Fundamentos y Normativas de Ciberseguridad

Gestión de información (respaldos y recuperación)

Estándar / Norma	Dominio / Control Específico	Exigencia Técnica sobre Respaldos
ISO/IEC 27001:2022	Anexo A.8.13 (*Information Backup*)	Requiere mantener copias de respaldo de la información, software y sistemas, realizando pruebas periódicas de acuerdo con la política de la organización.
NIST SP 800-53 (Rev. 5)	Control CP-9 (*Information System Backup*)	Exige respaldos frecuentes de datos de usuario/sistema, almacenamiento en ubicación secundaria externa (*off-site*) y protección contra acceso no autorizado.
NIST SP 800-34	*Contingency Planning Guide*	Establece las directrices para la creación de planes de contingencia en TI, clasificando la regla 3-2-1 como buena práctica para los objetivos RTO y RPO.
ISO 22301:2019	Cláusula 8.4 (*Business Continuity Plans*)	Obliga a garantizar la disponibilidad continua de los datos operativos críticos para limitar el impacto ante incidentes graves.
Reglamento NIS 2 (UE)	Art. 21 (*Medidas de gestión de riesgos*)	Exige a infraestructuras críticas contar con planes de gestión de continuidad, respaldos seguros y gestión de crisis.
IEC/ISA 62443	62443-2-4	**Política de Respaldo y Recuperación:** Obliga a definir formalmente qué datos e imágenes de sistemas deben respaldarse, la frecuencia, las responsabilidades y los planes de Continuidad del Negocio y Recuperación ante Desastres (DRP).

Estándar / Norma	Dominio / Control Específico	Exigencia Técnica sobre Respaldos
		• **SR 7.3 - Resource Backup:** El sistema OT debe proporcionar la capacidad de realizar respaldos de la información crítica del sistema (software, datos de configuración, archivos de lógica de control de PLCs, historiadores) sin interrumpir el proceso de producción en tiempo real. • **SR 7.4 - Resource Recovery and Reconstitution:** Capacidad del sistema para ser recuperado y llevado a un estado seguro conocido (*Known Good State*) tras un fallo catastrófico o infección.

Toda normativa exige traducir la regla 3-2-1 en dos métricas cuantificables de negocio:

- **RPO (*Recovery Point Objective*):** La cantidad máxima de datos (medida en tiempo) que la empresa puede permitirse perder. Determina la **frecuencia** con la que se deben ejecutar los respaldos de la regla 3-2-1.
- **RTO (*Recovery Time Objective*):** El tiempo máximo admisible para restaurar los sistemas tras una caída. Determina la **velocidad de transferencia y el tipo de medio** elegido para los 2 soportes diferentes.

Normatividad WORM (write once, read many)

Marco Normativo y Regulaciones Principales

- **SEC Rule 17a-4 (Financiero):** Exige que los registros financieros y transacciones se almacenen en medios inalterables e indelebles (WORM) para evitar la manipulación contable.
- **HIPAA (Salud):** Requiere que los registros médicos y datos de pacientes (*ePHI*) garanticen integridad estricta y trazabilidad a lo largo del tiempo.
- **GDPR / RGPD (Europa):** Aunque promueve el "derecho al olvido", en la conservación de pistas de auditoría (*logs*) e información fiscal exige el uso de mecanismos inmutables para cumplir con la rendición de cuentas.
- **ISO/IEC 27001 (Control A.8.10 - Eliminación de datos / Inmutabilidad):** Recomienda el uso de almacenamiento inmutable para resguardar copias de seguridad críticas frente a cifrados maliciosos.

Protección contra malware

Protección contra Malware (Control A.8.7)

El objetivo de este control es garantizar que la información y los recursos de procesamiento estén protegidos contra código malicioso (*malware*, *worms*, troyanos, *ransomware*).

Directivas y Requisitos Específicos:

- **Detección y Prevención en Múltiples Capas:** Implementación de soluciones antimalware en endpoints (EDR/XDR), servidores, correo electrónico y puertas de enlace (*gateways*).
- **Gestión de Firmas y Análisis Heurístico:** Mantenimiento de actualizaciones automáticas de patrones de firmas y uso de motores de detección basados en comportamiento.
- **Restricción de Software:** Aplicación de políticas de *whitelisting* (listas blancas de aplicaciones permitidas) o bloqueo de ejecución de scripts en directorios temporales.
- **Aislamiento y Respuesta:** Capacidad de aislar automáticamente los equipos infectados de la red para evitar la propagación lateral de gusanos (*worms*).
- **Concientización:** Capacitación periódica a los usuarios contra tácticas de ingeniería social (como el *phishing*) empleadas para ejecutar malware.

Análisis de Vulnerabilidades

ISO/IEC 27001:2022 / ISO/IEC 27002:2022

- **Control A.8.8 (Gestión de vulnerabilidades técnicas):** Exige la obtención oportuna de información sobre vulnerabilidades técnicas en los sistemas en uso, la evaluación de la exposición a las mismas y la toma de medidas adecuadas (parches o controles compensatorios).

- **Control A.8.25 (Ciclo de vida de desarrollo seguro):** Exige análisis de vulnerabilidades en el código (SAST/DAST) antes de desplegar aplicaciones a producción.

NIST SP 800-53 (Rev. 5) - EE.UU. / Estándar Global

- **Familia de Controles RA (Risk Assessment):**
  - **RA-5 (Vulnerability Monitoring and Scanning):** Exige el escaneo continuo de vulnerabilidades en la infraestructura, aplicaciones y dispositivos de red utilizando herramientas automáticas y actualizadas diariamente con feeds de vulnerabilidades (ej. CVE, NVD).

NIS2 (Directiva de la Unión Europea sobre Ciberseguridad)

- **Artículo 21:** Obliga a entidades esenciales e importantes a realizar evaluaciones regulares del nivel de madurez de ciberseguridad, incluyendo análisis de vulnerabilidades de la infraestructura crítica y de la cadena de suministro (*Supply Chain Security*).

Protección de datos personales

Las leyes de privacidad no detallan herramientas técnicas específicas, pero establecen la obligación legal de **probar técnicamente la efectividad de las medidas de seguridad**:

Ley / Regulación	Artículo / Sección	Exigencia Normativa
RGPD / GDPR (Unión Europea)	Art. 32.1.d	Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas para garantizar la seguridad del tratamiento.
HIPAA (Salud - EE.UU.)	45 CFR § 164.308(a)(1)	Evaluación de riesgos obligatoria para identificar vulnerabilidades en sistemas que manejen información médica electrónica (*ePHI*).
LFPDPPP (México) / Leyes locales	Secciones de Medidas Técnicas	Obligación de mantener los sistemas actualizados y realizar revisiones de seguridad periódicas para prevenir accesos no autorizados.

Ley antilavado de dinero LFPIORPI

La regulación se administra principalmente a través de la **Secretaría de Hacienda y Crédito Público (SHCP)**, la **Unidad de Inteligencia Financiera (UIF)** y el **Servicio de Administración Tributaria (SAT)**:

- **Sujetos Obligados (Actividades Vulnerables):** Personas físicas o morales que comercializan bienes o servicios de alto valor o susceptibles a ser usados para blanquear capitales sin pasar necesariamente por el sistema bancario tradicional.

Normatividad Aeroespacial

1. Controles Exigidos de Ciberseguridad en IA9100

Aunque la IA9100 no busca reemplazar un marco dedicado como la ISO/IEC 27001 o la CMMC (*Cybersecurity Maturity Model Certification*), sí obliga a que la **evaluación de riesgos tecnológicos e informáticos sea parte integral de la gestión de la calidad**:

- **Evaluación de Riesgos de Ciberseguridad (Cybersecurity Risk Assessments):** La organización debe evaluar y mitigar activamente el riesgo de ataques digitales en entornos de producción (IoT industrial, redes OT, sistemas ERP/MES) que puedan alterar la calidad o el diseño del producto.
- **Planes de Respuesta a Incidentes (Incidence Response Plans):** Contar con protocolos formalizados para responder ante ciberataques (como *ransomware*) garantizando la continuidad operativa y minimizando el impacto en la entrega de productos.
- **Protocolos de Acceso Seguro y Control de Usuarios:** Restricción y autenticación estricta para acceder a datos de ingeniería, software de fabricación, archivos de calibración y especificaciones de clientes.

- **Concientización del Personal:** Capacitación obligatoria para los empleados que manejan datos sensibles o críticos de la organización y de los clientes para evitar brechas por ingeniería social o descuidos informáticos.

2. Gestión de la Información Documentada y Protección de Datos

En el ámbito de la **gestión de la información**, la IA9100 amplía los requisitos tradicionales de documentación hacia la protección de activos digitales:

- **Protección de la Propiedad Intelectual e Información Técnica:** Se exige garantizar la confidencialidad e inalterabilidad de los diseños digitales de la industria de aviación, espacio y defensa (*Aviation, Space and Defense*).
- **Trazabilidad Digital Completa e Inmutabilidad:** Los registros de inspección, certificados de conformidad y datos de trazabilidad de los componentes deben resguardarse garantizando que no puedan ser modificados ni manipulados maliciosamente.
- **Control de Cambios en Archivos Digitales:** Control riguroso de versiones en los archivos informáticos involucrados en la producción y diseño (ej. modelos 3D y programas G-code).

3. Ciberseguridad en la Cadena de Suministro (Supply Chain)

Dado que las brechas de seguridad suelen ingresar a través de proveedores secundarios, la IA9100 refuerza los requisitos para la **gestión de proveedores**:

- **Cláusulas de Ciberseguridad en Contratos con Proveedores:** Incorporación de requisitos de seguridad de la información y controles de exportación de datos en los acuerdos de calidad acordados con subcontratistas.
- **Mitigación de Piezas Falsificadas vía Digital:** Uso de firmas digitales y trazabilidad basada en datos para verificar la autenticidad de materiales y componentes recibidos.

Alineación de la IA9100 con Marcos de Ciberseguridad

Para que una organización cumpla con las auditorías de la **IA9100**, su departamento de Calidad y su área de TI deben alinear sus controles con estándares complementarios reconocidos:

Marco / Estándar de Ciberseguridad	Relación con la IA9100
CMMC (EE. UU. - DoD)	Exigencia para contratistas de defensa. La IA9100 toma sus controles para asegurar la Información No Clasificada Controlada (CUI).
ISO/IEC 27001:2022	Proporciona el marco ideal para demostrar el cumplimiento de los controles de seguridad de la información exigidos en la IA9100.
NIST SP 800-171	Estándar de protección de datos técnicos sensibles ampliamente referenciado en las auditorías de proveedores de la IA9100.

BCP & DRP

ISO/IEC 22301:2019 (Sistemas de Gestión de Continuidad del Negocio)

Es la norma de referencia mundial. Regula la estructura que debe tener una organización para preparar, responder y recuperarse ante eventos disruptivos.

- **Análisis de Impacto al Negocio (BIA - *Business Impact Analysis*):** Exige identificar procesos críticos y definir métricas clave:
  - RTO (*Recovery Time Objective*): Tiempo máximo tolerable de interrupción.
  - RPO (*Recovery Point Objective*): Pérdida máxima tolerable de datos (medida en tiempo).
- **Estrategias de Recuperación:** Exige planes formales BCP y DRP probados mediante simulacros periódicos.

ISO/IEC 27001:2022 (Controles A.5.29 y A.5.30)

- **Control A.5.29:** Seguridad de la información durante una interrupción (asegurar que la seguridad no se degrade durante una crisis o activación del BCP).
- **Control A.5.30:** Preparación de las tecnologías de la información y comunicación para la continuidad del negocio (exige disponer de un DRP validado).

NIST SP 800-34 Rev. 1 (Guía de Planificación de Contingencias para TI)

Estándar desarrollado por el gobierno de EE.UU. ampliamente adoptado de forma global para estructurar el **DRP**:

- Establece las 7 etapas del ciclo de vida del DRP (desde el desarrollo de la política hasta las pruebas y el mantenimiento del plan).

HIPAA (EE.UU. / Estándar Global): Requisito **45 CFR § 164.308(a)(7)** exige un plan de contingencia obligatorio que incluya plan de respaldo de datos, plan de recuperación ante desastres y plan de operaciones de emergencia.

HIPPA

La **Ley de Portabilidad y Responsabilidad del Seguro Médico** (*HIPAA*, por sus siglas en inglés) es una ley federal de Estados Unidos promulgada en 1996. En el entorno de la ciberseguridad, HIPAA regula la forma en que los centros médicos, hospitales, aseguradoras y sus proveedores tecnológicos manejan e interactúan con la **Información de Salud Protegida Electrónica (ePHI)**.

Su principal objetivo es garantizar la **confidencialidad, integridad y disponibilidad** de los datos médicos de los pacientes frente a incidentes como filtraciones, accesos no autorizados y ataques informáticos (ej. *Ransomware)*

¿A quiénes aplica?

1. **Entidades Cubiertas (*Covered Entities*):** Proveedores de atención médica (médicos, clínicas, hospitales), planes de salud y centros de procesamiento de transacciones sanitarias.
2. **Socios Comerciales (*Business Associates*):** Terceros, contratistas o proveedores tecnológicos (servicios de nube, software de facturación, consultoras) que almacenan, transmiten o procesan datos ePH

Amenazas de Ciberseguridad Frecuentes bajo HIPAA

El sector salud es uno de los objetivos favoritos de los ciberdelincuentes por el alto valor de los datos médicos en el mercado negro. Los principales riesgos bajo el cumplimiento de HIPAA son:

- **Ransomware:** Secuestro de bases de datos de hospitales que interrumpe la atención a pacientes.
- **Phishing & Robo de Credenciales:** Ataques de ingeniería social para robar credenciales de acceso.
- **Dispositivos Pérdidos o Robados:** Laptops o unidades USB sin cifrar que contienen historias clínicas.
- **Filtraciones por Terceros:** Vulnerabilidades en los sistemas informáticos de proveedores externos.

Nota: El incumplimiento de HIPAA puede derivar en sanciones económicas que van desde miles hasta millones de dólares según el grado de negligencia, además de posibles responsabilidades legales y daños de reputación.

Checklist de Auditoría de TI para HIPAA

1.Fase 1: Evaluación de Riesgos e Inventario de Datos:Punto de partida obligatorio según la Regla de Seguridad.

- **Identificación de ePHI:** Mapear todos los sistemas, bases de datos, redes, servidores y dispositivos móviles que crean, reciben, mantienen o transmiten ePHI.
- **Inventario de Activos:** Registrar hardware, software, licencias de red y servicios en la nube (*SaaS/PaaS/IaaS*).
- **Evaluación de Amenazas:** Identificar vulnerabilidades internas y externas (p. ej., software obsoleto, configuraciones por defecto, accesos no autorizados).
- **Acuerdos de Socios Comerciales (BAA):** Verificar que existan contratos *Business Associate Agreements* firmados y actualizados con **todos** los proveedores de tecnología (nube, correo, software).

2.Fase 2: Salvaguardias Técnicas:Controles informáticos directos en la infraestructura.

- **Control de Acceso (Único e Individual):**
  - [ ] Cada usuario tiene un identificador único (prohibido compartir cuentas).
  - [ ] Principio de mínimo privilegio: el acceso a ePHI está restringido estrictamente según el rol.
  - [ ] Autenticación Multifactor (**MFA**) obligatoria para accesos remotos y sistemas críticos.
- **Cifrado (Encryption):**
  - [ ] Cifrado de datos en **tránsito** (*TLS 1.2+* en comunicaciones y correo).
  - [ ] Cifrado de datos en **reposo** (*AES-256* para discos, bases de datos y copias de seguridad).
- **Auditoría y Monitoreo:**
  - [ ] Logs/Registros habilitados en sistemas con ePHI (quién accedió, cuándo y qué modificó).
  - [ ] Revisión periódica de logs mediante SIEM o herramientas automatizadas.
- **Cierre de Sesión Automático:**
  - [ ] Tiempo de espera por inactividad activado en estaciones de trabajo y aplicaciones.

3.Fase 3: Salvaguardias Físicas:Protección de instalaciones y hardware.

- **Seguridad en Centro de Datos/Servidores:** Control de acceso físico (tarjetas magnéticas, biometría, cerraduras) limitado a personal autorizado.
- **Estaciones de Trabajo:** Pantallas orientadas fuera de la vista del público y filtros de privacidad en áreas transitadas.
- **Gestión de Dispositivos Móviles (MDM):** Capacidad de borrado remoto (*wipe*) para laptops y teléfonos corporativos o BYOD.
- **Destrucción de Medios:** Procedimientos de desmagnetización o destrucción física de discos duros antes de su desecho.

4.Fase 4: Respuesta a Incidentes y Continuidade de Negocio:Planes de contingencia y resiliencia.

- **Respaldo y Recuperación (Backups):**
  - [ ] Copias de seguridad automáticas, cifradas y probadas frecuentemente (regla 3-2-1).
  - [ ] Respaldo fuera del sitio (*offsite*) o en la nube para garantizar la disponibilidad.
- **Plan de Respuesta a Brechas (*Breach Notification Rule*):**
  - [ ] Protocolo claro para identificar y contener filtraciones.

- [ ] Mecanismo para notificar a los afectados y al HHS en el plazo legal (máximo 60 días).

- **Capacitación del Personal:** Talleres de concientización sobre *phishing* e ingeniería social impartidos al menos 1 vez al año.

.