nube y física*. https://www.upklatam.com/ciberseguridad-y-cloud/seguridad-en-la-nube-y-fisica/
- **PurpleSec.** (2024). *¿Qué es un diagnóstico de ciberseguridad?* https://purplesec.com/blog/2024/09/que-es-diagnostico-ciberseguridad/
- **SentinelOne.** (s.f.). *Principios de ciberseguridad*. https://www.sentinelone.com/es/cybersecurity-101/cybersecurity/cyber-security-principles/
- **Quintero, O. L.** (2020). Repositorio Institucional Uniremington. https://repositorio.uniremington.edu.co/server/api/core/bitstreams/05fc05ae-39b1-43cb-b160-a2ce68fcf398/content

- **Wikipedia.** (2026). *Seguridad informática.* https://es.wikipedia.org/wiki/Seguridad_informática