Catálogo de Requisitos de Seguridad y Privacidad

SIR-001: El sistema debe implementar control de acceso basado en roles (RBAC) para restringir el acceso a la ePHI se

Referencia normativa: NIST SP 800-53 Rev.5 AC-3, ISO 27002:2022 5.15, HIPAA 45 CFR §164.312(a)(1)

Prioridad: Alta

Justificacion: Minimiza el riesgo de acceso no autorizado a información sensible. Es fundamental para proteger la confidencialidad de los datos de salud.

Metodo validacion: Inspección del sistema de gestión de identidades y roles + prueba funcional de acceso.

Dependencias exclusiones: Depende de SIR-002 (gestión de identidades), excluye controles estáticos por usuario.

Categoria: Broken Access Control (OWASP A01:2021), CWE-862

Ejemplo practico: Usuario tipo "administrativo" no puede acceder a módulos clínicos como e-prescripción.

SIR-002: El sistema debe autenticar a los usuarios mediante credenciales fuertes con doble factor (2FA).

Referencia normativa: NIST SP 800-53 Rev.5 IA-2(1), ISO 27002:2022 5.17, DISA STIG V-222390

Prioridad: Alta

Justificacion: Previene el acceso fraudulento por robo o suplantación de credenciales, especialmente en entornos expuestos (teletrabajo, móviles).

Metodo validacion: Revisión de política de autenticación y pruebas de acceso con 2FA.

Dependencias exclusiones: Requiere integración de mecanismo 2FA seguro. Relacionado con SIR-001 y SIR-006.

Categoria: Identification and Authentication Failures (OWASP A07:2021), CWE-287

Ejemplo practico: Uso de aplicación de autenticación OTP como Google Authenticator o claves FIDO2.

SIR-003: Las sesiones de usuario deben cerrarse automáticamente tras 15 minutos de inactividad.

Referencia normativa: HIPAA 45 CFR §164.312(b), DISA STIG V-222389, NIST AC-12

Prioridad: Media

Justificacion: Reduce el riesgo de secuestro de sesión cuando un usuario deja una sesión activa sin supervisión.

Metodo validacion: Configuración del sistema + pruebas de expiración de sesión.

Dependencias exclusiones: Requiere mecanismo de monitoreo de actividad de sesión.

Categoria: Session Management, Broken Access Control

Ejemplo practico: El sistema cierra automáticamente la sesión del médico tras 15 minutos sin uso.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-004: Toda la información ePHI transmitida fuera del entorno seguro debe estar cifrada mediante TLS 1.2 o superior

Referencia normativa: HIPAA 45 CFR §164.312(e)(1), ISO 27799:2016 10.1, NIST SC-12, DISA STIG V-222396

Prioridad: Alta

Justificacion: Protege la confidencialidad e integridad de la ePHI durante su transmisión en redes no confiables.

Metodo validacion: Análisis de red, escaneo de configuración SSL/TLS.

Dependencias exclusiones: Complementa SIR-005 (cifrado en reposo), requiere certificados válidos.

Categoria: Cryptographic Failures (OWASP A02:2021), CWE-311

Ejemplo practico: El acceso a OpenEMR vía navegador se realiza exclusivamente por HTTPS.

SIR-005: La base de datos debe cifrar la ePHI en reposo usando AES-256.

Referencia normativa: NIST SC-28, ISO 27002:2022 10.1, HIPAA 45 CFR §164.312(a)(2)(iv)

Prioridad: Alta

Justificacion: Protege la confidencialidad de los datos en caso de acceso físico o lógico a los servidores.

Metodo validacion: Revisión técnica del sistema de almacenamiento y configuración de cifrado.

Dependencias exclusiones: Relacionado con SIR-004.

Categoria: Cryptographic Failures, Data at Rest Protection

Ejemplo practico: Cifrado de discos mediante LUKS o cifrado nativo en MySQL con claves almacenadas en KMS.

SIR-006: El sistema debe registrar y auditar todos los accesos a la ePHI, incluyendo fecha, usuario, acción y resultado.

Referencia normativa: NIST AU-2, ISO 27002:2022 5.25, HIPAA 45 CFR §164.312(b)

Prioridad: Alta

Justificacion: Permite detectar accesos no autorizados o anómalos a información crítica.

Metodo validacion: Revisión de archivos de log, pruebas de auditoría.

Dependencias exclusiones: Requiere mecanismos de retención y protección de logs (ver SIR-007).

Categoria: Security Logging and Monitoring (OWASP A09:2021), CWE-778

Ejemplo practico: Registro automático de todas las consultas y ediciones a fichas de pacientes.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-007: Los registros de auditoría deben almacenarse de forma protegida e inalterable durante al menos 6 años.

Referencia normativa: HIPAA §164.316(b), NIST AU-11, ISO 27002:2022 5.27

Prioridad: Alta

Justificacion: Garantiza evidencia de cumplimiento y soporte en auditorías.

Metodo validacion: Configuración de retención y control de integridad de logs.

Dependencias exclusiones: Requiere implementación de SIR-006.

Categoria: Audit and Accountability, Non-Repudiation

Ejemplo practico: Almacenamiento en sistema WORM o SIEM con control de integridad.

SIR-008: El sistema debe validar de forma estricta todos los datos introducidos por usuarios para evitar inyecciones S

Referencia normativa: OWASP A03:2021, CWE-89, CWE-77, NIST SI-10

Prioridad: Alta

Justificacion: Previene ataques que podrían comprometer la integridad del sistema y exfiltrar información sensible.

Metodo validacion: Revisión de código, pruebas de penetración y fuzzing.

Dependencias exclusiones: Relacionado con controles de desarrollo seguro.

Categoria: Injection, Improper Input Validation

Ejemplo practico: Uso de sentencias preparadas y validación de campos.

SIR-009: El sistema debe contar con un plan documentado y probado de continuidad de negocio para asegurar la disp

Referencia normativa: ISO 27002:2022 5.30, NIST CP-2, HIPAA 45 CFR §164.308(a)(7)(i)

Prioridad: Alta

Justificacion: Garantiza la disponibilidad de la ePHI ante desastres naturales, fallos tecnológicos o ataques.

Metodo validacion: Revisión del plan de continuidad y pruebas de simulación.

Dependencias exclusiones: Relacionado con SIR-010 y SIR-011.

Categoria: Business Continuity, Availability Management

Ejemplo practico: Plan de recuperación con objetivos RTO < 4h y RPO < 1h.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-010: El sistema debe realizar copias de seguridad automáticas y regulares de todos los datos que incluyan ePHI.

Referencia normativa: HIPAA 45 CFR §164.308(a)(7)(ii)(A), NIST CP-9, ISO 27002:2022 5.33

Prioridad: Alta

Justificacion: Asegura la restauración de la ePHI ante fallos o incidentes.

Metodo validacion: Auditoría de políticas de backup y verificación de registros.

Dependencias exclusiones: Relacionado con SIR-009 y SIR-005.

Categoria: Data Recovery, Resilience

Ejemplo practico: Copias incrementales diarias y completas semanales cifradas en AWS Glacier.

SIR-011: Deben implementarse mecanismos de alta disponibilidad y redundancia para servicios críticos del sistema EH

Referencia normativa: NIST SC-6, ISO 27002:2022 5.30, OWASP A08:2021

Prioridad: Alta

Justificacion: Minimiza el impacto de fallas en servicios críticos.

Metodo validacion: Inspección de arquitectura y simulación de fallos.

Dependencias exclusiones: Requiere monitoreo activo (ver SIR-012).

Categoria: Availability, Infrastructure Security

Ejemplo practico: Balanceo de carga activo-activo y clúster multi-zona en AWS.

SIR-012: Debe monitorizarse en tiempo real la disponibilidad de los componentes y generar alertas ante fallos o degrad

Referencia normativa: NIST IR-5, ISO 27002:2022 5.22, HIPAA §164.308(a)(6)

Prioridad: Alta

Justificacion: Permite la detección temprana de incidentes para reducir tiempos de recuperación.

Metodo validacion: Verificación de integración de herramientas de monitoreo.

Dependencias exclusiones: Complementa SIR-011 y SIR-009.

Categoria: Monitoring & Alerting, Logging and Monitoring

Ejemplo practico: Integración con Prometheus, Grafana y alertas en canales 24/7.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-013: El plan de continuidad debe incluir escenarios específicos de ciberataques como ransomware o denegación d

Referencia normativa: NIST CP-2, DISA STIG, ISO 27002:2022 5.24

Prioridad: Media

Justificacion: Asegura que el plan de continuidad aborde amenazas cibernéticas.

Metodo validacion: Análisis de escenarios y simulacros de recuperación.

Dependencias exclusiones: Relacionado con SIR-009, SIR-006 y SIR-010.

Categoria: Incident Response & Resilience

Ejemplo practico: Simulacros de ransomware con restauración desde backup limpio.

SIR-014: Se deben definir y probar procedimientos de operación manual temporal para continuidad mínima del servicio

Referencia normativa: ISO 27002:2022 5.29, NIST CP-10, Canada Health Infoway Req. 31

Prioridad: Media

Justificacion: Permite continuar con atención básica en caso de caída total del sistema digital.

Metodo validacion: Revisión documental y pruebas piloto offline.

Dependencias exclusiones: Complemento de SIR-009.

Categoria: Business Continuity, Offline Resilience

Ejemplo practico: Uso de formularios impresos para admisión y recetas, sincronizados posteriormente.

SIR-031: Las dependencias y componentes de terceros deben ser analizados contra vulnerabilidades conocidas (SBOM

Referencia normativa: OWASP A06:2021, NIST SI-7, ISO 27002:2022 5.23, DISA STIG V-222437

Prioridad: Alta

Justificacion: Previene explotaciones mediante componentes vulnerables.

Metodo validacion: Uso de escáneres de composición de software y alertas de CVE.

Dependencias exclusiones: Relacionado con SIR-032.

Categoria: Vulnerable Components, Software Supply Chain

Ejemplo practico: Implementar Dependabot o Snyk para revisar actualizaciones.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-015: El sistema debe permitir la recolección explícita y documentada del consentimiento informado del paciente ar

Referencia normativa: ISO 27799:2016 8.1.3, HIPAA §164.508, Canada Health Infoway Req. 4

Prioridad: Alta

Justificacion: Esencial para respetar los derechos del titular de los datos y cumplir regulaciones.

Metodo validacion: Verificación de pantallas/formularios y registro en base de datos.

Dependencias exclusiones: Requiere SIR-016 para revocación de consentimiento.

Categoria: Privacy Consent, Legal & Regulatory Compliance

Ejemplo practico: Consentimiento digital firmado en interfaz web previo al primer uso.

SIR-016: El sistema debe permitir que el paciente revoque su consentimiento previamente otorgado, reflejando el camb

Referencia normativa: HIPAA §164.522(b), ISO 27799:2016 8.1.4

Prioridad: Alta

Justificacion: Respetar la autonomía del paciente y permitir modificar decisiones previas.

Metodo validacion: Verificación de la interfaz de revocación y revisión de logs.

Dependencias exclusiones: Requiere SIR-015 implementado.

Categoria: Data Subject Rights, Consent Management

Ejemplo practico: Portal del paciente que permita revocar accesos sin afectar atención clínica.

SIR-017: El sistema debe aplicar principios de minimización de datos, recolectando y procesando solo la ePHI estrictar

Referencia normativa: ISO 27799:2016 7.1.3, NIST AP-1, Canada Health Infoway Req. 8

Prioridad: Alta

Justificacion: Reduce el riesgo de exposición innecesaria y fortalece la privacidad desde el diseño.

Metodo validacion: Análisis de procesos y formularios.

Dependencias exclusiones: Complementa SIR-015.

Categoria: Privacy by Design, Data Minimization

Ejemplo practico: Exclusión de campos irrelevantes como nacionalidad o religión.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-018: Debe implementarse trazabilidad detallada sobre qué usuarios acceden, consultan o modifican ePHI por pacie

Referencia normativa: HIPAA §164.312(b), ISO 27002:2022 5.26, NIST AU-3

Prioridad: Alta

Justificacion: Permite llevar auditorías efectivas y controlar el acceso a datos sensibles.

Metodo validacion: Revisión de logs segmentados por paciente.

Dependencias exclusiones: Complementa SIR-006 y SIR-007.

Categoria: Auditability, Data Provenance, Accountability

Ejemplo practico: Registro detallado de accesos a historias clínicas con IP y timestamp.

SIR-019: El sistema debe permitir que el paciente acceda y revise su propia ePHI de forma segura.

Referencia normativa: HIPAA §164.524, ISO 27799:2016 8.2.1, Canada Health Infoway Req. 5

Prioridad: Media

Justificacion: Fomenta la transparencia y el control por parte del paciente sobre sus datos.

Metodo validacion: Pruebas funcionales del portal del paciente.

Dependencias exclusiones: Relacionado con SIR-020.

Categoria: Data Subject Access, Transparency

Ejemplo practico: Acceso autenticado a historial clínico desde interfaz móvil.

SIR-020: El sistema debe permitir que el paciente solicite la rectificación de su ePHI cuando identifique errores.

Referencia normativa: HIPAA §164.526, ISO 27799:2016 8.2.2, NIST AP-2

Prioridad: Media

Justificacion: Garantiza la precisión de la información de salud.

Metodo validacion: Validación del flujo de solicitud y auditoría de cambios.

Dependencias exclusiones: Complementa SIR-019.

Categoria: Data Integrity, Accuracy, Patient Rights

Ejemplo practico: Solicitud de corrección mediante módulo de atención al paciente.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-021: El sistema debe anonimizar o seudonimizar los datos antes de su uso para fines secundarios.

Referencia normativa: ISO 27799:2016 9.3, NIST PM-19, Canada Health Infoway Req. 11

Prioridad: Alta

Justificacion: Protege la identidad del paciente en usos no asistenciales.

Metodo validacion: Hashing de identificadores y control de accesos.

Dependencias exclusiones: Complementa SIR-015 y SIR-017.

Categoria: Data Anonymization, Secondary Use Controls

Ejemplo practico: Reemplazo de identificadores por claves internas irreversibles.

SIR-022: El sistema debe aplicar políticas de retención mínima de ePHI conforme a requisitos legales y clínicos, elimina

Referencia normativa: HIPAA §164.316(b), ISO 27799:2016 9.1, NIST DM-2

Prioridad: Media

Justificacion: Disminuye el riesgo y controla el ciclo de vida de la ePHI.

Metodo validacion: Revisión de políticas y ejecuciones automatizadas.

Dependencias exclusiones: Requiere SIR-007.

Categoria: Data Lifecycle Management, Retention and Disposal

Ejemplo practico: Eliminación automática de datos que superen los 10 años de almacenamiento.

SIR-023: Los datos ePHI no deben transferirse a jurisdicciones fuera del país sin evaluaciones de riesgo y cumplimient

Referencia normativa: ISO 27799:2016 9.2, NIST PM-5, Canada Health Infoway Req. 14

Prioridad: Alta

Justificacion: Protege los derechos de los pacientes frente a legislaciones menos estrictas.

Metodo validacion: Evaluación contractual y de ubicación de servidores.

Dependencias exclusiones: Depende de políticas de cloud y geolocalización.

Categoria: Cross-Border Data Transfers, Legal Compliance

Ejemplo practico: Evaluación DPIA antes de usar proveedores cloud fuera de EE. UU. o Canadá.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-024: El sistema debe proteger los metadatos asociados a ePHI para evitar inferencias indebidas.

Referencia normativa: ISO 27799:2016 7.5.2, NIST AC-16, OWASP Top 10 Privacy Risks (P4)

Prioridad: Media

Justificacion: Una metadata inadecuada puede revelar información sensible indirecta.

Metodo validacion: Análisis de registros y eliminación de información sensible en los metadatos.

Dependencias exclusiones: Complementa SIR-021 y SIR-006.

Categoria: Metadata Privacy, Inference Protection

Ejemplo practico: Eliminación de autores, timestamps y ubicaciones en exportes de datos.

SIR-025: El sistema debe diferenciar claramente el acceso a datos identificables, seudonimizados y anonimizados med

Referencia normativa: ISO 27799:2016 8.1.6, NIST AC-16, Canada Health Infoway Req. 12

Prioridad: Alta

Justificacion: Establece barreras para minimizar el riesgo de reidentificación indebida.

Metodo validacion: Validación de matrices de permisos y simulación de accesos cruzados.

Dependencias exclusiones: Requiere SIR-001 y SIR-021.

Categoria: Data Segmentation, Role-Based Privacy Enforcement

Ejemplo practico: Acceso restringido a datos seudonimizados para investigación sin identificar al paciente.

SIR-026: El sistema debe permitir establecer políticas de acceso diferencial en función del contexto de uso (atención, a

Referencia normativa: ISO 27799:2016 8.1.5, NIST AC-3(3), Canada Health Infoway Req. 7

Prioridad: Alta

Justificacion: Reduce el riesgo de acceso indebido según el contexto de uso.

Metodo validacion: Verificación de configuraciones de acceso y análisis de logs.

Dependencias exclusiones: Relacionado con SIR-001 y SIR-025.

Categoria: Context-Aware Access Control, Least Privilege

Ejemplo practico: Acceso limitado a funciones críticas según el rol y contexto.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-027: El sistema debe notificar al paciente cuando su ePHI sea accedida para usos no asistenciales o por terceros.

Referencia normativa: HIPAA §164.528, ISO 27799:2016 8.2.3, Canada Health Infoway Req. 6

Prioridad: Media

Justificacion: Aumenta la transparencia y confianza al informar al paciente.

Metodo validacion: Verificación de logs y pruebas de notificación.

Dependencias exclusiones: Requiere SIR-006 y SIR-018.

Categoria: Transparency, Data Usage Notification

Ejemplo practico: Alerta automática por correo cuando se consulta el historial clínico.

SIR-028: El sistema debe aplicar validación estricta de entradas tanto del lado cliente como del servidor para prevenir i

Referencia normativa: OWASP A03:2021, CWE-20, CWE-89, DISA STIG V-222401, ISO 27002:2022 5.23

Prioridad: Alta

Justificacion: Previene ataques que puedan comprometer la integridad del sistema.

Metodo validacion: Revisión de código y pruebas de fuzzing.

Dependencias exclusiones: Relacionado con SIR-008.

Categoria: Input Validation, Secure Coding Practices

Ejemplo practico: Uso de filtros sanitizadores y consultas parametrizadas.

SIR-029: El sistema debe evitar el uso de credenciales hardcoded, usando mecanismos seguros para la gestión de sec

Referencia normativa: CWE-798, NIST SC-12, DISA STIG V-222440, ISO 27002:2022 8.2.4

Prioridad: Alta

Justificacion: Previene la exposición accidental de credenciales que comprometan la infraestructura.

Metodo validacion: Análisis de repositorios y uso de herramientas de escaneo.

Dependencias exclusiones: Complemento de políticas de DevSecOps.

Categoria: Credential Management, Secrets Handling

Ejemplo practico: Utilizar AWS Secrets Manager para almacenar claves API de forma segura.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-030: Todo código fuente debe ser revisado por al menos un segundo desarrollador antes de entrar a producción.

Referencia normativa: NIST SA-11, ISO 27002:2022 5.8, DISA STIG V-222433

Prioridad: Media

Justificacion: Detecta errores y vulnerabilidades que puedan pasar desapercibidos.

Metodo validacion: Revisión de pull requests y trazabilidad en CI/CD.

Dependencias exclusiones: Requiere prácticas de gestión de configuración (SIR-033).

Categoria: Code Review, Secure Development Lifecycle

Ejemplo practico: Uso de GitHub Actions para bloquear merges sin revisión doble.

SIR-032: El sistema debe aplicar parches de seguridad de manera periódica y automatizada.

Referencia normativa: NIST SI-2, DISA STIG V-222441, ISO 27002:2022 5.28

Prioridad: Alta

Justificacion: La aplicación oportuna de parches minimiza la exposición a vulnerabilidades conocidas.

Metodo validacion: Revisión de políticas de parches y registros de despliegue.

Dependencias exclusiones: Requiere mecanismos de pruebas en entornos de staging.

Categoria: Patch Management, System Hardening

Ejemplo practico: Automatización semanal de actualizaciones en contenedores Docker a través de pipelines.

SIR-033: Se debe implementar control de versiones y gestión de cambios en todos los activos de software.

Referencia normativa: ISO 27002:2022 5.8, NIST CM-3, DISA STIG V-222430

Prioridad: Media

Justificacion: Facilita la trazabilidad de cambios y auditoría.

Metodo validacion: Auditoría del sistema de control de versiones y gestión de ramas.

Dependencias exclusiones: Requiere una cultura DevSecOps consolidada.

Categoria: Configuration Management, Change Control

Ejemplo practico: Integración con GitLab y uso obligatorio de merge requests con revisión.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-034: El sistema debe incluir un proceso formal de gestión y respuesta a incidentes de seguridad.

Referencia normativa: ISO 27002:2022 5.25, NIST IR-4, HIPAA §164.308(a)(6)

Prioridad: Alta

Justificacion: Permite una respuesta rápida y coordinada ante incidentes para minimizar el impacto.

Metodo validacion: Documentación de procedimientos y simulacros de respuesta.

Dependencias exclusiones: Complementa SIR-012 y SIR-006.

Categoria: Incident Response, Security Operations

Ejemplo practico: Guía de actuación ante ransomware con responsables definidos.

SIR-035: Se deben definir métricas y criterios de severidad para clasificar los incidentes de seguridad.

Referencia normativa: NIST IR-4, ISO 27002:2022 5.25.3

Prioridad: Media

Justificacion: Facilita la priorización y respuesta a incidentes mediante clasificación estandarizada.

Metodo validacion: Verificación de la taxonomía y simulación de escalamiento.

Dependencias exclusiones: Requiere implementación de SIR-034.

Categoria: Incident Classification, Risk Management

Ejemplo practico: Clasificación de incidentes como "alto" si superan 500 registros comprometidos.

SIR-036: El sistema debe notificar al oficial de privacidad y seguridad, así como a los usuarios afectados, cuando ocur

Referencia normativa: HIPAA §164.404, ISO 27799:2016 8.3, NIST IR-6

Prioridad: Alta

Justificacion: Garantiza el cumplimiento legal y la transparencia en la gestión de brechas.

Metodo validacion: Verificación de notificaciones y revisión de logs de incidentes.

Dependencias exclusiones: Depende de SIR-034 y SIR-006.

Categoria: Breach Notification, Compliance

Ejemplo practico: Envío automático de alertas al oficial de seguridad y aviso a usuarios afectados.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-037: Todos los incidentes deben documentarse en un registro centralizado con fecha, tipo, impacto, medidas y seg

Referencia normativa: ISO 27002:2022 5.25.4, NIST IR-5, HIPAA §164.308(a)(6)(ii)

Prioridad: Media

Justificacion: La documentación detallada permite análisis forense y mejora continua.

Metodo validacion: Revisión de la documentación y simulación de incidentes.

Dependencias exclusiones: Relacionado con SIR-034 y SIR-035.

Categoria: Incident Tracking, Accountability

Ejemplo practico: Sistema interno que codifica y documenta cada incidente con responsables asignados.

SIR-038: El personal debe recibir formación periódica en detección, reporte y actuación ante incidentes de seguridad.

Referencia normativa: NIST AT-2, ISO 27002:2022 6.3, HIPAA §164.308(a)(5)

Prioridad: Media

Justificacion: La capacitación mejora la detección temprana de amenazas.

Metodo validacion: Registro de asistencias y evaluaciones formativas.

Dependencias exclusiones: Complementa SIR-034.

Categoria: Security Awareness, Human Risk Management

Ejemplo practico: Cursos anuales obligatorios sobre seguridad y respuesta a incidentes.

SIR-039: Todo acceso a OpenEMR debe estar sujeto a autenticación mediante credenciales únicas e intransferibles po

Referencia normativa: ISO 27002:2022 5.17, NIST IA-2, HIPAA §164.312(d)

Prioridad: Alta

Justificacion: Previene el acceso compartido o no autorizado, garantizando trazabilidad.

Metodo validacion: Revisión de políticas de autenticación y pruebas de acceso.

Dependencias exclusiones: Base para SIR-002 (2FA) y SIR-040.

Categoria: Authentication, Identity Assurance

Ejemplo practico: Acceso con usuario único, por ejemplo "medico1".

Catálogo de Requisitos de Seguridad y Privacidad

SIR-040: El sistema debe forzar el cambio periódico de credenciales según política definida (mínimo cada 90 días).

Referencia normativa: NIST IA-5(1), ISO 27002:2022 5.17.3, DISA STIG V-222402

Prioridad: Media

Justificacion: Minimiza riesgos asociados a credenciales antiguas.

Metodo validacion: Revisión de políticas y registros de cambio.

Dependencias exclusiones: Requiere SIR-039 y políticas de gestión de usuarios.

Categoria: Credential Lifecycle Management

Ejemplo practico: Cambio obligatorio de contraseña cada 90 días sin reutilización de las últimas 5.

SIR-041: Toda cuenta de usuario debe estar sujeta a un proceso de alta, baja y modificación controlado (ciclo de vida I

Referencia normativa: ISO 27002:2022 5.18, NIST AC-2, HIPAA §164.308(a)(3)

Prioridad: Alta

Justificacion: Asegura que solo usuarios autorizados tengan acceso y sean desactivados cuando ya no lo requieren.

Metodo validacion: Auditoría de procesos de provisión y revocación.

Dependencias exclusiones: Relacionado con SIR-001 y SIR-039.

Categoria: Identity Provisioning, Access Governance

Ejemplo practico: Revocación automática en menos de 24 horas al desvincular a un usuario.

SIR-042: Se deben registrar intentos de acceso fallidos y generar alertas ante patrones sospechosos (ej. 5 intentos).

Referencia normativa: NIST AC-7, ISO 27002:2022 5.17.6, OWASP A07:2021

Prioridad: Alta

Justificacion: Permite detectar ataques de fuerza bruta y accesos indebidos.

Metodo validacion: Simulación de fallos y revisión de logs.

Dependencias exclusiones: Relacionado con SIR-006 y SIR-012.

Categoria: Access Control Monitoring, Brute Force Protection

Ejemplo practico: Bloqueo temporal tras 5 intentos fallidos y notificación.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-043: El sistema debe soportar federación de identidad para facilitar el acceso seguro de usuarios externos (SSO, S

Referencia normativa: ISO 27002:2022 5.17.4, NIST IA-8, Canada Health Infoway Req. 20

Prioridad: Media

Justificacion: Facilita la integración segura con sistemas externos.

Metodo validacion: Pruebas de integración con proveedor federado.

Dependencias exclusiones: Requiere SIR-039 y compatibilidad con SSO.

Categoria: Federated Access, Interoperability

Ejemplo practico: Acceso mediante login federado sin creación de cuentas locales.

SIR-044: El sistema debe deshabilitar o eliminar todos los servicios, puertos y protocolos no utilizados en los servidor

Referencia normativa: DISA STIG APP3510, ISO 27002:2022 5.23, NIST CM-7

Prioridad: Alta

Justificacion: Reduce la superficie de ataque.

Metodo validacion: Escaneo de puertos y revisión de configuraciones.

Dependencias exclusiones: Requiere una política de configuración base.

Categoria: Attack Surface Reduction, Secure Configuration

Ejemplo practico: Deshabilitar servicios innecesarios como Telnet o FTP.

SIR-045: Todos los sistemas deben aplicar políticas seguras de contraseñas a nivel de sistema operativo.

Referencia normativa: DISA STIG APP3520, ISO 27002:2022 5.17, NIST IA-5

Prioridad: Alta

Justificacion: Aumenta la robustez de las credenciales y protege el acceso.

Metodo validacion: Revisión de configuraciones PAM/Linux y políticas de grupos en Windows.

Dependencias exclusiones: Complementa SIR-040 y SIR-002.

Categoria: System Authentication, Password Policy Enforcement

Ejemplo practico: Política de mínimo 12 caracteres, combinación de símbolos y bloqueo tras 5 intentos.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-046: El sistema debe mantener un benchmark de configuración segura basado en STIG, CIS o similar, revisado per

Referencia normativa: DISA STIG APP3500, ISO 27002:2022 5.23, NIST CM-6

Prioridad: Media

Justificacion: Define una línea base para configuraciones seguras en entornos heterogéneos.

Metodo validacion: Revisión periódica y documentación interna de benchmarks.

Dependencias exclusiones: Relacionado con SIR-044 y SIR-048.

Categoria: Configuration Baseline, Secure Build Standards

Ejemplo practico: Documentar la configuración estándar para servidores Ubuntu en Docker.

SIR-047: Las configuraciones de aplicaciones web deben evitar listados de directorios y acceso a archivos ocultos, y r

Referencia normativa: OWASP A05:2021, DISA STIG APP3525, CWE-200

Prioridad: Alta

Justificacion: Evita la exposición de información técnica y estructura interna.

Metodo validacion: Pruebas de escaneo web y análisis de configuración del servidor.

Dependencias exclusiones: Complementa SIR-004 y SIR-008.

Categoria: Security Misconfiguration, Information Disclosure

Ejemplo practico: Configurar Apache con 'Options -Indexes' y mensajes de error genéricos.

SIR-048: Toda configuración de sistema debe estar sujeta a control de cambios formal con aprobación y trazabilidad.

Referencia normativa: NIST CM-3, ISO 27002:2022 5.8, DISA STIG APP3505

Prioridad: Alta

Justificacion: Previene modificaciones no autorizadas y permite auditoría.

Metodo validacion: Revisión de registros y control de cambios.

Dependencias exclusiones: Requiere SIR-033 (gestión de versiones).

Categoria: Change Management, Configuration Control

Ejemplo practico: Uso de pull requests y tickets de aprobación para cambios en producción.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-049: El acceso a OpenEMR desde dispositivos móviles debe estar restringido a través de mecanismos como MDM

Referencia normativa: NIST AC-19, ISO 27002:2022 5.24, Canada Health Infoway Req. 19

Prioridad: Alta

Justificacion: Reduce el riesgo en dispositivos no gestionados o comprometidos.

Metodo validacion: Verificación de soluciones MDM y revisión de políticas de acceso.

Dependencias exclusiones: Complementa SIR-002 y SIR-041.

Categoria: Mobile Device Management, Endpoint Security

Ejemplo practico: Solo dispositivos registrados en MDM pueden acceder a la app.

SIR-050: El sistema debe exigir cifrado en disco completo en dispositivos móviles que accedan a ePHI.

Referencia normativa: HIPAA §164.312(a)(2)(iv), NIST MP-6, ISO 27002:2022 8.11

Prioridad: Alta

Justificacion: Protege datos locales en caso de pérdida o robo del dispositivo.

Metodo validacion: Verificación de configuraciones de cifrado en dispositivos gestionados por MDM.

Dependencias exclusiones: Requiere SIR-049.

Categoria: Data at Rest Protection, Device Hardening

Ejemplo practico: Uso de BitLocker o FileVault en laptops con acceso remoto.

SIR-051: Los dispositivos móviles deben tener políticas de bloqueo automático tras un período de inactividad definido

Referencia normativa: NIST AC-11, ISO 27002:2022 8.1.6, DISA STIG V-222389

Prioridad: Media

Justificacion: Evita accesos no autorizados cuando el dispositivo queda sin supervisión.

Metodo validacion: Revisión de políticas de bloqueo en MDM o mediante directivas del sistema.

Dependencias exclusiones: Relacionado con SIR-003 y SIR-049.

Categoria: Session Timeout, Mobile Access Control

Ejemplo practico: Bloqueo automático en 2 minutos sin actividad.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-052: Se debe permitir el borrado remoto de datos ePHI en dispositivos móviles extraviados o comprometidos.

Referencia normativa: ISO 27002:2022 8.13, NIST MP-6, Canada Health Infoway Req. 18

Prioridad: Alta

Justificacion: Previene la exposición de ePHI ante pérdida o robo del dispositivo.

Metodo validacion: Pruebas de borrado remoto y revisión de logs de eliminación.

Dependencias exclusiones: Depende de SIR-049.

Categoria: Remote Wipe, Incident Response

Ejemplo practico: Borrado remoto a través de MDM como Microsoft Intune.

SIR-053: El acceso a ePHI desde navegadores en dispositivos móviles debe requerir canales seguros (HTTPS) y expira

Referencia normativa: OWASP M2, HIPAA §164.312(e)(1), ISO 27002:2022 8.10

Prioridad: Alta

Justificacion: Mitiga riesgo de interceptación o secuestro de sesión en móviles.

Metodo validacion: Análisis de configuración TLS y políticas de expiración de sesión.

Dependencias exclusiones: Complementa SIR-004 y SIR-051.

Categoria: Secure Mobile Communication, Session Management

Ejemplo practico: Uso de HTTPS con HSTS y cookies configuradas con Secure y HttpOnly.

SIR-054: El sistema debe centralizar los registros de eventos de seguridad y actividad de usuarios en una solución SIE

Referencia normativa: NIST AU-6, ISO 27002:2022 5.26, HIPAA §164.312(b), DISA STIG APP3550

Prioridad: Alta

Justificacion: Facilita la detección de amenazas y evidencia forense.

Metodo validacion: Inspección de integración con SIEM y revisión de dashboards.

Dependencias exclusiones: Complementa SIR-006 y SIR-012.

Categoria: Security Logging and Monitoring, Threat Detection

Ejemplo practico: Envío de logs en tiempo real a SIEM como Splunk o Wazuh.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-055: Los registros deben conservarse de forma segura y protegida contra alteraciones durante al menos 6 años.

Referencia normativa: HIPAA §164.316(b)(2)(i), NIST AU-11, ISO 27002:2022 5.27

Prioridad: Alta

Justificacion: Proporciona trazabilidad legal y soporte en auditorías.

Metodo validacion: Verificación de almacenamiento inmutable y control de integridad.

Dependencias exclusiones: Complementa SIR-007 y SIR-054.

Categoria: Audit Log Retention, Evidence Preservation

Ejemplo practico: Uso de almacenamiento S3 con políticas de retención y protección.

SIR-056: El sistema debe permitir la generación automatizada de reportes de auditoría para revisiones periódicas.

Referencia normativa: ISO 27002:2022 5.26.3, NIST AU-6(3), Canada Health Infoway Req. 26

Prioridad: Media

Justificacion: Facilita el cumplimiento interno y externo.

Metodo validacion: Pruebas de generación de reportes y verificación de envíos.

Dependencias exclusiones: Relacionado con SIR-054.

Categoria: Audit Reporting, Periodic Review

Ejemplo practico: Envío automatizado mensual a través de un sistema de reportes.

SIR-057: Se deben definir y aplicar reglas de correlación en el SIEM para detectar patrones anómalos o indicios de atac

Referencia normativa: NIST AU-6(1), DISA STIG APP3555, ISO 27002:2022 5.22

Prioridad: Alta

Justificacion: Mejora la detección temprana y reduce el tiempo de respuesta ante incidentes.

Metodo validacion: Revisión de reglas implementadas y simulación de eventos anómalos.

Dependencias exclusiones: Requiere SIR-054.

Categoria: Threat Detection, Anomaly Correlation

Ejemplo practico: Reglas que detecten múltiples intentos fallidos seguidos de un acceso exitoso desde una IP diferente.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-058: El sistema debe permitir la visualización en tiempo real de indicadores de seguridad clave (KPI) mediante tabl

Referencia normativa: NIST IR-5, ISO 27002:2022 5.22, Canada Health Infoway Req. 27

Prioridad: Media

Justificacion: Permite supervisar en tiempo real la seguridad operativa.

Metodo validacion: Verificación de dashboards y pruebas con herramientas de monitoreo.

Dependencias exclusiones: Complementa SIR-057.

Categoria: Real-Time Monitoring, Operational Security

Ejemplo practico: Tablero que muestra en tiempo real el número de accesos fallidos por minuto.

SIR-059: El sistema debe contar con arquitectura redundante y balanceo de carga para asegurar la continuidad del ser

Referencia normativa: ISO 27002:2022 5.30, NIST SP 800-53 Rev.5 SC-6, Canada Health Infoway Req. 29

Prioridad: Alta

Justificacion: Permite mantener la disponibilidad de los servicios críticos de OpenEMR ante interrupciones, actualizaciones o fallos inesperados.

Metodo validacion: Pruebas de failover, revisión de configuración de balanceadores de carga y nodos redundantes.

Dependencias exclusiones: Relacionado con SIR-011 (Alta disponibilidad) y SIR-012 (Monitoreo).

Categoria: Availability, Fault Tolerance

Ejemplo practico: Configuración de balanceador de carga con múltiples instancias OpenEMR desplegadas en zonas de disponibilidad distintas (AWS Multi-AZ).

SIR-060: Los componentes críticos del sistema deben incluir mecanismos automáticos de detección de fallos y recupe

Referencia normativa: NIST SP 800-53 Rev.5 SC-7(8), ISO 27002:2022 5.30, DISA STIG APP3550

Prioridad: Alta

Justificacion: Minimiza el tiempo de inactividad ante fallos parciales, evitando la necesidad de intervención humana inmediata.

Metodo validacion: Simulación de fallos de servicio con verificación de autorrecuperación o reinicio automático.

Dependencias exclusiones: Complementa SIR-059 y SIR-012.

Categoria: Self-Healing Systems, Operational Resilience

Ejemplo practico: Uso de contenedores Docker orquestados por Kubernetes con liveness y readiness probes para reinicio automático.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-061: Debe existir un mecanismo de replicación síncrona o asíncrona para las bases de datos y almacenamiento qu

Referencia normativa: ISO 27002:2022 5.33, NIST SP 800-53 Rev.5 CP-6, HIPAA 45 CFR §164.308(a)(7)

Prioridad: Alta

Justificacion: Asegura la persistencia e integridad de datos clínicos en caso de falla del nodo principal o desastre físico.

Metodo validacion: Revisión de configuración de replicación y pruebas de conmutación por error.

Dependencias exclusiones: Relacionado con SIR-010 (copias de seguridad) y SIR-059.

Categoria: Data Replication, Disaster Recovery

Ejemplo practico: Replicación binaria MySQL entre servidores primario y secundario en distintas regiones geográficas.

SIR-086: Todas las comunicaciones entre clientes y APIs deben estar protegidas mediante HTTPS (TLS 1.2 o superior)

Referencia normativa: ISO 27002:2022 8.4.1, HIPAA §164.312(e)(1), NIST SC-12

Prioridad: Alta

Justificacion: Protege la confidencialidad e integridad de los datos clínicos transmitidos.

Metodo validacion: Análisis de tráfico de red y prueba de rechazo de conexiones HTTP no seguras.

Dependencias exclusiones: Relacionado con SIR-016 (cifrado en tránsito).

Categoria: Transport Security, Secure Communications

Ejemplo practico: Todo endpoint de API REST de OpenEMR responde con error 403 si la conexión no es HTTPS.

SIR-062: El sistema debe establecer objetivos de RTO y RPO documentados para cada servicio crítico y validarlos med

Referencia normativa: NIST SP 800-53 Rev.5 CP-2, ISO 27002:2022 5.31, Canada Health Infoway Req. 30

Prioridad: Media

Justificacion: Define expectativas claras de continuidad para cada componente esencial, mejorando la planificación y control del riesgo.

Metodo validacion: Documentación de RTO y RPO + evidencia de simulacros de recuperación.

Dependencias exclusiones: Requiere SIR-061 implementado.

Categoria: Business Continuity Metrics, Availability

Ejemplo practico: Servicio de laboratorio con RTO = 2h, RPO = 30 min probado mediante simulacro semestral.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-063: El sistema debe monitorear continuamente la disponibilidad de la infraestructura crítica y enviar alertas auton

Referencia normativa: NIST SP 800-53 Rev.5 IR-5, ISO 27002:2022 5.22, DISA STIG APP3540

Prioridad: Alta

Justificacion: Permite detectar y reaccionar rápidamente ante incidentes que comprometan la operación clínica.

Metodo validacion: Revisión de la plataforma de monitoreo, simulación de alerta y verificación de notificación.

Dependencias exclusiones: Complementa SIR-012 y SIR-054.

Categoria: Infrastructure Monitoring, Fault Detection

Ejemplo practico: Sistema Prometheus + Grafana con alertas vía Slack o Telegram a responsables de soporte 24/7.

SIR-064: El sistema debe garantizar la trazabilidad completa de todas las modificaciones realizadas sobre registros clí

Referencia normativa: ISO 27799:2016 8.3, NIST AU-3, HIPAA §164.312(b)

Prioridad: Alta

Justificacion: Permite auditoría clínica, análisis forense y control de calidad en registros de salud electrónicos (ePHI).

Metodo validacion: Verificación del log de auditoría detallado en los cambios sobre historias clínicas.

Dependencias exclusiones: Relacionado con SIR-006 (auditoría) y SIR-012 (monitorización de accesos).

Categoria: Auditability, Data Governance

Ejemplo practico: El sistema registra automáticamente que el Dr. López modificó el diagnóstico de un paciente el 10/04/2025 a las 16:45h, con detalle del campo alterado.

SIR-065: El sistema debe aplicar controles automáticos de integridad que validen que los datos clínicos almacenados n

Referencia normativa: ISO 27002:2022 8.16, NIST SI-7(1), HIPAA §164.312(c)(1)

Prioridad: Alta

Justificacion: Preserva la confiabilidad médica de los datos clínicos frente a errores, corrupción o ataques.

Metodo validacion: Verificación de uso de checksums, firmas digitales o registros hash sobre la ePHI.

Dependencias exclusiones: Requiere mecanismos criptográficos definidos en SIR-016.

Categoria: Integrity Monitoring, Data Protection

Ejemplo practico: Al guardar un resultado de laboratorio, el sistema genera automáticamente un hash y lo comprueba al recuperar el dato para detectar alteraciones.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-066: Debe establecerse un modelo de gobierno de datos que defina responsables, procesos de validación y contro

Referencia normativa: ISO 27799:2016 7.3, ISO 27002:2022 5.9, NIST PM-1

Prioridad: Media

Justificacion: Establece roles claros y controles sobre el ciclo de vida de los datos clínicos, promoviendo consistencia y confiabilidad.

Metodo validacion: Revisión de la política de gobierno de datos y existencia de comité o responsables asignados.

Dependencias exclusiones: Complementa SIR-001 y SIR-064.

Categoria: Data Stewardship, Governance Framework

Ejemplo practico: El Comité de Gobernanza de Datos valida mensualmente los indicadores de completitud y duplicados en los datos de pacientes.

SIR-067: Los datos clínicos deben estar sujetos a reglas de validación semántica y estructural antes de su persistencia

Referencia normativa: ISO 27799:2016 7.5, NIST SI-10, OWASP A08:2021

Prioridad: Alta

Justificacion: Evita que se almacenen registros con incoherencias clínicas, errores de formato o duplicidades.

Metodo validacion: Revisión de validadores automáticos implementados y testing con datos erróneos.

Dependencias exclusiones: Complementa requisitos de desarrollo seguro (SIR-028).

Categoria: Data Validation, Clinical Integrity

Ejemplo practico: El sistema impide guardar una prescripción con dosis negativa o edad inconsistente con la fecha de nacimiento registrada.

SIR-068: El sistema debe conservar los registros clínicos íntegros, completos y accesibles durante el tiempo legalmen

Referencia normativa: HIPAA §164.316(b)(2)(i), ISO 27799:2016 8.3.5, ISO 27002:2022 5.27

Prioridad: Alta

Justificacion: Asegura la disponibilidad legal, clínica y operativa de los datos de pacientes ante auditorías o tratamientos futuros.

Metodo validacion: Validación de políticas de retención y configuración de almacenamiento con acceso controlado y resiliencia.

Dependencias exclusiones: Relacionado con SIR-007 (backups) y SIR-055 (retención de logs).

Categoria: Data Retention, Legal Compliance

Ejemplo practico: El sistema conserva durante 10 años los historiales clínicos completos, accesibles bajo autenticación robusta y con mecanismos de archivo WORM.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-069: El sistema debe contar con soluciones antimalware actualizadas en todos los servidores y estaciones de trab

Referencia normativa: ISO 27002:2022 8.7, NIST SI-3, HIPAA §164.308(a)(5)(ii)(B)

Prioridad: Alta

Justificacion: Previene la infección por software malicioso que pueda comprometer la ePHI, afectar la disponibilidad del sistema o propagar ransomware.

Metodo validacion: Inspección de agentes antimalware instalados, políticas de actualización automática y reportes de eventos.

Dependencias exclusiones: Requiere políticas de protección de endpoint (SIR-050).

Categoria: Malware Protection, Endpoint Defense

Ejemplo practico: Uso de Microsoft Defender for Endpoint o Sophos Intercept X en servidores de OpenEMR con alertas centralizadas.

SIR-070: Debe implementarse un sistema de detección de intrusos (IDS) para monitorear tráfico y alertar sobre patrone

Referencia normativa: NIST SI-4, ISO 27002:2022 5.22, DISA STIG APP3540

Prioridad: Alta

Justificacion: Permite detectar ataques automatizados, escaneos y explotación de vulnerabilidades de forma proactiva.

Metodo validacion: Verificación de sensores IDS activos, reglas de detección y pruebas de escaneo controlado.

Dependencias exclusiones: Relacionado con SIR-012 (monitoreo) y SIR-057 (correlación en SIEM).

Categoria: Intrusion Detection, Network Monitoring

Ejemplo practico: Snort o Suricata desplegados en la capa de red con envío de eventos a un sistema SIEM.

SIR-071: Los servidores deben contar con capacidades EDR (Endpoint Detection and Response) que permitan análisis

Referencia normativa: NIST SP 800-94, ISO 27002:2022 8.7.4

Prioridad: Alta

Justificacion: Aumenta la capacidad de respuesta ante amenazas avanzadas que evaden los controles tradicionales.

Metodo validacion: Verificación de solución EDR desplegada y pruebas de simulación de actividad sospechosa.

Dependencias exclusiones: Complementa SIR-069.

Categoria: EDR, Behavioral Analysis

Ejemplo practico: CrowdStrike detecta ejecución de script inusual en servidor PHP y aísla automáticamente el endpoint.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-072: El sistema debe bloquear automáticamente direcciones IP que generen patrones de ataque automatizado com

Referencia normativa: OWASP A07:2021, NIST AC-7, ISO 27002:2022 5.17.6

Prioridad: Alta

Justificacion: Reduce el riesgo de intrusión por automatismos y herramientas de ataque de bajo costo.

Metodo validacion: Revisión de políticas de bloqueo (firewall o WAF) y pruebas de escaneo simuladas.

Dependencias exclusiones: Relacionado con SIR-042 (intentos fallidos de acceso).

Categoria: Brute Force Protection, Automated Threats

Ejemplo practico: Fail2ban bloquea una IP tras 5 intentos fallidos de autenticación en el frontend de OpenEMR.

SIR-073: Los archivos adjuntos y cargas de datos en OpenEMR deben ser escaneados por antivirus antes de almacena

Referencia normativa: ISO 27002:2022 8.7.2, HIPAA §164.308(a)(5)(ii)(B)

Prioridad: Media

Justificacion: Evita la introducción de malware a través de documentos adjuntos o ficheros subidos por usuarios internos o externos.

Metodo validacion: Revisión de configuración de escaneo en gateway o backend, y pruebas con archivos de prueba como EICAR.

Dependencias exclusiones: Relacionado con SIR-069.

Categoria: Malicious File Upload, Content Inspection

Ejemplo practico: OpenEMR envía los archivos PDF adjuntos por médicos a un antivirus ClamAV antes de almacenarlos en el sistema.

SIR-074: Se debe mantener un Software Bill of Materials (SBOM) actualizado con todas las bibliotecas, dependencias y

Referencia normativa: NIST SP 800-218, ISO 27002:2022 5.20, Executive Order 14028 (EEUU)

Prioridad: Alta

Justificacion: Permite identificar rápidamente componentes afectados por vulnerabilidades conocidas (p. ej., CVEs), mejorando la gestión del riesgo.

Metodo validacion: Generación automatizada de SBOM con herramientas como Syft o CycloneDX + validación en repositorio CI/CD.

Dependencias exclusiones: Relacionado con SIR-028 (ciclo de desarrollo seguro).

Categoria: Software Supply Chain, Component Inventory

Ejemplo practico: Integración de generación SBOM con Syft en cada build de contenedor Docker que incluya PHP/MySQL/JS de OpenEMR.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-075: Todos los paquetes, bibliotecas y artefactos de terceros utilizados deben verificarse mediante firma digital an

Referencia normativa: NIST SP 800-218 §5.2, ISO 27002:2022 8.8.4

Prioridad: Alta

Justificacion: Previene ataques por inyección de código malicioso en dependencias (ej. supply chain attacks como SolarWinds o log4j).

Metodo validacion: Revisión automatizada de firma o hash SHA-256 en pipeline CI/CD antes de permitir despliegue.

Dependencias exclusiones: Complementa SIR-074 y SIR-028.

Categoria: Package Verification, Supply Chain Integrity

Ejemplo practico: Rechazo automático de paquetes sin firma GPG válida al momento del build en GitLab CI.

SIR-076: Se debe contar con un proceso automatizado de detección de vulnerabilidades en dependencias de software

Referencia normativa: OWASP A06:2021, NIST SP 800-40 Rev.3, ISO 27002:2022 8.9.2

Prioridad: Alta

Justificacion: Reduce la exposición a vulnerabilidades conocidas mediante escaneo proactivo en bibliotecas integradas.

Metodo validacion: Uso de escáneres SCA (Software Composition Analysis) como Snyk, Grype o Trivy con reportes periódicos.

Dependencias exclusiones: Relacionado con SIR-074 y SIR-005.

Categoria: Vulnerability Scanning, Component Risk Management

Ejemplo practico: Trivy escanea cada imagen Docker y alerta sobre CVEs activos en las librerías del backend OpenEMR (p. ej., phpMyAdmin, Slim).

SIR-079: El acceso físico a las salas de servidores o centros de datos donde se almacena o procesa ePHI debe estar re

Referencia normativa: ISO 27002:2022 7.4, HIPAA §164.310(a)(1), NIST PE-3

Prioridad: Alta

Justificacion: Evita el acceso no autorizado a los sistemas físicos que contienen datos sensibles o respaldos críticos.

Metodo validacion: Inspección de registros de control de acceso físico, validación de mecanismos biométricos, tarjetas, cerraduras electrónicas.

Dependencias exclusiones: Relacionado con SIR-002 (control lógico de acceso) y SIR-010 (backups físicos).

Categoria: Physical Access Control, Environmental Security

Ejemplo practico: Acceso al cuarto de servidores mediante tarjeta RFID y validación biométrica, con registro de cada ingreso y salida.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-077: Todo software de terceros embebido debe tener una evaluación de seguridad previa antes de ser aprobado pa

Referencia normativa: ISO 27002:2022 5.19, NIST SA-12, Canada Health Infoway Req. 38

Prioridad: Media

Justificacion: Garantiza que los componentes externos cumplen los requisitos de seguridad y no introducen riesgos ocultos.

Metodo validacion: Checklist de revisión de software de terceros, revisión de licencias y resultado de análisis de vulnerabilidades.

Dependencias exclusiones: Complementa procesos de adquisición definidos en SIR-034.

Categoria: Third-Party Risk Management, Procurement Control

Ejemplo practico: Antes de integrar una nueva librería de facturación, se realiza un análisis estático con SonarQube y revisión de licencia GPL.

SIR-078: El sistema debe registrar todos los componentes de software externos en un inventario centralizado con meta

Referencia normativa: ISO 27002:2022 5.20.3, NIST CM-8, SPDX Specification v2.3

Prioridad: Media

Justificacion: Facilita la trazabilidad, auditoría de licencias y respuesta ante incidentes en la cadena de suministro.

Metodo validacion: Revisión del inventario de componentes y validación cruzada con el SBOM generado.

Dependencias exclusiones: Relacionado con SIR-074.

Categoria: Component Inventory, License Compliance

Ejemplo practico: Cada módulo importado se registra en un repositorio Git central con su SPDX, versión y condiciones de licencia.

SIR-080: Los equipos que contienen ePHI deben estar protegidos contra daños físicos por agua, fuego, humedad o sob

Referencia normativa: ISO 27002:2022 7.9, ISO 27799:2016 8.3.3, NIST PE-10

Prioridad: Alta

Justificacion: Minimiza el riesgo de pérdida de disponibilidad o integridad debido a fallos ambientales.

Metodo validacion: Revisión de infraestructura con sensores de temperatura, humedad, humo e instalación de UPS o detectores.

Dependencias exclusiones: Complementa requisitos de continuidad (SIR-062).

Categoria: Environmental Protection, Infrastructure Safeguards

Ejemplo practico: Uso de sensores IoT para monitoreo de humedad y temperatura, junto a extintores automáticos y alimentación eléctrica redundante.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-081: Debe mantenerse una política de zonas seguras con delimitación de áreas restringidas para equipos, redes y

Referencia normativa: ISO 27002:2022 7.5, NIST PE-5, HIPAA §164.310(a)(2)(iii)

Prioridad: Media

Justificacion: Reduce la exposición innecesaria de infraestructura crítica y facilita auditoría física.

Metodo validacion: Planos de zonas seguras, registro de autorización y cartelería física en áreas restringidas.

Dependencias exclusiones: Relacionado con SIR-079 y SIR-010.

Categoria: Secure Areas, Physical Zoning

Ejemplo practico: Delimitación de zona de respaldo físico y zona de comunicaciones con acceso solo al personal autorizado y cámaras de vigilancia.

SIR-082: Todo acceso físico debe registrarse, conservarse al menos por 1 año y estar disponible para auditoría en cas

Referencia normativa: ISO 27002:2022 7.4.3, NIST PE-6, Canada Health Infoway Req. 23

Prioridad: Media

Justificacion: Permite detectar accesos no autorizados, investigar incidentes y validar cumplimiento normativo.

Metodo validacion: Revisión de bitácoras físicas o electrónicas de acceso (logs, cámaras, tarjetas).

Dependencias exclusiones: Complementa SIR-079 y SIR-055.

Categoria: Physical Audit Trails, Access Logging

Ejemplo practico: Registro electrónico de entradas al centro de datos almacenado en sistema SIEM por 18 meses.

SIR-083: El sistema debe contar con políticas de ubicación segura y disposición controlada de dispositivos obsoletos

Referencia normativa: ISO 27002:2022 8.10.5, HIPAA §164.310(d)(2)(i)

Prioridad: Alta

Justificacion: Evita exposición de datos clínicos al retirar o desechar discos duros, medios de respaldo o terminales descontinuadas.

Metodo validacion: Revisión del procedimiento de baja de activos y evidencia de destrucción certificada o borrado seguro (wipe).

Dependencias exclusiones: Complementa SIR-036 y SIR-037.

Categoria: Asset Disposal, Data Remanence Protection

Ejemplo practico: Retiro de discos antiguos mediante protocolo de destrucción física con proveedor certificado, incluyendo número de serie y certificado.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-084: Toda API expuesta por OpenEMR debe requerir autenticación robusta basada en tokens seguros (OAuth 2.0, O

Referencia normativa: OWASP API1:2023, NIST AC-17, ISO 27002:2022 8.3.1

Prioridad: Alta

Justificacion: Previene el acceso anónimo o no autorizado a servicios críticos y datos ePHI.

Metodo validacion: Pruebas de acceso a endpoints sin token y validación de flujo de autorización OAuth2.

Dependencias exclusiones: Relacionado con SIR-002 (autenticación) y SIR-040 (sesiones).

Categoria: Authentication and Authorization for APIs

Ejemplo practico: Un cliente FHIR debe obtener previamente un token OAuth2 válido antes de invocar /Patient o /Observation.

SIR-085: Los tokens de acceso a APIs deben ser de corta duración (máximo 1 hora) y renovables mediante mecanismo

Referencia normativa: OWASP API2:2023, NIST SP 800-63B

Prioridad: Alta

Justificacion: Minimiza el riesgo en caso de robo o filtración de tokens de acceso.

Metodo validacion: Verificación de tiempos de expiración y rotación de tokens en la configuración del servidor de autorización.

Dependencias exclusiones: Complementa SIR-084.

Categoria: Token Management, API Session Security

Ejemplo practico: El token JWT emitido por el Authorization Server expira en 45 minutos y requiere refresh token para extender la sesión.

SIR-087: Cada endpoint de API debe validar estrictamente el formato, tipo y tamaño de todos los parámetros de entrad

Referencia normativa: OWASP API8:2023, NIST SI-10, ISO 27002:2022 8.12

Prioridad: Alta

Justificacion: Previene vulnerabilidades como SQL Injection, Command Injection y corrupción de datos clínicos.

Metodo validacion: Revisión de esquemas de validación (JSON Schema, XML Schema) y fuzz testing.

Dependencias exclusiones: Relacionado con SIR-028 (input validation general).

Categoria: Input Validation, API Security

Ejemplo practico: El endpoint /Patient no permite enviar IDs fuera del patrón regex especificado y rechaza campos inesperados.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-088: Debe implementarse un control de límite de tasa (Rate Limiting) por cliente API para evitar abusos y ataques d

Referencia normativa: OWASP API4:2023, NIST SC-5, ISO 27002:2022 8.4.2

Prioridad: Alta

Justificacion: Mitiga ataques de fuerza bruta, scraping masivo y abuso de recursos.

Metodo validacion: Pruebas de envío masivo de peticiones (> umbral) y verificación de respuestas 429 Too Many Requests.

Dependencias exclusiones: Complementa SIR-057 (SIEM correlación de anomalías).

Categoria: Rate Limiting, API Resource Protection

Ejemplo practico: Se configura un límite de 100 solicitudes/minuto por IP para la API de citas médicas de OpenEMR.

SIR-089: Debe existir un mecanismo de escaneo y auditoría automática de vulnerabilidades en las APIs expuestas de O

Referencia normativa: OWASP API6:2023, NIST RA-5, ISO 27002:2022 8.8.5

Prioridad: Alta

Justificacion: Permite detectar nuevas vulnerabilidades en interfaces de programación de forma proactiva.

Metodo validacion: Integración de escáneres de API security (p.ej., OWASP ZAP, Burp Suite Enterprise) en el pipeline CI/CD.

Dependencias exclusiones: Complementa procesos de análisis de vulnerabilidades SIR-005.

Categoria: API Vulnerability Management, Threat Detection

Ejemplo practico: Cada nuevo despliegue de OpenEMR ejecuta automáticamente un escaneo de seguridad sobre los endpoints /Patient, /Encounter, etc.

SIR-090: Todos los datos clínicos (ePHI) almacenados en servicios en la nube deben cifrarse en reposo mediante clave

Referencia normativa: ISO 27002:2022 8.10, NIST SC-12, HIPAA §164.312(a)(2)(iv)

Prioridad: Alta

Justificacion: Protege la confidencialidad de datos en reposo ante accesos no autorizados o errores de configuración en almacenamiento cloud.

Metodo validacion: Verificación de configuración de cifrado en S3, RDS y EBS con KMS y claves propias.

Dependencias exclusiones: Relacionado con SIR-016 (cifrado) y SIR-061 (backups cloud).

Categoria: Cloud Data Protection, Encryption at Rest

Ejemplo practico: Bucket S3 que contiene archivos PDF clínicos tiene habilitado cifrado AES-256 con clave KMS administrada por la organización.

Catálogo de Requisitos de Seguridad y Privacidad

SIR-091: Los buckets de almacenamiento (S3) no deben estar expuestos públicamente y deben tener políticas de acces

Referencia normativa: CIS AWS Benchmark 2.1, ISO 27002:2022 5.18, NIST AC-6

Prioridad: Alta

Justificacion: Previene fugas de datos clínicas debido a errores comunes de configuración en objetos en la nube.

Metodo validacion: Revisión de políticas de bucket y uso de herramientas como AWS Config, Prowler o ScoutSuite.

Dependencias exclusiones: Relacionado con SIR-001 (RBAC) y SIR-090 (cifrado).

Categoria: Cloud Storage Access Control, Least Privilege

Ejemplo practico: El bucket con datos de laboratorio tiene una política que solo permite lectura desde instancias EC2 autenticadas por IAM Role clínico.

SIR-092: El acceso a la consola de gestión cloud debe estar protegido mediante autenticación multifactor obligatoria (M

Referencia normativa: NIST IA-2(1), ISO 27002:2022 5.17, CIS AWS Benchmark 1.1

Prioridad: Alta

Justificacion: Evita el acceso no autorizado a la administración de recursos críticos en la nube, incluso en caso de fuga de credenciales.

Metodo validacion: Revisión de políticas IAM y configuración de MFA para root y usuarios con privilegios elevados.

Dependencias exclusiones: Relacionado con SIR-002 (autenticación).

Categoria: Cloud Console Security, MFA Enforcement

Ejemplo practico: La cuenta de administración AWS requiere autenticación con Yubikey o aplicación OTP para ingresar al panel de control.

SIR-093: Los recursos en la nube deben utilizar roles IAM específicos para cada función, evitando credenciales estática

Referencia normativa: NIST AC-6(10), ISO 27002:2022 5.18, OWASP Cloud-Native Top 10 A05

Prioridad: Alta

Justificacion: Reduce el riesgo de uso indebido de credenciales embebidas, minimiza superficie de ataque y fortalece trazabilidad.

Metodo validacion: Revisión de código fuente, pipelines y configuración de IAM roles por servicio.

Dependencias exclusiones: Complementa SIR-001 (RBAC) y SIR-025 (seguridad en CI/CD).

Categoria: IAM Roles, Cloud Identity Segregation

Ejemplo practico: Un pod de Kubernetes utiliza ServiceAccount con IAM Role asociado que permite acceso temporal a DynamoDB,

sin claves embebidas.

SIR-094: Todo tráfico entre componentes desplegados en la nube debe ser cifrado en tránsito utilizando TLS 1.2 o sup

Referencia normativa: ISO 27002:2022 8.4, NIST SC-12, HIPAA §164.312(e)(1)

Prioridad: Alta

Justificacion: Evita el espionaje de datos clínicos en tránsito, incluso dentro de entornos virtualizados que pueden ser compartidos.

Metodo validacion: Inspección de configuración de Load Balancer, certificados TLS, y política de comunicación VPC-to-VPC.

Dependencias exclusiones: Relacionado con SIR-086 (TLS general).

Categoria: Cloud Network Encryption, Internal Traffic Protection

Ejemplo practico: El balanceador de carga TLS ofusca el tráfico entre dos zonas de OpenEMR desplegadas en regiones distintas de AWS.

SIR-095: Debe activarse el logging centralizado de auditoría en servicios cloud (ej. AWS CloudTrail) y enviarse a un rep

Referencia normativa: NIST AU-2, ISO 27002:2022 5.22, DISA STIG Cloud Logging

Prioridad: Alta

Justificacion: Permite detectar, rastrear y responder ante actividades sospechosas o violaciones en recursos cloud.

Metodo validacion: Revisión de configuración de CloudTrail, validación de envío a bucket S3 WORM o integración con SIEM.

Dependencias exclusiones: Relacionado con SIR-054 (auditoría).

Categoria: Cloud Logging, Auditability, SIEM Integration

Ejemplo practico: Todas las acciones IAM y acceso a datos en AWS se registran en CloudTrail y se almacenan 12 meses con retención legal.

SIR-096: Las imágenes de contenedor utilizadas deben provenir de repositorios de confianza y ser escaneadas automá

Referencia normativa: NIST SP 800-190 Control 2.1, CIS Docker Benchmark 5.1

Prioridad: Alta

Justificacion: Previene el uso de imágenes contaminadas o comprometidas que puedan introducir vulnerabilidades en producción.

Metodo validacion: Integración de escaneo de imágenes (Trivy, Clair, Anchore) en pipelines CI/CD.

Dependencias exclusiones: Relacionado con SIR-076 (análisis de terceros) y SIR-005 (gestión de vulnerabilidades).

Categoria: Container Image Security, Supply Chain Integrity

Ejemplo practico: OpenEMR utiliza imágenes oficiales de PHP y MySQL validadas con Trivy antes de cada build en producción.

SIR-097: Se deben minimizar los privilegios de contenedores evitando el uso de contenedores privilegiados ('privileged

Referencia normativa: CIS Docker Benchmark 5.28, NIST SP 800-190 Control 3.1

Prioridad: Alta

Justificacion: Minimiza el impacto de compromisos permitiendo defensa en profundidad y evitando escaladas de privilegios.

Metodo validacion: Revisión de Dockerfiles y manifiestos de Kubernetes (PodSecurity Standards, PSPs o OPA policies).

Dependencias exclusiones: Relacionado con SIR-093 (IAM Roles).

Categoria: Container Runtime Security, Principle of Least Privilege

Ejemplo practico: Los pods de OpenEMR en Kubernetes ejecutan procesos como usuarios UID >10000 y sin capacidades de escalado de privilegios.

SIR-098: Todo acceso a la API Server de Kubernetes debe estar autenticado y autorizado estrictamente, registrando to

Referencia normativa: DISA Kubernetes STIG K8S-1, NIST AC-17, ISO 27002:2022 5.16

Prioridad: Alta

Justificacion: Controla el acceso administrativo sobre clústeres, evitando accesos no autorizados o acciones maliciosas.

Metodo validacion: Revisión de configuración RBAC, habilitación de Audit Logs, uso de cert-manager o políticas OIDC.

Dependencias exclusiones: Relacionado con SIR-002 (identidad), SIR-054 (auditoría).

Categoria: Kubernetes API Access Control, Audit Logging

Ejemplo practico: El API Server de Kubernetes OpenEMR utiliza OIDC federado con el proveedor corporativo de identidad y tiene RBAC estricto por namespace.

SIR-099: Las políticas de red (Network Policies) deben ser aplicadas para restringir la comunicación entre pods solame

Referencia normativa: NIST SP 800-190 Control 5.2, CIS Kubernetes Benchmark 5.2

Prioridad: Alta

Justificacion: Reduce la superficie de ataque lateral dentro del clúster en caso de compromiso de un pod.

Metodo validacion: Inspección de políticas de red aplicadas en namespaces y pruebas de conectividad entre pods no permitidos.

Dependencias exclusiones: Relacionado con SIR-094 (protección tráfico interno).

Categoria: Pod Network Segmentation, East-West Traffic Control

Ejemplo practico: Solo los pods de frontend OpenEMR pueden comunicarse hacia los pods de backend sobre puerto 3306/TCP.

SIR-100: Se debe habilitar y configurar correctamente mecanismos de aislamiento de namespaces, runtime security y c

Referencia normativa: DISA Kubernetes STIG K8S-3, NIST SP 800-190 Control 6.2

Prioridad: Alta

Justificacion: Previene ejecuciones no autorizadas, refuerza control de despliegue y mejora seguridad de clúster general.

Metodo validacion: Revisión de controladores habilitados (p.ej., PodSecurityAdmission, OPA/Gatekeeper), pruebas de políticas de admisión.

Dependencias exclusiones: Relacionado con SIR-028 (ciclo de desarrollo seguro).

Categoria: Kubernetes Admission Control, Cluster Hardening

Ejemplo practico: OpenEMR en Kubernetes utiliza Gatekeeper para aplicar políticas que bloquean despliegues con imágenes sin firmas válidas.

SIR-101: Se deben realizar copias de seguridad completas, automáticas y frecuentes de toda la ePHI, y estas deben alm

Referencia normativa: NIST SP 1800-25, ISO 27002:2022 8.13, HIPAA §164.308(a)(7)

Prioridad: Alta

Justificacion: Permite recuperar datos íntegros ante ataques de cifrado malicioso que comprometan los datos en producción.

Metodo validacion: Verificación de políticas de backup + evidencia técnica de WORM activado en almacenamiento de respaldo.

Dependencias exclusiones: Relacionado con SIR-010 (backups generales) y SIR-061 (replicación).

Categoria: Backup Protection, Ransomware Resilience

Ejemplo practico: Backups automáticos diarios en S3 Glacier con políticas de retención inmutable de 30 días.

SIR-102: Los entornos de respaldo y almacenamiento de copias deben estar segmentados de la red principal de produ

Referencia normativa: NIST SC-7(8), ISO 27002:2022 8.9.5

Prioridad: Alta

Justificacion: Evita que el ransomware cifre simultáneamente el entorno de producción y sus respaldos conectados.

Metodo validacion: Inspección de reglas de firewall, segmentación de red y rutas de acceso entre zonas.

Dependencias exclusiones: Relacionado con SIR-099 (segmentación de red).

Categoria: Network Isolation, Backup Segmentation

Ejemplo practico: Los servidores de respaldo están en una subred VPC separada sin conectividad de entrada desde instancias de frontend OpenEMR.

SIR-103: Debe implementarse una solución de protección contra ransomware en endpoints, servidores y cargas cloud

Referencia normativa: NIST SI-4(1), ISO 27002:2022 8.7.4

Prioridad: Alta

Justificacion: Detecta y bloquea patrones de cifrado masivo o acceso sospechoso a múltiples archivos clínicos.

Metodo validacion: Simulación de patrones de ransomware y análisis de respuesta automática (alertas, aislamiento de proceso).

Dependencias exclusiones: Relacionado con SIR-071 (EDR general).

Categoria: Endpoint Defense, Ransomware Detection

Ejemplo practico: CrowdStrike detecta múltiples renombrados de archivos .csv por parte de un proceso y detiene automáticamente su ejecución.

SIR-104: Debe configurarse una política de listas blancas de ejecución que limite los binarios y scripts permitidos en e

Referencia normativa: NIST SI-7(7), DISA STIG APP3530

Prioridad: Alta

Justificacion: Reduce la posibilidad de que código malicioso o no autorizado pueda ejecutarse dentro del sistema.

Metodo validacion: Revisión de configuración de AppLocker, SELinux o mecanismos equivalentes en servidores OpenEMR.

Dependencias exclusiones: Relacionado con SIR-069 (antimalware) y SIR-097 (privilegios mínimos en contenedores).

Categoria: Application Whitelisting, Execution Control

Ejemplo practico: El servidor de OpenEMR sólo permite ejecución de binarios en /usr/bin validados, bloqueando scripts desconocidos automáticamente.

SIR-105: El sistema debe enviar alertas en tiempo real al detectar patrones compatibles con ataques de ransomware, c

Referencia normativa: NIST IR-5, ISO 27002:2022 5.22, OWASP A09:2021

Prioridad: Alta

Justificacion: Permite una respuesta inmediata y reduce el alcance del cifrado automático.

Metodo validacion: Simulación de actividad ransomware-like y verificación de alerta generada en el SIEM o sistema de detección.

Dependencias exclusiones: Relacionado con SIR-057 (detección de anomalías).

Categoria: SIEM Correlation, Anomaly Detection

Ejemplo practico: SIEM detecta que un proceso ha accedido a 10.000 archivos en 5 minutos y envía alerta crítica al equipo de ciberseguridad.

SIR-106: El sistema debe limitar el número de cuentas con privilegios administrativos y definir roles separados para ge

Referencia normativa: ISO 27002:2022 5.18, NIST AC-6, HIPAA §164.312(a)

Prioridad: Alta

Justificacion: Reduce el riesgo de abuso de privilegios o errores administrativos al aplicar el principio de mínimo privilegio.

Metodo validacion: Revisión de roles en el sistema de gestión de usuarios e inspección de uso de cuentas admin.

Dependencias exclusiones: Relacionado con SIR-001 (RBAC general).

Categoria: Privileged Access Control, Role Separation

Ejemplo practico: El sistema separa el rol de 'Administrador del sistema' del 'Auditor clínico' y 'Usuario médico'.

SIR-107: Todo uso de cuentas con privilegios elevados debe ser registrado con auditoría detallada, incluyendo hora, a

Referencia normativa: NIST AU-2, ISO 27002:2022 5.22, HIPAA §164.312(b)

Prioridad: Alta

Justificacion: Permite trazabilidad total sobre cambios críticos, facilitando la detección de accesos indebidos o acciones peligrosas.

Metodo validacion: Análisis de logs de eventos privilegiados y correlación con justificaciones/documentación de acceso.

Dependencias exclusiones: Complementa SIR-054 (auditoría general).

Categoria: Privileged Session Auditing, Accountability

Ejemplo practico: El acceso a la base de datos por un administrador para restaurar registros clínicos queda registrado con detalle del cambio y motivo clínico.

SIR-108: El sistema debe permitir el uso de cuentas de emergencia ('break-glass') con acceso temporal y controlado, a

Referencia normativa: HIPAA §164.312(a)(1), NIST AC-2(5), ISO 27002:2022 5.17.7

Prioridad: Alta

Justificacion: Permite garantizar la atención médica urgente sin comprometer las políticas estándar de acceso y seguridad.

Metodo validacion: Verificación de existencia de usuarios break-glass + logs de activación + evidencia de control posterior.

Dependencias exclusiones: Relacionado con SIR-040 (sesiones) y SIR-002 (autenticación).

Categoria: Emergency Access Management, Clinical Override

Ejemplo practico: Ante un fallo de red o sistema SSO, se permite acceso con una cuenta de emergencia a través de MFA + log firmado del evento.

SIR-109: Debe realizarse una revisión periódica (al menos trimestral) de las cuentas con privilegios administrativos par

Referencia normativa: NIST AC-2(3), ISO 27002:2022 5.20.3

Prioridad: Media

Justificacion: Evita la acumulación de cuentas elevadas innecesarias y permite revocar accesos obsoletos.

Metodo validacion: Informe de revisión de cuentas privilegiadas firmado por el responsable de seguridad.

Dependencias exclusiones: Complementa SIR-106.

Categoria: Access Review, Privilege Governance

Ejemplo practico: La cuenta admin otorgada a un proveedor temporal fue desactivada tras revisión trimestral al comprobar su inactividad por 45 días.

SIR-110: Las credenciales de cuentas privilegiadas deben almacenarse y rotarse de forma automática mediante soluci

Referencia normativa: NIST IA-5, ISO 27002:2022 8.3.5

Prioridad: Alta

Justificacion: Evita filtraciones o reutilización indebida de credenciales sensibles en entornos clínicos críticos.

Metodo validacion: Inspección de uso de herramientas como HashiCorp Vault, CyberArk o AWS Secrets Manager.

Dependencias exclusiones: Relacionado con SIR-002 (credenciales).

Categoria: Credential Management, Secret Rotation

Ejemplo practico: Las contraseñas root de bases de datos clínicas se almacenan cifradas en CyberArk con rotación semanal automática.

SIR-111: El sistema debe garantizar que todo correo que contenga ePHI se transmita exclusivamente mediante canales

Referencia normativa: HIPAA §164.312(e)(1), ISO 27002:2022 8.4.1, NIST SP 800-52

Prioridad: Alta

Justificacion: Protege la confidencialidad de información clínica enviada por correo electrónico durante la transmisión.

Metodo validacion: Análisis de configuración SMTP, uso de STARTTLS obligatorio y pruebas con herramientas como checktls.com.

Dependencias exclusiones: Relacionado con SIR-086 (cifrado en tránsito general).

Categoria: Email Encryption, Transport Security

Ejemplo practico: Los informes de laboratorio enviados desde OpenEMR se transmiten vía SMTP seguro con STARTTLS activado y certificado válido.

SIR-112: Todo correo clínico debe estar protegido mediante mecanismos de autenticación de servidor como SPF, DKIM

Referencia normativa: NIST SP 800-45, ISO 27002:2022 8.11.4, CIS Controls v8 9.4

Prioridad: Alta

Justificacion: Evita el uso fraudulento de dominios clínicos para phishing o suplantación de identidad institucional.

Metodo validacion: Validación de registros DNS de SPF, DKIM y DMARC para los dominios de envío configurados.

Dependencias exclusiones: Complementa SIR-111.

Categoria: Email Authentication, Anti-Spoofing

Ejemplo practico: El dominio @openemrclinic.org tiene registros SPF/DKIM/DMARC activos y reportes de validación configurados.

SIR-113: El sistema debe permitir la detección y filtrado automático de correos con archivos adjuntos maliciosos o enl

Referencia normativa: ISO 27002:2022 8.7.3, NIST SI-3, HIPAA §164.308(a)(5)(ii)(B)

Prioridad: Alta

Justificacion: Evita infecciones por malware, ransomware y accesos maliciosos a través del canal de correo.

Metodo validacion: Pruebas con EICAR y enlaces simulados de phishing; revisión de filtros de gateway SMTP o solución MTA.

Dependencias exclusiones: Relacionado con SIR-069 (antimalware).

Categoria: Email Threat Protection, Content Filtering

Ejemplo practico: El gateway SMTP escanea los archivos adjuntos y bloquea cualquier ejecutable no firmado o archivo .js sospechoso.

SIR-114: Se debe proporcionar una alternativa segura para el intercambio de ePHI por correo mediante portales web co

Referencia normativa: HIPAA §164.312(e)(1), ISO 27002:2022 8.4.4

Prioridad: Media

Justificacion: Evita exponer información médica sensible incluso si el destinatario no soporta cifrado.

Metodo validacion: Revisión del sistema de mensajería segura o portales con acceso autenticado para pacientes o proveedores.

Dependencias exclusiones: Relacionado con SIR-041 (privacidad del paciente).

Categoria: Secure Messaging, Patient Communication

Ejemplo practico: OpenEMR genera un enlace único a un portal cifrado donde el paciente puede descargar su informe después de autenticarse.

SIR-115: Los logs de envío y recepción de correos clínicos relevantes deben ser auditables y conservarse durante al m

Referencia normativa: NIST AU-11, ISO 27002:2022 5.22, HIPAA §164.312(b)

Prioridad: Media

Justificacion: Permite rastrear incidentes, demostrar cumplimiento y responder ante incidentes de filtración o acceso indebido.

Metodo validacion: Revisión de registros SMTP o SIEM con logs de ID de mensaje, destinatario y timestamp.

Dependencias exclusiones: Relacionado con SIR-054 (logging).

Categoria: Email Logging and Auditability

Ejemplo practico: Cada mensaje enviado por el sistema genera un registro con asunto, destinatario y estado de entrega almacenado por 180 días.

SIR-116: Las bases de datos que almacenen ePHI deben estar cifradas en reposo utilizando mecanismos de cifrado rob

Referencia normativa: HIPAA §164.312(a)(2)(iv), ISO 27002:2022 8.10, NIST SC-12

Prioridad: Alta

Justificacion: Previene el acceso no autorizado a los datos clínicos incluso si se compromete el almacenamiento físico o virtual.

Metodo validacion: Inspección de configuración de cifrado en MySQL, RDS o motor de BBDD, validación de claves y algoritmo.

Dependencias exclusiones: Relacionado con SIR-016 (cifrado general).

Categoria: Database Encryption, ePHI Protection

Ejemplo practico: La base de datos MySQL de OpenEMR utiliza cifrado de tablas InnoDB mediante TDE y claves en AWS KMS.

SIR-117: El acceso a la base de datos debe estar restringido exclusivamente mediante usuarios autenticados y roles de

Referencia normativa: ISO 27002:2022 5.18, NIST AC-6, HIPAA §164.312(a)(1)

Prioridad: Alta

Justificacion: Evita accesos no trazables o generalizados que podrían manipular o exfiltrar registros clínicos.

Metodo validacion: Revisión de políticas de autenticación y existencia de cuentas con privilegios mínimos.

Dependencias exclusiones: Relacionado con SIR-001 (acceso lógico), SIR-106 (privilegios).

Categoria: Database Access Control, RBAC for Databases

Ejemplo practico: Solo el usuario 'openemr_app' puede conectarse a la base con permisos SELECT/INSERT específicos.

SIR-118: Todos los accesos y modificaciones a las bases de datos clínicas deben ser auditados con logs firmados o pr

Referencia normativa: HIPAA §164.312(b), ISO 27002:2022 5.22, NIST AU-2

Prioridad: Alta

Justificacion: Permite la trazabilidad completa y la detección de accesos indebidos o errores críticos.

Metodo validacion: Activación de log de auditoría binario o SQL + pruebas de integridad con hashing/cifrado.

Dependencias exclusiones: Relacionado con SIR-107 (auditoría de privilegios).

Categoria: Database Auditing, Integrity of Logs

Ejemplo practico: La auditoría de MySQL genera logs cifrados con firma digital y los envía a un SIEM para su verificación diaria.

SIR-119: Debe implementarse validación de integridad periódica sobre la base de datos clínica para detectar alteracion

Referencia normativa: ISO 27002:2022 8.16, NIST SI-7, HIPAA §164.312(c)(1)

Prioridad: Alta

Justificacion: Asegura que la información clínica no haya sido modificada, truncada o corrompida por errores o amenazas.

Metodo validacion: Revisión de scripts o procesos automáticos de verificación de checksums y registros hash.

Dependencias exclusiones: Relacionado con SIR-065 (integridad de datos).

Categoria: Database Integrity Checking, Anti-Tampering

Ejemplo practico: Un job diario verifica que los hashes SHA-256 de cada tabla coincidan con los almacenados en logs sellados.

SIR-120: Las instancias de base de datos deben estar protegidas mediante firewalls o grupos de seguridad que bloque

Referencia normativa: ISO 27002:2022 5.14, NIST SC-7, CIS MySQL Benchmark

Prioridad: Alta

Justificacion: Previene ataques de red (brute-force, SQL injection remota) y exposición de puertos críticos a internet.

Metodo validacion: Inspección de reglas de red (VPC, SG, IPTables) que aseguren restricción de acceso solo desde IPs permitidas.

Dependencias exclusiones: Relacionado con SIR-072 (protección por IP).

Categoria: Database Network Isolation, Firewalling

Ejemplo practico: El puerto 3306 de MySQL solo es accesible internamente por la subred de aplicaciones clínicas autenticadas.

SIR-121: [Opcional] Los modelos de IA clínica utilizados en decisiones deben ser trazables, incluyendo versión del mo

Referencia normativa: ISO 27002:2022 8.29, NIST SA-15(10)

Prioridad: Alta

Justificacion: Permite auditar y verificar la fiabilidad clínica de las decisiones algorítmicas.

Metodo validacion: Inspección de logs de predicción y almacenamiento de metadatos del modelo.

Dependencias exclusiones: Aplicable solo si se usan módulos de IA clínica.

Categoria: AI Model Traceability, Clinical Auditability

Ejemplo practico: Al registrar una predicción de riesgo, OpenEMR almacena que fue generada por el modelo 'risk-2025-v3' entrenado en enero.

SIR-122: [Opcional] Las decisiones automáticas asistidas por IA deben poder ser explicadas clínicamente en lenguaje

Referencia normativa: ISO 27002:2022 8.29, NIST RA-9

Prioridad: Media

Justificacion: Facilita la revisión humana informada, evita dependencia ciega del modelo y mejora confianza clínica.

Metodo validacion: Evaluación de la documentación o interfaz del sistema que muestre racional clínico o factores clave.

Dependencias exclusiones: Complementa SIR-121.

Categoria: Explainable AI, Clinical Transparency

Ejemplo practico: Un sistema de triaje muestra que la clasificación 'urgente' se basó en frecuencia cardíaca elevada y dificultad respiratoria detectada.

SIR-123: [Opcional] Las predicciones realizadas por motores de IA deben quedar registradas con marca de tiempo, usu

Referencia normativa: NIST AU-2, ISO 27002:2022 5.22, HIPAA §164.312(b)

Prioridad: Alta

Justificacion: Garantiza trazabilidad de recomendaciones clínicas para revisión o refutación en caso de error.

Metodo validacion: Verificación de logs clínicos con auditoría de predicciones y decisiones tomadas.

Dependencias exclusiones: Complementa SIR-121 y SIR-107.

Categoria: AI Prediction Logging, Accountability

Ejemplo practico: Se almacena que el modelo 'diabetes-risk-v2' recomendó intervención para el paciente 38219, revisado por el Dr. Pérez.

SIR-124: [Opcional] Los datos clínicos utilizados para entrenar o mejorar modelos de IA deben anonimizarse o seudon

Referencia normativa: ISO 27002:2022 8.11.3, HIPAA §164.514(b), NIST SP 800-53 PM-18

Prioridad: Alta

Justificacion: Evita exposición no justificada de ePHI en fases de entrenamiento o ajuste del modelo.

Metodo validacion: Verificación de que los datos exportados para IA no contienen identificadores directos ni indirectos.

Dependencias exclusiones: Relacionado con SIR-045 (minimización de datos).

Categoria: Data Minimization, Privacy-by-Design AI

Ejemplo practico: Los registros utilizados para refinar el modelo de detección de sepsis eliminan nombres, fechas y ubicaciones exactas.

SIR-125: [Opcional] Los modelos de IA deben someterse a validaciones periódicas para confirmar su precisión clínica

Referencia normativa: ISO 27002:2022 8.29.3, NIST SA-15(3)

Prioridad: Media

Justificacion: Evita que un modelo obsoleto siga operando con decisiones incorrectas que afecten al paciente.

Metodo validacion: Evidencia de evaluación periódica y métricas (precision, recall) frente a un set clínico de referencia.

Dependencias exclusiones: Complementa SIR-121.

Categoria: Model Monitoring, Clinical Accuracy Validation

Ejemplo practico: Cada 6 meses se evalúa el modelo de predicción de ECV usando registros validados y se documentan resultados.

SIR-126: Toda comunicación basada en HL7 FHIR debe realizarse exclusivamente a través de HTTPS (TLS 1.2 o superi

Referencia normativa: ISO 27002:2022 8.4.1, NIST SC-12, HIPAA §164.312(e)(1)

Prioridad: Alta

Justificacion: Protege la confidencialidad e integridad de la ePHI intercambiada entre sistemas interoperables.

Metodo validacion: Pruebas de conexión a endpoints FHIR con validación de TLS y rechazo de HTTP.

Dependencias exclusiones: Relacionado con SIR-086 (TLS general).

Catálogo de Requisitos de Seguridad y Privacidad

Categoria: FHIR Transport Layer Security, OWASP API A9

Ejemplo practico: El endpoint /fhir/Patient solo responde si se accede mediante conexión HTTPS con certificado válido CA.

SIR-127: El acceso a recursos FHIR debe requerir tokens con scopes definidos (OAuth 2.0) que limiten el acceso a los

Referencia normativa: NIST AC-17, ISO 27002:2022 5.18, SMART on FHIR

Prioridad: Alta

Justificacion: Aplica el principio de mínimo privilegio y protege recursos sensibles como Patient, Observation, Encounter.

Metodo validacion: Verificación de autorización por scope (p. ej., patient/*.read) y denegación de acceso sin token válido.

Dependencias exclusiones: Relacionado con SIR-084 (API auth).

Categoria: OAuth2 Scopes, FHIR Authorization

Ejemplo practico: Un token con scope 'patient/Observation.read' no puede acceder al recurso 'Patient.write'.

SIR-128: Cada transacción FHIR debe registrarse en logs auditables incluyendo ID de recurso accedido, tiempo, usuari

Referencia normativa: ISO 27002:2022 5.22, NIST AU-2, HIPAA §164.312(b)

Prioridad: Alta

Justificacion: Permite trazar el uso de APIs clínicamente sensibles y detectar usos indebidos o accesos masivos.

Metodo validacion: Inspección de logs de acceso FHIR en el servidor de OpenEMR y verificación de almacenamiento seguro.

Dependencias exclusiones: Relacionado con SIR-123 y SIR-054.

Categoria: FHIR Logging, API Auditing

Ejemplo practico: El log registra que el usuario 'externo@hospital.com' accedió al recurso /fhir/Patient/89213 a las 10:35 con app_id X.

SIR-129: Los parámetros de entrada a las APIs FHIR deben validarse estrictamente contra el perfil FHIR esperado y tam

Referencia normativa: OWASP API8:2023, ISO 27002:2022 8.12

Prioridad: Alta

Justificacion: Evita inyecciones, denegaciones de servicio por payloads extensos o malformaciones que comprometan el sistema.

Metodo validacion: Fuzzing de APIs FHIR, revisión de uso de librerías de validación HL7 estándar (p. ej., HAPI FHIR validator).

Dependencias exclusiones: Relacionado con SIR-087 (validación API general).

Categoria: Input Validation, FHIR Schema Compliance

Ejemplo practico: Se rechaza una carga FHIR con un 'Observation.valueQuantity' inválido o con campos no permitidos en el perfil implementado.

SIR-130: El sistema debe implementar limitación de tasas de acceso (rate limiting) por aplicación y usuario para endpo

Referencia normativa: OWASP API4:2023, NIST SC-5

Prioridad: Media

Justificacion: Evita abusos, scraping masivo de información sensible y ataques de denegación de servicio.

Metodo validacion: Pruebas de carga controlada y verificación de respuesta HTTP 429 al exceder umbral de peticiones.

Dependencias exclusiones: Relacionado con SIR-088 (rate limit general).

Categoria: Rate Limiting, API Resource Throttling

Ejemplo practico: Se limita a 60 peticiones por minuto por app_id; al superarlo se devuelve 429 y se registra intento excesivo.

SIR-131: Toda estación clínica o terminal físico que acceda a OpenEMR debe requerir autenticación individual del usua

Referencia normativa: HIPAA §164.310(a)(1), ISO 27002:2022 5.17.2, NIST AC-7

Prioridad: Alta

Justificacion: Evita accesos indebidos desde terminales compartidas o no supervisadas, protegiendo el acceso a ePHI.

Metodo validacion: Pruebas en estaciones de trabajo para verificar autenticación activa por usuario clínico.

Dependencias exclusiones: Relacionado con SIR-002 (acceso lógico).

Categoria: Workstation Access Control, Identity Enforcement

Ejemplo practico: Cada terminal en consulta requiere autenticación con usuario individual antes de acceder a OpenEMR, y se cierra automáticamente tras 5 minutos de inactividad.

SIR-132: Las estaciones clínicas deben bloquearse automáticamente tras un periodo definido de inactividad para preve

Referencia normativa: HIPAA §164.312(a)(2)(iii), ISO 27002:2022 5.17.6, DISA STIG

Prioridad: Alta

Justificacion: Reduce la posibilidad de exposición visual o manipulación de registros clínicos en entornos físicos compartidos.

Metodo validacion: Revisión de políticas de bloqueo de pantalla en estaciones y pruebas de inactividad.

Dependencias exclusiones: Relacionado con SIR-040 (sesiones).

Categoria: Session Timeout, Physical Endpoint Protection

Ejemplo practico: Después de 3 minutos sin actividad, el terminal clínico bloquea automáticamente la sesión y requiere reautenticación.

SIR-133: Las estaciones clínicas deben contar con mecanismos de protección antimanipulación física como anclajes, c

Referencia normativa: ISO 27002:2022 7.3, HIPAA §164.310(a)(2)(iii), NIST PE-3

Prioridad: Media

Justificacion: Evita que dispositivos sean robados, manipulados físicamente o usados como vía de ataque.

Metodo validacion: Inspección física de estaciones clínicas y validación de bloqueo de puertos USB no autorizados.

Dependencias exclusiones: Relacionado con SIR-079 (acceso físico).

Categoria: Endpoint Tamper Protection, Physical Security

Ejemplo practico: Estación de consulta anclada al escritorio, con BIOS bloqueada y puertos USB deshabilitados para prevenir conexión de medios extraíbles.

SIR-134: Debe instalarse software de gestión de endpoints (MDM/EDR) en todas las estaciones clínicas para control re

Referencia normativa: ISO 27002:2022 8.6.3, NIST CM-7, HIPAA §164.310(d)(1)

Prioridad: Alta

Justificacion: Permite monitorear y controlar estaciones clínicas, aplicar parches y responder a incidentes de forma centralizada.

Metodo validacion: Revisión de plataforma de gestión de endpoints y enrolamiento de estaciones.

Dependencias exclusiones: Relacionado con SIR-050 (gestión de dispositivos).

Categoria: Endpoint Management, Clinical Workstation Control

Ejemplo practico: Cada estación clínica tiene agente MDM que permite aplicar configuraciones de seguridad y borrar datos de forma remota en caso de pérdida.

SIR-135: Los dispositivos clínicos portátiles deben contar con cifrado completo de disco activado para prevenir pérdid

Referencia normativa: HIPAA §164.312(a)(2)(iv), ISO 27002:2022 8.10.3, NIST MP-5

Prioridad: Alta

Justificacion: Protege los datos almacenados localmente en portátiles o tablets usados en movilidad clínica.

Metodo validacion: Verificación de políticas de cifrado activo en sistemas operativos (BitLocker, FileVault, LUKS).

Dependencias exclusiones: Relacionado con SIR-015 (almacenamiento seguro).

Categoria: Full Disk Encryption, Mobile Endpoint Security

Ejemplo practico: La tablet del personal médico tiene activado cifrado LUKS, y requiere passphrase al encender.

SIR-136: Toda firma electrónica clínica debe estar asociada a una identidad verificada del firmante mediante un mecani

Referencia normativa: ISO 27002:2022 8.5.3, NIST IA-2, HIPAA §164.312(a)(1)

Prioridad: Alta

Justificacion: Garantiza que la firma corresponde a la persona autorizada, evitando suplantaciones.

Metodo validacion: Revisión de logs de firma con identidad única vinculada y uso de 2FA/MFA para confirmación.

Dependencias exclusiones: Relacionado con SIR-002 (autenticación) y SIR-084 (OAuth).

Categoria: Digital Signature Identity, Authentication Binding

Ejemplo practico: El médico que firma un consentimiento debe autenticarse con su token OTP antes de que se registre la firma.

SIR-137: Los documentos clínicos firmados deben contar con un mecanismo de validación criptográfica que garantice

Referencia normativa: ISO 27002:2022 8.3.5, HIPAA §164.312(c)(1)

Prioridad: Alta

Justificacion: Protege contra manipulaciones de documentos firmados como consentimientos, informes o recetas.

Metodo validacion: Verificación de integridad hash (p. ej., SHA-256) y comprobación de firma digital asociada.

Dependencias exclusiones: Relacionado con SIR-065 (integridad de ePHI).

Categoria: Document Integrity, Tamper Detection

Ejemplo practico: Cada receta firmada digitalmente contiene un sello hash y firma RSA que permite validar que no fue alterada.

SIR-138: Las firmas electrónicas deben registrar la fecha, hora, usuario firmante y contexto clínico en el que se genera

Referencia normativa: ISO 27002:2022 5.22, HIPAA §164.312(b), NIST AU-2

Prioridad: Alta

Justificacion: Asegura la trazabilidad y responsabilidad clínica ante auditorías o disputas legales.

Metodo validacion: Inspección de logs de firma asociados a los registros electrónicos firmados.

Dependencias exclusiones: Relacionado con SIR-107 (auditoría de privilegios).

Categoria: Signature Audit Trail, Clinical Accountability

Ejemplo practico: Al firmar un alta médica, el sistema registra: Dr. A. Pérez, 2025-05-02 11:22, motivo: alta postoperatoria.

SIR-139: Las firmas electrónicas clínicas deben estar protegidas contra reutilización o replicación en otros registros.

Referencia normativa: ISO 27002:2022 8.5.3, NIST SP 800-63B

Prioridad: Alta

Justificacion: Evita el uso fraudulento de firmas válidas en contextos distintos al original.

Metodo validacion: Verificación de unicidad y no transferibilidad de tokens de firma y restricciones por sesión.

Dependencias exclusiones: Relacionado con SIR-040 (sesión de usuario).

Categoria: Signature Replay Protection, Session Binding

Ejemplo practico: La firma digital emitida para un informe clínico no puede ser reutilizada para otro documento ni por otro usuario.

SIR-140: Debe permitirse la validación de firmas electrónicas incluso fuera del sistema OpenEMR, mediante verificació

Referencia normativa: ISO 27002:2022 8.5.3, NIST SA-4(7)

Prioridad: Media

Justificacion: Permite auditoría legal y validación de documentos firmados incluso por terceros o en contexto forense.

Metodo validacion: Revisión de mecanismos de exportación con firma XAdES/PAdES o certificados verificables.

Dependencias exclusiones: Complementa SIR-137.

Categoria: Signature Portability, Third-Party Verification

Ejemplo practico: Un consentimiento firmado digitalmente puede ser exportado como PDF con firma X.509 validable en Adobe Acrobat.

SIR-141: Se debe realizar una evaluación periódica de riesgos de seguridad sobre todos los activos que procesan o al

Referencia normativa: ISO 27002:2022 5.28, NIST RA-3, HIPAA §164.308(a)(1)(ii)(A)

Prioridad: Alta

Justificacion: Permite identificar nuevas amenazas, vulnerabilidades o impactos que comprometan la confidencialidad, integridad o disponibilidad de la ePHI.

Metodo validacion: Informe de evaluación de riesgos actualizado con evidencias de identificación, impacto y planes de tratamiento.

Dependencias exclusiones: Relacionado con SIR-062 (continuidad técnica).

Categoria: Risk Assessment, ePHI Exposure Management

Ejemplo practico: Cada 12 meses, el equipo de seguridad evalúa los riesgos del módulo de prescripción electrónica incluyendo nuevas dependencias.

SIR-142: Debe llevarse a cabo un Privacy Impact Assessment (PIA) ante cualquier nuevo tratamiento, módulo o integra

Referencia normativa: ISO 27002:2022 8.11.1, NIST PM-9, Canada Health Infoway Req. 16

Prioridad: Alta

Justificacion: Permite anticipar y mitigar riesgos para los derechos de los pacientes y su información personal.

Metodo validacion: Revisión documental del PIA realizado antes del despliegue de nuevos módulos, con evaluación de impacto legal y técnico.

Dependencias exclusiones: Relacionado con SIR-045 (minimización de datos).

Categoria: Privacy Impact Assessment, Data Protection

Ejemplo practico: Antes de integrar un nuevo sistema de telemedicina, se realiza un PIA para evaluar cómo se recopilan, almacenan y transfieren las videollamadas clínicas.

SIR-143: El sistema debe contar con una metodología definida para priorizar los riesgos detectados en función del imp

Referencia normativa: ISO 27005, NIST RA-2, HIPAA §164.308(a)(1)

Prioridad: Alta

Justificacion: Facilita decisiones de seguridad efectivas, asignación de recursos y remediación escalonada.

Metodo validacion: Verificación del uso de matriz de riesgo o metodología tipo OCTAVE, FAIR o similar aplicada a OpenEMR.

Dependencias exclusiones: Relacionado con SIR-141.

Categoria: Risk Prioritization, Impact Mapping

Ejemplo practico: Una vulnerabilidad en la API de resultados de laboratorio se clasifica como crítica por tener exposición externa y afectar integridad clínica.

SIR-144: La evaluación de riesgos debe actualizarse automáticamente o manualmente tras cualquier incidente de segu

Referencia normativa: ISO 27002:2022 5.28.2, NIST RA-4

Prioridad: Media

Justificacion: Garantiza que los riesgos emergentes se gestionen de forma reactiva tras eventos no previstos.

Metodo validacion: Verificación de que las evaluaciones se modificaron tras incidentes registrados en el SIEM o en el sistema de

tickets.

Dependencias exclusiones: Relacionado con SIR-105 (detección de ransomware) y SIR-057 (monitorización avanzada).

Categoria: Dynamic Risk Adjustment, Post-Incident Review

Ejemplo practico: Tras detectar un ataque a APIs FHIR, se actualiza el riesgo de exposición de datos clínicos remotos y se reevalúa la prioridad de mitigación.

SIR-145: Debe mantenerse evidencia documental de todas las evaluaciones de riesgos y decisiones asociadas durante

Referencia normativa: HIPAA §164.316(b), ISO 27002:2022 5.28.3

Prioridad: Media

Justificacion: Facilita auditorías, cumplimiento legal y análisis histórico de decisiones sobre seguridad clínica.

Metodo validacion: Auditoría de repositorio documental (con logs de versiones, decisiones tomadas y responsables).

Dependencias exclusiones: Relacionado con SIR-041 (derechos del paciente) y SIR-142 (PIA).

Categoria: Risk Documentation, Compliance Traceability

Ejemplo practico: El equipo de seguridad conserva los informes de evaluación de 2023 y 2024 en un sistema de gestión documental con control de versiones.

SIR-146: Las áreas físicas donde se alojan servidores que contienen ePHI deben contar con control de acceso físico m

Referencia normativa: HIPAA §164.310(a)(1), ISO 27002:2022 7.4.1, NIST PE-3

Prioridad: Alta

Justificacion: Evita accesos no autorizados a infraestructura crítica que podría comprometer la disponibilidad o confidencialidad de datos clínicos.

Metodo validacion: Verificación del sistema de control físico implementado (biométrico, tarjeta RFID) y registros de acceso.

Dependencias exclusiones: Relacionado con SIR-079 (acceso físico general).

Categoria: Physical Access Control, Facility Protection

Ejemplo practico: El CPD donde se aloja OpenEMR requiere tarjeta de proximidad y huella digital para ingreso al rack.

SIR-147: Las áreas sensibles deben contar con videovigilancia activa (CCTV) y grabación continua, conservada por al

Referencia normativa: ISO 27002:2022 7.5.5, HIPAA §164.310(b)

Prioridad: Media

Justificacion: Permite detectar y evidenciar accesos físicos indebidos o actividades sospechosas en zonas críticas.

Metodo validacion: Revisión del sistema CCTV, retención de grabaciones y protección de acceso a las mismas.

Dependencias exclusiones: Relacionado con SIR-082 (registros físicos).

Categoria: Physical Surveillance, CCTV Auditability

Ejemplo practico: Zona de servidores clínicos monitoreada con cámaras IP que almacenan 45 días de grabaciones cifradas.

SIR-148: Las instalaciones donde se operan sistemas clínicos deben tener sensores de intrusión, incendios, humedad

Referencia normativa: ISO 27002:2022 7.9.1, NIST PE-6

Prioridad: Alta

Justificacion: Mitiga riesgos físicos/ambientales que podrían afectar la disponibilidad e integridad del sistema clínico.

Metodo validacion: Inspección de sensores ambientales instalados y pruebas periódicas de su funcionamiento.

Dependencias exclusiones: Relacionado con SIR-080 (protección ambiental).

Categoria: Environmental Monitoring, Physical Safety

Ejemplo practico: El data center clínico incluye sensores de temperatura, CO2 y movimiento, conectados a panel central con alertas automáticas.

SIR-149: Debe aplicarse un registro obligatorio de visitantes a zonas restringidas físicas, incluyendo identificación, fec

Referencia normativa: ISO 27002:2022 7.4.3, HIPAA §164.310(a)(2)(iii), NIST PE-8

Prioridad: Media

Justificacion: Permite trazabilidad física, identificación de accesos no esperados y análisis forense ante incidentes.

Metodo validacion: Revisión del libro/log de visitantes y su custodia por seguridad física.

Dependencias exclusiones: Relacionado con SIR-082.

Categoria: Visitor Management, Physical Access Audit

Ejemplo practico: Toda persona que accede a la sala de servidores debe firmar su entrada, mostrar identificación y registrar el objetivo de su visita.

SIR-150: Se debe proteger contra accesos externos no vigilados mediante barreras físicas perimetrales, puertas contro

Referencia normativa: ISO 27002:2022 7.1.2, NIST PE-2

Prioridad: Alta

Catálogo de Requisitos de Seguridad y Privacidad

Justificacion: Previene accesos no autorizados a instalaciones físicas donde se procesan o almacenan datos clínicos sensibles.

Metodo validacion: Inspección física del perímetro, evaluación de medidas de entrada/salida, cámaras y sensores.

Dependencias exclusiones: Relacionado con SIR-133.

Categoria: Perimeter Protection, Facility Security

Ejemplo practico: El centro médico cuenta con cerraduras electrónicas, torniquetes de entrada y guardia presencial las 24h.