DIPLOMADO
CIBERSEGURIDAD
CAPACITACIÓN USACH - UNIVERSIDAD DE SANTIAGO DE CHILE

Verano 2024

Fundamentos de Controles

Fundamentos de NIST

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD
CAPACITACIÓN USACH - UNIVERSIDAD DE SANTIAGO DE CHILE

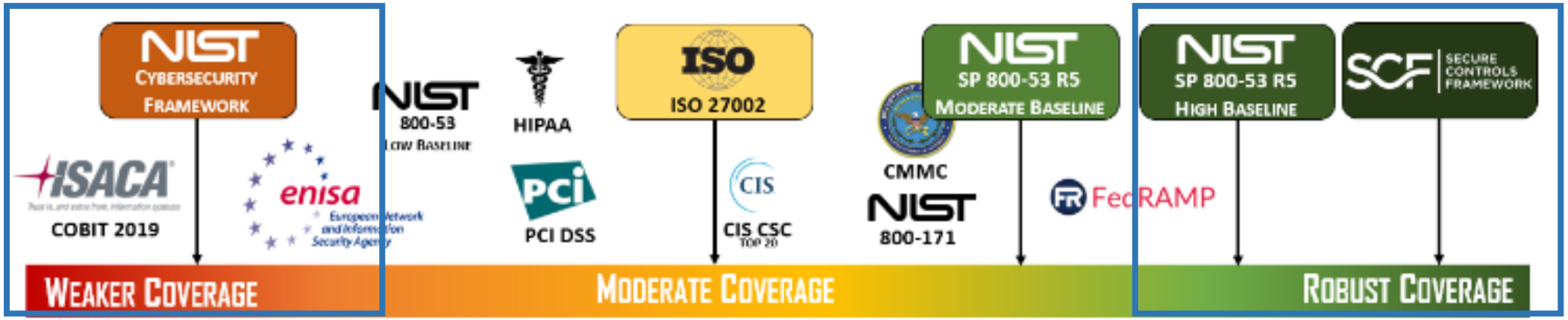
¿Por qué NIST?

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT

¿Por qué NIST?

Es útil primero definir los requisitos "imprescindibles" y luego los "deseables", ya que eso ayuda a orientar hacia el marco más adecuado para las necesidades específicas.



Menos Controles **Más Controles**

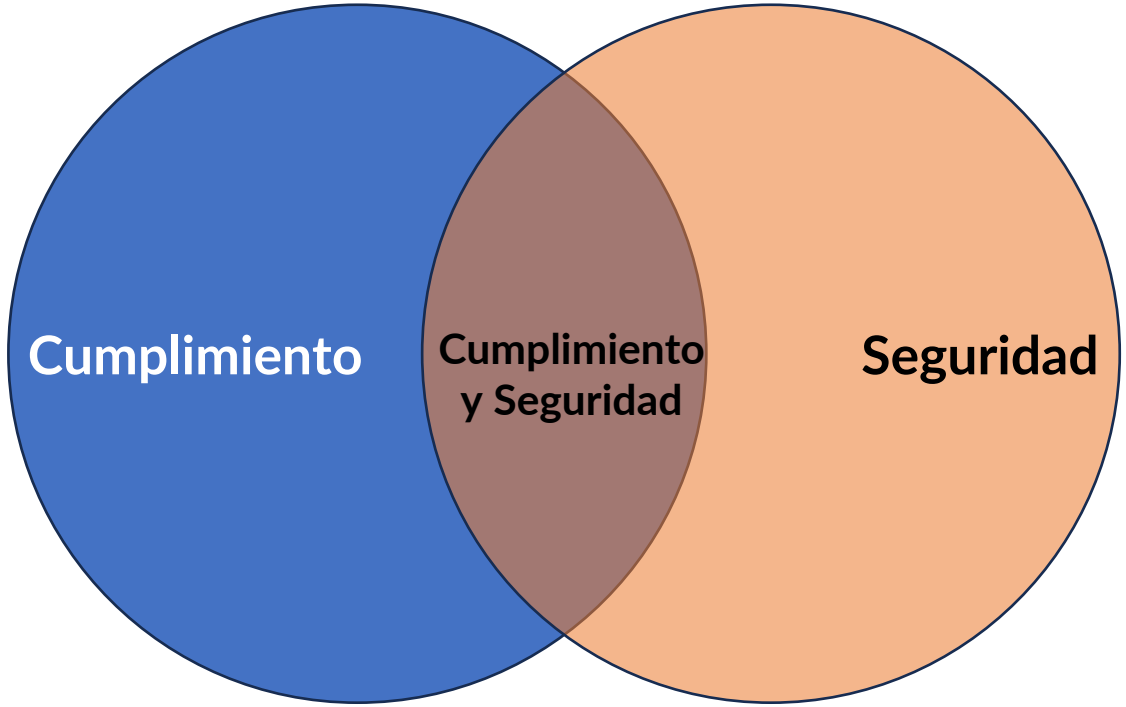
- El número de controles impacta el número de dominios que están cubiertos por un marco de ciberseguridad específico.
- A menor cantidad de controles, un framework puede parecer más sencillo de implementar, pero podría no proveer la cobertura necesaria para las necesidades de la organización.
- Definir el marco “adecuado” para la organización, es sobre todo, una decisión de negocios.

Fuente: Complianceforge – Cybersecurity Frameworks Comparison

Definir los Requisitos Mínimos de Seguridad

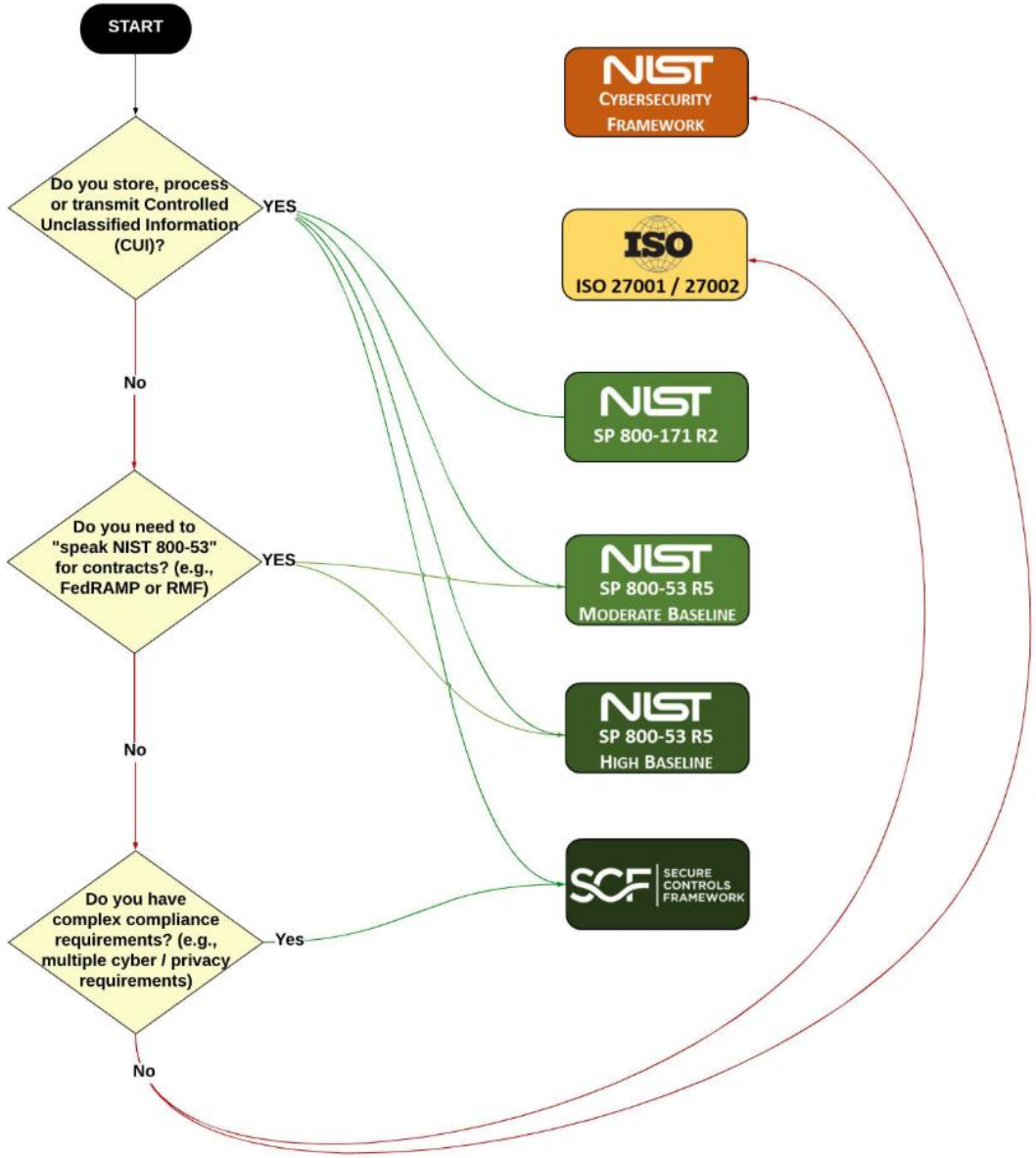
Los requisitos mínimos de seguridad son una combinación de requisitos obligatorios y opcionales, una combinación de lo que la organización está obligada y lo que desea.

Esta consideración es necesaria para balancear la dicotomía “empresa enfocada en el cumplimiento vs empresa segura” que determina si una organización



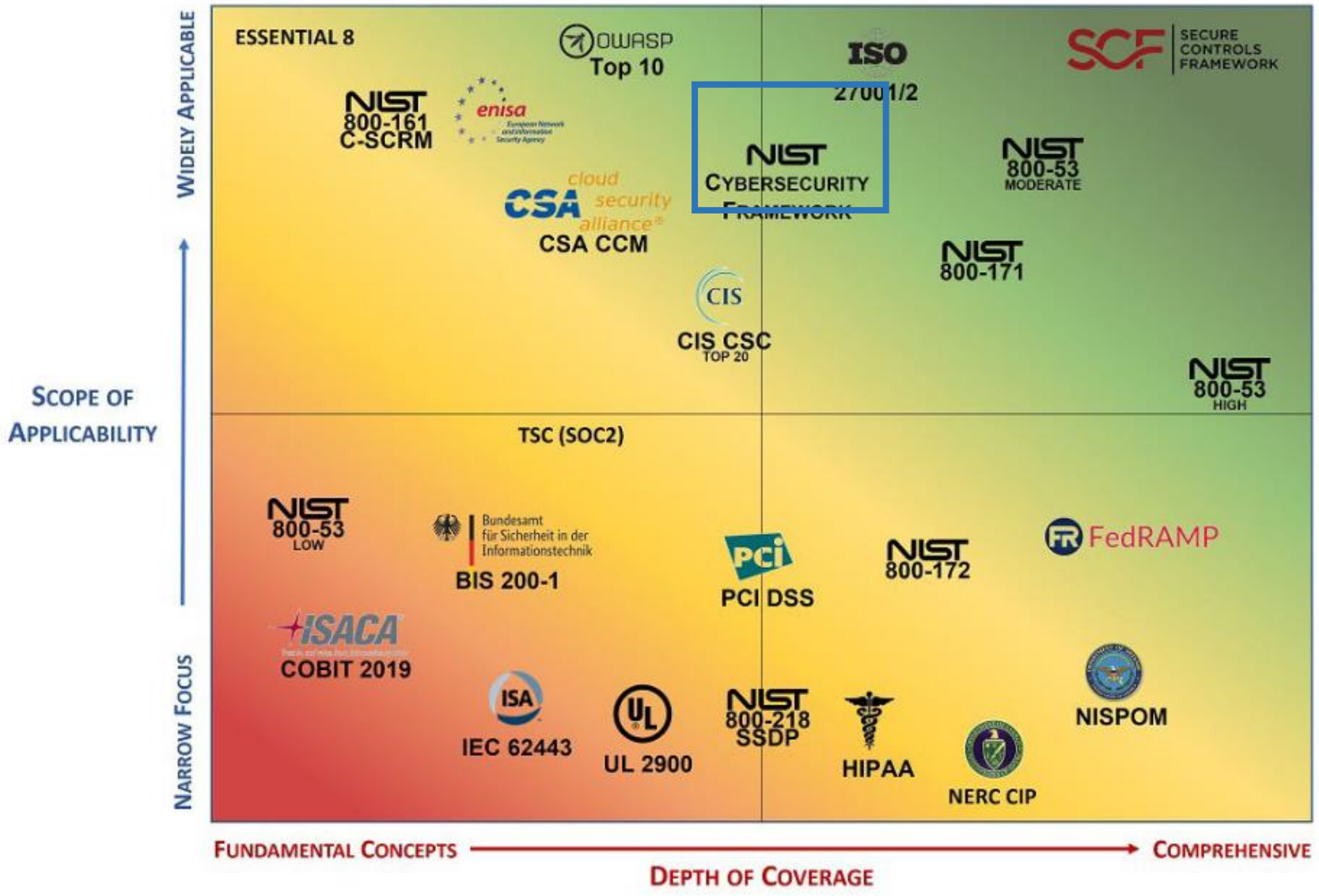
Fuente: Complianceforge – Cybersecurity Frameworks Comparison

No todos los frameworks son creados iguales



Fuente: Complianceforge – Cybersecurity Frameworks Comparison

No todos los frameworks son creados iguales



Fuente: Complianceforge – Cybersecurity Frameworks Comparison

DIPLOMADO
CIBERSEGURIDAD

Caracterización del Marco NIST

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT

Marco para Mejorar la Infraestructura Crítica de Ciberseguridad

- El marco de Ciberseguridad del NIST tiene un carácter no regulatorio que provee una metodología rigurosa para la identificación y gestión de riesgos.

- El marco se construye en base a un esfuerzo abierto y colaborativo, que da como resultado una herramienta flexible que puede ser usada en cualquier organización.

- El marco de ciberseguridad provee un proceso continuo para la gestión de riesgos de ciberseguridad.

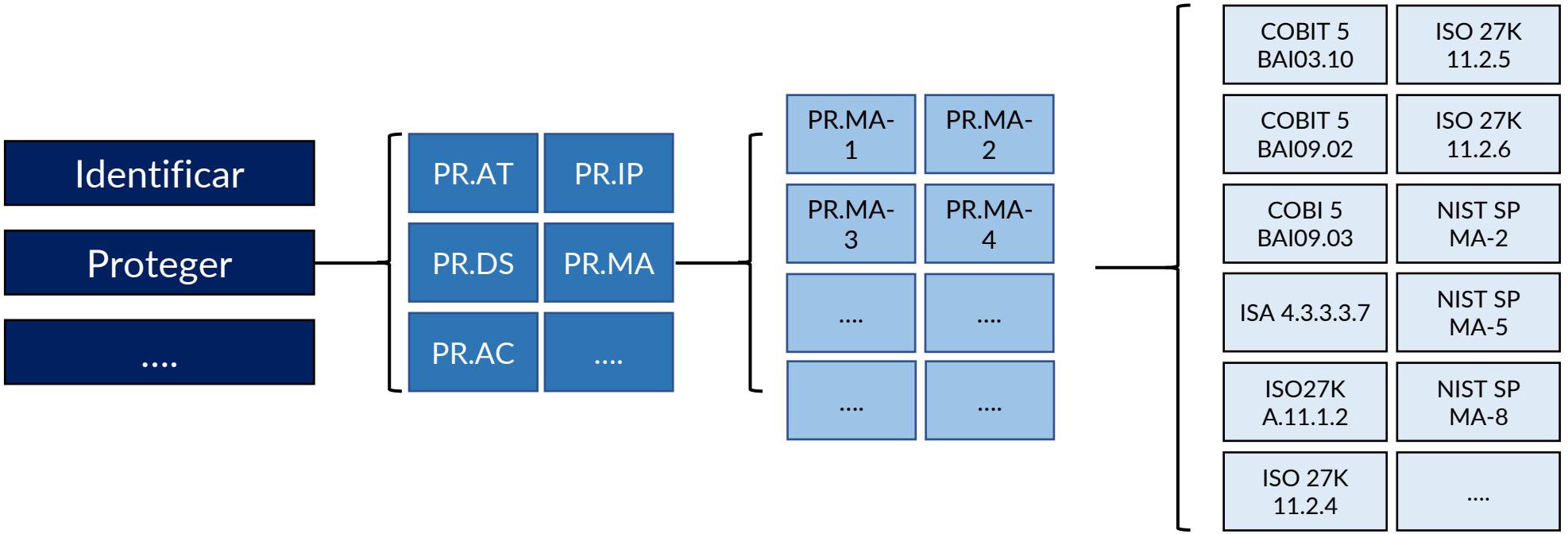
Los tres componentes del marco

- ***El Core del Marco***: El Core es un conjunto de actividades y resultados deseados, organizados en Categorías y alineados con Referencias Normativas a estándares aceptados por la industria. El Core del marco está compuesto de 5 funciones, 23 categorías y 108 subcategorías.

- ***Niveles de Implementación del Marco***: Describen como y en que grado el riesgo de ciberseguridad está gestionado al interior de una organización.

- ***Perfiles del Marco :*** El Perfil del Marco es la alineación de las Funciones, Categorías y Subcategorías con los requisitos empresariales, la tolerancia al riesgo y los recursos de la organización

El Core del Marco - Componentes



5 funciones

23 categorías

108 subcategorías

1504 referencias

Core del Marco - Funciones

Una ***función*** es una tipo de actividad de alto nivel, son: Identificar, Proteger, Detectar, Responder y Recuperar.

Core del Marco – Categorías

Una ***categoría*** está diseñada para cubrir la amplitud de los objetivos de ciberseguridad de la organización, cubriendo aspectos técnicos, personas y procesos.

IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
GESTIÓN DE ACTIVOS	CONTROL DE CONCIENTIZACIÓN	ANOMALÍAS Y EVENTOS	PLANES DE RESPUESTA	PLANES DE RECUPERACIÓN
AMBIENTE DE NEGOCIOS	CONCIENTIZACIÓN Y ENTRENAMIENTO	MONITOREO CONTÍNUO DE SEGURIDAD	COMUNICACIONES	COMUNICACIONES
GOBERNANCIA	SEGURIDAD DE DATOS	PROCESOS DE DETECCIÓN	ANÁLISIS	MEJORAS
EVALUACIÓN DE RIESGOS	PROTECCIÓN DE INFORMACIÓN Y PROCEDIMIENTOS		MITIGACIÓN	
ESTRATEGIA DE GESTIÓN DE RIESGOS			MEJORAS	

Core del Marco – Subcategorías

Las ***subcategorías*** son los niveles más detallados del marco, son declaraciones basados en los resultados que proporcionan consideraciones para crear o mejorar un programa de ciberseguridad.

FUNCION	*CATEGORIA*	*SUBCATEGORIA*
IDENTIFICAR	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresarialesse identifican y se administran de forma coherente.	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas
		ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.
		ID.AM-4: Los sistemas de información externos están catalogados.
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo yterceros interesados (por ejemplo,proveedores,clientes, socios) están establecidas.

Core del Marco – Referencia Normativa

FUNCION	CATEGORIA	SUBCATEGORIA	REFERENCIA NORMATIVA
IDENTIFICAR	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresarialesse identifican y se administran de forma coherente.	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados	· CIS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas	· CIS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 · NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.	· CIS CSC 12 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Los sistemas de información externos están catalogados.	· CIS CSC 12 · COBIT 5 APO02.02, APO10.04, DSS01.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	· CIS CSC 13, 14 · COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo yterceros interesados (por ejemplo,proveedores,clientes, socios) están establecidas.	· CIS CSC 17, 19 · COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Core del Marco – Referencia Normativa

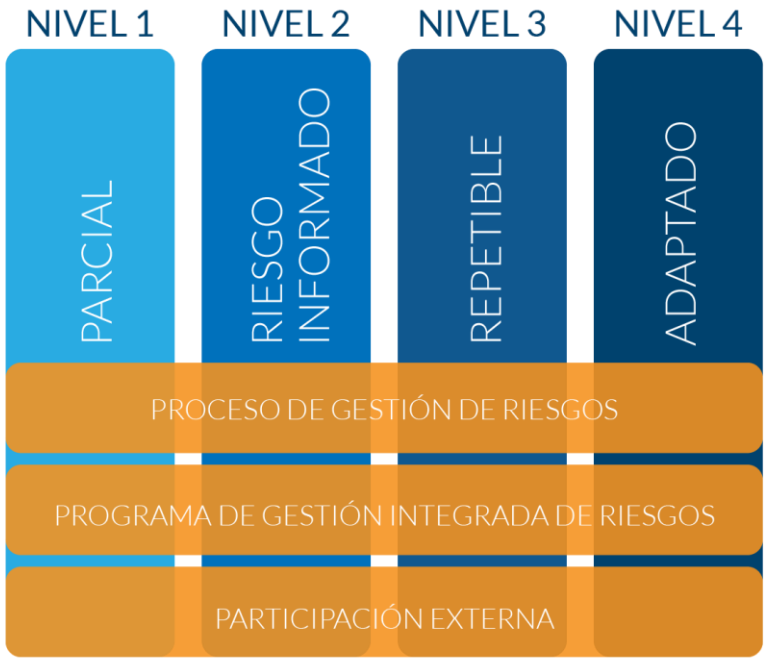
Entre las referencias normativas, destacan los marcos ISO/IEC 27001 y COBIT 5 como aquellos que no pertenecen al propio NIST y que son fundamento para la construcción de las subcategorías y controles asociados..

FUNCIONES / MARCOS	CIS CSC	COBIT 5	ISA 62443-2-1	ISA 62443	ISO/IEC 27001	NIST SP 800-53
DETECT (DE)	58	35	14	18	31	83
IDENTIFY (ID)	21	106	49	11	61	102
PROTECT (PR)	73	109	87	82	173	212
RECOVER (RC)	1	11	1		9	11
RESPOND (RS)	17	24	19	7	27	51
Total general	170	285	170	118	301	459

Niveles de Implementación del Marco

Los ***niveles de implementación*** describen el grado de rigor en que las prácticas de gestión de riesgos de ciberseguridad de una organización se alinean con lo planteado en el marco.

- Los niveles de implementación describe como el riesgo es gestionado al interior de la organización.
- Existen cuatro niveles (o estadios): Parcial, Informado, Repetible y Adaptado.
- Cada organización debe decidir cual nivel se acomoda a sus necesidades particulares. No todas las organizaciones buscarán el nivel mas alto.



Niveles de Implementación del Marco

- El marco es vehemente en expresar que los niveles de implementación no representan niveles de madurez, sin embargo, en la practica son similares. Lo importante es recordar que no todos los controles necesitan ser implementados en el nivel mas alto.

Características del Nivel de Implementación

	Nivel 1: Parcial	*Nivel 2: Riesgo informado*	*Nivel 3: Repetible*
Proceso de gestión de riesgos	El riesgo se gestiona de forma ad-hoc y reactiva. La priorización de actividades de ciberseg. No están directamente informadas por objetivos de riesgo, amenazas o requisitos empresariales.	Las prácticas de gestión de riesgos son aprobadas por la administración, pero posiblemente no son establecidas como políticas de toda la organización.	Las prácticas para la gestión de riesgos de la organización se aprueban formalmente y se expresan como políticas
Programa integrado de gestión de riesgos	Existe una conciencia limitada sobre el riesgo de seguridad cibernética a nivel organizacional. La organización implementa la gestión del riesgo de seguridad cibernética de forma irregular.	Existe una conciencia del riesgo de seguridad cibernética a nivel organizacional, pero no se ha establecido un enfoque en toda la organización para gestionar el riesgo de seguridad cibernética.	Existe un enfoque de toda la organización para gestionar el riesgo de seguridad cibernética. Las políticas, procesos y procedimientos informados sobre riesgos se definen e implementan según lo previsto, y se revisan
Participación externa	La organización no comprende su función en el ecosistema más amplio con respecto a sus dependencias o dependientes. En general desconoce los riesgos de la cadena de suministro de los productos y servicios que proporciona y que utiliza.	Generalmente, la organización entiende su función en el ecosistema más amplio con respecto a sus propias dependencias o dependientes, pero no ambos.	La organización entiende su función, dependencias y dependientes en un ecosistema más amplio y posiblemente contribuya a una más amplia comprensión de los riesgos por parte de la comunidad

Perfil del Marco

- El Perfil del Marco es la alineación de las Funciones, Categorías y Subcategorías con los requisitos empresariales, la tolerancia al riesgo y los recursos de la organización.

- Un Perfil permite a las organizaciones establecer una hoja de ruta para reducir el riesgo de seguridad cibernética que está bien alineada con los objetivos organizacionales y sectoriales, considera los requisitos legales o reglamentarios y las mejores prácticas de la industria, y refleja las prioridades de gestión de riesgos.

- Los perfiles se pueden utilizar para identificar oportunidades de mejora para mejorar la postura de ciberseguridad a través del análisis gap de lo actual y lo objetivo.

¿Qué hay de NIST 2.0?

Function

GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

- **Category**
  Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)
- **Category**
  Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)
- **Category**
  Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)
- **Category**
  Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID.GV-02)
- **Category**
  Policies, Processes, and Procedures (GV.PO): Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced (formerly ID.GV-01)
- **Category**
  Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy

DIPLOMADO
CIBERSEGURIDAD
CAPACITACIÓN USACH - UNIVERSIDAD DE SANTIAGO DE CHILE

Ejemplo de uso de NIST CSF (1.1)

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT

Paso 1: Definición de las capacidades

- Para comenzar, definiremos las dimensiones de capacidad desde un estándar: Process Assessement Model de ISACA.

	NIVEL DE CAPACIDAD	ATRIBUTOS
1	Realizado	▪ Proceso Incompleto ▪ Actividades ad-hoc
2	Gestionado	▪ Gestión del desempeño de la tarea ▪ Gestión del producto de la tarea
3	Establecido	▪ Definición del Proceso ▪ Despliegue del Proceso
4	Medible	▪ Medición del Proceso ▪ Control del Proceso
5	Optimizado	▪ Optimización del Proceso ▪ Innovación del Proceso

El modelo PAM se encuentra principalmente alineado a las capacidades descritas en el modelo ISO 33000

Paso 2: Identificar Prácticas

- Desde el modelo de Referencia del NIST

Función	Categoria	Subcategoría	Referencias Informativa
PR	Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	PR.AT-1: Todos los usuarios están informados y capacitados.	CIS CSC 17, 18 COBIT 2019 APO07.03, BAI05.07 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1
		PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	CIS CSC 5, 17, 18 COBIT 2019 APO07.02, DSS05.04, DSS06.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
		PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	CIS CSC 17 COBIT 2019 APO07.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Recomendaciones

- Procure entender el contexto.

Subcategoria
PR.AT-1: Todos los usuarios están informados y capacitados.

- Para seleccionar prácticas aplicables debe estar analizando en dicho contexto.

Referencias Informativa
CIS CSC 17, 18
COBIT 2019 APO07.03, BAI05.07
ISO/IEC 27001:2013 A.7.2.2, A.12.2.1

- Analice las prácticas más relevantes y atingentes al contexto dado.
- Seleccione todas las relevantes de acuerdo al contexto dado, si se repiten no importa.

Paso 3: Visión de Procesos desde COBIT

- Entienda las prácticas como un proceso, de hecho lo son, estableciendo el conjunto de actividades mínimas a realizar. En este sentido COBIT ayudará mucho.

APO07.03.01	Identificar las habilidades y competencias disponibles actuales
APO07.03.02	Identificar las brechas entre las habilidades requeridas y las disponibles. Desarrollar planes de acción
APO07.03.03	Revisar los materiales y programas de capacitación de forma regular.
APO07.03.04	Proporcionar acceso a los repositorios de conocimiento
APO07.03.05	Desarrollar y ofrecer programas de capacitación
APO07.03.06	Realizar evaluaciones periódicas

- Tener esta visión general más simple ayudará mucho en el alineamiento de las prácticas.

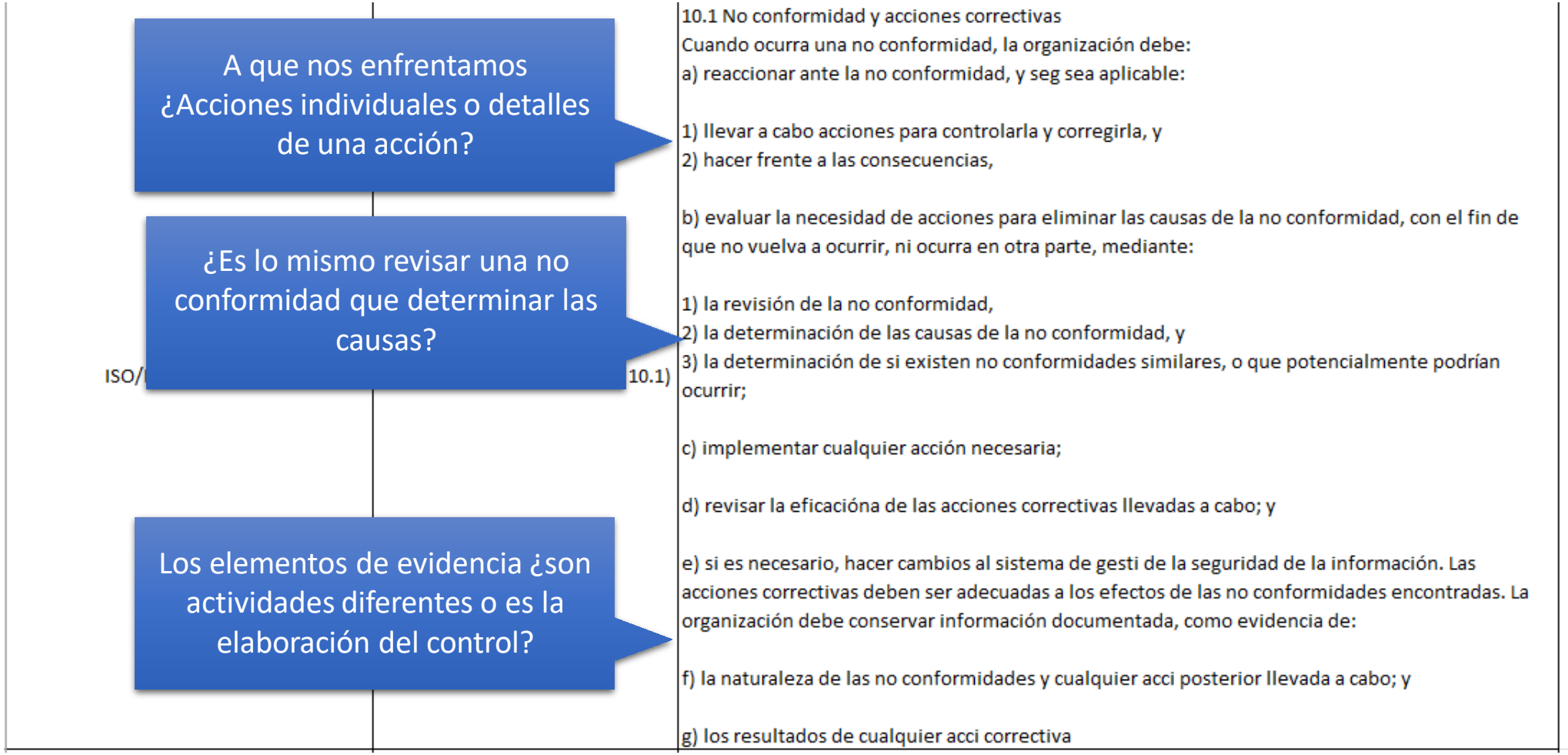
Paso 4: Evaluar Prácticas

	NIVEL DE CAPACIDAD	ATRIBUTOS
1	Realizado	▪ Proceso Incompleto ▪ Actividades ad-hoc
2	Gestionado	▪ Gestión del desempeño de la tarea ▪ Gestión del producto de la tarea
3	Establecido	▪ Definición del Proceso ▪ Despliegue del Proceso
4	Medible	▪ Medición del Proceso ▪ Control del Proceso
5	Optimizado	▪ Optimización del Proceso ▪ Innovación del Proceso

¿Qué atributo de capacidad demuestra cada control?

		os eventos de seguridad de la información se deberían notificar por los canales de gestión adecuados lo antes posible
ISO27002	16.1.5	La respuesta debería incluir la/el recogida de evidencias tan pronto como sea posible tras la ocurrencia del incidente;
ISO27002	16.1.5	La respuesta debería incluir la/el realización de un análisis forense de la seguridad de la información según se requiera
ISO27002	16.1.5	La respuesta debería incluir la/el comunicación de la existencia del incidente de seguridad de la información o cualquier otro detalle relev
ISO27002	16.1.5	La respuesta debería incluir la/el tratamiento de la debilidad o debilidades de seguridad de la información encontradas y que pudieran cau
ISO27002	16.1.2	Todos los trabajadores, contratistas y terceros deberían conocer su responsabilidad de comunicar cualquier evento de seguridad de la infor
ISO27002	16.1.4	Los eventos de seguridad de la información deberían ser evaluados y debería decidirse si se clasifican como incidentes de seguridad de la i
ISO27002	16.1.5	La respuesta debería incluir la/el aseguramiento de que todos los implicados en las actividades de respuesta a incidentes son adecuadame
ISO27002	16.1.5	La respuesta debería incluir la/el una vez que el incidente ha sido satisfactoriamente tratado, el cierre y registro formales del mismo
ISO27002	16.1.1	Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los i
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para la planificación y preparación de la r
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para monitorizar, detectar, analizar y com
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para registrar las actividades de gestión
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para el manejo de pruebas forenses se d
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para evaluar y tomar decisiones sobre ev
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos de respuesta incluyendo aquellos relativ
ISO27002	16.1.1	se deberían establecer procedimientos que aseguren que personal competente maneja los asuntos relacionados con los incidentes de seg
ISO27002	16.1.1	se deberían establecer procedimientos que aseguren que se implante un punto de contacto para la detección y comunicación de incidente
ISO27002	16.1.1	se deberían establecer procedimientos que aseguren que se mantienen contactos apropiados con las autoridades, grupos de interés exter
ISO27002	16.1.1	los procedimientos de comunicación deberían incluir la preparación de formularios de comunicación de eventos de seguridad de la inform
ISO27002	16.1.1	los procedimientos de comunicación deberían incluir el comportamiento adecuado que debería tomarse en caso de un evento de segurida
ISO27002	16.1.1	los procedimientos de comunicación deberían incluir la referencia a un proceso disciplinario formal establecido para tratar a los trabajador
ISO27002	16.1.1	los procedimientos de comunicación deberían incluir procesos de retroalimentación adecuados para garantizar que aquellas personas que
ISO27002	16.1.5	Los incidentes de seguridad de la información deberían ser respondidos de acuerdo con los procedimientos documentados.
ISO27002	16.1.7	La organización debería definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que pue
ISO27002	16.1.3	Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deberían ser obligados a anotar y not
ISO27002	16.1.6	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debería utilizarse para reducir la pr

Atención a la composición de los controles!



Paso 4: Evaluación de los atributos de capacidad

La respuesta debería incluir la recogida de evidencias tan pronto como sea posible tras la ocurrencia del incidente
(ISO27002 16.1.5)

	NIVEL DE CAPACIDAD	ATRIBUTOS	SIMPLIFICACIÓN
1	Realizado	▪ Proceso Incompleto ▪ Actividades ad-hoc	▪ Que la actividad se haga
2	Gestionado	▪ Gestión del desempeño de la tarea ▪ Gestión del producto de la tarea	▪ Que la actividad se haga bien
3	Establecido	▪ Definición del Proceso ▪ Despliegue del Proceso	▪ Que se documente cómo, quién, cuándo, dónde, por qué se hace la actividad
4	Medible	▪ Medición del Proceso ▪ Control del Proceso	▪ Que se mida el éxito y el desempeño de la actividad
5	Optimizado	▪ Optimización del Proceso ▪ Innovación del Proceso	▪ Que se mejore la actividad

La columna simplificación solo tiene fines de acelerar el ejercicio académico, no demuestra verdaderas capacidades ¡no reemplazan estudiar un marco formal!

Paso 4: Evaluación de los atributos de capacidad

La respuesta debería incluir la recogida de evidencias tan pronto com
ocurrencia del incidente
(ISO27002 16.1.5)

¡¡¡¡Recoge evidencias!!!!

	NIVEL DE CAPACIDAD	ATRIBUTOS	SIMPLIFICACIÓN
1	Realizado	▪ Proceso Incompleto ▪ Actividades ad-hoc	▪ Que la actividad se haga
2	Gestionado	▪ Gestión del desempeño de la tarea ▪ Gestión del producto de la tarea	▪ Que la actividad se haga bien
3	Establecido	▪ Definición del Proceso ▪ Despliegue del Proceso	▪ Que se documente cómo, quién, cuándo, dónde, por qué se hace la actividad
4	Medible	▪ Medición del Proceso ▪ Control del Proceso	▪ Que se mida el éxito y el desempeño de la actividad
5	Optimizado	▪ Optimización del Proceso ▪ Innovación del Proceso	▪ Que se mejore la actividad

La columna simplificación solo tiene fines de acelerar el ejercicio académico, no demuestra verdaderas capacidades ¡no reemplazan estudiar un marco formal!

Paso 4: Evaluación de los atributos de capacidad

Deberían **establecerse responsabilidades** a nivel de gestión para **asegurar que los procedimientos** para evaluar y tomar decisiones sobre eventos de seguridad y evaluar puntos débiles de la seguridad de la información se desarrollan y comunican adecuadamente dentro de la organización
(ISO27002 16.1.1)

	NIVEL DE CAPACIDAD	ATRIBUTOS	SIMPLIFICACIÓN
1	Realizado	▪ Proceso Incompleto ▪ Actividades ad-hoc	▪ Que la actividad se haga
2	Gestionado	▪ Gestión del desempeño de la tarea ▪ Gestión del producto de la tarea	▪ Que la actividad se haga bien
3	Establecido	▪ Definición del Proceso ▪ Despliegue del Proceso	▪ Que se documente cómo, quién, cuándo, dónde, por qué se hace la actividad
4	Medible	▪ Medición del Proceso ▪ Control del Proceso	▪ Que se mida el éxito y el desempeño de la actividad
5	Optimizado	▪ Optimización del Proceso ▪ Innovación del Proceso	▪ Que se mejore la actividad

La columna simplificación solo tiene fines de acelerar el ejercicio académico, no demuestra verdaderas capacidades ¡no reemplazan estudiar un marco formal!

Paso 4: Evaluación de los atributos de capacidad

Deberían **establecerse responsabilidades** a nivel de gestión para **asegurar que lo** tomar decisiones sobre eventos de seguridad y evaluar puntos débiles de la s desarrollan y comunican adecuadamente dentro de la org **(ISO27002 16.1.1)**

Definición del proceso: El proceso XYZ debe establecer responsabilidades

	NIVEL DE CAPACIDAD	ATRIBUTOS	SIMPLIFICACIÓN
1	Realizado	▪ Proceso Incompleto ▪ Actividades ad-hoc	▪ Que la actividad se haga
2	Gestionado	▪ Gestión del desempeño de la tarea ▪ Gestión del producto de la tarea	▪ Que la actividad se haga bien
3	Establecido	▪ Definición del Proceso ▪ Despliegue del Proceso	▪ Que se documente cómo, quién, cuándo, dónde, por qué se hace la actividad
4	Medible	▪ Medición del Proceso ▪ Control del Proceso	▪ Que se mida el éxito y el desempeño de la actividad
5	Optimizado	▪ Optimización del Proceso ▪ Innovación del Proceso	▪ Que se mejore la actividad

La columna simplificación solo tiene fines de acelerar el ejercicio académico, no demuestra verdaderas capacidades ¡no reemplazan estudiar un marco formal!

DIPLOMADO CIBERSEGURIDAD
CAPACITACIÓN USACH · UNIVERSIDAD DE SANTIAGO DE CHILE
CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE
ALIGNMENT

DIPLOMADO CIBERSEGURIDAD

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT

Paso 4: Un modelo de madurez podría verse como....

Marco	Referencia	Control	Nivel
ISO27002	16.1.2	Los eventos de seguridad de la información se deberían notificar por los canales de gestión adecuados lo antes posible	1
ISO27002	16.1.5	La respuesta debería incluir la/el recogida de evidencias tan pronto como sea posible tras la ocurrencia del incidente;	1
ISO27002	16.1.5	La respuesta debería incluir la/el realización de un análisis forense de la seguridad de la información según se requiera	1
ISO27002	16.1.5	La respuesta debería incluir la/el comunicación de la existencia del incidente de seguridad de la información o cualquier otro detalle releva	1
ISO27002	16.1.5	La respuesta debería incluir la/el tratamiento de la debilidad o debilidades de seguridad de la información encontradas y que pudieran cau	1
ISO27002	16.1.2	Todos los trabajadores, contratistas y terceros deberían conocer su responsabilidad de comunicar cualquier evento de seguridad de la infor	2
ISO27002	16.1.4	Los eventos de seguridad de la información deberían ser evaluados y debería decidirse si se clasifican como incidentes de seguridad de la i	2
ISO27002	16.1.5	La respuesta debería incluir la/el aseguramiento de que todos los implicados en las actividades de respuesta a incidentes son adecuadame	2
ISO27002	16.1.5	La respuesta debería incluir la/el una vez que el incidente ha sido satisfactoriamente tratado, el cierre y registro formales del mismo	2
ISO27002	16.1.1	Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los in	3
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para la planificación y preparación de la r	3
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para monitorizar, detectar, analizar y con	3
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para registrar las actividades de gestión c	3
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para el manejo de pruebas forenses se d	3
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos para evaluar y tomar decisiones sobre ev	3
ISO27002	16.1.1	deberían establecerse responsabilidades a nivel de gestión para asegurar que los procedimientos de respuesta incluyendo aquellos relativ	3
ISO27002	16.1.1	se deberían establecer procedimientos que aseguren que personal competente maneja los asuntos relacionados con los incidentes de seg	3
ISO27002	16.1.1	se deberían establecer procedimientos que aseguren que se implante un punto de contacto para la detección y comunicación de incidente	3
ISO27002	16.1.1	se deberían establecer procedimientos que aseguren que se mantienen contactos apropiados con las autoridades, grupos de interés exter	3
ISO27002	16.1.1	los procedimientos de comunicación deberían incluir la preparación de formularios de comunicación de eventos de seguridad de la inform	3
ISO27002	16.1.1	los procedimientos de comunicación deberían incluir el comportamiento adecuado que debería tomarse en caso de un evento de seguridad	3
ISO27002	16.1.1	los procedimientos de comunicación deberían incluir la referencia a un proceso disciplinario formal establecido para tratar a los trabajador	3
ISO27002	16.1.1	los procedimientos de comunicación deberían incluir procesos de retroalimentación adecuados para garantizar que aquellas personas que	3
ISO27002	16.1.5	Los incidentes de seguridad de la información deberían ser respondidos de acuerdo con los procedimientos documentados.	3
ISO27002	16.1.7	La organización debería definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que pue	3
ISO27002	16.1.3	Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deberían ser obligados a anotar y not	4
ISO27002	16.1.6	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debería utilizarse para reducir la pr	5

Paso 4: Un modelo de madurez podría verse como....

Marco	Referencia	Control	Nivel
CSC CIS v7	19.6	Publicar información relacionada con la notificación de anomalías e incidentes informáticos	1
CSC CIS v7	19.1	Documentar los procedimientos de respuesta de incidentes	3
CSC CIS v7	19.2	Asignar cargos y responsabilidades para la respuesta a incidentes	3
CSC CIS v7	19.3	Designar personal de gestión para apoyar el manejo de incidentes	3
CSC CIS v7	19.4	Idear estándares para toda la organización para reporte de incidentes	3
CSC CIS v7	19.5	Mantener información de contacto para reportar incidentes de seguridad	3
CSC CIS v7	19.8	Crear un esquema de priorización y puntuación de incidentes	3
CSC CIS v7	19.7	Llevar a cabo sesiones periódicas de escenarios de incidentes para el personal	5

Paso 4: Un modelo de madurez podría verse como....

Marco	Referencia	Control	Nivel CMI	Nivel PAN
COBIT 2019	DSS02.02	Registrar todas las solicitudes e incidentes de servicio, mediante el registro de toda la información relevante, para que pueda	2	1
COBIT 2019	DSS02.02	Permitir el análisis de tendencias, clasificar las solicitudes e incidentes de servicio, con identificación del tipo y categoría.	2	1
COBIT 2019	DSS02.02	Priorizar solicitudes e incidentes de servicio basados en la definición del servicio de SLA según el impacto y la urgencia para e	2	2
COBIT 2019	DSS02.03	Comprobar el derecho a las solicitudes de servicio, utilizando un flujo de proceso predefinido y cambios estándar, cuando sea posible	2	2
COBIT 2019	DSS02.03	Obtener la aprobación y confirmación financiera y funcional, si fuera necesario, o las aprobaciones predefinidas para los cambios está	2	2
COBIT 2019	DSS02.04	Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Referenciar los recursos de c	2	3
COBIT 2019	DSS02.04	Si un problema relacionado o error conocido no existe todavía y si el incidente satisface los criterios acordados para el registro de pro	2	3
COBIT 2019	DSS02.04	Asignar incidentes a funciones de especialista si se necesita una mayor habilidad. Contar con el nivel directivo adecuado, donde y si	2	3
COBIT 2019	DSS02.05	Seleccionar y aplicar las resoluciones de incidentes más adecuadas (solución workaround y/o solución permanente). 2	2	2
COBIT 2019	DSS02.05	Registrar, si se usaron, workarounds para la resolución de incidentes.	2	3
COBIT 2019	DSS02.05	Aplicar medidas correctivas, si se requieren.	2	2
COBIT 2019	DSS02.05	Documentar la resolución de incidentes y evaluar si la resolución puede usarse como una fuente de conocimiento futura.	2	3
COBIT 2019	DSS02.06	Comprobar con los usuarios afectados que la solicitud de servicio se ha cumplido de forma satisfactoria o el incidente se ha resuelto	2	2
COBIT 2019	DSS02.06	Cerrar las peticiones e incidentes de servicio	2	2
COBIT 2019	DSS02.07	Supervisar y hacer seguimiento al escalamientos y resoluciones de incidentes y solicitar procedimientos de manejo para progresar ha	2	2
COBIT 2019	DSS02.01	Definir esquemas de priorización y clasificación de solicitudes de servicios e incidentes, y los criterios para el registro de problemas.	3	3
COBIT 2019	DSS02.01	Definir modelos de incidentes sobre errores conocidos para permitir una resolución eficiente y eficaz.	3	3
COBIT 2019	DSS02.01	Definir modelos de solicitud de servicios conforme al tipo de solicitud de servicios para permitir la autoayuda y un servicio eficiente pa	3	3
COBIT 2019	DSS02.01	Definir las reglas y procedimientos de escalamiento de incidentes, sobre todo para incidentes importantes e incidentes de seguridad.	3	3
COBIT 2019	DSS02.01	Definir las fuentes de conocimiento sobre incidentes y solicitudes y describir cómo usarlas	3	3
COBIT 2019	DSS02.03	Cumplir con las solicitudes realizando el proceso de solicitud seleccionado. Cuando sea posible, usar menús automáticos de autoay	3	3
COBIT 2019	DSS02.07	Identificar las partes interesadas en la información y sus necesidades de datos o informes. Identificar frecuencia y medio de elaborac	3	3
COBIT 2019	DSS02.07	Producir y distribuir informes en el plazo debido o proporcionar un acceso controlado a los datos en línea.	4	4
COBIT 2019	DSS02.07	Analizar incidentes y solicitudes de servicio por categoría y tipo. Establecer tendencias e identificar patrones de problemas recurrente	4	4
COBIT 2019	DSS02.07	Usar la información como un insumo a la planificación de la mejora continua	5	5

Paso 5: Visión de Controles de ISO

- Comenzar a Mapear el proceso con ISO 27.001 primero.

Identificar las habilidades y competencias disponibles actuales
Identificar las brechas entre las habilidades requeridas y las disponibles. Desarrollar planes de acción
Revisar los materiales y programas de capacitación de forma regular.
Proporcionar acceso a los repositorios de conocimiento
Desarrollar y ofrecer programas de capacitación
Realizar evaluaciones periódicas

Definir procedimientos y responsabilidades de gestión para tratar la protección de los sistemas contra el código malicioso, la formación en su uso, así como en el informe y recuperación de los ataques de código malicioso

¿Me hago cargo en esta práctica de aquello destacado?

¿A cual actividad debería relacionarse?

Paso 5: Visión de Controles de ISO

- Comenzar a Mapear el proceso con ISO 27.001 primero.

Identificar las habilidades y competencias disponibles actuales
Identificar las brechas entre las habilidades requeridas y las disponibles. **Desarrollar planes de acción**
Revisar los materiales y programas de capacitación de forma regular.
Proporcionar acceso a los repositorios de conocimiento
Desarrollar y ofrecer programas de capacitación
Realizar evaluaciones periódicas

Un programa de concienciación en seguridad de la información debería tener como objetivo el hacer a todos los empleados y, cuando corresponda, a los contratistas, tomar conciencia de sus responsabilidades en materia de seguridad de la información y los medios disponibles para ejercerla.

Un programa de concienciación en seguridad de la información debería estar alineado con las políticas y procedimientos de seguridad más relevantes, teniendo en cuenta qué información de la organización debería ser protegida y los controles que han sido implantados para protegerla.

¿A cual actividad deberían relacionarse?

Paso 5: Visión de Controles de ISO

- Comenzar a Mapear el proceso con ISO 27.001 primero.

Identificar las habilidades y competencias disponibles actuales
Identificar las brechas entre las habilidades requeridas y las disponibles. Desarrollar planes de acción
Revisar los materiales y programas de capacitación de forma regular.
Proporcionar acceso a los repositorios de conocimiento
Desarrollar y ofrecer programas de capacitación
Realizar evaluaciones periódicas

El programa de concienciación debería incluir un conjunto de actividades tales como campañas (por ejemplo, un "día de la seguridad de la información") y la elaboración de folletos y boletines.

¿A cual actividad debería relacionarse?

Paso 5: Visión de Controles de ISO

- Comenzar a Mapear el proceso con el CIS, ideal verlo ya con la visión ISO.

Identificar las habilidades y competencias disponibles actuales
Identificar las brechas entre las habilidades requeridas y las disponibles. Desarrollar planes de acción
Revisar los materiales y programas de capacitación de forma regular.
Proporcionar acceso a los repositorios de conocimiento
Desarrollar y ofrecer programas de capacitación
Realizar evaluaciones periódicas

CIS 17.1	Lleve a cabo un análisis de la brecha de habilidades para comprender las habilidades y los comportamientos a los que los miembros de la fuerza de trabajo no se están adhiriendo, usando esta información para construir una hoja de ruta base de educación.
CIS 17.2	Realice capacitaciones para abordar el vacío de habilidades identificado para impactar positivamente el comportamiento de seguridad de los miembros de la fuerza laboral.
CIS 17.3	Cree un programa de concientización de seguridad para que todos los miembros de la fuerza laboral lo completen regularmente para asegurarse de que entienden y exhiben los comportamientos y las habilidades necesarias para ayudar a garantizar la seguridad de la organización. El programa de concientización de seguridad de la organización debe comunicarse de manera continua y atractiva.
CIS 17.4	Asegúrese de que el programa de concientización de seguridad de la organización se actualice con frecuencia (al menos una vez al año) para abordar nuevas tecnologías, amenazas, estándares y requisitos de negocio.
CIS 17.5	Capacite a los miembros de la fuerza de trabajo sobre la importancia de habilitar y utilizar la autenticación segura.
CIS 17.6	Capacite a los empleados sobre cómo identificar diferentes formas de ataques de ingeniería social, como phishing, fraudes telefónicos y llamadas de suplantación.
CIS 17.7	Capacite a los empleados sobre cómo identificar y almacenar, transferir, archivar y destruir información confidencial de manera adecuada.
CIS 17.8	Capacite a los miembros de la fuerza de trabajo para que conozcan las causas de las exposiciones involuntarias de datos, cómo perder sus dispositivos móviles o enviar correos electrónicos a la persona equivocada debido al autocompletado en el correo electrónico.
CIS 17.9	Capacitar a los empleados para que puedan identificar los indicadores más comunes de un incidente y poder informar tal incidente.

Paso 6: Resolviendo Problemas

Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información. **(ISO 27002 16.1.1)** **NIVEL 3**

Documentar los procedimientos de respuesta de incidentes .**(CIS 19.1)** **NIVEL 3**

Definir las reglas y procedimientos de escalamiento de incidentes, sobre todo para incidentes importantes e incidentes de seguridad.**(COBIT 2019 DSS02.01)** **NIVEL 3**

Paso 6: Resolviendo Problemas

Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
(ISO 27002 16.1.1) NIVEL 3

Documentar los procedimientos de respuesta de incidentes .**(CIS 19.1) NIVEL 3**

Definir las reglas y procedimientos de escalamiento de incidentes, sobre todo para incidentes importantes e incidentes de seguridad.**(COBIT 2019 DSS02.01) NIVEL 3**

Se deberían establecer y documentar procedimientos y responsabilidades de gestión y escalamiento para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.**(ISO 27002 16.1.1 + CIS 19.1 + DSS02.01 → Nivel 3)**