Resumen ejecutivo

OC2G — *Observa*. *Controla*. *Caza*. *Gobierna*. — es un framework de ciberseguridad estructurado en cuatro dominios funcionales con dependencias explícitas, diseñado para orientar la construcción progresiva de un programa de seguridad en organizaciones con entornos tecnológicos heterogéneos y recursos operativos limitados. Es una creación original de **MilpaSec**, desarrollada a partir de experiencia práctica en seguridad ofensiva y defensiva en el contexto latinoamericano.

El problema que resuelve

Las organizaciones de tamaño pequeño y mediano en México y Latinoamérica operan en una brecha real: las amenazas son sofisticadas, los frameworks internacionales de referencia son **abstractos** o están orientados a organizaciones con equipos de seguridad maduros, y el ecosistema de herramientas disponibles — aunque robusto — carece de un modelo que lo articule en un flujo coherente y progresivo. El resultado es predecible: controles implementados de forma aislada, sin criterio de priorización, sin visibilidad de dependencias entre capacidades y sin un programa de seguridad que avance de forma deliberada y medible.

OC2G nace para resolver esa brecha. No reemplaza los estándares internacionales — los precede. Provee el modelo de progresión que permite a una organización construir las capacidades fundacionales que **NIST CSF 2.0, CIS Controls v8** e **ISO/IEC 27001** asumen como prerrequisito.

El modelo

OC2G organiza las capacidades de seguridad en cuatro dominios con un orden técnicamente fundamentado:

D1 · Arquitectura y Activos — *Observa*. Establece la visibilidad completa del entorno tecnológico. Sin inventario confiable, ningún control posterior tiene base verificable.

D2 · Identidad y Control — *Controla*. Gobierna quién accede a qué, con qué privilegios y en qué condiciones. Opera sobre la infraestructura que **D1** desplegó.

D3 · Exposición y Superficie — *Caza*. Gestiona de forma continua la superficie de ataque activa — puertos expuestos, vulnerabilidades, **Shadow IT** y vectores de explotación mapeados contra **MITRE ATT&CK y OWASP Top 10.**

D4 · Gobernanza y Supervisión — *Gobierna*. Convierte la telemetría de **D2** y **D3** en decisiones, políticas y ciclos de mejora continua. Es el dominio que garantiza que el programa avanza y no se estanca.

Para quién es

OC2G está dirigido a directores de tecnología y seguridad que necesitan un modelo claro para estructurar y comunicar su programa de seguridad, a ingenieros y consultores que requieren un marco de referencia con dependencias explícitas y lenguaje técnico de autoridad, y a investigadores e instituciones académicas interesados en modelos de ciberseguridad adaptados a la realidad operativa de la región latinoamericana.

Valor diferencial

OC2G no es un catálogo de controles ni un estándar de certificación. Es un modelo de progresión con cuatro propiedades que los frameworks internacionales disponibles no combinan simultáneamente: dependencias explícitas entre capacidades, orden técnicamente fundamentado, principios rectores por dominio y alineación formal con **NIST CSF 2.0**, **CIS Controls v8, ISO/IEC 27001, MITRE ATT&CK** y **OWASP Top 10** como marcos de referencia de autoridad.

Acknowledgments

OC2G reconoce las contribuciones fundamentales de los siguientes organismos al campo de la ciberseguridad, cuyos marcos de referencia informan el diseño conceptual de este framework:

National Institute of Standards and Technology (NIST) — por el **Cybersecurity Framework 2.0**, que establece el lenguaje común de funciones de seguridad adoptado globalmente.

Center for Internet Security (CIS) — por los **CIS Controls v8** y los **CIS Benchmarks**, referencia de autoridad para la implementación de controles técnicos priorizados por impacto.

International Organization for Standardization (ISO) — por **ISO/IEC 27001:2022**, estándar global de gestión de seguridad de la información.

MITRE Corporation — por el framework **ATT&CK**, taxonomía de referencia para el conocimiento adversarial basado en comportamiento real de actores de amenaza.

OWASP Foundation — por el **OWASP Top 10**, referencia de autoridad para la gestión de riesgos en aplicaciones web.

1 — Introducción

1.1 – Problema actual

Las organizaciones de tamaño **pequeño y mediano** en México y Latinoamérica enfrentan un escenario de ciberseguridad estructuralmente adverso. No porque carezcan de conciencia sobre el riesgo — cada vez menos — sino porque operan en una **brecha real** entre la **sofisticación** de las amenazas actuales y la capacidad técnica**, presupuestaria y humana** disponible para contrarrestarlas.

Los actores de amenaza no distinguen por tamaño de organización. El ransomware, el movimiento lateral, el abuso de credenciales y la explotación de superficies expuestas afectan con igual o mayor impacto a una empresa de 15 personas que a una corporación con equipo de seguridad dedicado. **La diferencia está en la capacidad de respuesta** — y en si la organización **siquiera tiene visibilidad** de lo que está ocurriendo en su entorno antes de que sea tarde.

En este contexto, la **ausencia** de un programa de ciberseguridad estructurado no es una **decisión técnica**: **es un riesgo operativo, financiero y reputacional activo.** El problema no es falta de herramientas — existe un ecosistema open source robusto y funcional. El problema es la falta de un modelo que integre esas capacidades en un **flujo coherente, progresivo y adaptado a la realidad de la región.**

1.2 – Limitaciones de los enfoques existentes

Los frameworks de referencia internacionales disponibles hoy — **NIST Cybersecurity Framework, CIS Controls v8, ISO/IEC 27001, MITRE ATT&CK, OWASP Top 10** — representan contribuciones fundamentales al campo. **OC2G no existe para reemplazarlos ni para competir con ellos.** Existen, sin embargo, limitaciones estructurales que los hacen **insuficientes como punto de partida operativo** para el contexto al que este framework está dirigido.

El **NIST CSF 2.0** está diseñado como un lenguaje común de referencia, **abstracto** por definición. Sus funciones — **Govern, Identify, Protect, Detect, Respond, Recover** — describen *qué* debe existir en un programa de seguridad, pero deliberadamente no prescriben *cómo* ni en qué orden. Esa abstracción es una fortaleza para su adopción universal, pero representa una **barrera real** para organizaciones sin un equipo de seguridad maduro que pueda traducir ese lenguaje a controles concretos.

Los **CIS Controls v8** son un catálogo de controles técnicos bien estructurado y priorizado. Su valor es incuestionable como referencia de implementación. Sin embargo, su formato — una lista de 18 controles con salvaguardas asociadas — **no define un modelo de dependencias ni un flujo de madurez entre capacidades.** No responde a la pregunta de qué construir primero ni por qué ese orden importa.

ISO/IEC 27001 es el estándar de gestión de seguridad de la información más reconocido globalmente. Su orientación hacia la certificación formal, la documentación exhaustiva y la auditoría de tercera parte lo posicionan como un objetivo de madurez avanzada — **no como un punto de entrada para una organización que aún no tiene inventario de activos ni directorio de identidades.**

Es importante distinguir, sin embargo, que no todos los marcos de referencia relevantes para **OC2G** presentan estas limitaciones. **MITRE ATT&CK** y **OWASP Top 10** no son marcos de programa — **no intentan** estructurar un programa de seguridad completo ni definir un modelo de madurez organizacional. Son **marcos de referencia técnica: ATT&CK** provee el vocabulario para describir el comportamiento de los adversarios en términos de tácticas, técnicas y procedimientos; **OWASP Top 10** cataloga los riesgos de seguridad más críticos en aplicaciones web. **OC2G** no suple ni reemplaza ninguno de los dos **— los absorbe como lenguaje técnico dentro del dominio donde son más relevantes.**

El resultado de estas limitaciones es predecible: las organizaciones que intentan adoptar estos frameworks sin mediación terminan o bien paralizadas por la amplitud del alcance, o bien **implementando controles de forma aislada, sin coherencia sistémica, sin visibilidad de las dependencias entre capacidades y sin un criterio claro de progresión.**

1.3 – Origen y propósito de OC2G

OC2G — ***Observa. Controla. Caza. Gobierna.*** — nace como **respuesta directa** a esa brecha. Es un framework de ciberseguridad diseñado **para estructurar el pensamiento, la arquitectura y la progresión** de un programa de seguridad en organizaciones con recursos limitados, ecosistemas heterogéneos y necesidad de resultados concretos sobre presupuestos reales.

Su propósito no es reemplazar los frameworks existentes. Su propósito es articular un modelo de cuatro dominios con dependencias explícitas, flujo definido y principios rectores claros, que pueda ser adoptado como referencia conceptual por directores de tecnología, ingenieros de seguridad y consultores que operan en el contexto latinoamericano — y que sirva como **mapa de ruta** antes de que la organización esté en condiciones de abordar una certificación **ISO** o una implementación completa del **NIST CSF.**

El nombre del framework no es decorativo. Cada palabra es un dominio: ***Observa*** **lo que existe,** ***Controla*** **quién accede,** ***Caza*** **lo que está expuesto,** ***Gobierna*** **el programa completo.** Esa secuencia no es arbitraria — es una progresión de madurez con dependencias técnicas reales que se detallan en las secciones siguientes.

OC2G es una creación original de **MilpaSec**, desarrollada a partir de experiencia práctica en seguridad ofensiva y defensiva. El framework está alineado conceptualmente con **NIST CSF 2.0**, **CIS Controls v8** e **ISO/IEC 27001** como marcos de programa de referencia, e incorpora **MITRE ATT&CK** y **OWASP Top 10** como marcos de referencia técnica dentro de los dominios donde su lenguaje es operativamente relevante.

2 — Resumen del Framework

2.1 – Definición formal

OC2G es un **framework de ciberseguridad** estructurado en cuatro dominios funcionales con dependencias explícitas, diseñado para orientar la construcción progresiva de un programa de seguridad en organizaciones con entornos tecnológicos heterogéneos y recursos operativos limitados.

A diferencia de los marcos de referencia internacionales que describen capacidades de forma abstracta o catalogan controles de forma independiente**, OC2G define un modelo con flujo direccionado:** cada dominio tiene un rol específico en la cadena de madurez, recibe insumos definidos de dominios anteriores y produce salidas concretas hacia dominios posteriores. El orden no es sugerido — es funcional. **Implementar un dominio sin que el anterior esté operativo no es un atajo: es una dependencia no resuelta que compromete la efectividad del control.**

2.2 – Alcance y límites del documento

Alcance de este documento:

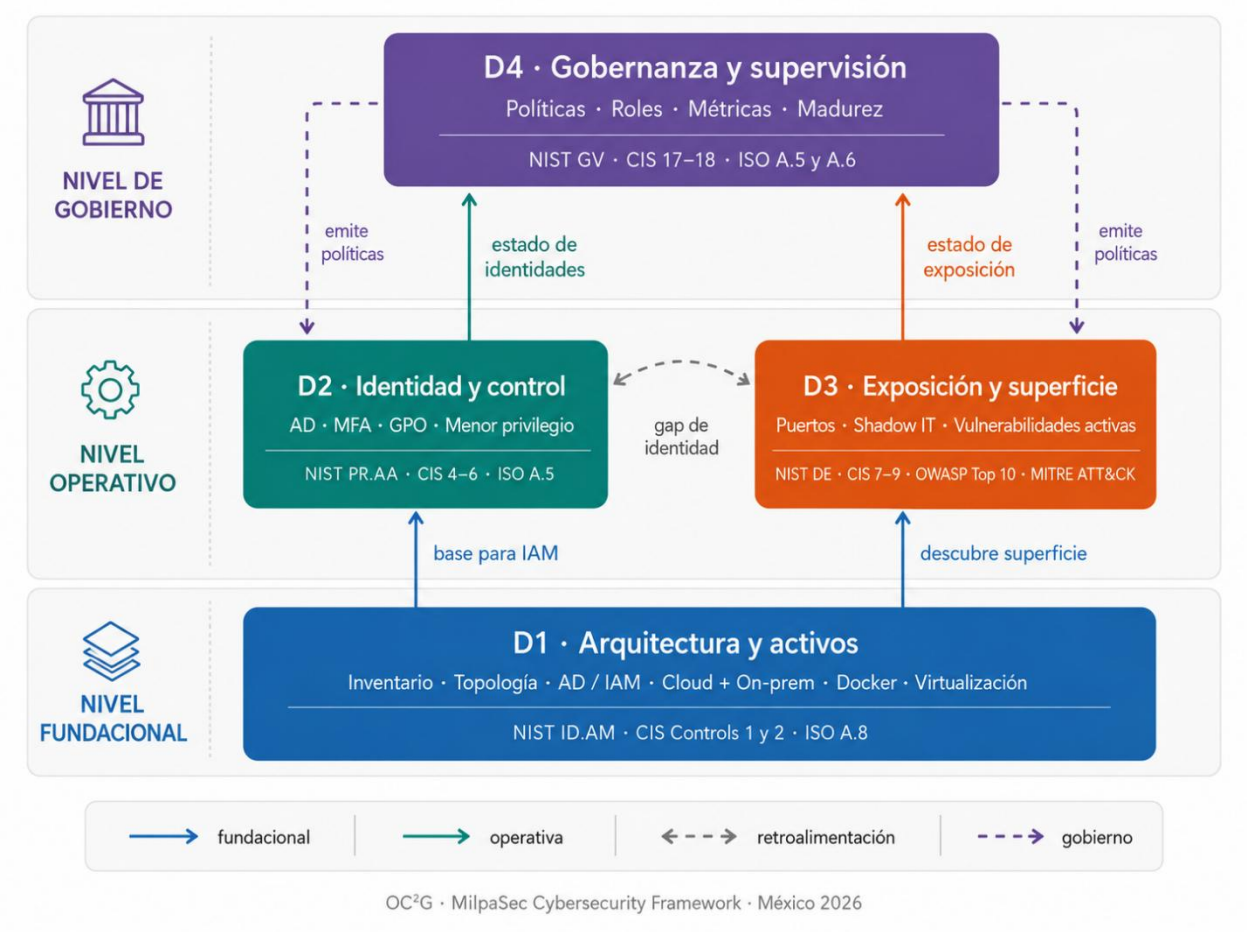
El presente documento define el modelo conceptual de **OC2G**: sus cuatro dominios, sus definiciones formales, los principios rectores, las dependencias entre dominios y la alineación con frameworks internacionales de referencia.

Los procedimientos de implementación técnica, selección de herramientas, configuraciones de sistemas, métricas operativas y guías de respuesta son derivados, existen y son parte de **OC2G**.

Contexto de aplicación:

OC2G está diseñado para su **aplicación en organizaciones de tamaño pequeño y mediano** operando en México y Latinoamérica, con ecosistemas tecnológicos que combinan infraestructura on—premise, servicios en la nube y entornos híbridos. **Sus principios son transferibles a cualquier contexto organizacional**, pero su lenguaje, referencias normativas y criterios de priorización **responden a la realidad operativa de la región.**

2.3 – Modelo del framework



El modelo **OC2G** se organiza en cuatro dominios distribuidos en tres niveles funcionales: un nivel fundacional, un nivel operativo y un nivel de gobierno.

D1 · Arquitectura y Activos ocupa el nivel **fundacional. Es el único dominio sin dependencias de entrada dentro del framework — opera sobre la realidad tecnológica de la organización tal como existe.** Su función es producir visibilidad: un inventario completo y confiable de activos, identidades y superficie tecnológica sobre el cual todos los dominios superiores construyen sus controles. Sin **D1** operativo, **ningún control posterior tiene base verificable.**

D2 · Identidad y Control y **D3 · Exposición y Superficie** ocupan el nivel operativo. **Ambos reciben de D1 los insumos que necesitan** — **D2** recibe la estructura de activos para construir el control de acceso e identidades; **D3** recibe el inventario de activos para mapear la superficie de ataque activa. **Operan en paralelo,**

pero no de forma independiente: entre ambos existe un vínculo de retroalimentación denominado ***gap de identidad*****,** que representa la brecha medible entre activos descubiertos en **D1** y activos con identidad gestionada en **D2**. Ese gap no es un error del modelo — es un indicador de riesgo explícito que el framework expone deliberadamente.

D4 · Gobernanza y Supervisión ocupa el nivel de gobierno. Recibe de **D2** el estado continuo de las identidades y de **D3** el estado de exposición de la organización. Con esa información, **D4** gobierna el ciclo de mejora: define políticas, establece responsabilidades, mide madurez y emite directrices que retroalimentan a **D2** y **D3.** Es el único dominio con flujo descendente — **su salida modifica el comportamiento de los dominios operativos.**

Tipos de flujo en el modelo:

El modelo contempla cuatro tipos de relación entre dominios, cada uno con un rol distinto en la cadena:

- **Fundacional** — **D1** hacia **D2** y **D3.** Provee la base sin la cual los dominios operativos no pueden funcionar.
- **Operativa** — **D2** y **D3** hacia **D4.** Alimenta el nivel de gobierno con estado real del entorno.
- **Retroalimentación** — Entre **D2** y **D3.** Expone la brecha de identidad como señal de riesgo activo.
- **Gobierno** — **D4** hacia **D2** y **D3.** Emite políticas que ajustan los controles operativos según el contexto de riesgo vigente.

El modelo no es puramente secuencial ni puramente cíclico. **Es un flujo dirigido con un ciclo de gobierno en la capa superior** — lo que permite tanto una adopción progresiva por fases como una operación continua una vez que todos los dominios están activos.

3 — Fundamentos del diseño

3.1 – Por qué cuatro dominios

La decisión de estructurar **OC2G** en cuatro dominios no responde a una preferencia estética ni a una analogía con frameworks existentes. Responde a un análisis de las capacidades mínimas que un programa de seguridad necesita para ser funcionalmente coherente, y a la identificación de los puntos naturales de cohesión y separación entre esas capacidades.

Cada dominio agrupa capacidades que comparten el mismo objeto de control, el mismo momento en la cadena de madurez y el mismo tipo de pregunta que responden:

D1 responde a ***¿qué existe?*** — el dominio de la realidad tecnológica de la organización. **D2** responde a ***¿quién accede y en qué condiciones?*** — el dominio del control sobre las identidades y los privilegios. **D3** responde a ***¿qué está expuesto y qué puede ser explotado?*** — el dominio de la superficie de ataque activa. **D4** responde **a *¿cómo se gobierna y mejora el programa?*** — el dominio de la dirección estratégica.

Tres dominios colapsarían una separación que es técnicamente necesaria — por ejemplo, fusionar identidad y activos en un solo dominio elimina la distinción entre saber que un activo existe y saber quién tiene acceso a él, que son capacidades con ciclos de vida, herramientas y responsabilidades distintas. Cinco o más dominios fragmentarían capacidades que son naturalmente cohesivas, introduciendo complejidad de gestión sin beneficio proporcional en claridad o control.

Cuatro dominios es el número mínimo suficiente para que el modelo sea completo, y el número máximo razonable para que sea adoptable.

3.2 – Por qué ese orden y esas dependencias

El orden de los dominios en **OC2G** no es una recomendación de buenas prácticas — es una consecuencia de dependencias técnicas reales. Invertir ese orden no produce un programa de seguridad más ágil: produce controles sin base verificable.

D1 antes que cualquier otro dominio porque el inventario de activos es el prerrequisito técnico de todo control posterior. No es posible gestionar identidades asociadas a sistemas que no están inventariados. No es posible mapear superficie de ataque sobre activos que no se conocen. No es posible medir madurez sobre una base de datos de realidad incompleta. La visibilidad no es el primer paso porque sea conveniente — es el primer paso porque sin ella, el resto del programa opera sobre supuestos, no sobre hechos.

D2 y D3 después de D1 y en paralelo entre sí porque ambos dependen del inventario que **D1** produce, pero son independientes en su objeto de control. **D2** controla identidades y privilegios — opera sobre *quién*. **D3** gestiona exposición y vulnerabilidades — opera sobre *qué está abierto y qué puede ser explotado*. Aunque son paralelos en su nivel de madurez, están conectados por el ***gap de identidad***: la brecha entre activos descubiertos en **D1** y activos con identidad gestionada en **D2.** Esa brecha no es un

error del modelo — es un indicador de riesgo que el framework expone deliberadamente como señal medible.

D4 después de D2 y D3 porque el gobierno de un programa de seguridad requiere estado real del entorno para ser efectivo. Definir políticas antes de tener visibilidad de identidades y exposición produce documentos sin anclaje en la realidad operativa. **D4** no puede gobernar lo que no puede medir, y no puede medir lo que **D2** y **D3** aún no han instrumentado. Una vez que esos dominios están activos, **D4** cierra el ciclo emitiendo políticas que ajustan los controles de **D2** y **D3** según el contexto de riesgo vigente — generando el único flujo descendente del modelo.

3.3 – Qué resuelve OC2G respecto a otros modelos

OC2G no nace de la crítica a los frameworks existentes sino de la observación de una brecha de adopción concreta: organizaciones que conocen **NIST, CIS** e **ISO** pero no tienen un modelo que les diga cómo articular esas referencias en un programa coherente, progresivo y adaptado a sus condiciones reales.

Respecto al NIST CSF 2.0: El **CSF** describe seis funciones — **Govern, Identify, Protect, Detect, Respond, Recover** — de forma deliberadamente abstracta para garantizar su aplicabilidad universal. No prescribe orden de adopción ni define dependencias entre funciones. **OC2G** toma esa abstracción y la convierte en un modelo con flujo dirigido, dependencias explícitas y principios rectores por dominio. No es una implementación del **NIST CSF** — es un modelo de progresión que puede usarse como puente hacia él.

Respecto a CIS Controls v8: Los **CIS Controls** son un catálogo de 18 controles priorizados por impacto, con salvaguardas específicas y grupos de implementación por madurez. Su valor como referencia técnica es incuestionable. Sin embargo, el catálogo no define un modelo de dependencias entre controles ni un flujo de construcción de capacidades. **OC2G** es complementario: sus dominios absorben los controles **CIS** relevantes dentro de cada capa, pero los organiza en una estructura con lógica de progresión que el catálogo por sí solo no provee.

Respecto a ISO/IEC 27001: ISO 27001 es el estándar de gestión de seguridad de la información más reconocido globalmente, orientado hacia la certificación formal mediante un **Sistema de Gestión de Seguridad de la Información.** Su rigor documental y su orientación a auditoría de tercera parte lo posicionan como un objetivo de madurez avanzada. **OC2G** no compite con ese objetivo — lo precede. Un programa estructurado con **OC2G** genera las capacidades y la evidencia que acercan a una organización a una postura certificable, sin requerir que la certificación sea el punto de partida.

Respecto a MITRE ATT&CK y OWASP Top 10: Estos marcos ocupan un rol distinto en la arquitectura de referencia de **OC2G**. **No son marcos de programa** — no definen cómo estructurar ni gobernar un programa de seguridad. Son marcos de lenguaje técnico. **MITRE ATT&CK** provee la taxonomía para describir el comportamiento de los adversarios en términos de tácticas, técnicas y procedimientos, y es el vocabulario natural del tercer dominio del framework — ***Caza*** — donde la detección de exposición activa y la identificación de superficie explotable requieren precisamente ese nivel de especificidad técnica. **OWASP Top 10** cumple un rol equivalente en el contexto de aplicaciones web, catalogando los vectores de ataque más críticos que cualquier programa de seguridad debe contemplar al evaluar su superficie digital. **OC2G**

no reimplementa ninguno de los dos — **los reconoce como referencias técnicas de autoridad dentro del dominio donde son operativamente relevantes.**

4 — Dominios principales

4.1 – Arquitectura y Activos

D1 · Arquitectura y Activos

Observa. Alineación: **NIST CSF 2.0 ID.AM · CIS Controls v8 1, 2 · ISO/IEC 27001 A.8**

El primer dominio del framework establece la visibilidad completa del entorno tecnológico de la organización. Cubre la totalidad de los activos que componen la infraestructura — endpoints, servidores, servicios, identidades, software y activos en la nube — y los organiza en un inventario centralizado con relaciones definidas entre activo, usuario, ubicación y servicio. **D1** no produce controles de seguridad directamente: produce la base de datos de realidad sobre la cual todos los controles posteriores operan. Es el único dominio del framework sin dependencias de entrada — su insumo es el entorno tecnológico tal como existe.

1. Definición

D1 es el dominio de visibilidad y gestión de activos tecnológicos. Define los procesos, capacidades y estructuras necesarias para descubrir, clasificar e inventariar de forma continua todos los activos que componen el entorno tecnológico de la organización, incluyendo infraestructura física, virtual, en la nube y activos de software.

2. Propósito

Proveer una base de información confiable, completa y actualizada sobre la realidad tecnológica de la organización, sobre la cual se construyen los controles de identidad, la gestión de exposición y el gobierno del programa de seguridad.

3. Alcance

- Descubrimiento de activos mediante agentes y escaneo de red.
- Inventario centralizado en una base de datos de gestión de configuración **(CMDB).**
- Clasificación de activos por tipo, criticidad y propietario.
- Mapeo de relaciones activo–usuario–servicio–ubicación.
- Gestión del ciclo de vida de activos: incorporación, cambio y baja.
- Despliegue y registro de infraestructura base del framework como activos gestionados.
- Despliegue de infraestructura de directorio centralizado como activo de infraestructura.

- Hardening de endpoints con imagen base reproducible.
- Aplicación de configuraciones de seguridad en servidores mediante automatización

4. Capacidades clave

- Identificación automática y continua de activos en el entorno.
- Normalización y enriquecimiento del inventario.
- Mapeo de dependencias entre activos y servicios.
- Aprovisionamiento de endpoints desde imagen base controlada.
- Aplicación de políticas de configuración centralizadas (GPO / Ansible).
- Detección de activos no gestionados o fuera de baseline.

5. Relaciones

Inputs: Entorno tecnológico real de la organización — no recibe insumos de otros dominios. Es el punto de entrada del framework.

Outputs:

- → **D2:** Estructura de activos como base para el control de acceso e identidades.
- → **D3:** Inventario de activos como referencia para el mapeo de superficie de ataque.

6. Principio rector

"No puedes proteger lo que no sabes que existe. "

4.2 – Identidad y Control

Controla. Alineación: **NIST CSF 2.0 PR.AA · CIS Controls v8 4, 5, 6 · ISO/IEC 27001 A.5**

El segundo dominio del framework gobierna quién accede a qué, en qué condiciones y con qué nivel de privilegio. Parte de la infraestructura de directorio que **D1** desplegó y la convierte en un sistema de control activo: gestiona el ciclo de vida completo de las identidades, aplica el principio de menor privilegio, instrumenta autenticación fuerte y establece las políticas que determinan el comportamiento de los usuarios y dispositivos en el entorno. La identidad mal gestionada es el vector de compromiso más frecuente en organizaciones de tamaño pequeño y mediano — credenciales compartidas, privilegios excesivos y ausencia de autenticación fuerte representan el camino de menor resistencia para cualquier actor de amenaza con acceso inicial al entorno.

1. Definición

D2 es el dominio de gestión de identidades y control de acceso. Define los procesos, capacidades y políticas necesarias para gobernar el ciclo de vida completo de las identidades en la organización —

usuarios, dispositivos y cuentas de servicio — garantizando que cada acceso esté autenticado, autorizado y alineado con el principio de menor privilegio.

2. Propósito

Reducir la superficie de ataque asociada a identidades comprometidas, privilegios excesivos y accesos no gestionados, mediante el control centralizado de quién puede acceder a qué recursos, desde qué dispositivos y en qué condiciones.

3. Alcance

- Gestión del ciclo de vida de identidades: aprovisionamiento, modificación y baja.
- Aplicación del principio de menor privilegio y separación de funciones.
- Autenticación multifactor **(MFA)** para accesos críticos.
- Gestión de cuentas privilegiadas y cuentas de servicio.
- Definición y aplicación de políticas de acceso mediante **GPO.**
- Control de acceso basado en roles **(RBAC).**
- Rotación automatizada de credenciales locales.
- Gestión de sesiones privilegiadas.

4. Capacidades clave

- Gobierno centralizado de identidades sobre infraestructura de directorio.
- Aplicación de políticas de contraseñas y bloqueo de cuentas.
- Detección de cuentas con privilegios excesivos o sin actividad.
- Eliminación de credenciales compartidas entre dispositivos.
- Control de acceso administrativo local sin contraseñas compartidas.
- Aplicación de configuraciones de seguridad en endpoints vía políticas centralizadas.

5. Relaciones

Inputs:

- ← **D1:** Infraestructura de directorio desplegada · Inventario de activos y usuarios como base para la gestión de identidades.

Outputs:

- → **D4:** Estado continuo de identidades — quién existe, qué privilegios tiene, dónde hay desviaciones respecto a la política.

Retroalimentación:

- ↔ **D3:** ***Gap de identidad*** — brecha medible entre activos descubiertos en **D1** y activos con identidad gestionada en **D2**. Esta brecha no es un error del modelo — es un indicador de riesgo explícito que el framework expone deliberadamente como señal de atención para ambos dominios.

6. Principio rector

"Ningún acceso sin identidad verificada. Ninguna identidad sin privilegio justificado. "

4.3 – Exposición y superficie

Caza. Alineación: **NIST CSF 2.0 DE · CIS Controls v8 7, 8, 9 · ISO/IEC 27001 A.8 · OWASP Top 10 · ATT&CK**

El tercer dominio del framework gestiona la exposición activa de la organización — lo que puede ser descubierto, enumerado y explotado por un actor de amenaza desde dentro o fuera del entorno. **D3** no opera sobre supuestos: opera sobre evidencia. Toma el inventario de activos que **D1** produjo, cruza ese inventario contra la superficie real expuesta y determina qué está abierto, qué está vulnerable y qué está fuera del control de **D2**. A diferencia de **D1** y **D2**, que son dominios de construcción y control, **D3** es un dominio de detección y reducción activa — su operación es continua, no puntual, porque la superficie de ataque cambia con cada cambio en el entorno. El lenguaje técnico de este dominio está anclado en dos marcos de referencia de autoridad: **MITRE ATT&CK**, que provee la taxonomía para describir cómo los adversarios descubren, enumeran y explotan superficies expuestas en términos de tácticas, técnicas y procedimientos; y **OWASP Top 10**, que cataloga los vectores de ataque más críticos en aplicaciones web y es referencia obligatoria para cualquier organización con superficie digital expuesta.

1. Definición

D3 es el dominio de gestión de exposición y superficie de ataque. Define los procesos, capacidades y criterios necesarios para descubrir, evaluar y reducir de forma continua la superficie explotable de la organización — incluyendo servicios expuestos, vulnerabilidades activas en sistemas y aplicaciones, activos no gestionados y vectores de ataque identificables desde una perspectiva adversarial.

2. Propósito

Identificar y reducir de forma continua la superficie de ataque activa de la organización, priorizando la remediación de exposiciones según su criticidad y su potencial de explotación real, antes de que un actor de amenaza las aproveche.

3. Alcance

- Descubrimiento y análisis de puertos y servicios expuestos en la red.

- Gestión continua de vulnerabilidades en sistemas operativos, servicios y aplicaciones.
- Identificación y clasificación de **Shadow IT** — activos operando fuera del control corporativo.
- Evaluación de seguridad en aplicaciones web alineada con **OWASP Top 10.**
- Correlación entre activos descubiertos en **D1** y activos con identidad gestionada en **D2** — medición del ***gap de identidad.***
- Análisis de exposición desde perspectiva adversarial referenciado en **MITRE ATT&CK.**
- Gestión del ciclo de remediación: identificación, priorización, remediación y verificación.
- Detección de configuraciones inseguras y desviaciones respecto al baseline establecido en **D1**.

4. Capacidades clave

- Escaneo continuo de superficie de ataque interna y externa.
- Identificación de vulnerabilidades activas con correlación a **CVEs** y **CVSS.**
- Priorización de remediación basada en criticidad real y potencial de explotación.
- Detección de activos expuestos sin identidad gestionada en **D2.**
- Evaluación de vectores de ataque web mediante referencia **OWASP Top 10.**
- Mapeo de técnicas adversariales activas contra la superficie identificada, usando taxonomía **MITRE ATT&CK.**
- Detección de exposición derivada de configuraciones por defecto no endurecidas.
- Identificación de rutas de movimiento lateral potencial en el entorno.

5. Relaciones

Inputs:

- ← **D1:** Inventario de activos como referencia base para correlacionar superficie descubierta.
- ← **D4:** Políticas de gestión de riesgo y criterios de priorización de remediación.

Outputs:

- → **D4:** Estado de exposición de la organización — superficie activa, vulnerabilidades abiertas, backlog de remediación priorizado y riesgos derivados de activos no controlados.

Retroalimentación:

- ↔ **D2:** ***Gap de identidad*** — activos con exposición activa que carecen de identidad gestionada en **D2** representan un riesgo compuesto: superficie explotable sin control de acceso asociado.

6. Principio rector

“Lo que no se mide no se puede reducir. Toda superficie no gestionada es superficie comprometible. “

4.4 – Gobernanza y supervisión

Gobierna. Alineación: **NIST CSF 2.0 GV · CIS Controls v8 17, 18 · ISO/IEC 27001 A.5, A.6**

El cuarto dominio del framework opera en un nivel distinto a los tres anteriores**. D1, D2** y **D3** construyen capacidades técnicas, instrumentan controles y generan telemetría continua sobre el estado del entorno. **D4** toma esa información y la convierte en decisiones, políticas y ciclos de mejora sostenida. Sin gobierno, un programa de seguridad es un conjunto de controles técnicos sin dirección estratégica — efectivo en el corto plazo, frágil ante el cambio. **D4** es el dominio que garantiza que **OC2G** no sea una implementación puntual sino un programa vivo: mide el estado real del entorno contra los objetivos definidos, identifica desviaciones, emite políticas que ajustan los controles operativos y asegura que la organización avanza en madurez de forma deliberada y medible. Es también el dominio que conecta el programa de seguridad con el cumplimiento normativo aplicable en el contexto latinoamericano.

1. Definición

D4 es el dominio de gobernanza y supervisión del programa de seguridad. Define los procesos, estructuras de responsabilidad y mecanismos de medición necesarios para dirigir, evaluar y mejorar de forma continua el programa de ciberseguridad de la organización, asegurando su alineación con los objetivos del negocio, los requisitos normativos aplicables y el estado real del entorno tecnológico.

2. Propósito

Garantizar que el programa de seguridad de la organización opera con dirección estratégica clara, responsabilidades definidas, métricas de madurez verificables y un ciclo de mejora continua que responde al estado real del entorno — no a supuestos estáticos.

3. Alcance

- Definición y mantenimiento de políticas de seguridad de la organización.
- Establecimiento de roles y responsabilidades en el programa de seguridad.
- Medición de madurez del programa mediante indicadores derivados de **D2** y **D3**.
- Gestión de riesgos de seguridad como proceso formal y continuo.
- Supervisión del cumplimiento normativo aplicable.
- Emisión de directrices que ajustan los controles operativos de **D2** y **D3**.
- Gestión de auditorías internas del programa.
- Comunicación del estado de seguridad a la dirección de la organización.

4. Capacidades clave

- Gobierno del ciclo de vida de políticas de seguridad.
- Supervisión continua del estado de identidades reportado por **D2.**
- Supervisión continua del estado de exposición reportado por **D3.**
- Gestión formal del riesgo con criterios de aceptación, mitigación y escalamiento.
- Medición de progresión de madurez del programa a lo largo del tiempo.
- Coordinación de respuesta ante desviaciones críticas identificadas en dominios operativos.
- Alineación del programa con marcos normativos aplicables en el contexto latinoamericano.

5. Relaciones

Inputs:

- ← **D2:** Estado continuo de identidades — cobertura, desviaciones respecto a política, cuentas con privilegios no justificados.
- ← **D3:** Estado de exposición — superficie activa, vulnerabilidades abiertas, backlog de remediación, riesgos derivados de activos no controlados.

Outputs:

- → **D2:** Políticas de control de acceso, criterios de privilegio mínimo y directrices de gestión de identidades.
- → **D3:** Políticas de gestión de riesgo, criterios de priorización de remediación y umbrales de exposición aceptable.

Nota: **D4** es el único dominio del framework con **flujo descendente.** Su salida no alimenta a un dominio superior — cierra el ciclo de gobierno emitiendo políticas que modifican el comportamiento de los dominios operativos según el contexto de riesgo vigente.

6. Principio rector

"La seguridad sin gobierno es táctica. Con gobierno, es estrategia sostenible. "

5 – Framework mapping

Esta sección establece la correspondencia formal entre los dominios de **OC2G** y los marcos de referencia internacionales con los que el framework está alineado. El propósito del mapping no es demostrar equivalencia — **OC2G** no es una reimplementación de ninguno de estos marcos. Su propósito es proveer al lector un punto de anclaje claro entre el modelo **OC2G** y los estándares que ya conoce, facilitando su adopción como referencia complementaria dentro de programas de seguridad existentes.

5.1 – OC2G ↔ NIST CSF 2.0

El **NIST Cybersecurity Framework 2.0** organiza sus capacidades en seis funciones: **Govern, Identify, Protect, Detect, Respond** y **Recover**. **OC2G** no mapea todas las funciones del **CSF** — su alcance es deliberadamente más acotado, cubriendo las capacidades fundacionales de un programa de seguridad antes de abordar **respuesta y recuperación.**

OC2G	NIST CSF 2.0	Observación
D1 · Arquitectura y Activos	**Identify** — ID.AM (Asset Management)	**D1** cubre la totalidad de la función **Identify** en su componente de gestión de activos.
D2 · Identidad y Control	**Protect** — PR.AA (Identity Management & Access Control)	**D2** cubre el componente de identidad y control de acceso dentro de **Protect.**
D3 · Exposición y Superficie	**Detect** — DE (Continuous Monitoring)	**D3** cubre la detección continua de exposición activa y vulnerabilidades.
D4 · Gobernanza y Supervisión	**Govern** — GV (Organizational Context, Risk Management, Policy)	**D4** cubre el núcleo de la función **Govern**: políticas, roles, riesgo y mejora continua.

*Funciones del **NIST CSF 2.0** fuera del alcance de **OC2G** en este documento: **Respond** y **Recover.** Estas funciones corresponden a capacidades de respuesta a incidentes y continuidad operativa, desarrolladas en documentos de implementación derivados del framework.*

5.2 – OC2G ↔ CIS Controls v8

Los **CIS Controls v8** organizan sus 18 controles en tres grupos de implementación **(IG1, IG2, IG3)** según el nivel de madurez de la organización. **OC2G** absorbe los controles **CIS** más relevantes dentro de cada dominio, organizándolos en una estructura de dependencias que el catálogo **CIS** por sí solo no define.

OC2G	CIS Controls v8	Controles principales
D1 · Arquitectura y Activos	**IG1 / IG2**	**CIS 1** — Inventario de activos de hardware · **CIS 2** — Inventario de activos de software · **CIS 4** — Configuración segura de activos empresariales
D2 · Identidad y Control	**IG1 / IG2**	**CIS 5** — Gestión de cuentas · **CIS 6** — Gestión de control de acceso
D3 · Exposición y Superficie	**IG2 / IG3**	**CIS 7** — Gestión continua de vulnerabilidades · **CIS 8** — Gestión de registros de auditoría · **CIS 9** — Protección de correo electrónico y navegador web
D4 · Gobernanza y Supervisión	**IG2 / IG3**	**CIS 17** — Gestión de respuesta a incidentes · **CIS 18** — Pruebas de penetración

5.3 – OC2G ↔ ISO/IEC 27001

ISO/IEC 27001:2022 organiza sus controles en el Anexo A, estructurado en cuatro categorías: controles organizacionales, controles de personas, controles físicos y controles tecnológicos. El mapping de **OC2G** con **ISO 27001** no es exhaustivo — se presentan los controles del Anexo A más directamente relacionados con cada dominio.

OC2G	ISO/IEC 27001:2022	Controles Anexo A principales
D1 · Arquitectura y Activos	**A.8** — Controles tecnológicos	**A.8.1** Dispositivos de usuario final · **A.8.8** Gestión de vulnerabilidades técnicas · **A.8.9** Gestión de configuración
D2 · Identidad y Control	**A.5** — Controles organizacionales · **A.8** — Controles tecnológicos	**A.5.15** Control de acceso · **A.5.16** Gestión de identidades · **A.5.17** Información de autenticación · **A.8.2** Derechos de acceso privilegiado
D3 · Exposición y Superficie	**A.8** — Controles tecnológicos	**A.8.7** Protección contra malware · **A.8.8** Gestión de vulnerabilidades · **A.8.20** Seguridad en redes
D4 · Gobernanza y Supervisión	**A.5** — Controles organizacionales · **A.6** — Controles de personas	**A.5.1** Políticas de seguridad · **A.5.2** Roles y responsabilidades · **A.5.8** Seguridad de la información en gestión de proyectos · **A.6.3** Concienciación y formación

5.3 – OC2G ↔ MITRE ATT&CK

MITRE ATT&CK es un marco de conocimiento adversarial que cataloga las tácticas, técnicas y procedimientos utilizados por actores de amenaza reales. Su relación con **OC2G** es de naturaleza técnica y está concentrada principalmente en **D3**, donde provee el lenguaje para describir, clasificar y priorizar la superficie explotable desde una perspectiva adversarial.

OC2G	Tácticas MITRE ATT&CK	Relación
D1 · Arquitectura y Activos	**Discovery** (TA0007)	**D1** construye el inventario que permite detectar técnicas de reconocimiento interno — **T1018** Remote System Discovery, **T1082** System Information Discovery
D2 · Identidad y Control	**Credential Access** (TA0006) · **Privilege Escalation** (TA0004) · **Lateral Movement** (TA0008)	**D2** mitiga técnicas como **T1550.002** Pass the Hash, **T1078** Valid Accounts, **T1484** Domain Policy Modification
D3 · Exposición y Superficie	**Reconnaissance** (TA0043) · **Initial Access** (TA0001) · **Discovery** (TA0007) · **Execution** (TA0002)	**D3** identifica y reduce la superficie explotable mapeada contra técnicas activas del adversario
D4 · Gobernanza y Supervisión	—	**D4** no mapea directamente a tácticas ATT&CK — opera sobre el programa, no sobre técnicas individuales

5.4 – OC2G ↔ OWASP Top 10

OWASP Top 10 cataloga los diez riesgos de seguridad más críticos en aplicaciones web. Su relación con **OC2G** está concentrada en **D3**, donde la evaluación de superficie digital expuesta incluye necesariamente los vectores de ataque web más prevalentes.

OC2G	OWASP Top 10 (2021)	Relación
D3 · Exposición y Superficie	**A01** — Broken Access Control	**D3** identifica configuraciones de control de acceso deficientes en aplicaciones expuestas.
D3 · Exposición y Superficie	**A02** — Cryptographic Failures	**D3** detecta servicios con cifrado débil o ausente en la superficie expuesta.
D3 · Exposición y Superficie	**A03** — Injection	**D3** incluye la evaluación de vectores de inyección en aplicaciones web dentro del scope de superficie.
D3 · Exposición y Superficie	**A05** — Security Misconfiguration	**D3** correlaciona configuraciones inseguras detectadas contra el baseline establecido en **D1.**
D3 · Exposición y Superficie	**A06** — Vulnerable and Outdated Components	**D3** gestiona el inventario de componentes vulnerables como parte del ciclo de remediación continua.
D2 · Identidad y Control	**A07** — Identification and Authentication Failures	**D2** aborda directamente los fallos de autenticación e identificación como parte del control de identidades.

*Los riesgos **OWASP** no mapeados explícitamente corresponden a capacidades de desarrollo seguro y revisión de código — fuera del alcance del presente documento y desarrollados en documentos de implementación derivados.*

6 – Pautas de uso

Esta sección orienta al lector sobre cómo utilizar **OC2G** como marco de referencia en distintos contextos profesionales. Dado que este documento es conceptual y no un manual de implementación, las guías de uso que se presentan a continuación son de naturaleza metodológica — describen cómo pensar con **OC2G**, no cómo ejecutar sus controles técnicos.

6.1 – OC2G como modelo de evaluación de madurez

El uso más inmediato de **OC2G** es como instrumento de diagnóstico. Cada dominio define capacidades con alcance y propósito explícitos, lo que permite evaluar el estado actual de un programa de seguridad de forma estructurada — identificando qué dominios están operativos, cuáles están parcialmente cubiertos y cuáles están ausentes.

El proceso de evaluación sigue la lógica de dependencias del modelo:

La evaluación comienza siempre en **D1**. Si el inventario de activos es incompleto o inexistente, cualquier control en **D2** o **D3** está operando sobre una base no verificable — independientemente de su sofisticación técnica. Esta es la primera pregunta que **OC2G** obliga a responder: **¿la organización sabe con certeza qué existe en su entorno?**

Con **D1** evaluado, se procede a **D2 y D3 en paralelo**. En **D2** la pregunta central es si las identidades están gestionadas de forma centralizada, con privilegios justificados y autenticación fuerte. En **D3** la pregunta es si la organización tiene visibilidad continua de su superficie expuesta y un ciclo de remediación activo. El ***gap de identidad*** entre ambos dominios — activos descubiertos en **D1** sin identidad gestionada en **D2** — es un indicador de riesgo directo que la evaluación debe medir explícitamente.

D4 se evalúa último, porque su efectividad depende de que **D2** y **D3** estén generando telemetría real. Un dominio de gobierno sin insumos verificables no es gobierno — es documentación.

6.2 – OC2G en un engagement de consultoría o auditoría

Para un consultor externo o auditor, **OC2G** provee un lenguaje estructurado para comunicar hallazgos, brechas y recomendaciones a distintas audiencias simultáneamente — técnica y directiva — sin perder precisión ni accesibilidad.

Los dominios actúan como unidades de reporte independientes pero interconectadas. Un hallazgo en **D1** — por ejemplo, activos no inventariados — tiene implicaciones directas y trazables en **D2** y **D3**, lo que permite construir una narrativa de riesgo coherente en lugar de una lista de hallazgos aislados. Esta trazabilidad entre dominios es uno de los valores diferenciales de **OC2G** como herramienta de comunicación en un contexto de auditoría.

El mapping con **NIST CSF 2.0**, **CIS Controls v8, ISO/IEC 27001, MITRE ATT&CK** y **OWASP Top 10** — detallado en la sección 5 — permite al auditor anclar cada hallazgo de **OC2G** a controles y referencias

internacionales reconocidas, añadiendo credibilidad técnica al reporte sin necesidad de traducción adicional entre frameworks.

6.3 – OC2G como referencia para directores de tecnología y seguridad

Para un **director de TI, CISO o responsable de seguridad**, **OC2G** ofrece un modelo de conversación estructurada con la dirección de la organización. Los cuatro dominios — con sus principios rectores, sus dependencias explícitas y su progresión de madurez — traducen la complejidad técnica de un programa de seguridad en una narrativa estratégica comprensible.

El framework permite responder tres preguntas directivas con precisión:

¿Dónde estamos? — La evaluación de madurez por dominio provee un estado actual verificable, no una percepción subjetiva del nivel de seguridad de la organización.

¿Qué construimos primero? — El orden de dominios y sus dependencias dan una respuesta técnicamente fundamentada a la pregunta de priorización de inversión en seguridad.

¿Cómo sabemos que avanzamos? — Cada dominio tiene capacidades definidas cuya presencia o ausencia es verificable. El avance no se mide en documentos producidos sino en capacidades operativas activas.

6.4 — OC2G como estructura para equipos de seguridad internos

Para un equipo técnico interno **— ingenieros de seguridad, sysadmins, analistas** — **OC2G** provee un modelo mental compartido que organiza las responsabilidades, evita la duplicación de esfuerzos y hace explícitas las dependencias entre capacidades que distintas personas o áreas pueden estar gestionando de forma aislada.

Un equipo que adopta **OC2G** como referencia puede organizar su trabajo en torno a los dominios: quién es responsable de **D1**, qué criterio define que **D2** está operativo, qué métricas alimenta **D3** hacia **D4**. Esa claridad estructural reduce la fricción operativa y hace el programa de seguridad auditable internamente sin necesidad de una consultoría externa.

El framework también provee un criterio de progresión: antes de invertir esfuerzo en capacidades de **D3**, el equipo puede verificar que **D1** está completo y que **D2** tiene cobertura suficiente. Sin ese criterio, los equipos técnicos tienden a construir capacidades sofisticadas sobre bases incompletas — un patrón de riesgo común en organizaciones de crecimiento acelerado.

6.5 — OC2G como puente hacia frameworks internacionales

OC2G no es un destino de madurez — es un punto de partida estructurado. Una organización que opera con los cuatro dominios activos ha construido las capacidades fundacionales que los frameworks internacionales asumen como prerrequisito: visibilidad de activos, control de identidades, gestión de exposición y gobierno del programa.

Desde ese punto, la adopción de **NIST CSF 2.0** en su totalidad — incluyendo las funciones **Respond** y **Recover** — es un paso natural con base verificable. La certificación **ISO/IEC 27001** deja de ser un objetivo inalcanzable y se convierte en una formalización de capacidades que la organización ya tiene operativas. Los grupos de implementación **IG2** e **IG3** de **CIS Controls v8** dejan de ser aspiracionales y se convierten en la expansión lógica de lo que **D3** y **D4** ya están construyendo.

Ese es el propósito final de **OC2G**: no reemplazar los estándares internacionales sino hacer que sean alcanzables.

7 – Referencias

Las siguientes referencias corresponden a los marcos, estándares y recursos de autoridad que fundamentan el diseño conceptual de **OC2G.** Se presentan organizadas por tipo de referencia.

7.1 — Marcos de programa

National Institute of Standards and Technology (NIST) NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: U.S. Department of Commerce, 2024. https://www.nist.gov/cyberframework

Center for Internet Security (CIS) CIS Controls v8: Critical Security Controls for Effective Cyber Defense. East Greenbush, NY: CIS, 2021. https://www.cisecurity.org/controls/v8

International Organization for Standardization (ISO) ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection: Information Security Management Systems — Requirements. Ginebra: ISO, 2022. https://www.iso.org/standard/27001

7.2 — Marcos de referencia técnica

MITRE Corporation MITRE ATT&CK Framework — Enterprise Matrix. McLean, VA: MITRE, 2024. https://attack.mitre.org

OWASP Foundation OWASP Top 10:2021 — Top 10 Web Application Security Risks. OWASP Foundation, 2021. https://owasp.org/Top10

7.3 – Recursos complementarios

Center for Internet Security (CIS) CIS Benchmarks — Secure Configuration Guidelines. East Greenbush, NY: CIS, 2024. https://www.cisecurity.org/cis—benchmarks

NIST National Vulnerability Database (NVD) National Vulnerability Database. Gaithersburg, MD: U.S. Department of Commerce, 2024. https://nvd.nist.gov