

Introducción a la Ciberseguridad

Teoría: Javier Díaz

jdiaz@unlp.edu.ar

Práctica: Soledad Gomez

Ulises Cabrera

ISO/IEC 27032 (Cybersecurity Guidelines)

- ISO/IEC 27032 → protección del ciberespacio: redes interconectadas, usuarios, servicios y confianza digital. ◇
Objetivo:
- Establece un marco de cooperación entre múltiples actores (usuarios, proveedores, gobiernos, CERTs/CSIRTs) para reducir los riesgos derivados de la interconexión global.
- Publicación:  Año: 2012

ISO/IEC 27032 (Cybersecurity Guidelines)

- La ciberseguridad extiende la seguridad de la información al entorno distribuido, interconectado y compartido entre múltiples dominios.
 - Seguridad del ciberespacio:
 - Amenazas en entornos interconectados (malware, phishing, ataques de red).
 - Protección de la información compartida: entre usuarios, organizaciones y plataformas.
 - Identidad digital y confianza: autenticación, gestión de identidades, privacidad.
 - Gestión de incidentes y cooperación: coordinación con CERT/CSIRT, respuesta colaborativa.

ISO/IEC 27032 (Cybersecurity Guidelines)

Principios rectores

- Colaboración intersectorial: cooperación entre gobiernos, sector privado, academia y usuarios.
- Confianza y gestión de identidad: fortalecimiento de autenticación, integridad y no repudio.
- Protección de infraestructuras críticas: enfoque preventivo frente a amenazas emergentes.
- Conciencia y capacitación: desarrollo de cultura cibersegura en todos los niveles.
- Resiliencia del ciberespacio: detección temprana, respuesta coordinada y recuperación.

Frameworks y Regulaciones en Ciberseguridad...

7. CMMC (Cybersecurity Maturity Model Certification – EE.UU.)

Descripción: Modelo de madurez de ciberseguridad para contratistas del Departamento de Defensa de EE.UU.

Referencia: U.S. Department of Defense. *CMMC Model v2.0*.

<https://www.cisa.gov/resources-tools/resources/cybersecurity-maturity-model-certification-20-program>

8. HIPAA (Health Insurance Portability and Accountability Act – EE.UU.)

Descripción: Norma que regula la seguridad y privacidad de la información médica y sanitaria.

Referencia: U.S. Department of Health & Human Services. HIPAA Security Rule

<https://www.hhs.gov/hipaa/index.html>

Cybersecurity Maturity Model Certification (CMMC)

- El CMMC es un modelo de madurez en ciberseguridad desarrollado por el Departamento de Defensa de los Estados Unidos (DoD) para evaluar, estandarizar y certificar el nivel de seguridad de los contratistas y proveedores que manejan información del gobierno federal.
- Objetivo: Garantizar que las organizaciones que participan en la Defensa Industrial Base (DIB) protejan adecuadamente la información sensible, especialmente: FCI (Federal Contract Information) y CUI (Controlled Unclassified Information)

Cybersecurity Maturity Model Certification (CMMC)

- El CMMC es un modelo de madurez en ciberseguridad desarrollado por el Departamento de Defensa de los Estados Unidos (DoD) para evaluar, estandarizar y certificar el nivel de seguridad de los contratistas y proveedores que manejan información del gobierno federal.
- Objetivo: Garantizar que las organizaciones que participan en la Defensa Industrial Base (DIB) protejan adecuadamente la información sensible, especialmente: FCI (Federal Contract Information) y CUI (Controlled Unclassified Information)

Cybersecurity Maturity Model Certification (CMMC)

Nivel	Enfoque	Controles / Referencias
Nivel 1 – Foundational	Prácticas básicas de higiene cibernética. Protege FCI.	17 prácticas (basadas en FAR 52.204-21).
Modelo basado en tres niveles Nivel 2 – Advanced	Implementación formal de políticas y procesos. Protege CUI.	110 controles de NIST SP 800-171 Rev.2.
Nivel 3 – Expert	Gestión avanzada de amenazas persistentes (APT).	Basado en NIST SP 800-172 + prácticas adicionales DoD.

Cybersecurity Maturity Model Certification (CMMC)

Características del modelo:

- Cada nivel incluye los requisitos del anterior (enfoque incremental).
- Los controles son verificables mediante auditorías realizadas por Third Party Assessment Organizations (C3PAOs).
- Enfocado en evaluar la madurez organizacional, no solo la existencia de controles técnicos.

Dimensiones evaluadas:

1. Políticas y procedimientos.
2. Capacidades técnicas y gestión de riesgos.
3. Procesos de mejora continua.

Cybersecurity Maturity Model Certification (CMMC)

Año	Versión / Evento	Descripción
2019	Inicio del programa CMMC	El Departamento de Defensa de EE. UU. (DoD) lanza el proyecto CMMC para mejorar la ciberseguridad de la Defense Industrial Base (DIB).
Enero 2020 Línea temporal del CMMC	Publicación del CMMC v1.0	Primera versión oficial del modelo con 5 niveles de madurez y 171 prácticas basadas en NIST SP 800-171.
Noviembre 2021	CMMC v2.0 (revisión mayor)	Reducción de niveles (de 5 a 3), alineación más estricta con NIST SP 800-171 y simplificación de requisitos.
2022–2024	Periodo de transición y armonización	Se desarrolla el programa de auditorías y certificaciones (C3PAO). CISA y DoD publican guías y portales oficiales.
2025 (actual)	Implementación progresiva obligatoria	A partir de 2025, CMMC v2.0 se integra formalmente en los contratos del DoD y en las auditorías de proveedores.

Cybersecurity Maturity Model Certification (CMMC)

Implementación del CMMC en la industria

- Requisito obligatorio en contratos del Departamento de Defensa (DoD).
- Escalable a otros sectores críticos (energía, infraestructura, manufactura).
- Integra controles de marcos como NIST CSF, CIS Controls e ISO/IEC 27001.

Beneficios:

- Estandariza la seguridad en la cadena de suministro de defensa.
- Promueve madurez progresiva en la gestión cibernética.
- Aumenta la confianza del gobierno y la industria en los contratistas.

HIPAA Health Insurance Portability & Accountability Act

HIPAA: ley federal de los Estados Unidos promulgada en 1996, para proteger la privacidad, seguridad y disponibilidad de la información médica

Objetivo general: Garantizar que los datos de salud personales sean

- **Confidenciales:** sólo accesibles a personas autorizadas.
- **Íntegros:** no alterados o destruidos sin autorización.
- **Disponibles:** accesibles cuando se necesiten para la atención médica.

Ámbito de aplicación:

- **Hospitales, clínicas y laboratorios.**
- **Compañías de seguros y prestadores de salud.**
- **Proveedores tecnológicos que procesen información médica**

HIPAA Health Insurance Portability & Accountability Act

Regla	Propósito	Enfoque técnico
Privacy Rule (2003)	Define derechos del paciente sobre su información médica.	Establece políticas de acceso, uso y divulgación del PHI.
Security Rule (2005)	Establece salvaguardas administrativas, físicas y técnicas.	Incluye autenticación, control de acceso, cifrado y auditorías.
Breach Notification Rule (2009)	Obliga a reportar incidentes de seguridad y filtraciones.	Requiere notificación a usuarios y autoridades en ≤ 60 días.
Omnibus Rule (2013)	Actualiza definiciones y extiende responsabilidades.	Integra a proveedores tecnológicos (cloud, software médico).

HIPAA Health Insurance Portability & Accountability Act

Salvaguardas técnicas exigidas por la Security Rule:

- **Control de acceso:** autenticación y autorización de usuarios.
- **Auditoría y trazabilidad:** registro de accesos y modificaciones.
- **Integridad de datos:** mecanismos contra alteraciones no autorizadas.
- **Transmisión segura:** cifrado de datos en tránsito (TLS, VPN).

HIPAA Health Insurance Portability & Accountability Act

Implementación y certificación

Obligaciones de cumplimiento:

- Evaluaciones periódicas de riesgo (*Risk Assessment*).
- Políticas de seguridad documentadas.
- Capacitación de personal.
- Firma de acuerdos de confidencialidad con terceros (*Business Associate Agreements*).

HIPAA Health Insurance Portability & Accountability Act

Relación con la ciberseguridad y la PKI:

- Uso de **certificados digitales X.509** para asegurar comunicaciones y autenticación.
- Encriptación de datos sensibles almacenados o transmitidos.
- Integración con marcos como **NIST CSF**, **ISO/IEC 27001** y **HITRUST CSF** (framework derivado de HIPAA).

Frameworks y Regulaciones en Ciberseguridad...

9. PCI DSS (Payment Card Industry Data Security Standard)

Descripción: Estándar de seguridad de la industria de tarjetas de pago, obligatorio para entidades que procesan, almacenan o transmiten datos de titulares de tarjetas.

Referencia: PCI Security Standards Council. (2022). PCI DSS v4.0.

<https://www.pcisecuritystandards.org/resources-overview/>

10. Reglamento Europeo de Ciberseguridad.

Establece requisitos para la ciberseguridad de productos con componentes digitales, y la enmienda al Reglamento de Ciberseguridad de 2019 (Reglamento (UE) 2019/881), que amplía los esquemas de certificación a servicios de seguridad gestionados.

Referencia: Decreto EU 2024/2847

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202402847

Introducción al PCI DSS

2004: Visa, MasterCard, American Express, Discover y JCB— unificaron estándares de seguridad (p.ej. Visa CISP o MasterCard SDP) en un marco común llamado PCI DSS v1.0. para proteger los datos de los titulares.

En 2006, se formalizó la creación del Payment Card Industry Security Standards Council (PCI SSC)

Desde entonces, el estándar ha evolucionado:

- o v1.0 (2004) — primera versión.
- o v2.0 (2010) — mejoras en prácticas de evaluación.
- o v3.2 (2016) — refuerzos en autenticación y cifrado.
- o v4.0 (2022) —enfoque en seguridad continua y modelos basados en riesgo.

Objetivos fundamentales de PCI DSS

Obligatorio para todas las organizaciones que procesan, almacenan o transmiten datos de tarjetas

1. Construir y mantener una red segura.
2. Proteger los datos del titular de la tarjeta.
3. Mantener un programa de gestión de vulnerabilidades.
4. Implementar medidas de control de acceso.
5. Monitorear y probar regularmente las redes.
6. Mantener una política de seguridad de la información.

Requisitos principales de cumplimiento

Construir y mantener una red y sistemas seguros

1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.
2. No usar contraseñas ni parámetros predeterminados de seguridad. Proteger los datos del titular de la tarjeta

Proteger los datos almacenados del titular de la tarjeta.

3. Cifrado, truncamiento, hashing, etc
4. Cifrar la transmisión de datos del titular de la tarjeta a través de redes abiertas y públicas. TLS 1.2 o superior.

Requisitos principales de cumplimiento

Mantener un programa de gestión de vulnerabilidades

5. Usar y actualizar regularmente software antivirus o antimalware.
6. Desarrollar y mantener sistemas y aplicaciones seguros. Aplicar parches, revisar código, desarrollo seguro.

Implementar medidas de control de acceso

7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber. Mínimo privilegio.
8. Identificar y autenticar el acceso a los componentes del sistema. Credenciales únicas, MFA
9. Restringir el acceso físico a los datos del titular de la tarjeta.

Requisitos principales de cumplimiento

Monitorear y probar regularmente las redes

10. Rastrear y monitorear todos los accesos a los recursos de red y datos del titular de la tarjeta.
11. Probar regularmente los sistemas y procesos de seguridad.
Escaneos, pentest, revisiones de configuración

Mantener una política de seguridad de la información

12. Mantener una política que aborde la seguridad de la información para todo el personal.

Validación y Cumplimiento

- **Según el volumen de transacciones, las organizaciones deben realizar:**
 - Autoevaluación (SAQ) o
 - Auditoría externa por Qualified Security Assessor (QSA).
- **Certificación anual y escaneo trimestral de vulnerabilidades.**
- **No cumplir puede implicar multas, pérdida de contrato con proveedores de pago y perdida de habilitación.**

Reglamento Europeo de Ciberseguridad

Reglamento Europeo de Ciberseguridad (UE) 2019/881 y su enmienda 2024/2847

Reglamento (UE) 2019/881, conocido como Cybersecurity Act.

- Objetivo: Reforzar la confianza y seguridad en el mercado digital europeo.
- Crea un marco común de certificación para productos, servicios y procesos TIC.
- Autoridad principal: ENISA (Agencia de la Unión Europea para la Ciberseguridad).

Ciberseguridad 2019 a la actualización 2024

El Reglamento (UE) 2024/2847, adoptado en octubre de 2024, modifica y amplía el Reglamento 2019/881.

Novedades principales:

- Introduce requisitos de ciberseguridad para productos con componentes digitales (IoT, software embebido, hardware inteligente, etc.).
- Extiende los esquemas de certificación a servicios de seguridad gestionados (SOC, CSIRT, MDR, MSSP).
- Refuerza el rol de ENISA como autoridad de evaluación y coordinación
- **Amplía el alcance del marco de certificación a:**
 - Productos con componentes digitales (hardware, software embebido, IoT).
 - Servicios de seguridad gestionados (MSSP, SOC, CSIRT).

Certificación Europea de Ciberseguridad

Tres niveles de garantía:

1. Básico — controles mínimos, autoevaluación.
2. Sustancial — auditorías independientes, gestión de riesgos.
3. Alto — validación estricta, pruebas y supervisión continua.

Aplicable a:

- o Dispositivos conectados (IoT, routers, PLCs).
- o Plataformas de software y servicios cloud.
- o Proveedores de servicios de seguridad gestionados.

Impacto en el ecosistema tecnológico

Implicancias para la industria y los profesionales TIC

- Las empresas deberán demostrar cumplimiento de estándares de seguridad para comercializar en la UE.
- Los desarrolladores y proveedores de TI deben integrar la ciberseguridad desde el diseño (security by design).
- Se fomenta la interoperabilidad y la confianza digital entre Estados miembros.
- Abre oportunidades laborales en evaluación, auditoría y certificación.

Ecosistema: fabricantes, proveedores, autoridades, usuarios.

Resiliencia e ICs: normas complementarias

Directiva NIS2 (UE 2022/2555) — “Directiva sobre medidas para un alto nivel común de ciberseguridad”. Sustituye NIS1 (2016).

Impone obligaciones de resiliencia operativa y gestión de incidentes a energía, transporte, salud, educación, administración, etc.

Cyber Resilience Act (CRA, aprobado en 2024) Exige que todos los productos con elementos digitales se diseñen con seguridad integrada y mantenimiento durante su ciclo de vida. software, hardware y firmware.

CER Directive (UE 2022/2557) — “Critical Entities Resilience Directive”. Obliga a los Estados miembros a garantizar la resiliencia física y digital de las infraestructuras críticas esenciales (energía, transporte, agua, salud, administración pública, etc.).

Política Seguridad de la Información

- Modelo de Política de Seguridad de la Información para Organismos Públicos.

<https://www.argentina.gob.ar/noticias/elaboran-modelo-de-politica-de-seguridad-de-la-informacion-para-organismos-publicos>

- Requisitos mínimos de Seguridad de la Información para Organismos. Decisión Administrativa 641/2021 Jefatura de Gabinete de Ministros.
- Política de seguridad de la información de las Instituciones Universitarias Públicas.
 - Resolución C.E. CIN: 1669/22

Aspectos a incluir en Política de Ciberseguridad

Protección de datos: El RGPD establece los requisitos específicos para empresas y organizaciones sobre recogida, almacenamiento y gestión de los datos personales. Se aplican tanto a las organizaciones europeas como a las organizaciones que tienen su sede fuera de la UE.

Responsable de Privacidad de la Información de la Organización, CPO

Datos personales

Privacidad

Derecho al olvido

Https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Estructura en Seguridad de la Información

- Organización: Política Seguridad de la Información
 - Comité de Ciberseguridad
 - CISO (Chief Information Security Officer) Reporta a la alta gerencia.
 - Definir la estrategia de ciberseguridad.
 - Gestionar políticas y cumplimiento normativo.
 - Evaluar y mitigar riesgos organizacionales.
 - Coordinar equipos (SOC, CSIRT, IT, Legal).
 - Comité de Ciberseguridad
- Director en Privacidad (CPO)
 - RGPD es el Reglamento General de Protección de Datos de la Unión Europea
 - CCPA (Ley de Privacidad del Consumidor de California)

Estructuras Ciberseguridad

- **SOC (Security Operations Center)**
 - Monitorear en tiempo real la infraestructura.
 - Uso de **SIEM, IDS/IPS, EDR**.
 - Detección y respuesta inicial a incidentes.
 - Generación de alertas y reportes.
- **CSIRT (Computer Security Incident Response Team)**
 - Gestión completa de incidentes (detección, contención, erradicación, recuperación).
 - Coordinación con organismos externos y reguladores.
 - Análisis forense y lecciones aprendidas.
 - Elaborar planes de respuesta y continuidad.