UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

GUÍA PARA DEFINIR LA CIBERSEGURIDAD RAZONABLE

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

GUÍA PARA DEFINIR LA CIBERSEGURIDAD RAZONABLE

Análisis Ejecutivo, Regulatorio y Operativo del Marco del CIS (Versión 1.1)

Center for Internet Security (CIS) | Evaluación Técnica y Legal de Ciberseguridad

---

1. Contexto Estratégico y Problema Fundamental

En la era digital actual, la ciberseguridad ha evolucionado aceleradamente de ser una disciplina puramente técnica y confinada a los departamentos de TI, a convertirse en un pilar central de la **gestión del riesgo corporativo, el buen gobierno y la gobernanza jurídica global**. Sin embargo, existe un vacío jurisprudencial y normativo crítico: **no existe un estándar legal mínimo nacional o intersectorial unificado que defina qué constituye una 'seguridad de datos razonable'** [cite: 1].

Ante la ausencia de una norma federal taxativa en los Estados Unidos, los tribunales y reguladores abordan los incidentes de brechas de datos mediante el marco de litigios del **derecho común (Common Law) bajo alegaciones de negligencia** [cite: 1]. Esto exige probar un 'deber de cuidado' (Duty of Care) y demostrar que la entidad omitió ejercer el grado de prudencia que una organización 'razonable' habría aplicado bajo circunstancias similares [cite: 1, 18]. El resultado ha sido una parálisis operativa y legal caracterizada por:

- **Incertidumbre jurídica ex ante:** Las organizaciones no cuentan con criterios técnicos claros sobre qué controles implementar antes de sufrir un incidente para garantizar cumplimiento legal [cite: 1, 3].
- **Batallas confusas de peritos:** En litigios post-incidentes, el fallo suele depender de 'combates de expertos' con opiniones encontradas y subjetivas [cite: 3, 8].

- **Ecosistema regulatorio fragmentado:** Multiplicación de estatutos sectoriales o estatales que exigen 'seguridad razonable' sin definir las salvaguardas operativas concretas para alcanzarla [cite: 1, 3, 4].

> ■ **OBJETIVO CENTRAL DE LA GUÍA CIS**
> *El Center for Internet Security (CIS), en colaboración con juristas, jueces y expertos en ciberseguridad, propone una solución metodológica: definir la razonabilidad antes del incidente (ex ante) mediante marcos operativos prescriptivos y priorizados (Controles CIS) respaldados por un análisis de riesgo con equilibrio de costos y daños (CIS RAM) [cite: 1, 3].*

2. El Mosaico Regulatorio y Legal de la Ciberseguridad

El marco normativo aplicable a la protección de datos e infraestructura se encuentra fuertemente atomizado [cite: 1, 4]. A continuación se sintetiza el panorama legislativo actual [cite: 4-8]:

A. Regulaciones Federales Sectoriales

La legislación federal en EE. UU. no es holística, sino sectorial e inconsistente [cite: 4]:

Estatuto / Regulación	Ámbito de Aplicación	Exigencia Central de Ciberseguridad
HIPAA / HITECH [cite: 5, 86]	Sector Salud	Salvaguardas administrativas, físicas y técnicas para la ePHI [cite: 86].
GLBA / FTC Safeguards Rule [cite: 5, 87]	Instituciones Financieras	Programa integral de seguridad basado en evaluaciones de riesgo [cite: 87].

FISMA / FIPS 200 [cite: 5, 86, 87]	Agencias Federales y Contratistas	Cumplimiento obligatorio de estándares NIST SP 800-53 / FIPS 200 [cite: 86, 87].
SEC Cybersecurity Rules (2023) [cite: 5, 87]	Empresas Públicas (Bolsa)	Divulgación obligatoria de incidentes materiales en 4 días hábiles [cite: 87].
CIRCIA (2022) [cite: 5, 86, 87]	Infraestructura Crítica	Notificación obligatoria de incidentes y pagos de ransomware a CISA [cite: 4, 87].

B. Legislación Estatal y Leyes de Puerto Seguro (Safe Harbor)

Mientras que el 100% de los estados de EE. UU. cuentan con leyes de notificación de violaciones de datos y cerca del 40% exige seguridad razonable de datos, **cinco estados pioneros han establecido leyes de 'Puerto Seguro' (Safe Harbor)** que ofrecen incentivos legales explícitos para las organizaciones que adopten marcos reconocidos como los Controles del CIS o NIST CSF [cite: 1, 4, 6]:

Estado y Estatuto	Mecanismo de Incentivo Legal	Criterio de Evaluación
Ohio (R.C. § 1354) [cite: 6, 29]	Defensa afirmativa completa contra demandas por negligencia en brechas [cite: 29].	Alineación del programa con NIST CSF, CIS Controls o ISO 27000 [cite: 10].
Utah (Utah Code 78B-4-	Defensa afirmativa legal en litigios civiles por	Implementación voluntaria y

P7) [cite: 6, 29]	brechas de datos [cite: 29].	mantenimiento de un marco aceptado [cite: 29].
Connecticut (P.A. 21-119) [cite: 6, 28]	Exención o límite a la imposición de daños punitivos [cite: 28].	Adopción comprobable de mejores prácticas reconocidas [cite: 28].
Iowa (Iowa Code Ch. 554G) [cite: 6, 28]	Defensa afirmativa contra reclamos de responsabilidad tortuosa [cite: 28].	Cumplimiento de un programa de ciberseguridad basado en estándares [cite: 28].
Nevada (NRS § 603A.210) [cite: 6, 29]	Requisito obligatorio para entidades que gestionan PII estatal [cite: 9, 29].	Uso explícito de medidas de CIS Controls o NIST [cite: 9, 29].

3. Criterios de Razonabilidad y la Metodología CIS RAM

Para definir si un programa es 'razonable', la jurisprudencia moderna y la Ley de Ohio establecen que el alcance de la seguridad no debe ser absoluto ni arbitrario, sino ajustado a los siguientes **cinco factores estructurales** [cite: 10]:

- **Tamaño y complejidad de la organización:** Determina la escala operativa y los recursos exigibles [cite: 10, 20].
- **Naturaleza y alcance de las actividades:** Evalúa el modelo de negocio y vectores de exposición [cite: 10, 20].
- **Sensibilidad de la información protegida:** A mayor valor o criticidad de los datos (PII, ePHI), mayor rigor técnico [cite: 10, 20].
- **Costo y disponibilidad de herramientas:** Análisis de viabilidad técnica y financiera [cite: 10, 20].

- **Recursos disponibles:** Proporcionalidad entre el presupuesto corporativo y la salvaguarda [cite: 10, 20].

El Método de Evaluación de Riesgos CIS RAM (Duty of Care Risk Analysis)

El marco CIS RAM opera sobre el estándar de análisis de riesgo basado en el Deber de Cuidado (DoCRA) [cite: 81]. A diferencia de los modelos puramente internos (que solo evalúan pérdidas para la empresa), CIS RAM exige evaluar el impacto reputacional, financiero y operativo sobre terceros y la sociedad [cite: 3, 81, 82]. Se rige por tres principios irrenunciables [cite: 9. 81]:

- **Principio 1 (Análisis Multi-parte):** Debe evaluarse el riesgo potencial para la propia organización y para todas las partes interesadas o individuos que podrían sufrir daños [cite: 9, 81].
- **Principio 2 (Aceptación de Riesgo Proporcional):** Los riesgos solo son aceptables si no imponen un perjuicio no remediado a terceros y se mantienen bajo un 'tope de impacto' razonable [cite: 10, 81, 82].
- **Principio 3 (Proporcionalidad de Salvaguardas):** La carga o costo financiero/operativo de implementar una salvaguarda no debe superar el riesgo que previene [cite: 10, 81]. Si la salvaguarda cuesta menos que el daño predecible, omitirla es irrazonable [cite: 82].

4. Marco Operativo: Los 18 Controles Críticos del CIS

Los Controles del CIS se han consolidado como el **estándar de facto operacional global** gracias a su enfoque altamente prescriptivo, priorizado y basado en datos reales de amenazas [cite: 11, 30]. Mitigan aproximadamente el **86% de las técnicas del marco MITRE ATT&CK** en general, y el 74% a través del nivel básico IG1 [cite: 30]. Se articulan en torno a 18 controles estructurados y 153 salvaguardas [cite: 17, 42]:

- **Control 1: Inventario y Control de Activos Empresariales:** Monitoreo activo, descubrimiento diario e inventario de hardware y dispositivos [cite: 39, 44].

- **Control 2: Inventario y Control de Activos de Software:** Control de software autorizado, listas de permitidos (allowlist) y eliminación de no soportado [cite: 39, 45, 47].
- **Control 3: Protección de Datos:** Clasificación, cifrado en reposo y en tránsito, retención, borrado seguro y DLP [cite: 39, 48, 52].
- **Control 4: Configuración Segura de Activos y Software:** Líneas base (benchmarks), hardenizado, bloqueo de sesión y gestión de puertos/firewalls [cite: 39, 53, 54].
- **Control 5: Gestión de Cuentas:** Gobernanza de credenciales, inventario de cuentas de usuario/administrador/servicio y deshabilitación inactiva [cite: 39, 57].
- **Control 6: Gestión del Control de Acceso:** MFA obligatorio (acceso remoto, admin, SaaS), control basado en roles (RBAC) y SSO centralizado [cite: 39, 59, 60].
- **Control 7: Gestión Continua de Vulnerabilidades:** Escaneos automatizados internos/externos, parcheo automatizado y remediación basada en riesgo [cite: 40, 60-62].
- **Control 8: Gestión de Registros de Auditoría:** Centralización de logs (SIEM), sincronización horaria (NTP) y retención mínima de 90 días [cite: 40, 62, 64].
- **Control 9: Protección de Correo y Navegadores Web:** Filtrado DNS/URL, pasarela antimalware y configuración estricta DMARC/SPF/DKIM [cite: 40, 64, 65].
- **Control 10: Defensa contra Malware:** Antimalware gestionado centralmente, análisis de comportamiento y antiexplotación [cite: 40, 66, 67].
- **Control 11: Recuperación de Datos:** Respaldos automatizados, aislados/inmutables, cifrados y pruebas trimestrales de restauración [cite: 40, 67, 68].
- **Control 12: Gestión de la Infraestructura de Red:** Arquitectura segura, segmentación, uso de protocolos seguros (802.1X, SSH/HTTPS) y AAA [cite: 40, 68, 69].
- **Control 13: Monitoreo y Defensa de la Red:** Detección y prevención de intrusos (NIDS/NIPS, HIDS/HIPS), EDR y correlación de alertas [cite: 40, 70-72].

- **Control 14: Concientización en Seguridad y Capacitación:** Capacitación anual/continua, prevención de phishing/pharming y formación por roles [cite: 40, 73, 74].
- **Control 15: Gestión de Proveedores de Servicios:** Inventario, clasificación de riesgo, auditorías (SOC 2) y cláusulas contractuales de seguridad [cite: 41, 74, 75].
- **Control 16: Seguridad del Software de Aplicación:** Ciclo de vida de desarrollo seguro (SDLC), análisis estático/dinámico (SAST/DAST) y SBOM [cite: 40, 75-77].
- **Control 17: Gestión de Respuesta ante Incidentes:** Plan de respuesta, designación de responsables, simulacros (tabletop) y análisis post-incidente [cite: 40, 78, 79].
- **Control 18: Pruebas de Penetración:** Pentesting periódico externo e interno para validar la efectividad de los controles [cite: 40, 79, 80].

Implementación Gradual por Grupos (Implementation Groups - IGs)

Para garantizar la escalabilidad técnica y económica, los Controles CIS dividen sus 153 salvaguardas en tres Grupos de Implementación (IGs) [cite: 30]:

Grupo de Implementación	Perfil Institucional	Cobertura de Defensa MITRE
IG1 (Higiene Cyber Básica) [cite: 30]	Pymes o entidades con recursos de TI limitados y baja complejidad [cite: 30].	Mitiga ~74% de las técnicas de ataque del MITRE ATT&CK [cite: 30].
IG2 (Madurez Intermedia) [cite: 30]	Empresas con infraestructuras complejas y datos sensibles/regulados [cite: 30].	Amplía la defensa frente a ataques dirigidos y amenazas complejas [cite: 30].
IG3 (Defensa Avanzada)	Organizaciones de	Mitiga ~86% del catálogo

[cite: 30]	infraestructura crítica o de técnicas de ataque expuestas a APTs [cite: globales [cite: 30]. 30].

5. Caso de Estudio Práctico: Anonyco, Inc.

El documento presenta la experiencia real de **Anonyco, Inc.**, un fabricante de productos ligeros en el suroeste de EE. UU. con 10 a 20 empleados [cite: 34]. El caso ilustra cómo las falencias de ciberseguridad generan contingencias financieras y legales catastróficas [cite: 34, 35]:

- **El Incidente Interno y la Pérdida Millonaria:** Un ex-empleado desvinculado retuvo acceso remoto a los sistemas de Anonyco debido a la falta de procesos de revocación de credenciales (Control 6) [cite: 34, 35]. Suplantando la identidad de la empresa, negoció un contrato de 7 cifras con un cliente clave y desvió la firma final hacia un competidor donde se había vinculado [cite: 34, 35].
- **Desafío Regulatorio de Expansión:** Al intentar negociar con industrias altamente reguladas, Anonyco se enfrentó a estrictos mandatos de seguridad de datos como requisito contractual [cite: 35]. La falta de gobernanza amenazaba con bloquear su crecimiento comercial y exponer a la empresa a litigios de responsabilidad [cite: 35].
- **Transformación mediante CIS Controls:** Anonyco realizó una evaluación de riesgos e implementó salvaguardas prioritarias: inventario de hardware/software, endurecimiento de configuraciones, restricción de privilegios admin, cifrado, filtro de correo y capacitación activa del personal [cite: 35, 36]. Como resultado, logró proteger la integridad de sus datos, asegurar la admisibilidad de pruebas en discovery y cumplir con las exigencias de clientes regulados [cite: 35, 37].

6. Lista de Verificación para la Formulación de Políticas

Para garantizar que el programa corporativo sea defensible ante tribunales y reguladores, la alta dirección debe aplicar la siguiente **Lista de Verificación de Políticas de Razonabilidad** (Apéndice L) [cite: 89]:

[ ] Comprender la misión, las partes interesadas y las obligaciones legales de la organización [cite: 89].

[ ] Desarrollar e implementar un programa de ciberseguridad formal por escrito [cite: 89].

[ ] Identificar y asignar recursos dedicados: fondos, personal, herramientas automatizadas y tercerización [cite: 89].

[ ] Alinear e implementar un marco de ciberseguridad reconocido por la industria (ej. CIS Controls) [cite: 89].

[ ] Medir continuamente la conformidad con el marco y corregir las brechas identificadas [cite: 89].

[ ] Ejecutar evaluaciones periódicas de riesgo que ponderen el impacto interno y a terceros (CIS RAM) [cite: 89].

[ ] Someter el programa a auditorías e inspecciones independientes de forma periódica [cite: 89].

[ ] Establecer roles, responsabilidades y capacitación obligatoria en concientización cibernética [cite: 89].

[ ] Formalizar un plan probado de respuesta a incidentes y capacidades operativas de recuperación de datos [cite: 89].

7. Conclusiones y Recomendaciones para la Alta Dirección

Desde una perspectiva experta en ciberseguridad y derecho corporativo, la guía del CIS demuestra que la 'seguridad razonable' ya no es un concepto indeterminado sujeto a la especulación judicial post-incidente [cite: 1, 3]. Las organizaciones pueden proteger sus activos y blindar su responsabilidad legal adoptando un enfoque proactivo ex ante [cite: 3].

Recomendaciones Estratégicas:

- **Adopción del Grupo de Implementación 1 (IG1) como Línea Base Obligatoria:** Cualquier empresa, independientemente de su tamaño, debe asegurar el cumplimiento del IG1 de los Controles CIS para garantizar una higiene cibernética mínima defensible en tribunales [cite: 30].
- **Institucionalizar el Análisis de Riesgo Multi-parte (CIS RAM):** Superar las evaluaciones de riesgo puramente financieras e integrar el cálculo de daños a terceros para alinearse con las exigencias regulatorias modernas de los Fiscales Generales [cite: 81, 84].
- **Aprovechar los Estatutos de Puerto Seguro:** Para organizaciones que operen en jurisdicciones con leyes de Puerto Seguro (o comercialicen con entidades en EE. UU.), formalizar la adopción del marco para obtener defensas afirmativas ante posibles litigios [cite: 1, 6, 28].