SGSI 27001:2022 y CSF 2.0

CÓRDOBA CREA FUTURO

Este módulo profundiza en dos grandes marcos para la gestión de la seguridad de la información: la norma internacional ISO/IEC 27001:2022 (SGSI) y el **NIST Cybersecurity Framework 2.0** (CSF 2.0). A lo largo de las unidades, se explicarán desde los fundamentos hasta las aplicaciones avanzadas, con un enfoque práctico y orientado a casos reales. Al final, se incluyen actividades prácticas, un laboratorio guiado con herramientas gratuitas, y lecturas recomendadas para afianzar los conocimientos.

Unidad 1: Seguridad de la información y sistema de gestión de seguridad de la información (SGSI)

Unidad 1: Seguridad de la información y sistema de gestión de seguridad de la información (SGSI)

Esta unidad tiene como objetivo comprender la estructura y las novedades de la Norma ISO 27001:2022 (International Organization for Standardization [ISO] e International Electrotechnical Commission [IEC], 2022), los elementos principales de un sistema de gestión de seguridad de la información (SGSI) y cómo aplicar un SGSI en la práctica (roles, alcance, políticas, objetivos, inventario de activos y ciclo de mejora continua). Se presentará un caso práctico de aplicación de un SGSI en una organización ficticia para ilustrar los conceptos.

1. 1. Presentación y estructura de la ISO 27001:2022 (cambios desde la versión previa)

La ISO/IEC 27001 es la norma internacional que establece los requisitos para poner en marcha un sistema de gestión de seguridad de la información (SGSI) en una organización. La versión más reciente, ISO/IEC 27001:2022, actualiza y reemplaza a la versión 2013, introduce cambios importantes en la estructura de controles y algunas mejoras en los requisitos de gestión.

Estructura principal de ISO 27001:2022

La norma se divide en dos partes: en primer lugar, están las cláusulas 4–10, que contienen los requisitos del sistema de gestión (lo que la organización debe hacer en cuanto a los procesos de gestión), y, por otra parte, está el anexo A, que lista los controles de seguridad sugeridos para tratar los riesgos identificados (prácticas específicas de seguridad). Las cláusulas siguen la estructura de alto nivel común a todas las normas de sistemas de gestión (anexo SL), lo cual incluye los siguientes aspectos: contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora continua. Esta estructura permite

integrar el SGSI con otros sistemas de gestión (calidad, continuidad de negocio, etcétera) en la organización.

Cambios importantes en la versión 2022 vs. 2013

La actualización de 2022 trajo, sobre todo, una reorganización de los controles de seguridad en el anexo A para alinearse con la nueva ISO 27002:2022 (guía de buenas prácticas). Los cambios más destacados son los que se mencionan a continuación:

- **reducción del número total de controles** de ciento catorce (en 2013) a noventa y tres controles en 2022. Esto se logró mediante la fusión o consolidación de controles redundantes. Aunque hay menos controles listados, no se eliminaron requisitos de seguridad importantes, sino que estos se agruparon de forma más eficiente para evitar repeticiones.

- **Introducción de once controles nuevos** en el anexo A para cubrir amenazas y tecnologías emergentes que no estaban explícitamente abordadas en 2013. Estos nuevos controles incluyen temas como, por ejemplo, inteligencia de amenazas, seguridad en la nube, continuidad de las TIC, monitoreo físico, gestión de configuraciones, eliminación segura de información, enmascaramiento de datos, prevención de fugas (DLP), actividades de monitoreo, filtrado web y codificación segura, entre otros. En la siguiente lista, se resumen los once controles añadidos:

  - **inteligencia de amenazas**. Proceso para recolectar y analizar información sobre las amenazas actuales y anticiparse a incidentes

- **Seguridad de la información para servicios en la nube**: requisitos de control y acuerdos para uso seguro de servicios *cloud* (protección de datos en la nube, controles de acceso, etcétera).
- **Preparación de las TIC para la continuidad del negocio**: asegurarse de que la infraestructura de TI esté preparada para incidentes graves y alineada con las necesidades identificadas en el análisis de impacto al negocio (BIA).
- **Monitoreo de la seguridad física**: aplicación de sistemas de vigilancia para prevenir accesos físicos no autorizados en áreas en las que se procesan datos confidenciales.
- **Gestión de la configuración**: establecimiento de procesos para configurar y mantener sistemas de manera segura, lo que evita errores de configuración que puedan abrir brechas.
- **Eliminación de información**: procedimientos para borrar información de forma segura cuando esta ya no se necesita, lo que permite cumplir requisitos legales (como, por ejemplo, el Reglamento General de Protección de Datos de la Unión Europea [RGPD]) y reducir riesgo de filtración
- **Enmascaramiento de datos**: técnicas como enmascaramiento, seudonimización o anonimización de datos sensibles, especialmente datos personales, para protegerlos en entornos no productivos o frente a accesos no autorizados.

- **Prevención de fuga de datos (DLP)**: mecanismos para evitar la salida no autorizada de información confidencial, que incluyen clasificar la información, monitorear canales de salida (correo, web, USB, etcétera) y bloquear o alertar ante intentos de exfiltración.
- **Actividades de monitoreo**: aumento de las capacidades de registro y monitoreo continuo de actividades en la red y sistemas para detectar comportamientos anómalos o incidentes de seguridad rápidamente.
- **Filtrado web**: control del acceso a sitios web maliciosos o no autorizados mediante herramientas de filtrado de URL y concienciación a usuarios, lo que reduce la exposición a contenido peligroso.
- **Codificación segura**: adopción de prácticas de desarrollo seguro en el ciclo de vida del *software* (antes, durante y después de escribir código) para reducir vulnerabilidades en las aplicaciones.

[1] Reglamento de la Unión Europea 679 de 2016 [Parlamento Europeo]. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). 27 de abril de 2016.

- **Reclasificación de controles en categorías más simples**: en lugar de los catorce dominios temáticos de controles que existían en la edición 2013, ahora los noventa y tres controles del anexo A se agrupan en cuatro grandes categorías (temas). A continuación, las presentamo.

1. **Controles organizacionales** (A.5): treinta y siete controles sobre procesos organizativos generales, como gestión de activos, relación con proveedores, continuidad del negocio, seguridad de la información en proyectos, etcétera.
2. **Controles de personas** (A.6): ocho controles relativos a la seguridad vinculada con el personal, como, por ejemplo, controles de RR. HH. (fidelidad del personal, formación en seguridad, responsabilidades de usuarios, teletrabajo, notificación de incidentes).
3. **Controles físicos** (A.7): catorce controles para proteger los activos físicos y entornos (instalaciones, equipos, centros de datos, medios de almacenamiento, cableado, áreas seguras, protección contra incendios, etcétera).
4. **Controles tecnológicos** (A.8): treinta y cuatro controles de seguridad específicos de tecnología (protección de redes, sistemas y aplicaciones). Incluye controles sobre gestión de identidades y accesos, cifrado, seguridad en comunicaciones, copias de seguridad, gestión de vulnerabilidades, prevención de *malware*, monitoreo y detección de incidentes, entre otros.

Figura 1: Evolución de la estructura de ISO/IEC 27001. Comparación de las versiones 2005, 2013 y 2022 (dominios/temas y número de controles)

Fuente: [imagen sin título sobre evolución de la estructura de ISO/IEC 27001], s. f., https://bit.ly/47QPi8n.

- **Eliminación de objetivos de control**: en ISO 27001:2013, los controles del anexo A se agrupaban bajo «objetivos de control» descriptivos. En la nueva versión, esos objetivos de control explícitos desaparecen; ahora, cada control tiene un «propósito» definido en ISO 27002:2022 (una breve descripción de la finalidad del control) en lugar de agruparse bajo objetivos generales. Esto simplifica la presentación y se centra directamente en los controles y su propósito.

- **Atributos para clasificar controles**: ISO 27002:2022 introdujo cinco atributos opcionales para etiquetar los controles (por ejemplo: tipo de control preventivo/detectivo, propiedad de seguridad asociada —confidencialidad, integridad, disponibilidad—, función de ciberseguridad —identificar, proteger, dominio de seguridad, etcétera—). Estos atributos no son requisitos de ISO 27001, pero sirven para que la organización pueda filtrar o presentar los controles desde diferentes perspectivas. Por ejemplo, un control puede etiquetarse como «detectivo» y asociado a la propiedad «integridad», lo cual ayuda a identificar qué controles son detectivos o cuáles protegen la

integridad de la información. Esta es una novedad interesante para análisis internos, aunque su uso es opcional.

- **Cambios menores en requisitos de las cláusulas 4–10**: la norma ISO 27001:2022 mantiene en esencia los mismos requisitos de SGSI que la versión 2013, con pequeños ajustes para mejorar la claridad y alinearse con la estructura de alto nivel. Entre los cambios sutiles, están los siguientes:

  - **inclusión de la planificación de cambios al SGSI** (nueva cláusula 6.3) para gestionar de forma controlada cualquier modificación en el sistema de gestión (por ejemplo, cambios organizativos, introducción de nuevos procesos, o la propia transición de 2013 a 2022).
  - Énfasis en la necesidad de **definir criterios** para los procesos del SGSI y asegurar su ejecución controlada (cláusula 8.1).
  - Mayor precisión en requisitos de **medición y evaluación** del desempeño del SGSI (cláusula 9.1), lo que deja claro que se debe evaluar la eficacia del sistema y no solo hacer monitoreo pasivo.
  - Considerar necesidades y expectativas de las partes interesadas también en la revisión por la dirección (cláusula 9.3), lo que asegura que la alta dirección tome en cuenta requisitos de clientes, reguladores, socios, etcétera, en la gestión de la seguridad.
  - En general, lenguaje más claro y preciso en varias cláusulas para evitar

ambigüedades en la interpretación durante auditorías.

En resumen, la ISO 27001:2022 mejora la relevancia y modernización de los controles de seguridad, manteniendo el mismo enfoque de sistema de gestión de mejora continua que tenía la versión 2013. Las organizaciones certificadas en ISO 27001:2013 deben planificar su transición a la nueva versión antes de fines de 2025 (ISO estableció un período de transición de tres años desde la publicación). Para nuevas aplicaciones, ya se debe usar directamente la versión 2022.

Importante: aunque ISO 27001:2022 trae nuevos controles, la aplicación de cada control depende del resultado del análisis de riesgos de la organización y de las necesidades aplicables. No es obligatorio aplicar todos los controles del anexo A; pero cualquier exclusión debe justificarse en la declaración de aplicabilidad (SoA, *statement of applicability*). La selección de controles debe basarse en los riesgos identificados: los controles son medidas para mitigar riesgos, por lo que, si un riesgo no es significativo o no aplica en el contexto, la organización puede decidir no aplicar ciertos controles, documentando la razón. Esto refuerza que ISO 27001 es un modelo adaptable según el contexto de la organización y su apreciación de riesgos.

1. 2. Roles, alcance, política y objetivos de seguridad en el SGSI

Poner en marcha un SGSI efectivo requiere definir claramente quién hará qué, sobre qué información aplicará controles, con qué directrices y para qué metas. Esta sección cubre cuatro pilares principales:

- roles y responsabilidades;
- alcance del SGSI;
- política de seguridad de la información, y
- objetivos de seguridad.

Roles y responsabilidades en seguridad de la información

La norma ISO 27001 destaca la importancia del liderazgo y la asignación de responsables en el SGSI. La alta dirección de la organización debe demostrar compromiso aprobando la política de seguridad, asignando los recursos necesarios y designando roles claves. Algunos roles típicos en un SGSI avanzado incluyen los que se describen a continuación:

- **alta dirección** (ejecutivos). Tienen la responsabilidad última del SGSI. Deben establecer la dirección estratégica de la seguridad, integrarla con los objetivos del negocio y asegurarse de que se cumplan las políticas y los objetivos de seguridad. Pueden delegar tareas diarias, pero no pueden delegar su responsabilidad final sobre la seguridad. La alta dirección también revisa periódicamente el desempeño del SGSI (revisión por la dirección, cláusula 9.3) y toma decisiones sobre mejoras.
- **Líder de seguridad de la información** (CISO o equivalente): es la persona encargada de coordinar y mantener el SGSI en el día a día. Este rol (a veces llamado «responsabilidad del SGSI» o un «representante de la dirección» en seguridad) se ocupa de desarrollar políticas, evaluar riesgos, liderar iniciativas de seguridad, coordinar auditorías internas,

concienciar al personal, etcétera. Debe tener autoridad suficiente para aplicar cambios y acceso a la alta dirección para reportar el desempeño de la seguridad. En organizaciones pequeñas, puede ser un gerente de TI con funciones de seguridad; en organizaciones grandes, un CISO con un equipo de seguridad.

- **Propietarios de activos de información**: son individuos designados para ser responsables de un activo o conjunto de activos (por ejemplo, el propietario de un sistema o de una base de datos crítica). Su rol es asegurar que esos activos se gestionen y se clasifiquen apropiadamente y que también los controles necesarios se apliquen. Por ejemplo, el jefe del área financiera podría ser el dueño de los activos de información financiera (sistemas contables, datos de clientes) y decidir quién puede acceder y qué nivel de protección necesitan.

- **Propietarios de riesgos/controles**: en enfoques avanzados, a cada riesgo significativo identificado se le asigna un propietario de riesgo (responsable de gestionar ese riesgo), y a cada control importante un propietario de control (responsable de aplicar y vigilar la eficacia de ese control). Esto crea trazabilidad entre riesgos identificados y las personas encargadas de mitigarlos. Por ejemplo, el responsable de continuidad del negocio podría ser propietario de riesgos relacionados con desastres naturales y también propietario de los controles de respaldo y recuperación.

- **Equipo de seguridad/IT/riesgos**: involucrar a personal técnico de TI (administradores de red, sistemas, desarrolladores) y también a áreas de riesgo operativo o auditoría interna es vital. La seguridad de la información es interdisciplinaria, por lo que suele haber un comité de seguridad o de riesgos en el que participan representantes de diversas áreas para coordinar políticas y responder incidentes.

- **Todos los empleados y terceros**: cada persona que maneja información tiene responsabilidad de seguir las políticas de seguridad. Por este motivo, la organización debe comunicar claramente esas responsabilidades. Por ejemplo, todos deben entender que tienen la obligación de reportar incidentes de seguridad, cumplir con la política de contraseñas, respetar la clasificación de la información, etcétera. En relación con este aspecto, la ISO 27001 pide evidencias de que se comunican las políticas y obligaciones a todo el personal. En contratos con terceros (proveedores, socios), también se deben definir cláusulas de seguridad y responsabilidades (por ejemplo, un proveedor de servicios *cloud* debe adherirse a ciertos controles).

En definitiva, un SGSI bien gobernado requiere establecer roles claros (qué unidad o persona es responsable de cada aspecto de seguridad) y evitar lagunas o superposiciones. Un método que se usa es definir una matriz RACI (*responsible*, *accountable*, *consulted*, *informed*) para distintos procesos de seguridad, o un organigrama de seguridad. Esta claridad organizacional previene confusiones y asegura que las tareas críticas (como gestionar parches de seguridad, atender alertas, revisar *logs*, etcétera) tengan un dueño asignado.

Alcance del SGSI

Antes de profundizar en controles, la organización debe definir el alcance de su sistema de gestión de seguridad de la información (Cláusula 4.3 de ISO 27001). El alcance delimita qué partes de la organización y qué activos de información quedan cubiertos por el SGSI y, por ende, por la certificación ISO 27001. Una definición correcta del alcance es crucial y estratégica.

- El alcance puede abarcar toda la organización o solo una parte. Por ejemplo, una multinacional podría limitar el alcance inicialmente a una filial o a un departamento específico (como «departamento de TI y sus servicios en la sede central»). Se recomienda mantener un alcance manejable al iniciar e ir ampliándolo gradualmente. Un alcance demasiado amplio podría complicar la implantación; uno demasiado estrecho podría dejar por fuera activos críticos.

- Debe considerar ubicaciones físicas, procesos, unidades organizativas, servicios y sistemas. Por ejemplo: «el SGSI cubre los procesos de desarrollo de *software* y operaciones de TI del centro de datos X, incluyendo todos los sistemas de información y personal asociado a dichos procesos, en las oficinas de la ciudad Y». Esto especifica claramente qué instalaciones y procesos están «dentro» del SGSI.

- También se suelen identificar explícitamente las exclusiones. Por ejemplo: «quedan excluidos del alcance los sistemas y procesos de la red de tiendas minoristas, que se gestionan separadamente». Las exclusiones

deben tener justificación y no debilitar el SGSI; no sería aceptable excluir arbitrariamente activos para esquivar controles si esos activos están conectados con el entorno en alcance y podrían afectar la seguridad.

- El alcance debe tener en cuenta dónde están los activos de información vitales. Si la información crítica de la empresa se procesa en un sistema externo o en una sucursal, debería considerarse incluirlos. ISO 27001 sugiere basar el alcance en la ubicación e importancia de los activos de información, los procesos de negocio que los usan y las partes interesadas.

- Una vez definido, el alcance se documenta y se usa para centrar el análisis de riesgos solo en ese universo. Además, los auditores verificarán que la declaración de alcance sea adecuada y que todos los riesgos dentro de ese alcance se gestionan. Un truco práctico es adjuntar un diagrama o mapa de alcance indicando, por ejemplo, qué sitios, departamentos o sistemas están cubiertos, lo que ayuda a todos a entender límites.

Determinar el alcance correctamente es un balance: incluir lo suficiente para proteger lo que importa, pero no tanto que se vuelva inmanejable.

Ejemplo: una empresa de *software* decide certificar su SGSI centrándolo en su servicio SaaS principal. Define el alcance como «infraestructura y procesos relacionados con la plataforma SaaS X, incluyendo desarrollo, pruebas, aplicación en la nube y soporte técnico, abarcando las oficinas de Buenos Aires y el centro de datos en AWS (región US-*east*-1)». Esto deja fuera otras áreas como RR. HH. o finanzas, que quizás la empresa maneja por separado. Así concentran el SGSI en su activo más crítico (la plataforma) inicialmente, con intención de más adelante ampliarlo a toda la compañía.

Política de seguridad de la información

La política de seguridad es un documento de alto nivel, aprobado por la dirección, que establece las directrices y los compromisos generales de la organización en materia de seguridad de la información. La ISO 27001 (cláusula 5.2) requiere que exista una política que sea apropiada al propósito de la organización, incluya objetivos o marco para fijar objetivos de seguridad, se comprometa a cumplir requisitos aplicables (leyes, contratos) y a la mejora continua del SGSI, y que esté documentada, comunicada y disponible a las partes interesadas pertinentes.

En términos simples, la política responde al qué y por qué de la seguridad en la empresa, lo que sirve como carta de intención. A continuación, se presentan algunos puntos típicos que cubre una buena política de seguridad:

- **propósito y alcance**. Declara que la política aplica a la organización (o al alcance definido del SGSI) y al uso de todos los sistemas de información de esta.
- **Objetivos generales de seguridad:** por ejemplo, «proteger la confidencialidad, integridad y disponibilidad de la información de clientes y de la empresa», «cumplir con las leyes y regulaciones de protección de datos», «gestionar los riesgos de seguridad de manera sistemática».

- **Compromiso de la dirección**: la política suele llevar una declaración de apoyo explícito de la gerencia. Por ejemplo: «la dirección se compromete a proporcionar los recursos necesarios y liderar la aplicación de esta política y del SGSI, así como a la mejora continua de la seguridad de la información».

- **Roles principales**: puede establecer quién es el responsable de mantener la política (por ejemplo, el CISO) y que todos los empleados y terceros tienen responsabilidad de cumplirla.

- **Directrices claves o principios**: sin entrar en detalles técnicos (eso corresponde a políticas específicas o procedimientos), la política madre puede enumerar principios: «todo activo de información debe tener un responsable asignado y un nivel de clasificación», «se aplicará el principio de mínimo privilegio en el control de accesos», «todos los empleados recibirán capacitación en seguridad anualmente», «los incidentes de seguridad deben reportarse inmediatamente al *service desk*», etcétera. Son lineamientos generales que luego se desarrollarán en normas más concretas.

- **Cumplimiento y sanciones**: a menudo, se incluye una nota de que el incumplimiento de la política podría ocasionar sanciones disciplinarias (para destacar que no es opcional) y que la empresa vigilará el cumplimiento.

- **Aprobación formal**: firma o nombre del director general o equivalente, con fecha. Esto demuestra que es respaldada desde arriba.

Es importante que la política sea clara y breve (ideal de una o dos páginas) y que esté alineada con los objetivos del negocio. Debe ser comunicada a todo el personal. Por ejemplo, muchas empresas la publican en la intranet corporativa o la entregan al contratar a alguien, y solicitan incluso una firma de aceptación. Tener una política bien comprendida «desde la cúpula hasta la base» crea una cultura de seguridad unificada.

Además de la política general, habitualmente, se desarrollan políticas específicas o estándares sobre temas particulares: política de control de accesos, política de clasificación de la información, política de uso aceptable, política de seguridad física, etcétera. Estas derivan de la política madre y proveen requisitos más detallados. Por ejemplo, la política general puede decir «la información se clasificará por niveles de sensibilidad», y una norma de clasificación de la información definirá qué niveles existen (por ejemplo, pública, interna, confidencial, secreta) y cómo etiquetar documentos. Estas *sub-policies* también forman parte del SGSI y suelen enumerarse en el SoA para mostrar qué controles de anexo A se cubren con ellas.

Objetivos de seguridad de la información

Siguiendo las mejores prácticas de gestión (como ISO 9001 de calidad), ISO 27001 requiere establecer objetivos medibles de seguridad (cláusula 6.2). Estos objetivos deben derivar de la política y de la evaluación de riesgos, y sirven para centrar esfuerzos e impulsar la mejora continua. A diferencia de la política (que es más permanente), los objetivos se suelen plantear a corto/mediano plazo y revisarse al menos anualmente.

Características de buenos objetivos de seguridad de la información

- **Específicos y medibles**: por ejemplo, «reducir en un 50 % el número de incidentes de *malware* reportados en el próximo año» o «lograr que el 100 % de los empleados haga el curso de concienciación en seguridad antes de fin de año». Deben poder cuantificarse para saber si se alcanzaron. Un mal ejemplo

sería «mejorar la seguridad de la información», que es vago e inmensurable.

- **Alineados con objetivos del negocio**: si la empresa tiene como objetivo estratégico, digamos, expandir el comercio electrónico, un objetivo de seguridad relacionado podría ser «aplicar autenticación multifactorial en la plataforma de *e-commerce* para Q4 2025». Debe aportar valor al negocio, no ser seguridad por seguridad.

- **Asignados y con plazo**: debe quedar claro quién es responsable de lograr cada objetivo y en qué marco de tiempo. Por ejemplo, el objetivo de reducción de *malware* puede asignarse al equipo de *IT security*, con plazo a doce meses.

- **Realistas, pero desafiantes**: se busca incentivar la mejora. Si nunca se han hecho formaciones, un objetivo realista sería lograr 80 % de empleados formados, en lugar de 100 % el primer año, pero siempre buscando superarse.

- **Documentados y evaluados**: ISO pide mantener información documentada de los objetivos y planes para alcanzarlos (qué se hará para lograrlos, qué recursos se necesitan). En las revisiones gerenciales (al menos anuales), se verifica el grado de cumplimiento y se establecen nuevos objetivos o ajustes.

Ejemplos adicionales de objetivos de seguridad

- «Disminuir el tiempo promedio de respuesta a incidentes críticos de cinco horas a dos horas antes de final de año».
- «Certificar el SGSI bajo ISO 27001:2022 antes de Q3 del año próximo». Este es un objetivo típico inicial cuando se arranca la aplicación.
- «Auditar al 90 % de los proveedores críticos de TI en materia de seguridad antes de renovar sus contratos».
- «Aumentar el porcentaje de sistemas con parches de seguridad al día al 95 %».
- «Llevar a cabo dos simulacros de recuperación de desastres en el año y documentar lecciones aprendidas de cada ejercicio».

Estos objetivos guían las iniciativas del plan de trabajo de seguridad. Al evaluarlos periódicamente, la organización puede ver tendencias (mejoró o empeoró la postura de seguridad) y demostrar tanto internamente como ante auditores externos que el SGSI produce mejoras concretas (por ejemplo, menos incidentes, mejor cumplimiento legal, etcétera).

Finalmente, cabe notar la importancia de comunicar y alinear estos elementos: todos en la organización deben conocer la política y entender los objetivos relevantes a su rol. La integración de roles, alcance, política y objetivos crea la base sobre la cual se construirá el resto del SGSI (análisis de riesgos, controles, procedimientos).

1. 3. Inventario y clasificación de activos de información

Un activo de información es cualquier recurso que posee la organización que tiene valor y contiene o procesa información. Puede ser un activo **tangible** como *hardware* (servidores, PC, dispositivos móviles), documentos físicos, o **intangible** como datos electrónicos, bases de datos, *software*, credenciales, conocimientos, servicios en la nube, etcétera. Gestionar adecuadamente los activos es de suma importancia porque no se puede proteger lo que no se sabe que existe. Por este motivo, la ISO 27001 incluye controles específicos para inventariar y clasificar activos de información (por ejemplo, control 5.9 «Inventario de activos» y control 5.10 «Uso aceptable de activos» en la versión 2022 correspondientemente, antes 8.1.1/8.1.2 en 2013).

Inventario de activos

Consiste en crear y mantener un registro detallado de todos los activos de información relevantes dentro del alcance del SGSI. Este registro típicamente incluye para cada activo: nombre o identificación, tipo (*hardware*, *software*, dato, etcétera), ubicación, propietario (persona responsable asignada), valor o criticidad y otra información útil (como clasificación de sensibilidad, fecha de adquisición, *software* versionado, etcétera). Un inventario puede tomar forma de una hoja de cálculo, una base de datos o un sistema de gestión de activos dedicado.

Pasos para construir un inventario

- **Definir categorías de activos**: por ejemplo, información (datos), *software*, *hardware*, servicios, personas, instalaciones. Algunas metodologías listan activos primarios (información) y secundarios (los que soportan a la información: *hardware*, *software*, personas, locales). Se debe decidir qué nivel de detalle manejar: por ejemplo, inventariar cada documento individual es inviable; se cuentan conjuntos (como «base de datos de clientes», «repositorio de código fuente», «archivo físico de contratos 2020–2023»).

- **Relevar los activos existentes**: esto implica entrevistas con áreas de negocio y TI, revisión de sistemas, etcétera. Herramientas de descubrimiento automatizado pueden ayudar para *hardware*/*software* en red (por ejemplo, escaneos de red para encontrar servidores), pero la información no técnica (por ejemplo, qué documentos tiene legal) requiere interacción con los responsables.

- **Registrar en el inventario**: listar cada activo con sus atributos.

A continuación, se presenta un extracto de ejemplo de inventario:

- activo: «ERP financiero – servidor SQL prod»; tipo: software/información; descripción: base de datos financiera; ubicación: data center central; propietario: gerente de finanzas; valor: crítico (procesa estados financieros); clasificación: confidencial.
- Activo: «oficina – contratos legales físicos 2022»; tipo: información física; ubicación: archivo en oficina central; propietario: jefe legal; valor: medio; clasificación: secreto (contiene datos sensibles de clientes).
- Activo: «portal web corporativo»; tipo: servicio en la nube; ubicación: AWS; propietario: marketing; valor: alto (imagen corporativa, recolección de leads); clasificación de información: pública (contenido del sitio), pero con componentes internos (panel admin).

- **Mantener el inventario actualizado**: no sirve de nada crear la lista y olvidarla. Se requiere un proceso para actualizar cuando hay cambios, es decir, altas de nuevos sistemas, bajas de servidores retirados, cambios de propietario por rotación de personal, etcétera. Muchas organizaciones integran esto con sus procesos de compra de TI o control de cambios: cada nuevo proyecto debe considerar agregar los activos al inventario.

Clasificación de la información

Una vez identificados los activos (especialmente los de tipo «información»), es crucial clasificarlos según su nivel de sensibilidad o criticidad. La clasificación establece etiquetas o categorías que indican qué tan protegida debe ser cierta información. Esto permite aplicar controles proporcionales: información altamente confidencial necesitará cifrado fuerte, accesos muy limitados, etcétera, mientras que información pública no requiere medidas tan estrictas.

Un esquema de clasificación clásico es usar tres o cuatro niveles. A continuación, se presenta un ejemplo con cuatro niveles:

1. **Pública**: información que se puede difundir libremente. Su divulgación no causa daño. Por ejemplo, contenido del sitio web público, material de *marketing* publicado, folletería.

2. **Interna** (o uso interno): información de uso dentro de la organización, cuya divulgación no autorizada tendría impacto bajo. Por ejemplo, políticas internas genéricas, procedimientos operativos, comunicados internos sin datos sensibles.

3. **Confidencial**: información sensible que podría causar un impacto significativo si se divulga a personas no autorizadas. Por ejemplo, datos personales de clientes, contratos, planes de negocio, registros financieros. Es la categoría más común para datos que requieren protección seria.

4. **Secreta** (o información restringida de máxima confidencialidad): información de altísima sensibilidad, acceso muy limitado, cuyo compromiso tendría impacto crítico. Por ejemplo, secretos industriales, credenciales de alto privilegio, informes de fusiones antes de ser públicas, claves criptográficas raíz (algunas

organizaciones usan «muy confidencial» o «restricta» en vez de «secreta»).

Cada organización puede adaptar las definiciones a su realidad e incluso tener menos o más niveles. Lo importante radica en los siguientes aspectos:

- estén claramente definidas las categorías y los criterios para asignar información a cada una.
- Se proporcionen marcas o etiquetas para identificar la clasificación. Por ejemplo, en documentos electrónicos o correos, anteponer [público], [interno], [confidencial] en el asunto o encabezado; en papel, sellos o membretes de «confidencial».
- Se definan controles asociados a cada clasificación: por ejemplo, «documentos confidenciales deben almacenarse cifrados y solo personal con necesidad de conocer accede»; «*e-mails* con archivos secretos no se pueden enviar fuera del dominio corporativo»; «información pública no requiere medidas especiales».
- Se capacite a los usuarios en comprender cómo clasificar y manejar cada tipo.

Activos no informáticos

La seguridad de la información no es solo TI. El inventario y clasificación deben considerar activos intangibles y de conocimiento. Por ejemplo, la «imagen corporativa» o la «reputación» a veces se listan como activos de información, dado que un incidente podría dañarlas. También el conocimiento de los empleados (*know-how*) puede verse como activo. Estos son difíciles de cuantificar, pero es útil reconocerlos en el alcance de riesgos.

Cadena de custodia de activos

Un buen SGSI lleva registro de la asignación y retorno de activos a empleados. Por ejemplo, cuando ingresa un empleado, se documenta qué activos se le entregan (*laptop*, tarjeta de acceso, cuentas de sistemas), y, cuando egresa, se verifica que devuelva o se le retire el acceso. Esto evita «activos huérfanos» que nadie controla.

En resumen, inventariar y clasificar activos sienta la base para identificar riesgos (¿qué pasa si un activo específico es comprometido?), priorizar esfuerzos (los activos más críticos merecen más atención) y aplicar controles adecuados a cada caso. Por ejemplo, sin un inventario no sabríamos qué parches aplicar porque no sabríamos qué software tenemos; sin clasificación, podríamos gastar recursos cifrando incluso información trivial o, peor, podríamos subestimar la protección de datos sensibles.

La ISO 27001:2022 alienta estas prácticas. De hecho, uno de los nuevos controles incorporados (5.9) destaca la importancia de mantener un inventario actualizado y definir propietarios para cada activo. Además, la declaración de aplicabilidad (SoA) mencionada requiere que la organización justifique la aplicación (o no) de controles como los de clasificación de la información —es decir, debe demostrar cómo aborda la protección diferencial de información según importancia.

Ejemplo práctico de clasificación

Pensemos en el caso de una clínica médica. Podría definir lo siguiente: datos de historias clínicas = «secreto» (contienen información de salud personal, altísima sensibilidad, acceso mínimo); datos administrativos de pacientes (nombre, contacto, facturación) = «confidencial»; políticas internas de la clínica = «interno»; página web pública con consejos de salud = «pública». Así, cuando diseñe controles: las historias clínicas irán cifradas en la base de datos, con control de acceso estricto y seudonimizadas cuando sea posible; los datos administrativos confidenciales se protegen, pero con accesos más amplios para personal de facturación, etcétera. Si ocurriese un incidente, las medidas de respuesta variarán según qué clasificación esté involucrada (un *leak* de datos «secretos» es crítico, de datos «públicos» es menos grave).

En resumen, el proceso de inventario y clasificación es la fase «identificar» dentro del SGSI, fundamental antes de «proteger». Sin este paso, el SGSI navegaría a ciegas.

1. 4. El SGSI como ciclo de mejora continua PDCA y evidencias auditables

Una de las ideas centrales de ISO 27001 es que la gestión de la seguridad debe ser un proceso continuo y dinámico, no un proyecto que se hace una vez y se olvida. Para lograrlo, la norma adopta el modelo PDCA (*plan-do-check-act*), conocido también como círculo de Deming o ciclo de mejora continua. A continuación, se explica cómo se aplica PDCA en un SGSI y qué evidencias auditables se generan en cada fase.

Plan (planificar): en esta fase, se establece la base del SGSI. Incluye comprender el contexto (interno y externo) y las partes interesadas (ISO 27001 [cláusula 4]), definir el alcance (4.3), elaborar la política (5.2), asignar roles (5.3) y, muy importante, hacer la apreciación de riesgos (cláusulas 6.1.2 y 6.1.3) y planificar el tratamiento de riesgos.

Planificar significa diseñar el plan de seguridad: identificar riesgos, evaluar impactos y probabilidades, decidir cómo tratarlos (aplicar controles, evitar, transferir o aceptar el riesgo), y generar el plan de tratamiento de riesgos. En esta etapa, también se establecen los **objetivos de seguridad** (6.2) y los planes para lograrlos. Las evidencias claves que se generan en la fase plan son las siguientes:

- metodología de evaluación de riesgos documentada (criterios de riesgo, criterios de aceptación de riesgo).
- Inventario de activos y riesgos (resultado del análisis de riesgos): típicamente una matriz o registro de riesgos con amenazas, vulnerabilidades, impactos, niveles de riesgo y decisiones de tratamiento.
- Declaración de aplicabilidad (SoA) inicial: un documento que lista todos los controles del anexo A indicando cuáles se aplicarán y cuáles no, con justificación. El SoA conecta la fase de plan (riesgos identificados) con la de do (controles implementados).

- Plan de tratamiento de riesgos: lista de acciones o proyectos para aplicar controles, con responsables y fechas.

- Política de seguridad aprobada y quizás políticas específicas en borrador.

- Objetivos de seguridad establecidos junto con indicadores para medirlos y planes para alcanzarlos.

***Do* (hacer/implementar)**: es la ejecución de lo planificado. En esta fase, se aplican los controles de seguridad seleccionados para tratar los riesgos. También se pone en marcha la operación diaria del SGSI: capacitación y concienciación al personal, gestión de accesos, procedimientos operativos de respaldo, mantenimiento de sistemas, monitoreo de eventos, gestión de incidentes de seguridad, etcétera. Básicamente, es «hacer seguridad» día a día conforme a las políticas y los controles definidos.

Evidencias típicas de la fase *do*

- **Procedimientos y registros operativos**: por ejemplo, registros de copias de seguridad hechas, bitácoras de mantenimiento de servidores, listas de control de acceso actualizadas, *tickets* de incidentes resueltos, etcétera. Todo aquello que demuestre que los controles se están llevando a cabo.

- **Capacitaciones hechas**: listas de asistencia a entrenamientos de seguridad, resultados de *quizzes* de concienciación, comunicaciones enviadas al personal sobre nuevas políticas.

- **Reportes de seguimiento**: algunas organizaciones generan informes periódicos de seguridad (mensuales, trimestrales) con

métricas como intentos de ataque bloqueados, vulnerabilidades descubiertas y corregidas, etcétera.

- **Aplicación técnica de controles**: evidencias de que se configuró un *firewall* según las políticas, de que se activó el cifrado en *laptops*, de que se instaló un sistema antivirus en todos los equipos, etcétera. Pueden ser capturas de pantalla, configuraciones exportadas, o informes de herramientas (por ejemplo, un informe de que 100 % de estaciones tienen AV actualizado).

- **Contratos de seguridad con terceros**: si en la fase *plan* se detectó el riesgo en proveedores, en *do* se firma un acuerdo de nivel de servicio con cláusulas de seguridad, etcétera.

La fase *do* suele ser la más larga en tiempo, es la «vida operativa» del SGSI. En este punto, la organización realmente protege y gestiona su seguridad continuamente.

Check (verificar): en esta fase, se evalúa el desempeño del SGSI y se comprueba si lo aplicado es eficaz y conforme a lo planificado. Incluye actividades de monitorización, medición, auditorías internas y revisión por la dirección. Las cláusulas relevantes de ISO 27001 aquí son la 9.1 (medición y monitoreo), 9.2 (auditoría interna) y 9.3 (revisión gerencial).

Evidencias auditables en *check*

- **Resultados de medición y monitoreo**: por ejemplo, indicadores de cumplimiento de objetivos (¿se redujeron los incidentes en X %?), métricas de seguridad (número de incidentes, tiempos de respuesta, porcentaje de sistemas parchados, etcétera). Muchas de

estas métricas se preparan para la revisión de dirección.

- **Informe(s) de auditoría interna**: ISO requiere que al menos anualmente se lleve a cabo una auditoría interna del SGSI, es decir, un autoexamen sistemático que demuestre que la organización cumple sus propios procedimientos y la norma. El resultado es un informe documentado que lista hallazgos: no conformidades (incumplimientos), observaciones, oportunidades de mejora. Este informe es evidencia fundamental de la fase *check*.

- **Acta o informe de revisión por la dirección**: la alta dirección debe reunirse (usualmente anual) para revisar el SGSI (se discuten resultados de auditorías, estado de acciones previas, cambios en circunstancias, logros de objetivos, nuevos riesgos, etcétera). Queda documentado en un acta con las decisiones tomadas (por ejemplo, aprobar nuevo presupuesto para seguridad, cambiar un objetivo, necesitar más personal, etcétera).

- **Evidencias de cumplimiento legal**: parte de la verificación es garantizar que se cumplen requisitos legales y contractuales (por ejemplo, si aplica GDPR, demostrar que se hicieron las evaluaciones de impacto, etcétera).

- **Revisión de riesgos actualizada**: a veces, como parte del *check*, se reevalúan ciertos riesgos para ver si bajaron con los controles aplicados o si surgieron nuevos riesgos.

En esta fase, la organización detecta desviaciones o áreas de mejora. Por ejemplo, la auditoría interna podría descubrir que no todos los usuarios cambiaron sus contraseñas en noventa días según política (hallazgo), o que falta formalizar un procedimiento. Asimismo, la revisión gerencial podría notar que, a pesar de menos incidentes, la satisfacción de clientes bajó por demoras (indicando un efecto colateral a revisar). Todo esto alimenta la siguiente fase.

Act (actuar/ajustar): la última fase cierra el ciclo alimentando la mejora continua. Consiste en tomar acciones correctivas o de mejora con base en lo encontrado en *check*. La ISO 27001 (cláusula 10) habla de acciones para abordar no conformidades y mejorar continuamente la eficacia del SGSI.

Ejemplos de acciones *act*

- **Corrección de no conformidades**: si la auditoría interna halló que cierto control no se aplicó, en *act* se designan acciones para corregirlo. Por ejemplo, si faltaba un registro, se crea; si un procedimiento no se seguía, se reentrena al personal o se modifica el procedimiento para que sea aplicable.

- **Mejoras preventivas**: más allá de los fallos, la organización puede detectar oportunidades de mejora. Por ejemplo, quizás el indicador de tiempo de respuesta a incidentes cumplió la meta, pero se cree que se puede mejorar aún más aplicando una nueva herramienta SIEM. Entonces, en *act* se planifica ese proyecto.

- **Actualización de documentación**: después de cambios, se actualizan políticas, procedimientos, evaluaciones de riesgo. Por ejemplo, surgen nuevas amenazas (*ransomware targeting* su sector); entonces,

en *act* se actualiza la apreciación de riesgos para incluirlo y se planifican controles nuevos.

- **Refinamiento de objetivos**: si se lograron objetivos fácilmente, quizá se endurecen para el próximo período; si no se lograron, se analiza por qué y se ajustan o se ponen recursos adicionales.

Un concepto importante en *act* es la acción correctiva formal: ISO pide evidenciar que, cuando ocurre un incidente o no conformidad, se analiza su causa raíz y se toman medidas para que no se repita. Esto implica documentar el problema, causa y acción correctiva aplicada. Por ejemplo: incidente «ingreso no autorizado a una cuenta admin»; causa: credencial compartida y sin 2FA; acción: se aplica autenticación multifactor y se prohíbe compartir cuentas.

Evidencias típicas de *act*

- **Registro de acciones correctivas/mejora**: muchas organizaciones llevan un *log* o plan de mejoras, en el que apuntan fecha, descripción de la mejora, responsable, estado.
- **Informes de cierre de no conformidades**: por ejemplo, al cabo de tres meses de la auditoría interna, se genera un informe de que todas las NC fueron atendidas, con evidencias de corrección.

- **Nuevos procedimientos o políticas actualizadas**: si la mejora requirió crear/modificar documentos, quedarán como evidencia (con control de versión mostrando la fecha del cambio).

- **Lecciones aprendidas de incidentes**: informes *post mortem* de incidentes significativos, con las mejoras aplicadas.

Tras *act*, se vuelve a *plan* y el ciclo continúa, idealmente con un SGSI cada vez más maduro y eficaz. Este concepto cíclico está explícitamente mencionado en ISO 27001, que indica que el SGSI debe mantenerse y mejorarse continuamente (cláusula 10).

Evidencias auditables y certificación

Un SGSI avanzado genera bastante documentación. Parte será requerida en auditorías de certificación ISO 27001. Por ejemplo, los auditores querrán ver los siguientes aspectos:

- la política de seguridad aprobada.
- El alcance definido del SGSI.
- El análisis de riesgos documentado y vigente.
- La declaración de aplicabilidad actualizada, lo que muestra la justificación de cada control aplicado/no aplicado.
- Procedimientos y registros que demuestren aplicación de controles (listas de acceso, reportes de antivirus, etcétera).
- Registros de auditorías internas y revisiones de dirección.
- Evidencia de acciones correctivas ante fallos.
- Registros de entrenamiento en seguridad del personal (para verificar concienciación).
- Documentación de requisitos legales aplicables (por ejemplo, si manejan datos personales, evidencia de cumplimiento de Ley de Protección de Datos).

La frase «evidencias auditables» significa que no basta decir «hacemos tal cosa»; hay que poder mostrar registro objetivo de que se hace. En auditoría, «lo que no está documentado, no existe». Por esta razón, aunque a veces es visto burocrático, un SGSI requiere llevar registros. Un punto de equilibrio importante es no burocratizar de más: se debe documentar lo necesario para demostrar eficacia, pero evitando que la seguridad se vuelva un ejercicio de *paperwork* desconectado de la realidad. La automatización ayuda: por ejemplo, en lugar de hacer *checklists* en papel para verificación diaria de *logs*, se puede tener un sistema SIEM que genere reportes (la evidencia puede ser digital).

La mejora continua como cultura: más allá de la certificación, adoptar PDCA inculca una mentalidad de que la seguridad siempre puede fortalecerse. Las amenazas evolucionan constantemente, así que un SGSI debe igualmente evolucionar. Organizaciones maduras integran PDCA en su gobernanza de seguridad: reuniones mensuales de un comité de seguridad (*plan*/*do*/*check* en pequeño ciclo), revisiones trimestrales con gerencia, etcétera, no solo una vez al año por cumplir. Así, detectan antes los desvíos y reaccionan con agilidad.

Relación con NIST CSF: interesantemente, el ciclo PDCA de ISO 27001 se alinea con la idea de **funciones** de NIST CSF (identificar, proteger, detectar, responder, recuperar, gobernar), que veremos en la unidad 2. Ambos comparten la lógica de ciclo de vida. Por ejemplo, «*identify*» en CSF corresponde a *plan* (identificar riesgos y activos), «*protect*» a *do* (aplicar controles), «*detect*» y «*respond*» a *check*/*act* (monitorear y responder), etcétera. Esta compatibilidad facilita que muchas organizaciones usen ISO 27001 e inspiren su operación en marcos como NIST para los detalles, o viceversa.

Para cerrar esta unidad, consolidemos con un caso práctico integrado todos estos elementos del SGSI en acción.

Caso práctico: implementación inicial de un SGSI en una empresa de servicios financieros

Contexto

FinBanco S. A. es una entidad mediana de servicios financieros que maneja datos sensibles de clientes (nombres, cuentas bancarias, historiales crediticios). La gerencia, preocupada por

riesgos cibernéticos y para cumplir regulaciones, decide poner en marcha un SGSI y buscar certificación ISO 27001. Veamos cómo FinBanco aborda los pasos principales.

- **Alcance y política**: la empresa define el alcance del SGSI abarcando todas las operaciones de banca electrónica y tratamiento de datos de clientes en la oficina central de Buenos Aires. Excluyen, por ahora, sucursales pequeñas (que planean incluir en el futuro). Aprueban una política de seguridad en la que declaran su compromiso de proteger datos de clientes conforme a leyes (Ley de Protección de Datos Personales) y estándares internacionales, asignando al CIO como líder del SGSI. La política establece que la confidencialidad de la información financiera del cliente es prioritaria, y ordena clasificar la información y aplicar controles estrictos.

- **Roles y organización**: el CEO de FinBanco firma la política, lo que demuestra su apoyo. Nombra al CIO como responsable global del SGSI (similar a un CISO). Se forma un Comité de Seguridad con el CIO, el gerente de TI, el de Riesgos, y representante de Auditoría Interna, que se reunirá mensualmente. Asignan propietarios: gerente de Banca Digital es dueño de los datos de clientes; gerente de Infraestructura es dueño de los servidores y las redes. Todos los empleados reciben un comunicado en el que se les explica la política y sus responsabilidades (no compartir contraseñas, reportar incidentes, etcétera).

- **Inventario y clasificación**: un equipo liderado por el CIO lleva a cabo sesiones con cada departamento para identificar activos.

Descubren, por ejemplo: una base de datos principal de clientes (en un servidor SQL), un servidor web de banca *online*, PC de analistas que descargan reportes, archivos en papel de contratos antiguos, correos electrónicos con datos sensibles, etcétera. Con esa información, construyen un **Inventario**. Luego, definen **clasificaciones:**

- datos personales y financieros de clientes. Clasificación = confidencial alta (similar a secreto). Es decir, requieren cifrado y acceso muy restringido.
- Datos agregados no identificables (por ejemplo, estadísticas): internos, sensibles, moderados.
- Publicaciones de tasas de interés y promociones: públicas, sin restricción.
- Documentos legales internos: confidenciales.
- Y así sucesivamente con cada tipo de información.

Etiquetan la base de datos de clientes como «confidencial alta». Implementan que toda pantalla o reporte con esos datos muestre la etiqueta «**confidencial**». Los archivos de contrato físico se sellan como «**confidencial**» y se guardan bajo llave con registro de acceso

- **Análisis de riesgos** (plan): identifican amenazas. *Hackers* externos podrían atacar la banca *online*, empleados internos podrían filtrar datos, *malware* podría cifrar los servidores, desastres naturales podrían inutilizar el data center, etcétera. Para cada riesgo, evalúan impacto (muy alto si filtran

datos de clientes; multa y pérdida reputacional) y probabilidad (moderada por intento de ciberataques frecuentes). Priorizan riesgos altos como «robo de datos de clientes por ciberdelincuentes» y «*ransomware* en servidor central». Deciden llevar a cabo el siguiente tipo de tratamientos:

- para el riesgo de robo de datos. Aplicar multifactor en acceso de administradores, monitoreo de intrusiones, pruebas de penetración periódicas.
- Para *ransomware*: segmentar la red, tener *backups offline* diarios, entrenar empleados contra phishing.
- Para riesgo de empleado interno deshonesto: aplicar control de doble custodia (ningún empleado puede bajar todos los datos sin que salte una alerta), revocar accesos inmediatamente al egreso, monitorizar actividades inusuales.

Documentan todo en una matriz de riesgos. También preparan la declaración de aplicabilidad: deciden aplicar la mayoría de controles del anexo A dada la criticidad (por ejemplo, controles de cifrado, control de acceso, registro de eventos, seguridad en redes, etcétera). Deciden no aplicar, por ejemplo, el control de seguridad de desarrollo de *software* seguro porque FinBanco no desarrolla *software* internamente (usa paquetes comerciales). Justifican en la SoA: «no aplica por no tener desarrollo *in-house*».

- **Implementación de controles (do)**

Siguiendo el plan:

- compran e instalan un *firewall* de nueva generación en la frontera de red con monitoreo de intrusiones (IPS). Configuran reglas para bloquear IP maliciosas conocidas.
- Habilitan **cifrado** de la base de datos de clientes y de los discos de servidores.
- Implementan **doble autenticación (2FA)** para todos los empleados al VPN y sistemas críticos.
- Redactan procedimientos: cómo gestionar incidentes (un plan de respuesta), cómo hacer *backup* (política de respaldo diario con regla 3-2-1), cómo manejar cuentas de usuarios (creación, baja).
- Realizan una **formación en seguridad** para todo el personal, cubriendo *phishing*, uso aceptable de *e-mail*, etcétera. Guardan lista de asistentes y calificaciones de un *quizz*.
- Mejoran la seguridad física del data center: cerraduras electrónicas, cámara de vigilancia (evidencia de control 7.4 de monitoreo físico).
- Firman con su proveedor de hosting un **acuerdo de nivel de servicio (SLA)** que incluye cláusulas de seguridad (notificación de incidentes en 24 h, cifrado de *backups*, etcétera).
- Establecen un **sistema SIEM** para centralizar *logs* de servidor web, base de datos y *firewall*, con alertas en tiempo real al equipo de TI ante eventos sospechosos (por ejemplo, múltiples intentos fallidos de *login* de administrador).

Todo lo anterior genera evidencias: configuraciones de *firewall* exportadas, actas de instalación de cámaras, registros de la capacitación. El SGSI de FinBanco comienza a funcionar operativamente.

- **Verificación** (*check*): tras unos meses de operación, FinBanco ejecuta una auditoría interna. Un auditor interno (de la división de riesgos) revisa si los controles implementados siguen las políticas:

  - revisa muestras de registros. Encuentra que se están haciendo *backups* diarios (bien), pero nota que en dos servidores no se aplicaron parches en el tiempo establecido (hallazgo menor).
  - Entrevista a empleados: la mayoría conoce la política, pero algunos nuevos no recibieron la inducción de seguridad (hallazgo: brecha en capacitación).
  - Lanza un *test de phishing simulado*: 10 % de empleados hizo clic en un enlace falso. No es terrible, pero es área de mejora (objetivo futuro: reducir a 5 %).
  - Comprueba el cumplimiento legal: todo *ok* con protección de datos personales (tienen consentimiento de clientes y medidas adecuadas).
  - Revisa *logs*: detecta que, si bien hay SIEM, las alertas no estaban afinadas y algunas posibles amenazas pasaron sin investigación (hallazgo a ajustar).

  El auditor interno genera un **informe** en el que lista tres no conformidades menores y varias recomendaciones. La dirección se reúne

en la revisión anual del SGSI. Observan: se cumplió el objetivo de dos simulacros de recuperación (los hicieron, salieron bien), disminuyeron incidentes en un 30 % respecto al año anterior, pero hubo un incidente real en el que un empleado envió por error datos de un cliente a otro (error humano). Deciden que hay que reforzar la concienciación. La revisión concluye con decisiones: invertir en una herramienta de clasificación de documentos para evitar envíos erróneos, y mejorar el proceso de parches.

- **Acciones correctivas (act)**

  FinBanco elabora un **plan de mejora**:

  - para los parches atrasados, TI implementó un nuevo sistema de gestión de actualizaciones centralizado y define un KPI para que 95 % de sistemas estén parchados en quince días. En tres meses se corrige y el auditor interno verifica cumplimiento.
  - Para capacitación de nuevos: recursos humanos y seguridad aplican que todo empleado nuevo reciba entrenamiento dentro de sus primeros quince días. Documentan este proceso nuevo.
  - Después del incidente de envío erróneo de datos, definen un nuevo control (herramienta DLP en correo que detecte y alerte si se adjuntan datos de clientes sin cifrar). A los dos meses la instalan y prueban.
  - El SIEM se reconfigura para afinar alertas y se asigna formalmente un analista de TI

para revisarlas diariamente. Se añade esa revisión al *checklist* diario de TI.

- Fijan un nuevo objetivo para el próximo año: «reducir la tasa de clic en *phishing* al 5 %» y planean campañas trimestrales de *phishing* simulado con *feedback* personalizado a quien caiga.

Todas estas acciones quedan registradas. Al cabo de un año, FinBanco invita a un auditor externo y logra la certificación ISO 27001:2022, presentando como evidencia toda la documentación y mejoras logradas. Sin embargo, más allá del certificado, lo importante es que han establecido un **proceso vivo**: cada año repiten el ciclo PDCA, adaptando la seguridad a nuevas amenazas (por ejemplo, incorporan un control de *threat intelligence* [inteligencia de amenazas], para estar al día en tácticas de fraude financiero). Así, mantienen su SGSI relevante y eficaz en protección de datos de sus clientes y los intereses de la empresa.

Este caso ilustra cómo todos los elementos —estructura de la norma, roles, alcance, políticas, inventarios, controles, ciclo PDCA— se articulan en la práctica. En la siguiente unidad, exploraremos el NIST Cybersecurity Framework 2.0, que complementa este enfoque de gestión con un marco flexible de controles y funciones de ciberseguridad, profundizando en aspectos de gobernanza, riesgo e infraestructura.

CONTINUAR

Unidad 2: NIST CSF 2.0 y gobernanza

Unidad 2: NIST CSF 2.0 y gobernanza

En esta unidad, el objetivo es conocer la estructura y los componentes del *framework* de ciberseguridad NIST CSF (Instituto Nacional de Estándares y Tecnología [NIST], 2024) versión 2.0, incluyendo sus seis funciones principales (*identify*, *protect*, *detect*, *respond*, *recover*, y la nueva función *govern*); entender los énfasis nuevos de la versión 2.0 en gobernanza, gestión de riesgos, cadena de suministro e identidad; aprender cómo se usan los perfiles, niveles (*tiers*) y métricas para aplicar y evaluar el marco, y, finalmente, apreciar la trazabilidad entre controles específicos y procesos de gestión de riesgos dentro del CSF 2.0. Se presentará un caso práctico de aplicación de NIST CSF en una organización ficticia y cómo este marco se integra con un SGSI.

2. 1. Introducción al NIST Cybersecurity Framework 2.0

El NIST Cybersecurity Framework (CSF) es un marco de referencia desarrollado por el National Institute of Standards and Technology (NIST) de EE. UU., inicialmente publicado en 2014 para mejorar la ciberseguridad en infraestructuras críticas. Su adopción se ha extendido globalmente a organizaciones de todos los sectores debido a su carácter práctico y flexible. A diferencia de ISO 27001 (una norma de sistema de gestión certificable), el NIST CSF es voluntario y no certificable, centrado en buenas prácticas y guías para gestionar riesgos de ciberseguridad. Se puede usar como complemento a ISO 27001 o de forma independiente.

En febrero de 2024, NIST publicó la versión 2.0 final del CSF, la primera gran actualización desde 2014 (la versión 1.1 se lanzó en 2018 con cambios menores). CSF 2.0 trae mejoras significativas para ampliar su aplicabilidad y actualizarlo ante nuevas amenazas. Entre los cambios generales, están los siguientes:

- incorporación explícita de la función *govern* (gobernar). Eleva la importancia de la gobernanza de ciberseguridad al mismo nivel que las funciones técnicas. Esto responde a la necesidad de involucrar liderazgo y gestión de riesgos corporativos en la seguridad (no verlo solo como tema técnico).

- Enfoque ampliado a todos los sectores y tamaños de organización: si bien nació para infraestructuras críticas, ahora CSF 2.0 se presenta útil para cualquier organización, desde pymes hasta gobiernos y ONG. Incluye guías flexibles para adaptarse según recursos disponibles.

- Mayor énfasis en seguridad de la cadena de suministro y gestión de terceros: reconociendo que muchos incidentes provienen de proveedores (*third-parties*), la nueva versión refuerza prácticas para identificar y gestionar riesgos en la cadena de suministro digital.

- Integración con estándares internacionales: se ha alineado mejor terminología y estructura para mapear fácilmente CSF con ISO 27001:2022, COBIT, la directiva NIS2 europea, etcétera. Esto facilita a organizaciones globales cumplir múltiples marcos con un solo esfuerzo.

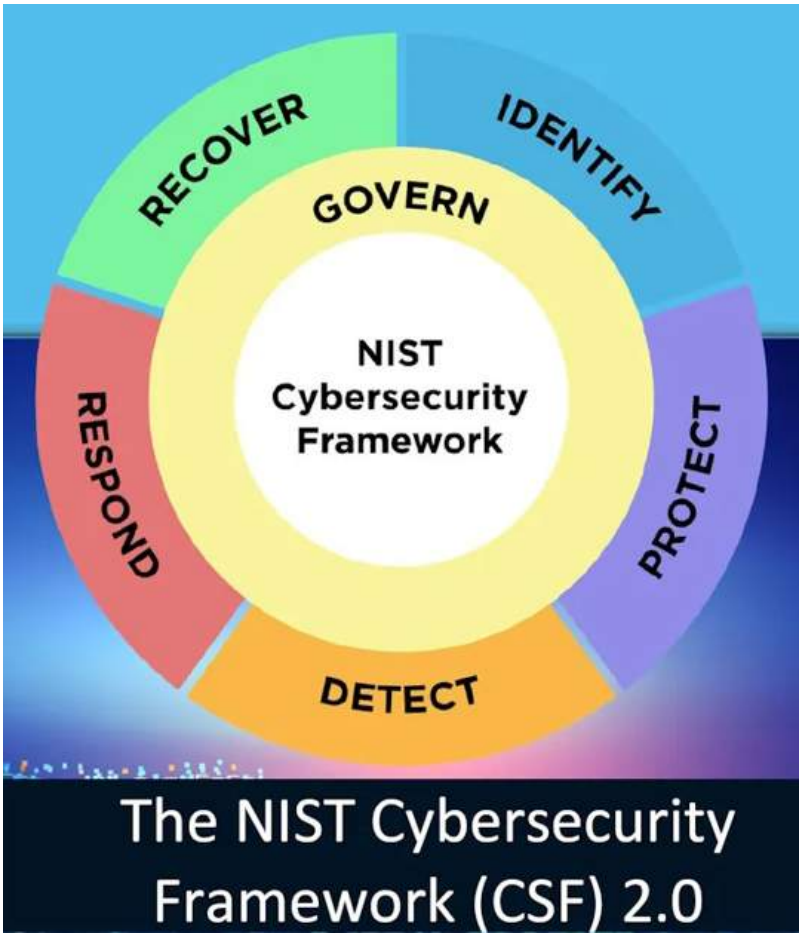
- Introducción de más recursos y herramientas: NIST acompañó CSF 2.0 con un portal interactivo, plantillas de perfiles, guías rápidas e implementación *examples*, para ayudar a las organizaciones a adoptarlo paso a paso. Esto reduce la confusión que algunos manifestaban al interpretar controles.

En esencia, CSF 2.0 mantiene el núcleo de la versión previa, pero lo fortalece en gobernanza y medición. Como se mencionó, no es una normativa obligatoria (salvo para ciertas agencias federales en EE. UU.), sino un **lenguaje común** para gestionar ciberseguridad. Muchas empresas lo usan para evaluar su postura de seguridad y comunicarla a la dirección o clientes de forma estructurada.

2. 2. Funciones principales del NIST CSF 2.0: *identify, protect, detect, respond, recover y govern*

El *framework core* del NIST CSF está organizado en un conjunto de funciones de alto nivel, que representan las fases o pilares de un programa integral de ciberseguridad. En CSF 1.1 había cinco funciones (*identify*, *protect*, *detect*, *respond*, *recover*). La versión 2.0 añade una sexta función al inicio: *govern* (gobernar). Estas funciones, en conjunto, proporcionan una visión completa del ciclo de vida de la gestión del riesgo de ciberseguridad.

Figura 2: Gráfico ilustrativo de las seis funciones centrales del NIST Cybersecurity Framework 2.0.



Fuente: [imagen sin título sobre gráfico ilustrativo de las seis funciones centrales del NIST Cybersecurity Framework], s. f., https://bit.ly/3XIU4i0.

A continuación, se describe cada función y sus categorías principales.

Govern (gobernar [nueva función en CSF 2.0]): se refiere a establecer la estructura organizativa, políticas, procesos y la cultura necesarios para que la ciberseguridad se gestione alineada con los objetivos del negocio y las obligaciones legales En otras palabras, es la capa de gobernanza corporativa de la seguridad. Incluye asegurar que la dirección se involucre, definir roles y responsabilidades claras, gestionar la estrategia de riesgos de ciberseguridad a nivel organización y supervisar el desempeño.

Categorías de *govern*

CSF 2.0 define seis categorías dentro de la función gobernar.

- **GV.OR** (contexto organizacional): entender el contexto de la organización, su misión, objetivos y cómo la ciberseguridad encaja en ellos. Incluye considerar requisitos legales, normativos y las partes interesadas en ciberseguridad.

- **GV.RM** (estrategia de gestión de riesgos): establecer cómo se gestionan los riesgos de ciberseguridad (metodologías, apetito de riesgo, criterios de aceptación, integración con gestión de riesgos empresarial).

- **GV.RR** (roles, responsabilidades y autoridad): definir quién hace qué en ciberseguridad, asignando autoridades adecuadas. Esto refleja lo tratado en la unidad 1 sobre roles del SGSI.

- **GV.PO** (políticas): establecer políticas de ciberseguridad (principios y reglas organizacionales), asegura que existan políticas aprobadas y comunicadas.

- **GV.OV** (supervisión): proveer supervisión de la función de ciberseguridad por parte del liderazgo (por ejemplo, juntas directivas recibiendo reportes, seguimiento a métricas).

- **GV.SC** (gestión de riesgo de cadena de suministro): incorporar la seguridad de proveedores y terceros en la gestión de riesgos global. Dado el foco en *supply chain*, se agregó esta categoría específica para asegurarse de que se evalúen y mitiguen riesgos que vienen de fuera de la organización (*software* de terceros, servicios *cloud*, proveedores de TI).

Las actividades claves en *govern* incluyen fijar apetito de riesgo formalmente, integrar ciber en la gestión de riesgos de empresa, asegurar que los líderes (C-suite, directorio) reciban información periódica de seguridad, y establecer **líneas de reporte** claras (por ejemplo, que un CISO reporte al directorio riesgos regularmente). En resumen, *govern* se trata de crear el entorno organizacional propicio para que las otras funciones (*identify*, *protect*, etcétera) ocurran de manera coordinada y con respaldo ejecutivo.

- ***Identify*** (identificar): es la función base. Comprende desarrollar una comprensión de la organización para manejar los riesgos de ciberseguridad. Equivale a reconocer qué activos tenemos, qué riesgos enfrentamos y cuál es nuestro entorno. Sin esta fase, las siguientes no pueden ser efectivas.

Categorías de *identify* (versión 2.0)

Son tres categorías.

- **ID.AM** (*asset management* [gestión de activos]): inventario de activos físicos, *software*, datos, y recursos organizacionales y conocer su importancia. Similar a lo visto en unidad 1 (inventario de activos de información).
- **ID.RA** (*risk assessment* [evaluación de riesgos]): identificar vulnerabilidades, amenazas internas y externas, y llevar a cabo evaluaciones de riesgo de ciberseguridad. Incluye determinar impactos potenciales y priorizar riesgos.

- **ID.IM** (*improvement* [mejora]): esta categoría es nueva en CSF 2.0. Se refiere a identificar oportunidades de mejora continua del programa de ciberseguridad e incorporar aprendizajes pasados en la gestión actual.

Las actividades claves en *identify* incluyen mapear la superficie de ataque (qué sistemas existen, dónde están las informaciones críticas), comprender el entorno de negocio y dependencias (por ejemplo, rol en la cadena de suministro global), identificar requerimientos legales aplicables, determinar la postura actual de seguridad y dónde hay brechas. En la práctica, esta función produce resultados como listas de activos priorizados, un registro de riesgos (*risk register*), y define el contexto para planificar la función *protect*. Es el análogo a la fase «planificar» y «contexto» de ISO 27001: tener clara la foto inicial.

- ***Protect*** (proteger): se centra en aplicar salvaguardas o medidas de protección para limitar o contener el impacto de potenciales eventos de ciberseguridad. Es la función que abarca todos los controles preventivos y de mitigación que se ponen en marcha para proteger activos y garantizar la entrega de los servicios esenciales.

Categorías de *protect*

La versión 2.0 reorganiza un poco las categorías (respecto a 1.1) y son cinco.

- **PR.AA** (*identity management*, *authentication and access control* [gestión de identidades y control de accesos]): incluye prácticas de control de acceso lógico y físico, gestión de identidades, autenticación (por ejemplo, MFA) y sesiones. Es vital asegurar que solo quienes deben acceden a información/sistemas, y que

la identidad de usuarios y dispositivos está verificada.

- **PR.AT** (*awareness and training* [concienciación y capacitación]): asegurar que el personal y partes relevantes reciben entrenamiento adecuado en seguridad y concienciación de ciberamenazas. La gente educada es una capa protectora (evita *phishing*, errores humanos).

- **PR.DS** (*data security* [seguridad de datos]): protecciones para garantizar la confidencialidad, integridad y disponibilidad de la información. Incluye cifrado, protección de datos en reposo y tránsito, gestión de claves, políticas de retención y destrucción de datos, etcétera.

- **PR.PS** (*platform security* [seguridad de plataformas]): mecanismos para proteger las plataformas de TI y OT (tecnología operativa) incluyendo mantenimiento seguro, gestión de configuraciones seguras, endurecimiento de sistemas. Se centra en garantizar que sistemas y dispositivos tengan configuración segura y se mantienen así.

- **PR.IR** (*technology infrastructure resilience* [resiliencia de la infraestructura tecnológica]): controles para asegurar la resiliencia de sistemas y servicios ante eventos (por ejemplo, *backups*, planes de continuidad, redundancia, gestión de capacidad). Si ocurre algo, la infraestructura debe resistir o recuperarse rápido.

Actividades claves en *protect*

Estas pueden ser aplicar *firewalls*, control de accesos basado en roles, segmentar redes, hacer mantenimiento preventivo, actualizaciones/*patchemangement*, gestionar vulnerabilidades (*scans* y remediación), establecer políticas de uso aceptable, usar herramientas DLP, etcétera. El objetivo es reducir la probabilidad de incidentes y limitar posibles daños si uno ocurre. Representa la puesta en práctica de los controles planificados durante *identify/govern*.

- ***Detect*** (detectar): esta función se centra en la detección temprana de incidentes o eventos anómalos. Asume que, a pesar de las protecciones, algunos ataques o fallos ocurrirán, por lo que es crítico descubrirlos oportunamente antes de que causen demasiado daño

Categorías de *detect*

CSF 2.0 las redujo a dos (eran tres en v1.1).

- **DE.CM** (*continuous monitoring* [monitoreo continuo]): vigilancia continua de redes, sistemas y el entorno para identificar eventos de ciberseguridad y verificar la efectividad de los controles protectores. Incluye monitoreo de anomalías, intrusiones, desempeño de sistemas, etcétera.

- **DE.AE** (*adverse events analysis* [análisis de eventos adversos]): capacidad para analizar alertas e información recolectada para determinar si indican un evento de ciberseguridad y comprender su naturaleza/alcance. O sea, es el proceso de

triage e investigación inicial cuando se detecta alg.

Actividades claves en *detect*

Estas incluyen el uso de SIEM/SOAR para correlacionar logs de seguridad y generar alertas, aplicar IDS/IPS, hacer análisis de tráfico en busca de comportamientos sospechosos, establecer procedimientos de monitoreo 24/7 (propio o tercerizado), emplear detección de *endpoint* (EDR), y hacer pruebas periódicas (como ejercicios de Red Team) para asegurarse de que la organización podría detectar un ataque simulado. Un buen *framework* de detección reduce el *dwell time* (tiempo que un atacante permanece sin ser descubierto).

- ***Respond* (responder)**

Esta función cubre las acciones a tomar una vez detectado un incidente para controlarlo y reducir su impacto. Incluye planificar previamente cómo responder y gestionar adecuadamente los incidentes en curso.

Categorías de *respond*

Hay cuatro categorías.

- **RS.MA** (*incident management* [gestión de incidentes]): ejecución de procesos de respuesta durante y después de un incidente. Asegura que existe un plan de respuesta a incidentes y se sigue.
- **RS.AN** (*analysis* [análisis del incidente]): actividades de análisis profundo durante la respuesta, para entender completamente el incidente, su origen, alcance, impacto. Incluye

realizar forense digital, determinar qué datos fueron afectados, etcétera.

- **RS.CO** (*response communications* [comunicación durante la respuesta]): gestión de las comunicaciones internas y externas mientras se responde al incidente. Esto abarca notificar a la dirección, al equipo legal, a clientes/reguladores si corresponde y mantener informados a *stakeholders* con transparencia.

- **RS.MI** (*mitigation* [mitigación]): acciones para contener y erradicar el incidente. Por ejemplo, aislar sistemas comprometidos, eliminar *malware*, aplicar parches, cambiar credenciales comprometidas, etcétera, para evitar que el incidente se propague o vuelva a ocurrir.

Actividades claves en *respond*

Tener un equipo de respuesta entrenado (CSIRT o similar), *playbooks* para distintos tipos de incidentes (por ejemplo, *ransomware*, DDoS, fuga de datos), hacer *drills* o simulacros regularmente, y al ocurrir un incidente real, llevar registro de todas las acciones y decisiones (lo cual servirá para análisis posterior). Un punto crítico es la comunicación: las decisiones de cuándo y cómo notificar (por ejemplo, avisar a clientes de un *breach*) son parte de esta función.

- ***Recover*** (recuperar): la función final se ocupa de las actividades para restaurar cualquier capacidad o servicio afectado tras un incidente y volver a la operación normal, aprendiendo de la experiencia. Apunta a la resiliencia organizacional.

Categorías de *recover*

Son dos categorías.

- **RC.RP** (*recovery planning* [planificación de la recuperación]): ejecución de planes para restablecer sistemas y datos luego de un incidente. Incluye planes de continuidad de negocio, de recuperación de desastres, etcétera.
- **RC.CO** (*recovery communications* [comunicación postincidente]): las comunicaciones coordinadas con interesados durante y después de la recuperación. Abarca informes finales a la dirección, notificación de resolución a clientes/autoridades, comunicados de prensa si era público, etcétera.

Actividades claves en *recover*

Estas incluyen: uso de *backups* para restaurar datos perdidos, conmutación a sitios alternos si un centro de datos quedó inutilizado, ejecución de planes de contingencia manual si los sistemas no están operativos (por ejemplo, procesos en papel temporales), análisis de lecciones aprendidas para mejorar planificaciones futuras. Una vez recuperado todo, se suele hacer un informe *post mortem* del incidente para documentar qué ocurrió, cómo se resolvió y qué mejoras se harán (eso retroalimenta *govern*/*identify*).

Estas seis funciones no son secuenciales estrictamente, sino más bien concurrentes y complementarias. Es decir, la organización debe sostener capacidades en las seis áreas en todo momento: mientras protege, también debe estar lista para detectar, etcétera. Sin embargo, hay cierta lógica de flujo: *govern* establece el marco*, identify* y *protect* previenen,

detect encuentra problemas, *respond* los ataca, *recover* restablece y de nuevo *govern* ajusta y comunica.

En CSF 2.0, se destaca que las seis funciones juntas brindan una visión integral de cómo gestionar el riesgo de ciberseguridad. También se menciona que esta estructura permite una comunicación sencilla hacia ejecutivos: por ejemplo, un reporte al directorio puede estructurarse en estas seis áreas para resumir la postura de ciberseguridad. La nueva función *govern* encaja perfectamente con la necesidad de tratar la ciberseguridad como riesgo empresarial, lo que facilita conversaciones con niveles ejecutivos en su lenguaje (riesgos, políticas, cumplimiento).

2. 3. Enfoque en riesgo, cadena de suministro e identidad en CSF 2.0

La versión 2.0 del NIST CSF hace hincapié especial en algunos aspectos que merecen atención.

Gestión de riesgos (*risk management*): la gestión de riesgos es la columna vertebral del CSF. Desde la función *govern* (estrategia de riesgo) hasta *identify* (evaluación de riesgos) y todas las demás (que son básicamente respuestas al riesgo), el CSF 2.0 refuerza que debe haber un proceso de riesgo bien establecido. Se alinea con *frameworks* de *risk management* como NIST SP 800-39 e ISO 31000. En CSF 2.0 se deja claro que el proceso subyacente para aplicar el *framework* es un ciclo de gestión de riesgos adaptativo. Por ejemplo, la función *govern* requiere definir apetito/tolerancia al riesgo, y los *tiers* (niveles) miden la madurez con que la organización gestiona el riesgo (lo veremos en 2.4). La consideración de riesgo es continua: incluso la función *recover* incluye analizar si nuevos riesgos surgieron tras un incidente y ajusta el programa.

En resumen, NIST CSF 2.0 integró totalmente el concepto de riesgo: no es una lista de controles sin contexto, sino un ciclo para identificar y mitigar riesgos de acuerdo a prioridades del negocio. Esto lo hace muy semejante en filosofía a ISO 27001, lo que facilita mapeo mutuo.

Cadena de suministro (*supply chain*): como anticipamos, CSF 2.0 destaca la seguridad de la cadena de suministro de una manera mucho mayor que CSF 1.1. Esto era de esperar dados incidentes de alto perfil vía proveedores (por ejemplo, ataque SolarWinds en 2020, en el que comprometieron a miles de organizaciones a través de una actualización de *software* de un tercero). Los aspectos de *supply chain* aparecen en varias funciones.

- en *identify* (ID.SC en v1.1), se consideraba entender el rol de la organización en la cadena de suministro y riesgos asociados. En CSF 2.0 este punto está tanto en *govern* (GV.SC) como en *identify* (por ejemplo, ID.BE Business Environment consideraba *supply chain*; posiblemente ahora ID.IM toca mejoras en esa área).

- La nueva categoría **GV.SC** dentro del dominio de gobernar garantiza atención ejecutiva a riesgos de terceros. Esto implica, por ejemplo, que la dirección exija evaluación de seguridad a proveedores críticos o tenga políticas para terceros.

- En ***protect*** y ***detect***, se asume que los controles se extienden a terceros: por ejemplo, concienciación (PR.AT) podría incluir concienciación a contratistas; monitoreo continuo (DE.CM) puede incluir monitorizar conexiones de proveedores a tus sistemas.

- Adicionalmente, NIST publicó guías como SP 800-161 (gestión de riesgos de *supply*

chain) que complementan CSF. CSF 2.0 referencia alinearse con esas prácticas.

Concretamente, se espera que organizaciones usando CSF 2.0:

- identifiquen sus proveedores y dependencias críticas, y valoren riesgos de cada uno (¿qué pasa si tal proveedor es comprometido?).
- Exijan controles de seguridad a terceros (por contrato, evaluaciones de cumplimiento, certificaciones).
- Monitoreen la seguridad de proveedores (por ejemplo, pedir reportes periódicos o usar servicios de *ratings* de seguridad).
- Tengan planes ante fallo de un proveedor (resiliencia: alternativas, etcétera).

Supply chain risk es ahora un *outcome* a lograr explícitamente con CSF 2.0, no algo tácito. Esto cierra una brecha de v1.1 y refleja la realidad actual de ecosistemas interconectados.

- **Identidad** (*identity*): el término identidad en ciberseguridad abarca gestión de identidades digitales y accesos (IAM [*identity and access management]).* Ya en CSF 1.1 se le daba importancia (categoría PR.AC [control de acceso]). En CSF 2.0, *identity management* aparece nombrado más prominentemente en la categoría **PR.AA (**identity management, authentication and access control). Esto recalca asegurar:

- **identidades confiables**. Cada usuario, sistema, dispositivo tiene una identidad única y autenticada. Aplica principios de *zero trust* en los que la identidad es el nuevo perímetro.
- **Autenticación robusta**: uso de autenticación *multifactor*, métodos seguros y gestión de credenciales adecuada.
- **Menor privilegio**: identidad ligada a roles con privilegios mínimos necesarios (y revocación oportuna si cambia rol).
- **Identidad de dispositivos/servicios**: no solo usuarios, también maquinaria, API, microservicios deben tener identidades gestionadas (certificados, *tokens).*

Además, en la versión 1.1 tras actualizaciones se mencionó *identity proofing* (verificación de identidad de usuarios) y mejoras en autenticación. En la 2.0, si bien no agrega una categoría nueva sobre identidad, la inclusión del término en el título PR.AA. refleja la tendencia de verlo integral con *access control*.

Cabe notar que la función ***govern*** en su categoría de roles/responsabilidades (GV.RR.) también cubre el asegurarse de asignar propietarios para la gestión de identidades en la organización.

En la práctica, la relevancia es que un programa CSF 2.0 debe prestar atención a IAM como pilar de la seguridad. Esto concuerda con marcos como Zero Trust Architecture (NIST SP 800-207), en los que la identidad verificada es central en cada acceso. Entonces, aplicar CSF 2.0 implica fortalecer sistemas de *single sign-on*, directorios centrales (AD/LDAP), técnicas de *identity federation*, recertificación periódica de accesos, etcétera.

Otros enfoques notables

CSF 2.0 también destaca los siguientes aspectos:

- **medición de resultados** (*metrics*). Anima a organizaciones a medir su postura en términos de los *outcomes* del *framework*. Esto lo desarrollamos en la sección 2.4.

- *Cybersecurity outcomes vs. controls*: NIST CSF habla de resultados de seguridad en vez de controles específicos. Por ejemplo, un *outcome* se puede definir como las anomalías en la red que se detectan y analizan (*detect*). Cómo lograrlo (qué tecnología o control usar) queda a elección. Esta flexibilidad es deliberada.

- **Alineación con conceptos actuales**: introduce referencias a ciberresiliencia, modelos de madurez, y, como vimos, al ciclo completo de riesgo. Todo para que el *framework* siga siendo moderno.

En síntesis, CSF 2.0 pone la gobernanza, el riesgo y la identidad al frente junto con la protección técnica tradicional. Esto lo hace un marco muy completo, que guía tanto a equipos técnicos (qué capacidades de *identify*/*protect*/etcétera, desarrollar) como a gerencia (cómo gobernar la seguridad y exigir a terceros).

2. 4. Perfiles, tiers (niveles) y métricas operativas en CSF 2.0

Además del *framework core* (funciones, categorías, subcategorías), el CSF provee otros componentes para su uso práctico.

Perfiles (*profiles*): un perfil del CSF es una representación de la postura de ciberseguridad de la organización en términos de los resultados (subcategorías) del *CSF core*. Básicamente,

es una selección o priorización de subcategorías que son relevantes según el contexto particular. Hay dos tipos claves.

- **Perfil actual** (*current profile*): describe el estado actual de la organización. Es decir, para cada subcategoría del *framework*, se evalúa si esa actividad/resultado está aplicando plenamente, parcialmente o no implementado. Por ejemplo, una subcategoría dice ID.RA-3: se identifican amenazas internas y externas. La organización evaluaría su nivel actual: tal vez tiene un proceso formal de *threat intel*, así que lo marca como aplicado.

- **Perfil objetivo** (*target profile*): describe el estado deseado o a lograr en el futuro (por ejemplo, en uno o dos años). Puede incluir subcategorías adicionales que hoy no están aplicadas. Siguiendo el ejemplo, quizás hoy no tienen un proceso de *threat intel* robusto (lo marcan como parcial en actual), pero en el perfil objetivo quieren tenerlo aplicado. Entonces, definirá proyectos para lograrlo (contratar un servicio de inteligencia de amenazas, etcétera).

Un *gap analysis* entre perfil actual y objetivo muestra las brechas a cerrar. Esto orienta la planificación de inversiones en ciberseguridad. Por ejemplo, si en la función *detect* la mayoría de subcategorías están en «no implementado» en el perfil actual, pero se quieren en «implementado» en el objetivo, eso implica priorizar montar capacidades de monitoreo, SOC, etcétera.

CSF 2.0 promueve el uso de perfiles para personalizar el *framework* a la realidad de cada entidad. NIST incluso provee plantillas de perfiles comunitarios para distintos sectores (financiero, salud, etcétera) para servir como base. Un perfil sectorial, por ejemplo, para

financiero, podría indicar qué subcategorías son de alta importancia (como muchas de *protect*/*detect*) y cuáles menos.

En resumen, los perfiles responden al siguiente interrogante: ¿qué subcategorías del *framework* son pertinentes para mi organización y cuál es mi situación en cada una? Permite a dos empresas en rubros distintos centrar diferente manteniendo el lenguaje común del CSF.

Implementation tiers (niveles de implementación): son descriptores que caracterizan la madurez o rigor de la gestión de ciberseguridad de la organización, especialmente en términos de integración con el manejo de riesgos organizacional. No se deben confundir con niveles de seguridad o calificativos de «bueno/malo» estrictamente; más bien reflejan cuán formal y adaptativo es el programa de seguridad de la empresa.

Los cuatro *tiers* definidos (que permanecen igual que en v1.1, con alguna refinación de descripción).

- ***Tier* 1: *partial*** (parcial). La gestión de ciberseguridad es *ad hoc* y reactiva, con poca organización. No hay prácticas formalizadas; la concienciación del riesgo es limitada, la ciberseguridad no está integrada en la cultura o gobernanza general. Ejemplo: una pyme que hace algunas cosas de seguridad (usa antivirus, contrata soporte TI ocasional), pero sin política ni evaluación formal de riesgos. Depende mucho de los esfuerzos individuales.

- ***Tier* 2: *risk-informed*** (informado por riesgo): hay prácticas aprobadas y cierta conciencia del riesgo a nivel gerencial, pero no están estandarizadas en toda la organización. Se aplican políticas o procesos en algunas áreas, pero no consistentemente. Ejemplo: la empresa tiene políticas de seguridad, hace evaluaciones de riesgo básicas, pero la

implementación varía por departamentos. Empieza a integrar seguridad en decisiones.

- ***Tier* 3: *repeatable*** (repetible): las prácticas de seguridad están formalizadas como políticas y procedimientos, y hay consistencia organizacional. La gestión del riesgo de ciberseguridad está alineada con los objetivos corporativos y se aplica en todos los departamentos de forma más o menos uniforme. Se revisan periódicamente los procesos. Ejemplo: la empresa tiene SGSI o similar, realiza auditorías internas, la alta dirección está involucrada regularmente. Es capaz de aprender de experiencias y ajustar procesos.

- ***Tier* 4: *adaptive*** (adaptable): la organización no solo tiene procesos definidos, sino que además los optimiza continuamente de manera proactiva. La cultura organizacional valora la ciberseguridad; se usan indicadores avanzados y técnicas predictivas para anticipar problemas. La gestión de seguridad es dinámica, basada en lecciones aprendidas y adaptaciones constantes. Ejemplo: organizaciones líderes que integran inteligencia de amenazas en tiempo real, responden muy rápido a nuevos riesgos, y la ciberseguridad forma parte de decisiones estratégicas automáticamente.

Importante: No se espera que todas las organizaciones alcancen *tier* 4 ni es necesariamente deseable que todas lo intenten. El *tier* adecuado depende del contexto y apetito de riesgo. Una pequeña empresa puede considerar que *tier* 2 es aceptable para sus fines, mientras un banco quizás aspire a *tier* 3. Lo valioso es ser consciente de dónde se ubica uno y si ese nivel corresponde con las necesidades. Por ejemplo, una crítica a versiones previas era pensar que

hay que «subir de nivel» siempre; NIST aclaró que los *tiers* no son un *ranking*, sino una herramienta de caracterización. Si la organización detecta que está en *tier* 1 pero su entorno de amenazas es complejo, debería aspirar a *tier* 2 o 3. Sin embargo, si está en *tier* 3 y eso es suficiente, no tiene obligación de ser *tier* 4.

Los *tiers* se aplican a los perfiles organizativos. Es decir, puedes decir «mi perfil actual está en *tier* 2 general, aspiramos a *tier* 3 en estos aspectos...». En CSF 2.0 se alienta su uso para priorizar mejoras (por ejemplo, «queremos pasar de gestión de riesgos informal a formal, de *tier* 2 a *tier* 3 en dos años») y para comunicar a partes externas cuán robusto es tu programa.

Métricas operativas

Si bien NIST CSF no prescribe métricas específicas, la nueva versión anima a las organizaciones a medir la efectividad de la ciberseguridad en términos de los *outcomes* del *framework*. Esto se conecta con *govern* y con *check* (medición continua). Algunos ejemplos de métricas ligadas a subcategorías son los siguientes:

- porcentaje de activos inventariados (relacionado con ID.AM).
- Tiempo promedio para aplicar parches críticos (PR.IP [procesos de protección]).
- Porcentaje de usuarios que aprobaron entrenamiento (PR.AT).
- Número de incidentes detectados internamente vs reportados por terceros (DE.CM efectividad).
- Tiempo de respuesta a incidentes desde detección a contención (RS.MI).
- Tiempo de recuperación de servicios críticos tras interrupción (RC.RP).
- Cumplimiento de políticas en auditorías (GV.PO).

CSF 2.0, al alinear atributos con las propiedades de seguridad y funciones de NIST, permite también usar esos atributos para métricas. Por ejemplo, se puede filtrar controles que son detectivos y medir cuántos se han implementado completamente.

Además, se menciona el *dashboarding* para juntas directivas: dado que muchos directorios piden informes de ciberseguridad, el CSF provee un marco consistente para presentar métricas agregadas. Por ejemplo, presentar «estado por función: identificar 80 % completo, proteger 70 %, detectar 50 %, etcétera». Aunque es una simplificación, es útil comunicativamente. En CSF 2.0, NIST publicó un CSF 2.0 *reference tool* que permite exportar datos en formatos legibles y *machine readable* (JSON, Excel), lo que ayuda a organizaciones a integrar la evaluación CSF con herramientas GRC y generar métricas automáticamente. Por ejemplo, se puede mapear internamente controles aplicados a las subcategorías y que un *dashboard* muestre porcentaje de cumplimiento por subcategoría o función.

En resumen, perfiles, *tiers* y métricas son los componentes que permiten adaptar el CSF a cada organización y medir el progreso.

- Los perfiles contestan: ¿qué queremos lograr en ciberseguridad? ¿Dónde estamos ahora?
- Los *tiers* contestan: ¿cómo de madura es nuestra gestión del riesgo de ciberseguridad?
- Las métricas contestan: ¿estamos mejorando? ¿Cómo demostramos la eficacia de nuestras prácticas?

Con CSF 2.0, se refinaron guías para todos ellos: NIST ofrece plantillas de perfiles comunitarios, definió mejor los *tiers* y dejó claro su uso y dotó de herramientas para *mapping* y métricas (como la *cybersecurity and privacy reference tool*, CPRT mencionada). Todo esto facilita la implementación práctica.

2. 5. Trazabilidad de controles, riesgo y procesos en el CSF 2.0

El concepto de **trazabilidad** se refiere a poder vincular claramente los elementos de la gestión: objetivos → riesgos → controles → resultados. En contextos de ciberseguridad, esto significa lo siguiente:

- poder rastrear cómo cada riesgo identificado está siendo tratado por uno o varios controles o actividades (subcategorías del CSF o controles ISO, etcétera).
- Poder mapear cómo un control aplicado responde a uno o varios riesgos y cumple con ciertos requisitos/estándares.
- Asegurar que cada proceso de seguridad o procedimiento se deriva de un control deseado, y a su vez de un requisito de negocio o riesgo.

CSF 2.0, al igual que ISO 27001, promueve esta trazabilidad de varias formas.

- **Matriz de mapeo entre *frameworks***: NIST provee mapeos de CSF subcategorías a otros estándares, por ejemplo, a SP 800-53 (controles de seguridad) o ISO 27001:2022. Esto permite que una organización pueda decir: «para cumplir con la subcategoría PR.DS-1 (protección de datos en reposo), aplicamos el control ISO 27001 A.8.11 (enmascaramiento de datos), y eso mitiga el riesgo X de fuga de datos». Este tipo de alineación ayuda a evitar duplicidades y a ver huecos.
- **Declaración de aplicabilidad vs. perfil**: en ISO, la SoA es la herramienta de trazabilidad

de controles aplicados/no aplicados. En CSF, el perfil objetivo sirve similar: indica qué subcategorías (controles a alto nivel) la organización ha decidido perseguir. De ese modo, cualquier control específico aplicado debe corresponder a una subcategoría en el perfil objetivo, lo que garantiza que es relevante. Por ejemplo, si en el perfil incluyeron «DE.CM-1: monitoreo de redes», se espera ver controles implementados de monitoreo (IDS, SIEM) trazables a ese *outcome*.

- **Integración con procesos de negocio**: CSF 2.0 subraya la necesidad de integrar ciberseguridad en procesos empresariales más amplios. Esto implica trazabilidad al revés: por ejemplo, un proceso de lanzamiento de un nuevo producto debe incluir la subcategoría PR.IP-3 (procedimientos de cambio gestionados) para asegurar seguridad en cambios. Así, se puede trazar que el proceso de *change management* incorpora consideraciones de seguridad (control de cambio seguro).

- **Trazabilidad hasta la capa de gestión de riesgo corporativo**: con *govern*, se espera que los riesgos de ciberseguridad se reflejen en los registros de riesgos corporativos de alto nivel. Así, un riesgo de «interrupción de operaciones por ciberataque» puede ser un *top risk* en el ERM (*enterprise risk management*) de la empresa. La respuesta a ese riesgo se traza a implementar subcategorías de *respond*/*recover*. Esto crea la línea de trazabilidad: riesgo empresarial → subcategorías CSF (capacidades de seguridad) → controles específicos

implementados → métricas de eficacia. Un director podría preguntar: «¿cómo estamos mitigando el riesgo de *ransomware*?» y la organización podría trazar la respuesta desde los controles (*backups*, *training*, EDR) hacia la subcategoría (PR.DS-1, PR.PS-3, DE.CM-1, RS.MI-1, RC.RP-1, etcétera) y mostrar métricas (por ejemplo, «hemos reducido el tiempo de recuperación a < cuatro horas, probado en simulacros»).

Un apoyo tecnológico a la trazabilidad es la herramienta de referencias informativas (CSF *reference tool*) y la *cybersecurity profile*/*reference tool* que lanzó NIST. Permite cargar tus perfiles, mapear contra más de cincuenta documentos (incluyendo normativas sectoriales). Así, por ejemplo, una empresa regulada (PCI DSS, HIPAA) puede trazar que subcategorías del CSF satisfacen qué requisitos de esas normas, evitando duplicar esfuerzos.

En la práctica, muchas organizaciones crean matrices de correspondencia. Por ejemplo, una tabla con columnas: riesgo, CSF subcategoría, control aplicado, procedimiento, evidencia. Esto demuestra para cada riesgo cómo se trata y cómo se verifica. Tanto auditores internos como externos aprecian esa claridad.

Ejemplo de trazabilidad

Tomemos la subcategoría PR.AA-1. «Las identidades digitales y credenciales se administran de manera centralizada con políticas». La empresa lo vincula a los siguientes aspectos:

- - riesgo. «Usuarios con privilegios excesivos podrían abusar acceso» (riesgo interno).
- Controles implementados: aplicar un sistema IAM central (*active directory*) con revisiones trimestrales de privilegios y aplicar MFA para acceso de *admins*.

- **Procedimiento**: «PRO-IAM-01 gestión de cuentas y recertificación» documentado.

- Evidencia: *logs* de AD de asignación de roles, reporte de última recertificación de accesos con correcciones hechas. Métrica: «% de cuentas inactivas deshabilitadas por mes» (como indicador de que se gestiona limpieza de identidades.

Así, si un auditor pregunta por PR.AA-1, pueden mostrar todo ese hilo. Si pregunta cómo mitigamos el riesgo de abuso interno, igualmente le muestran el mismo hilo. Esto es trazabilidad bidireccional.

Trazabilidad y mejora continua

Cuando ocurre un incidente, la trazabilidad permite ver qué fallo:

- ¿se identificó el riesgo? Si no, hay que actualizar la fase *identify*

- ¿Qué controles estaban supuestos a mitigar? Si había subcategorías marcadas como implementadas (por ejemplo, DE.CM-1 «monitoreo de redes») y aun así no se detectó el ataque, indica un *gap* en la implementación o efectividad. Entonces en *act* se mejora ese control (afinar SIEM) y se registra esa lección.

En CSF 2.0, la idea es moverse de simplemente «cumplir *checklist* de controles» a gestionar la seguridad con base en *outcomes* y riesgos, lo que naturalmente implica mantener esta trazabilidad.

Para completar la perspectiva de la unidad, veamos cómo una organización puede aplicar CSF 2.0 en un caso práctico y cómo se vincula con su SGSI.

Caso práctico: aplicación del NIST CSF 2.0 en una empresa manufacturera global

Contexto

ACME Corp es una empresa manufacturera con plantas en varios países. No está obligada a ninguna regulación específica de TI, pero maneja propiedad intelectual valiosa (diseños de productos) y su operación depende de sistemas OT (tecnología operacional) en fábricas. Han hecho esfuerzos de seguridad informales, pero tras incidentes globales como *ransomware* en cadenas de suministro, deciden adoptar el NIST CSF 2.0 para mejorar su postura y comunicársela a socios comerciales que lo requieren.

Pasos que ACME sigue

Involucrar la gobernanza (*govern*)

El CEO de ACME nombra al CFO como responsable ejecutivo de ciberseguridad (*sponsor*) y crea un comité de riesgos donde la ciberseguridad es un punto permanente. Adoptan la función *govern* del CSF:

- desarrollan una estrategia de ciberseguridad (GV.RM) alineada al plan estratégico de la empresa: priorizan proteger la continuidad de fabricación y la propiedad intelectual.
- Definen tolerancia al riesgo: deciden que la empresa no puede tolerar más de cuatro horas de paro de planta por incidente (criterio de impacto).
- Asignan responsables: el CIO lidera TI, el gerente de Ingeniería lidera OT, ambos

comparten responsabilidades en ciberseguridad (dividen roles pero con coordinación).

- Ajustan políticas: actualizan la política corporativa de riesgo para incluir explícitamente ciberseguridad como riesgo de nivel empresarial que requiere informes trimestrales al directorio (GV.PO, GV.OV).

- Lanzan un programa de evaluación de proveedores críticos (GV.SC): identifican diez proveedores de *software*/*hardware* de planta y les envían un cuestionario basado en CSF para evaluar su nivel, pidiendo mejoras contractualmente.

Perfil actual y objetivo (*identify*/*govern*)

ACME hace un *assessment* inicial (perfil actual) contra las subcategorías de CSF 2.0. Descubren, por ejemplo, lo siguiente:

- en *identify* están débiles. No tenían un inventario completo de dispositivos OT, ni un registro central de datos sensibles. Puntúan varias subcategorías ID.AM e ID.RA como «parcialmente implementadas».

- En *protect* medianamente: tienen antivirus en PC de oficina, pero las máquinas industriales (PLC, SCADA) no están segmentadas ni protegidas adecuadamente (fallo en PR.PS [*platform security*]).

- En ***detect*** muy bajo: no hay monitoreo continuo en las redes de las plantas (DE.CM no implementado).

- En ***respond/recover*** moderado: tienen plan de continuidad para desastres naturales, pero no uno específico de ciberincidentes (*no formal incident response plan*, RS.MA incompleto.

- *Govern* consideraron incipiente, pero con la nueva estructura piensan madurarlo a *tier* 3.

Definen su perfil objetivo a dos años: quieren todas las subcategorías en aplicado en nivel básico. Priorizan algunas: ID.AM-3 (inventario de datos), PR.PS-5 (configuraciones seguras en equipos), DE.CM-1 (monitoreo), RS.MI-1 (acciones de mitigación), RC.RP-1 (plan de recuperación). Esas son críticas para su contexto.

Implementación (*protect*/*detect*): con el *roadmap* del perfil objetivo, ACME emprende varios proyectos.

- Proyecto Inventario 360: implementan una herramienta de descubrimiento de activos en la red de planta para listar todos los dispositivos (*sensors*, PLCs, etcétera) y una clasificación de datos corporativos en sus servidores de diseño. Esto cubre ID.AM y parte de ID.RA.

- Proyecto Segmentación y Zero Trust OT: establecen zonas y *conduits* en la red industrial con *firewalls* entre planta y oficina, lo que restringe comunicación (PR.AA *identity*, PR.PT *networks*). Cada máquina OT ahora tiene una identidad en el sistema (certificado) y solo se comunica con servidores permitidos.

- Actualizan control de accesos: integran autenticación *multifactor* para VPN de ingenieros que acceden a OT (PR.AA).

- Implementan *EDR (endpoint detection and response)* en PC y un sistema de monitoreo de red OT (NDR) para detectar anomalías en protocolos industriales (DE.CM).

- Desarrollan un *playbook* de respuesta a *ransomware*: qué hacer si una planta sufre un ataque (RS.MA/CO). Incluye aislar la planta de la red corporativa, notificar al CISO global, involucrar al proveedor de ciberseguros, etcétera.

- Hacen *backup offline* de los controladores lógicos programables (PLC) cada semana (RC.RP).

- Inician inteligencia de amenazas compartida: se suscriben a una plataforma sectorial (por ejemplo, un ISAC de manufactura) para recibir alertas de *malware* que afecte a *robots* de línea (eso apoya ID.RA-5 y GV.SC [colaboración con sector y cadena]).

Todo esto se documenta. Hacen su SoA propio (aunque no certificarán ISO, llevan un registro mapeando subcategorías CSF a acciones internas).

Métricas y monitoreo (*detect*/*govern*/*check*): ACME configura un *dashboard* para monitorear el progreso.

- Miden porcentaje de dispositivos OT inventariados (ahora 90 %, meta 100 %).
- Miden incidentes detectados en planta vs. por terceros. En año 1, detectaron internamente tres de cuatro incidentes (bueno, meta mantener > 80 %).
- ***Board report***: el CISO presenta cada trimestre un resumen por función: por ejemplo, *identify*: 70 % completo, *major gap* en *inventory* en dos plantas; *protect*: 60 %, *next quarter focusing on OT patching*; *detect*: *improved from* 20 % *to* 50 % *via new* SOC; *respond*/*recover*: *IR plan in place, to be drilled Q4; govern: tier moved de 1 a 2, aim Tier 3*

next year [traducido a español obviamente para la junta directiva local]. Esto al *board* le resulta entendible y pueden decidir recursos (asignaron más presupuesto para monitoreo tras ver *detect* bajo).

Tier y mejora continua (*govern*/*act*)

Tras un año, evalúan su tier.

- Inicialmente estaban *tier* 1 (prácticas *ad hoc*). Con las formalizaciones, ya se sitúan en *tier* 2 (prácticas aprobadas, aún no integrales pero avanzando).
- Quieren llegar a *tier* 3: integrarlo en cultura. Para ello, planean incluir ciberseguridad en la inducción de todos los empleados de planta (no solo IT), incorporar objetivos de ciber en evaluaciones de desempeño de mandos medios (responsabilidad compartida), y establecer simulacros regulares en cada fábrica con lecciones aprendidas.

Un ejemplo de *incident respond*: reciben *intel* de que un *ransomware* apunta a PLC de cierto fabricante (*threat intel*). Gracias a su programa (ID.RA), verifican que tienen 5 PLC de ese tipo en dos plantas. Proactivamente, aplican parches provistos por fabricante (*protect*) y aumentan el monitoreo en esos equipos (*detect*). De ese modo, evitan la infección cuando la ola de ataques sucede en el sector. Informan esto al directorio como «caso de éxito de nuestra mejora en ciberresiliencia». Esto reafirma la utilidad de invertir en CSF.

En este caso, ACME no busca certificación, pero logra con NIST CSF 2.0 una estructura para su programa y puede demostrar a sus clientes (varias automotrices que exigen seguridad) su madurez. Por ejemplo, completan perfiles de ciberseguridad que algunos clientes envían, alineando respuestas a CSF: «tenemos implementadas al 100 % las funciones *identify-detect-respond* según NIST CSF», lo cual genera confianza. También, internamente, la integración con la gobernanza (incluir ciber en gestión de riesgos corporativa) les da más visibilidad.

En conjunción, ACME podría en un futuro decidir certificar ISO 27001 para su área de IT corporativa, ya con mucho camino avanzado gracias a CSF.

De esta forma vemos cómo NIST CSF 2.0 se aplica de manera práctica, haciendo hincapié en gobernanza, riesgos adaptados a la cadena de suministro (identificaron proveedores OT con posibles riesgos), identidad (asegurando accesos a OT), y usando perfiles/*tiers* para medir progreso.

Conclusiones

Con lo estudiado en unidad 1 (SGSI ISO 27001) y unidad 2 (NIST CSF 2.0), queda de manifiesto que ambos enfoques no compiten, sino que se complementan. ISO 27001 provee el sistema de gestión formal y certificable (el «cómo gestionar» con mejora continua), mientras NIST CSF ofrece un marco flexible de controles y resultados (el «qué hacer» específico en ciberseguridad). No es raro que organizaciones adopten ambos: por ejemplo, aplican un SGSI ISO 27001 para la disciplina de gestión y usan CSF como guía para evaluar y mejorar controles, e incluso para comunicar con *stakeholders* no técnicos.

La seguridad de la información y la ciberseguridad requieren un enfoque sistemático y adaptable. La ISO 27001:2022 nos da el sistema de gestión y los controles actualizados, mientras que el NIST CSF 2.0 aporta un marco flexible centrado en resultados y gobernanza. Al dominar ambos, el profesional *semisenior/senior* está equipado para construir programas de seguridad sólidos, alineados con estándares internacionales y resilientes frente a las amenazas actuales. Se sugiere seguir practicando estas metodologías en entornos simulados y reales; la experiencia combinada con estos marcos te formará como un líder en gobierno de seguridad, gestión de riesgo y protección de datos.

A continuación, se proponen algunas actividades prácticas para afianzar conocimientos, así como un laboratorio guiado con herramientas gratuitas y lecturas recomendadas para profundizar en gobierno, riesgo y protección de datos en un nivel avanzado.

Actividades prácticas

Se sugiere al estudiante llevar a cabo las siguientes actividades para aplicar los conceptos aprendidos. Estas actividades están diseñadas para un nivel *semi-senior*, combinando reflexión teórica con aplicación práctica en escenarios simplificados.

1. **Definir alcance y activos clave**: imagina una organización pequeña (por ejemplo, una clínica dental con cinco empleados). Redacta cuál sería el alcance de un SGSI para proteger la información de la clínica, indicando qué áreas incluirías. Luego, lista al menos cinco activos de información importantes dentro de ese alcance (por ejemplo, «historiales clínicos de pacientes en formato digital», «servidor de gestión de citas», etcétera) e identifique el propietario de cada activo. Discuta brevemente qué podría excluirse del alcance y por qué (justificación de exclusiones).

2. **Clasificación de información**: a partir de los activos anteriores, asigne una clasificación de seguridad a cada uno (pública, interna, confidencial, secreta, según corresponda). Justifique su clasificación. Por ejemplo: «historiales clínicos, clasificación: confidencial (contiene datos personales sensibles según la ley, requieren alta protección)». Para cada activo, menciona al menos un control o medida que se debería aplicar acorde a su clasificación (por ejemplo, «historiales clínicos, deberían cifrarse y requerir 2FA para acceso»).

3. **El ciclo PDCA en un incidente**: imagina que en la clínica ocurrió un incidente. Un *malware* cifró la base de datos de pacientes dejándola

inaccesible por dos días. Describa cómo se manifestaría cada fase PDCA del SGSI en la gestión de este incidente:

- *plan*. ¿Qué se debería haber previsto (por ejemplo, análisis de riesgo identificó *ransomware*, plan de respuesta, *backups* planificados)?
- *Do:* ¿qué controles habrían estado en ejecución (por ejemplo, *backups* se hacían, antivirus funcionando, personal entrenado)?
- *Check:* ¿cómo se detectó el incidente y cómo se evaluó la respuesta (por ejemplo, auditoría interna descubre fallo en actualización de parches que permitió *malware*, revisión de dirección analiza impacto)?
- *Act:* ¿qué acciones de mejora se toman tras el incidente (por ejemplo, aplicar parches pendientes, refuerzo de formación *anti-phishing*, mejorar frecuencia de *backups*)?

Redacta la respuesta hilando la secuencia y asegurando mejoras para prevenir repetición.

4 **Mapeo ISO 27001. NIST CSF**: elige cinco controles del anexo A de ISO 27001:2022 (puede ser de la lista de once nuevos controles, u otros a elección). Para cada control, identifique a qué **función**(es) y categoría(s) del NIST CSF correspondería. «Control A.8.11 – *Data masking:* corresponde a la función *protect*, categoría PR.DS (*data security*), dado que es una técnica de protección de datos confidenciales». Haga

esto con cinco controles distintos, explicando brevemente la relación. Esto le ayudará a ver la alineación entre ambos marcos.

5 **Evaluación de perfiles (actual vs. objetivo)**: imagínate al responsable de seguridad de la clínica y usa un fragmento del NIST CSF para evaluar su estado. Toma la función ***identify*** con sus categorías (*asset management*, *risk assessment*, *improvement*):

- lista las subcategorías correspondientes (por ejemplo, ID.AM-1: se tiene un inventario de activos físicos/*soft*..., etcétera, puede abreviar la idea).
- Evalúe en la clínica ficticia si esa subcategoría está aplicada, parcial o no implementada actualmente (perfil actual). Justifica con una frase.
- Luego, define cómo debería estar en un perfil objetivo en un año y qué harías para lograrlo.

Por ejemplo: «ID.AM-1 inventario de activos – actual: parcial (tenemos lista de equipos de cómputo, pero no de datos ni software); objetivo: implementado (haremos un inventario completo incluyendo archivos de pacientes, *software* usado, etcétera, usando una hoja de cálculo centralizada compartida por todo el personal)». Haz esto para al menos tres subcategorías de *identify* a modo ilustrativo.

6 **Caso integrador**: desarrolla un minicaso (unas diez líneas) en el que una empresa sufre un ataque de *phishing* que compromete datos de clientes. En tu relato, incluye lo siguiente:

- cómo falló alguna función del CSF (por ejemplo, falló *protect awareness* porque el empleado no reconoció *phishing*).
- Qué control ISO 27001 podría no haber estado implementado o falló (por ejemplo, falta de capacitación A.6.3 o control de *phishing*).
- Cómo responderían y qué mejoras harían (funciones *respond* y *recover*, más *plan* (*govern*) a futuro).

Este ejercicio integrará tu comprensión narrativa de ambos marcos trabajando juntos.

Revisa tus respuestas comparando con conceptos de las unidades. Estas actividades permiten detectar áreas a reforzar (por ejemplo, si cuesta mapear controles a CSF, repasar la sección 2.5).

Laboratorio guiado: herramientas gratuitas y hojas de cálculo

En este laboratorio práctico, emplearemos herramientas accesibles (gratuitas) y plantillas para simular la implementación de ciertas partes de un SGSI y evaluar la ciberseguridad con NIST CSF. Asegúrate de seguir los pasos en orden, reflexionando sobre los resultados.

Escenario de laboratorio

Continuaremos con la clínica dental ficticia del ejercicio anterior, ahora aplicando elementos de su SGSI y evaluando su madurez con CSF. No se requieren conocimientos técnicos profundos, solo uso de herramientas ofimáticas y sitios web.

Paso 1: Crear un inventario de activos con una hoja de cálculo

- Descarga la plantilla gratuita ISO 27001 Asset Inventory (en Excel) ofrecida por Secureframe o usa una provista por tu instructor. Si no dispones de una, puedes crear una tabla en blanco con columnas: ID, nombre de activo, tipo, ubicación, propietario, valor/impacto, clasificación.

- Lista al menos diez activos de la clínica. Incluye dos activos de tipo información (por ejemplo, «base de datos de pacientes»), dos de *hardware* (por ejemplo, «servidor clínico», «PC recepción»), dos de *software* (por ejemplo, «sistema de turnos»), dos de personas (por ejemplo, «dentista principal»), dos servicios de terceros (por ejemplo, «servicio de respaldo en nube»).

- Rellena los campos para cada uno. Usa la columna Valor para indicar crítico/alto/medio/bajo. Clasifica la información según definió (pública, interna, confidencial...).

- Ahora, usa las funciones de filtrado de la hoja para responder: ¿cuántos activos confidenciales hay? ¿Quién es el propietario de los activos más críticos? Anota estas respuestas.

- **Resultado esperado**: un inventario tabulado (ejemplo de fila: ID=1, Nombre="Historiales Pacientes DB", Tipo=Información digital, Ubicación=Servidor clínico, Propietario=Dra. Gómez (Directora), Valor=Crítico, Clasificación=Confidencial).

Paso 2: Evaluar riesgos con una plantilla

- Usando el inventario, identifica tres riesgos: por ejemplo, «pérdida de datos de pacientes por fallo de disco», «acceso no autorizado a historia clínica», «*ransomware* cifrando el servidor».

- Descarga una plantilla gratuita de evaluación de riesgos ISO 27001 (varias consultoras las ofrecen; por ejemplo, Secureframe tiene un Excel editable, o la guía del NIST 800-30 Appendix K ofrece un formato simple). Alternativamente, crea columnas: riesgo, impacto (1-5), probabilidad (1-5), nivel (impacto x probabilidad), controles existentes, tratamiento planificado.

- Califica el impacto y la probabilidad para cada riesgo. Por ejemplo, *ransomware* [impacto 5] (muy alto, clínica parada), prob 3 (moderado, ha habido intentos en sector).

- La hoja debe calcular nivel (puede poner fórmula =Impacto*Probabilidad). Identifica cuál riesgo es más alto. Decide un plan de tratamiento para ese: por ejemplo, «implementar *backup offline* y entrenamiento *phishing*».

- **Resultado esperado**: una minimatriz de riesgos. Verifica que los riesgos ligados a activos confidenciales tiendan a salir con un impacto alto. Esto muestra la importancia de la clasificación en la valoración de riesgos.

Paso 3: Declaración de aplicabilidad (SoA) simplificada en hoja

- Toma la lista de once nuevos controles de ISO 27001:2022. En una nueva hoja, crea columnas: control, ¿aplica? (sí/no), justificación (si no aplica).

- Marca para la clínica cuáles aplican. Por ejemplo:

  - amenazas (*threat intel*). Quizás «no aplica» por ser pequeña, justificar «nos basamos en fuentes públicas, no capacidad propia de *intel*».
  - Seguridad en la nube: si usan respaldo en nube, «sí aplica. Tenemos lineamientos de uso seguro de nube».
  - Continuidad TIC: «sí. Crítico para seguir operando ante un fallo, usaremos *backups*».
  - Monitoreo físico: tienen una oficina pequeña. «Sí, cerraduras y alarma, aunque sea básica».
  - Configuración: «sí, mantenemos PC con configuraciones por defecto seguras y actualizaciones».
  - Enmascaramiento de datos: «no, por ahora no compartimos datos para *testing*, no aplica».
  - DLP: «sí, vigilamos no enviar datos de pacientes por *e-mail* no seguro».
  - *Web filtering*: «sí, instalamos filtrado web en PC para evitar webs maliciosas».

- *Secure coding*: «no, no desarrollamos *software* propio», etcétera.

- Esto te lleva a pensar en los controles concretos y su relevancia. En la clínica, probablemente seis de los once apliquen.

- **Resultado esperado**: un SoA parcial con al menos once filas, algunas «no» justificadas. Guarda esta hoja; podría servir para cuando apliques esos controles.

Paso 4: Uso del NIST CSF online tool o PDF (resource guide)

- NIST ofrece una herramienta en línea (CSF 2.0 *reference tool*) y documentos PDF en español. Accede a la guía de recursos CSF 2.0 (en español). Si no es posible, usa la versión web en inglés: https://www.nist.gov/cyberframework.

- Navega las funciones y categorías. Identifica al menos una subcategoría de cada función que consideres prioritaria para la clínica:

  - gobernar, quizás GV.PO (políticas) o GV.RR (roles definidos).
  - Identificar: ID.AM-1 (inventario de activos).
  - Proteger: PR.AA-1 (gestión de identidades) o PR.DS-1 (protección de datos en reposo).
  - Detectar: DE.CM-1 (monitoreo de redes).
  - Responder: RS.MI-1 (mitigación de incidentes).

- Recuperar: RC.RP-1 (plan de recuperación ejecutado).

- Anota esas subcategorías seleccionadas y compara con lo que has hecho en pasos previos: ¿tiene la clínica algo para cada una? Por ejemplo, inventario (ID.AM) sí lo hizo; plan de recuperación (RC.RP), tal vez no formal, debería hacerlo.

- **Resultado esperado**: una lista de seis subcategorías con brecha actual vs. deseado. Esto es un miniperfil actual/objetivo conceptual.

Paso 5: Evaluar la clínica con una herramienta de diagnóstico CSF

- Opcionalmente, usa un servicio en línea gratuito que evalúe madurez NIST CSF. Por ejemplo, **CyberDay** ofrece un *assessment* rápido gratis. Regístrate con un *e-mail* (si cómodo) y completa las preguntas cortas. Suelen preguntar si tiene políticas, si monitorea *logs*, etcétera. Al final, obtienes un puntaje o informe.

- Si no deseas usar la web, responde manualmente un cuestionario simplificado (como el de UpGuard CSF Template que contiene preguntas por función).

- Revisa el resultado: ¿qué áreas salen más débiles? ¿Coincide con lo que preveía (por ejemplo, *detect* muy bajo porque no hay monitoreo 24/7)? Anota tres recomendaciones

que la herramienta sugiere o que tú deduzcas de las áreas débiles.

- **Resultado esperado**

Un breve diagnóstico, por ejemplo: «nivel general: básico. Prioridades de mejora: implementar monitoreo de seguridad (detectar), formalizar gestión de identidades (proteger), y definir plan de respuesta a incidentes (responder)».

Paso 6: Simular respuesta a un incidente (juego de roles)

- Haz un *mini-tabletop exercise*: imagina que ocurre un incidente. El antivirus detecta un *ransomware* en la PC de recepción. ¿Qué haces tú primero, segundo, tercero?

  - Primero (detectar): aislar la PC (quitar de la red), evaluar alcance (¿afectó al servidor de datos?).
  - Segundo (responder): notificar a todos (RS.CO), apagar sistemas afectados, llamar a técnico, etcétera. Seguir tu plan de respuesta (si lo tuvieras; si no, improvisar con lógica).
  - Tercero (recuperar): restaurar la PC con backup o reinstalar, verificar integridad de datos de pacientes.
  - Extra (comunicar): avisar a pacientes si datos se comprometieron (no es altamente regulado quizás, pero ético considerarlo).

- Documenta esas acciones en secuencia temporal (incluso usando una lista numerada.

- Luego determina: ¿qué controles fallaron que permitieron el incidente? Por ejemplo: quizá un usuario abrió *phishing* → falló *protect, awareness; ransomware* entró → falló *protect.*AV o *patch*; no se detectó hasta que cifró → falla *detect*. ¿Qué mejoras implementarías? Por ejemplo, filtrar correo *phishing*, segmentar red para que PC no infecte servidor, etcétera.

- **Resultado esperado**: un pequeño reporte de incidente con «línea de tiempo de acciones» y «lecciones aprendidas». Esto integra todo: muestra cómo su SGSI/CSF reacciona y se ajusta.

Al completar este laboratorio, habrás empleado **herramientas concretas**: Excel para activos y riesgos, un portal de CSF, quizás un servicio de evaluación. Habrás generado artefactos similares a los de un consultor en un proyecto real (inventario, matriz de riesgo, SoA, perfil CSF). Guarda esos documentos; pueden servirte de plantilla en el mundo real. Lo importante es el proceso reflexivo: cómo cada herramienta se vincula con los conceptos teóricos.

Si haces el laboratorio en grupo, compara los resultados con compañeros: ¿listaron los mismos activos? ¿Obtuvieron iguales prioridades CSF? Esto enriquece la comprensión, dado que no hay una única respuesta correcta, sino un análisis contextual.

Lecturas recomendadas

Para profundizar en los temas de este módulo, se sugieren las siguientes lecturas y recursos, todos accesibles en línea.

ISO27000.es. (s. f.). *Liderazgo en ISO 27001 – Cómo ponerlo en práctica*. ISO27000.es. https://www.normaiso27001.es/liderazgo-en-iso-27001/.

PCG. (2025). *ISO 27001:2022 – The Latest Version with 11 new Controls*. https://pcg.io/insights/iso-27001-2022-new-controls/.

WeLiveSecurity (ESET). (2023). *ISO 27001:2022: ¿qué cambios introdujo el nuevo estándar de seguridad?* https://www.welivesecurity.com/la-es/2023/02/09/iso-270012022-cambios-nuevo-estandar-seguridad/.

NIST Cybersecurity Framework 2.0 (documentos oficiales)

NIST publicó la versión final del CSF 2.0 junto con recursos en múltiples idiomas. Se recomienda:

Instituto Nacional de Estándares y Tecnología. (2024). Marco de Ciberseguridad del NIST: Versión 2.0 — Núcleo (Core) (NIST Special Publication 1299). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.spa.pdf.

La página oficial de NIST CSF (en inglés), que incluye *mappings* e información actualizada:

Censinet. (s. f.). *ISO 27001 and NIST CSF: Control Mapping Checklist*. https://www.censinet.com/perspectives/iso-27001-and-nist-csf-control-mapping-checklist.

Cyber Sierra Knowledge Team. (27 de mayo de 2025). *Key Changes in NIST CSF 2.0: A Comprehensive Guide*. Cyber Sierra. https://cybersierra.co/blog/key-changes-in-nist-csf-2-0-a-comprehensive-guide/.

Ribeiro, A. (27 de febrero de 2024). *NIST releases CSF 2.0 focused on governance and supply chain security across sectors*. Industrial Cyber. https://industrialcyber.co/nist/nist-releases-csf-2-0-focused-on-governance-and-supply-chain-security-across-sectors/.

Herramientas y plantillas gratuitas

Fitzgerald, A. y Leung, C. (25 de agosto de 2025). *ISO 27001:2022 and ISO 27002:2022 Explained: How to Comply Before October 2025 Deadline*. Secureframe. https://secureframe.com/blog/iso-27001-2022.

arunsivadasan. (20 de mayo de 2024). NIST CSF 2.0 to ISO 27001:2022 mapping (Excel). [Comentario en foro en línea]. Reddit.

https://www.reddit.com/r/cybersecurity/comments/1gsxthr/nist_csf_20_to_iso_270012022_mapping_excel/

.

UpGuard. (2025). NIST CSF Risk Assessment Template [Plantilla de evaluación de riesgo]. https://www.upguard.com/templates/nist-csf-risk-assessment.

Foros y comunidades

Para dudas prácticas, los foros de profesionales en seguridad son muy valiosos. Un ejemplo de esto es la comunidad de Reddit r/cybersecurity y r/ISO27001, en la que se discutió la llegada de ISO 27001:2022 y CSF 2.0 (experiencias reales, consejos). Participar o leer allí mantiene actualizado con problemas reales que otros enfrentan.

ISOTools Excellence. (s. f.). *Norma ISO 27001: qué es y por qué es importante*. https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/.

Normativas locales sobre protección de datos

Dado que el curso es en Argentina, es útil revisar la Ley de Protección de Datos Personales (Ley 25326) y su reglamentación, que, aunque no técnica, establece principios que un SGSI debe contemplar (por ejemplo, medidas de seguridad para datos sensibles, notificación de brechas [la futura Ley de Delitos Informáticos podría requerirlo]). No son lecturas «de disfrute», pero conocer las obligaciones legales nacionales complementa la aplicación de ISO/NIST en el contexto local. Se recomienda leer aquellas que llamaron su atención durante el estudio (por ejemplo, si te intrigaron los atributos de controles en ISO 27002, puedes profundizar en la ISO 27002:2022 si tienes acceso).

CONTINUAR

Referencias

[Imagen sin título sobre evolución de la estructura de ISO/IEC 27001]. (s. f.). https://web-assets.esetstatic.com/wls/2023/02/iso.27001-2022-cambios-estandar-seguridad.jpg.

[Imagen sin título sobre gráfico ilustrativo de las seis funciones centrales del NIST Cybersecurity Framework]. (s. f.). https://quizlet.com/987559559/isc-module-1-flash-cards/.

Instituto Nacional de Estándares y Tecnología. (2024). *Marco de Ciberseguridad del NIST, Versión 2.0* (NIST Cybersecurity Framework N.º 2.0). https://www.nist.gov/cyberframework/.

International Organization for Standardization [ISO] e International Electrotechnical Commission [IEC]. (2022). Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos (Norma ISO/IEC 27001. https://www.iso.org/es/norma/27001.

Reglamento de la Unión Europea 679 de 2016 [Parlamento Europeo]. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). 27 de abril de 2016.

CONTINUAR

Descarga en PDF

PDF

SGSI 270012022 y CSF 2.0.pdf

891.8 KB