TRES ÁMBITOS DE SEGURIDAD DIGITAL

W. Carrillo
7690-20-12345 Universidad Mariano Gálvez
Programación I
wcarrillo@example.com

Resumen
Este artículo delimita y compara tres conceptos que suelen emplearse indistintamente en el ámbito profesional: ciberseguridad, seguridad informática y seguridad de la información. El objetivo es clarificar su alcance, activos protegidos, marcos de referencia y tipos de controles típicos para orientar decisiones de gobierno, riesgo y cumplimiento en organizaciones que dependen de tecnologías digitales. Se empleó un enfoque analítico comparativo sintetizando estándares y guías de adopción amplias (por ejemplo, ISO/IEC 27001, NIST CSF, OWASP). Como resultados, se establece que: (i) la seguridad de la información es el paraguas estratégico centrado en la preservación de la confidencialidad, integridad y disponibilidad del activo información sin importar su soporte; (ii) la seguridad informática se enfoca en salvaguardar recursos computacionales (sistemas operativos, aplicaciones, datos en sistemas) y suele materializarse mediante controles técnicos y operativos en el entorno de TI; y (iii) la ciberseguridad abarca la protección frente a amenazas que se originan o se materializan en el ciberespacio (redes, servicios en línea, infraestructura crítica, identidades digitales), integrando prevención, detección, respuesta y recuperación ante incidentes. Las conclusiones proveen una guía práctica para alinear roles, métricas y controles con cada ámbito, evitando solapamientos y brechas de protección.

Palabras clave: ciberseguridad; seguridad informática; seguridad de la información; gestión de riesgos; cumplimiento

Desarrollo del tema

1. Tres definiciones operativas

Seguridad de la información (InfoSec). Disciplina de gestión orientada a proteger la información como activo, en cualquier formato (digital, físico, verbal), mediante políticas, procesos y controles que preserven confidencialidad, integridad y disponibilidad (CIA). Su ámbito natural es el Sistema de Gestión de Seguridad de la Información (SGSI) y la gestión de riesgos a nivel organizacional.

Seguridad informática. Conjunto de controles y prácticas aplicadas al entorno computacional (hardware, sistemas operativos, aplicaciones, bases de datos, dispositivos finales y centros de datos). Suele considerarse un subconjunto técnico de la seguridad de la información, enfocado en endurecimiento de sistemas, gestión de parches, control de acceso, respaldos y continuidad de servicios de TI.

Ciberseguridad. Protección de redes, sistemas, servicios y usuarios frente a amenazas que se originan o transitan por el ciberespacio. Integra prevención, detección, respuesta y recuperación ante incidentes como intrusiones, ransomware, phishing, ataques DDoS y fraude digital. Incluye dimensiones de inteligencia de amenazas, arquitectura Zero Trust, monitoreo continuo, orquestación y respuesta a incidentes.

2. Alcances y activos protegidos

Dimensión	Seguridad de la información	Seguridad informática / Ciberseguridad
Enfoque	Gobierno, riesgo y cumplimiento	Controles técnicos y operativos
Activos	Información en cualquier soporte	Infraestructura, sistemas, identidades, datos
Ámbito	Políticas, SGSI, riesgos, auditoría	Endurecimiento, arquitectura, monitoreo, IR
Controles típicos	Clasificación, riesgos, formación	MFA, cifrado, segmentación, backup/DR, SIEM/SOAR
Marcos	ISO/IEC 27001/27002, ISO 31000	NIST CSF, SP 800-53/61, OWASP, MITRE ATT&CK

3. Relación jerárquica y complementariedad

La seguridad de la información establece la dirección estratégica y los criterios de aceptación de riesgo. La seguridad informática materializa los controles técnicos que reducen la probabilidad e impacto sobre sistemas que procesan información. La ciberseguridad aporta capacidades especializadas para amenazas modernas, priorizando visibilidad, detección y respuesta.

4. Objetivos y métricas orientadas al valor

Seguridad de la información: reducir riesgo residual a niveles aceptables y evidenciar cumplimiento. *Métricas*: madurez del SGSI, activos clasificados, riesgos fuera del apetito.
Seguridad informática: asegurar operación confiable de TI. *Métricas*: tiempo medio de parcheo, cifrado en reposo/en tránsito, cumplimiento de hardening.
Ciberseguridad: minimizar tiempo de permanencia del atacante y pérdidas por incidentes. *Métricas*: MTTD/MTTR, cobertura de telemetría, eficacia de ejercicios de respuesta.

5. Controles ilustrativos por ámbito

InfoSec: política de clasificación y tratamiento de datos; evaluación de riesgos; NDA; gestión de terceros; concienciación.
Seguridad informática: gestión de vulnerabilidades; RBAC; cifrado de discos y bases; copias verificadas; continuidad y recuperación.
Ciberseguridad: MFA e IAM; segmentación y Zero Trust; EDR/XDR y SIEM/SOAR; pentesting; plan de IR con ejercicios.

6. Casos de uso

Finanzas: SGSI define políticas y riesgos; TI aplica cifrado y accesos; ciberseguridad monitoriza fraude y ejecuta playbooks.
Servicios públicos en línea: InfoSec estructura la gobernanza; TI asegura disponibilidad; ciberseguridad defiende contra DDoS, phishing y toma de cuentas con SOC.

7. Roles y responsabilidades

Dirección y comité de riesgos; CISO; Arquitectura/TI; SOC/IR; dueños de proceso.

8. Ruta de adopción

(1) Alcance y mapa de activos; (2) valoración de riesgos; (3) alineación de controles técnicos; (4) monitoreo continuo y respuesta; (5) medición y mejora continua.

Conclusiones

La seguridad de la información provee el marco; la seguridad informática implementa controles de TI; la ciberseguridad enfrenta amenazas del ciberespacio. La articulación de roles, métricas y marcos (ISO/IEC, NIST, OWASP) evita solapamientos y brechas.

Bibliografía

ISO. (2022). *ISO/IEC 27001:2022*. International Organization for Standardization.
NIST. (2024). *Cybersecurity Framework 2.0*. U.S. Dept. of Commerce.
NIST. (2012). *SP 800-61 Rev.2*. U.S. Dept. of Commerce.

OWASP Foundation. (2021). *OWASP Top 10*.