



Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)

Desarrollando un programa de ciberseguridad para la USACH



Profesor
Juan Ignacio Iturbe A



Contexto

- La USACH cuenta con alrededor 4000 personas contratadas entre académicos y administrativos en 40 Departamentos académicos.
- Cuentan con un conjunto de tecnologías que habilitan a los académicos, administrativos y estudiantes avanzar en su investigación y educación.
- El 2022 se seleccionó el NIST CSF para la formulación de su programa de ciberseguridad.
- Estos esfuerzos fueron acompañados por los estudiantes de la asignatura de Ciberseguridad.



UNIVERSIDAD
DE SANTIAGO
DE CHILE

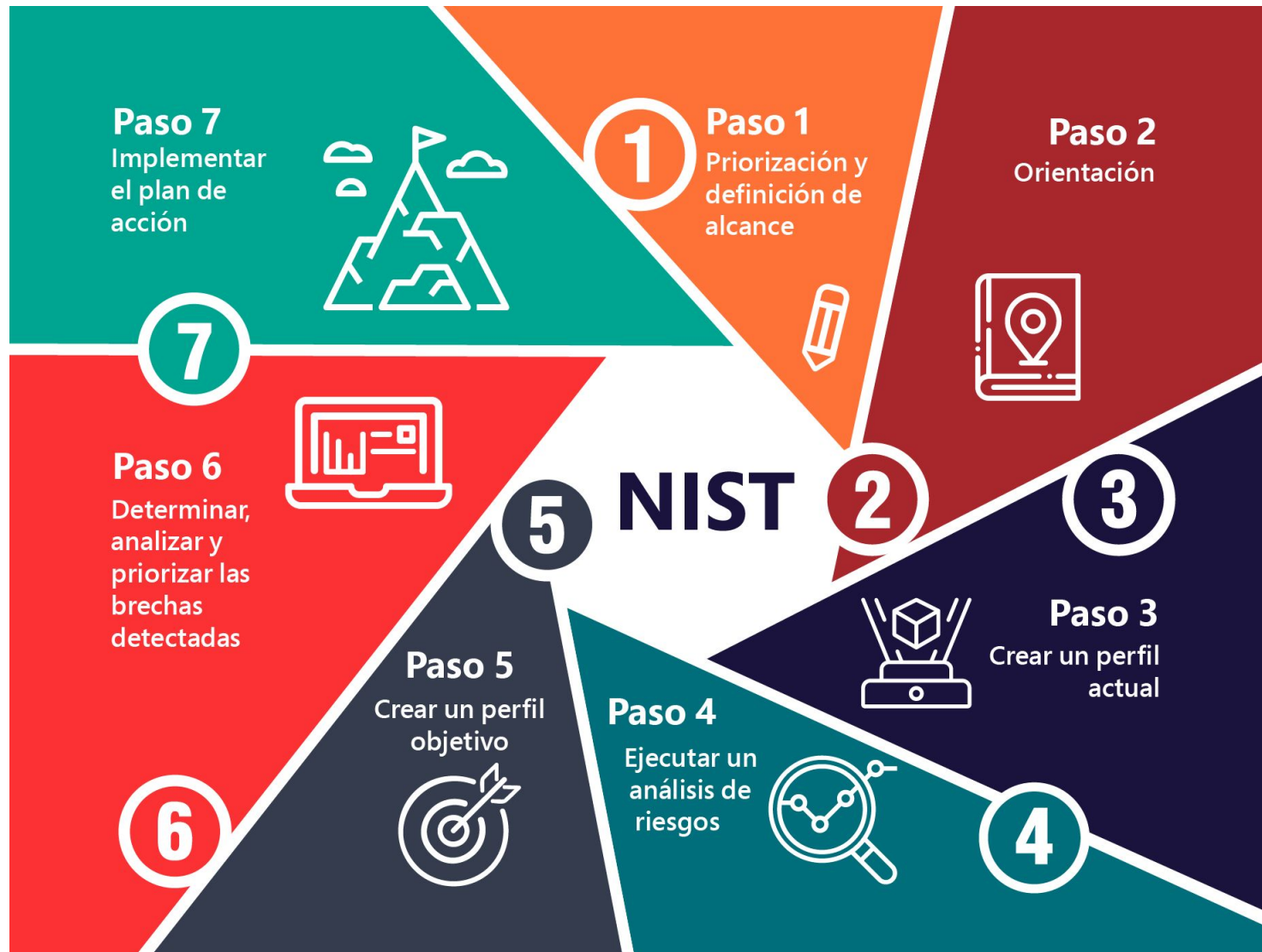
Organigrama USACH ([Link](#))



El desafío

- Modelo descentralizado utilizando administración local de TI específico para las necesidades de los Departamentos (1 o 2 personas orientada por Departamento académico).
- Se aprecia personal informático en diversas unidades administrando sistemas específicos.
- Empresa externa administra las redes y comunicaciones, da soporte tecnológico a las unidades (de forma remota), y administra los servicios de autenticación, correo electrónico e Internet. También administra infraestructura TI (ej. Servidores Web, DNS, antivirus, firewalls, entre otros).
- El presupuesto se aprueba centralizadamente para la compra de hardware y software de uso masivo.
- El presupuesto ha aumentado en los últimos años, debido al reemplazo de plataformas.
- Este modelo le provee poca agilidad a los departamentos. Además, esto implica sus propios procesos de gestión y gobernanza, resultando en los siguientes desafíos:
 - Riesgo debido a la inconsistencia en la aplicación de control de seguridad.
 - Riesgo debido a las brechas de los controles de seguridad a través de los departamentos.
 - Gasto en ciberseguridad mínimo.
 - Duplicación del esfuerzo.
 - Solamente existe una política de seguridad de la información y no se ha bajado a políticas específicas ni procedimientos.

Recordemos...





NIST CSF - Paso 1: Priorización y Alcance

- La organización identifica sus **objetivos empresariales** o de **misión** y las **prioridades organizacionales de alto nivel**.
- Con esta información, la organización toma decisiones estratégicas con respecto a las implementaciones de ciberseguridad y **determina el alcance de los sistemas y activos** que respaldan la línea o proceso comercial seleccionado.
- Se puede adaptar el marco para **admitir las diferentes líneas de negocio o procesos** dentro de una organización, que pueden tener diferentes necesidades empresariales y la tolerancia al riesgo asociada.
- Las **tolerancias de riesgo** pueden reflejarse en un nivel de Implementación objetivo.



Aplicación paso 1: Objetivos y prioridades

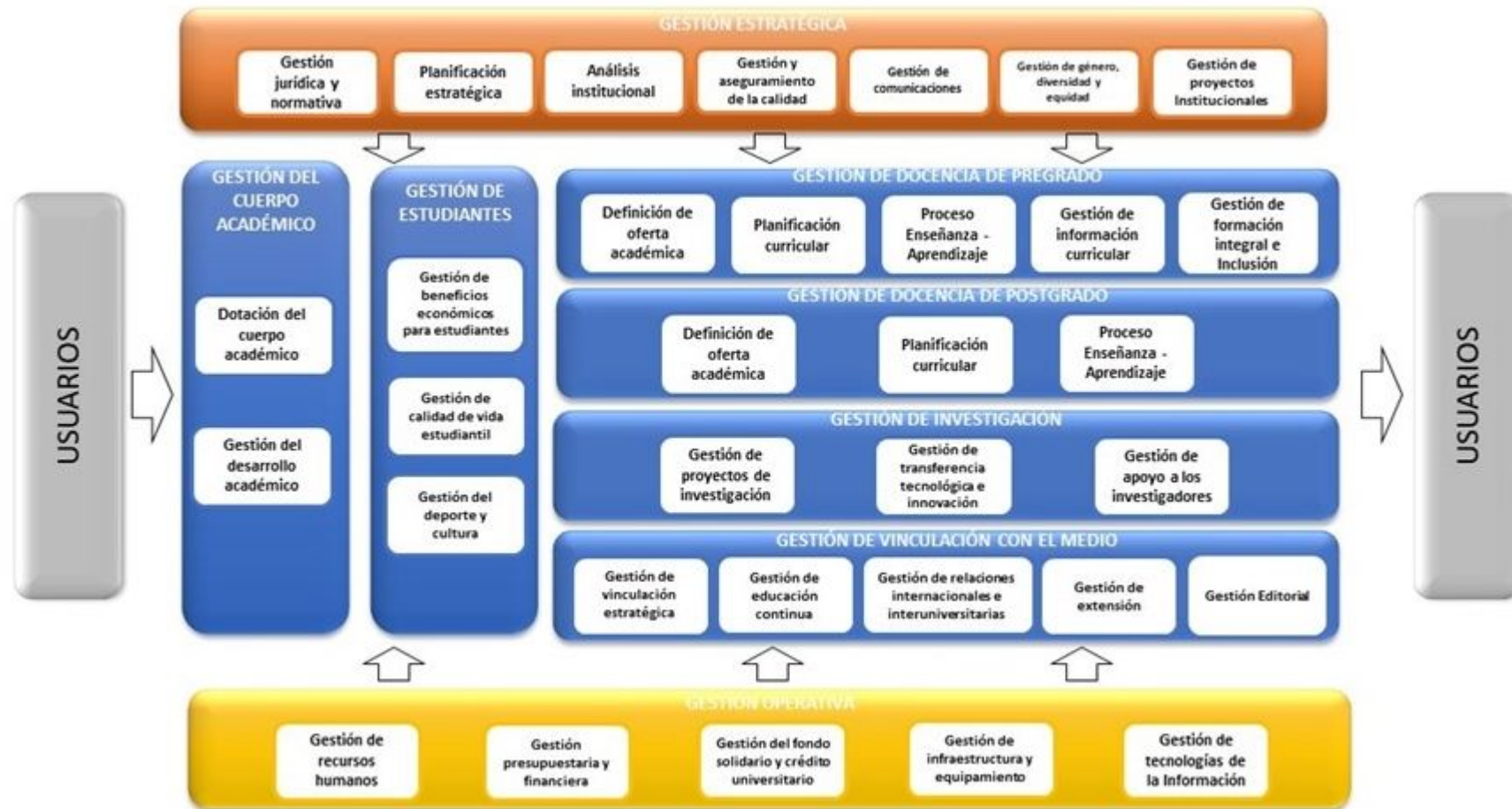
Objetivos empresariales (PEI Institucional 2020-2030):

- “Fomentar el desarrollo de una cultura de transformación digital en toda la comunidad universitaria”
- “Desarrollar la infraestructura y asegurar el uso de tecnologías pertinentes a los desafíos de la próxima década”
- “Asegurar una oferta académica, metodologías y tecnologías de enseñanza pertinentes a los desafíos de la próxima década”

Prioridades organizacionales de alto nivel

- Se determinó que la gestión de la docencia de pregrado es un proceso prioritario y que es necesario asegurar.

Aplicación paso 1: Determinación de proceso prioritario

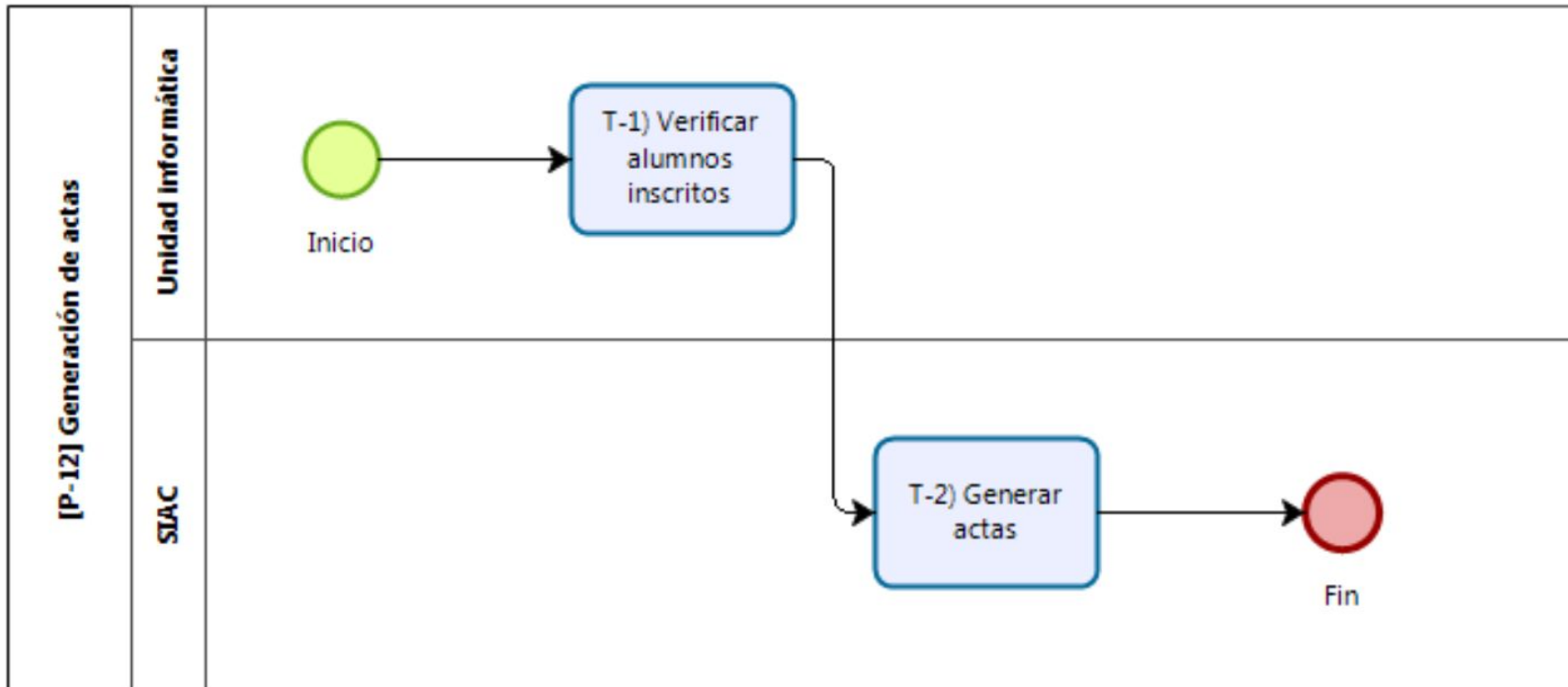


Fuente:
<https://www.dca.usach.cl/sistema-de-gesti%C3%B3n-de-la-calidad>

- Luego se determina que el proceso “Gestión de información curricular” es uno de los prioritarios para la organización.
- Sin embargo, este es un proceso que engloba a más subprocesos.

Aplicación paso 1: Determinación de proceso prioritario

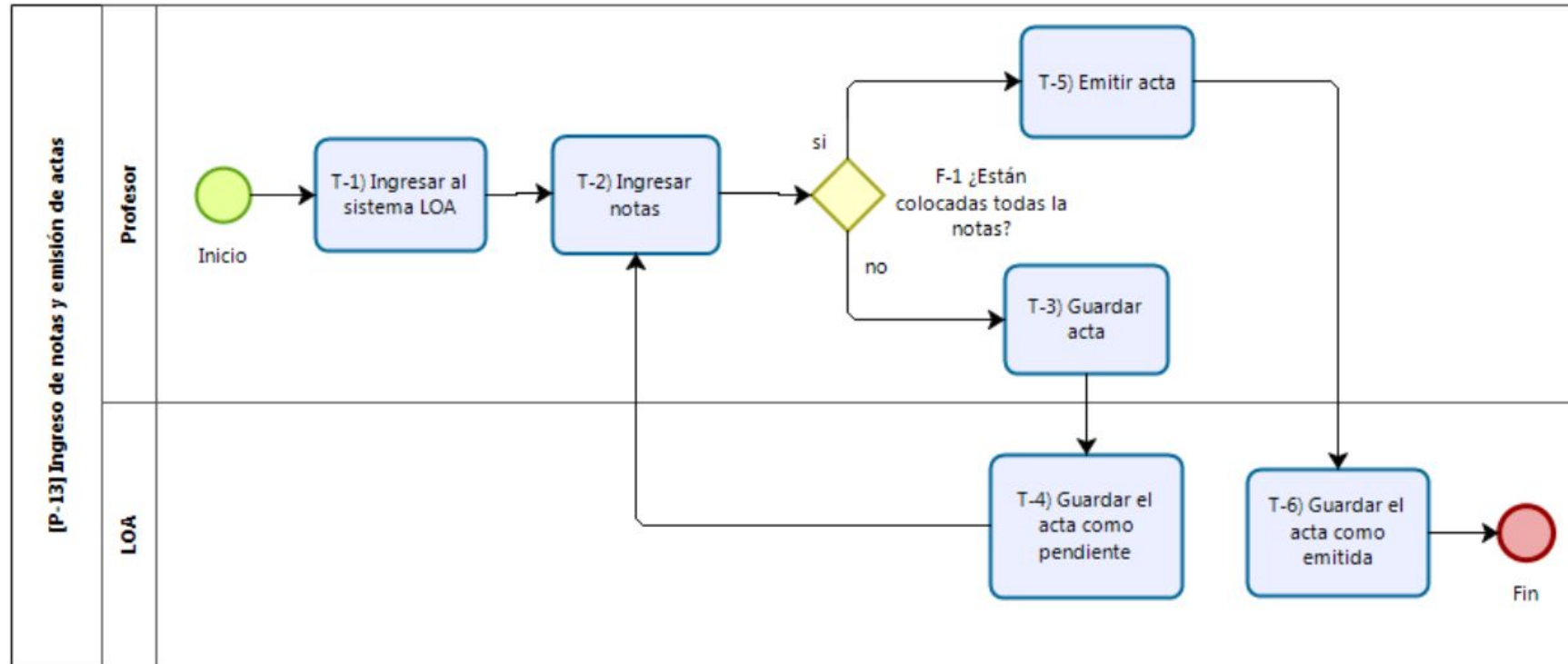
Proceso de ingreso de notas: Generación de actas



(Brown, 2016)

Aplicación paso 1: Determinación de proceso prioritario

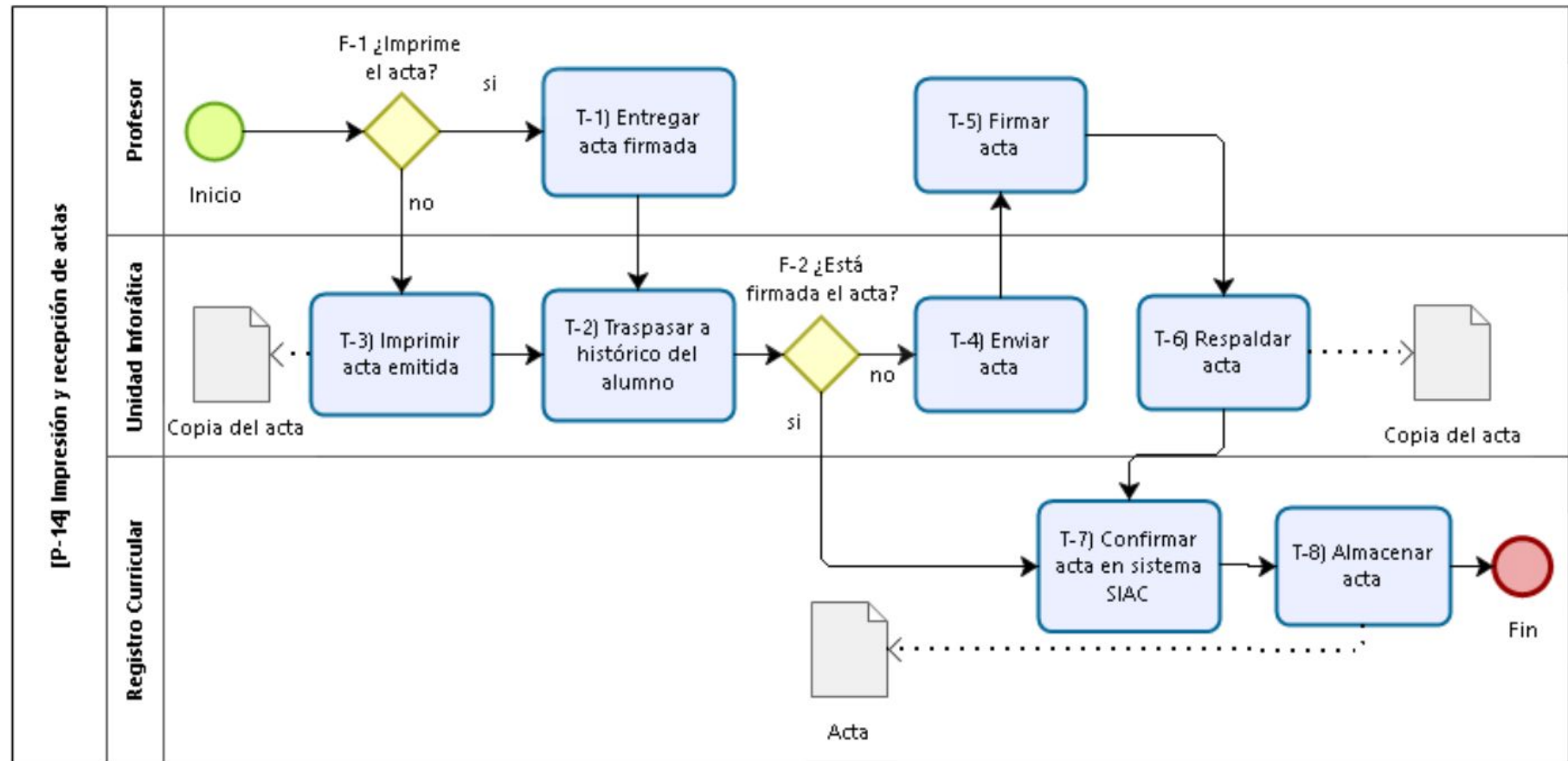
Proceso de ingreso de notas: Ingreso de notas y emisión de actas



(Brown, 2016)

Aplicación paso 1: Determinación de proceso prioritario

Proceso de ingreso de notas: Impresión y recepción de actas



(Brown, 2016)



NIST CSF - Paso 2: Orientación

- Una vez que se ha determinado el alcance del programa de ciberseguridad para la línea de negocio o el proceso, la organización **identifica los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general.**
- La organización luego consulta las fuentes para **identificar las amenazas y vulnerabilidades** aplicables a esos sistemas y activos.

Aplicación paso 2: Orientación

- ¿Sistemas involucrados?
 - Ej. LOA
- ¿Activos involucrados?
 - Ej. Acta de nota sin firmar
- ¿Requisitos reglamentarios?
 - Ej. Reglamento General de Régimen de estudios ([link](#))
- ¿Enfoque de riesgo?
 - ISO 31.000
 - Evaluación de riesgos cualitativa.
 - Se deben mitigar aquellos riesgos extremos.

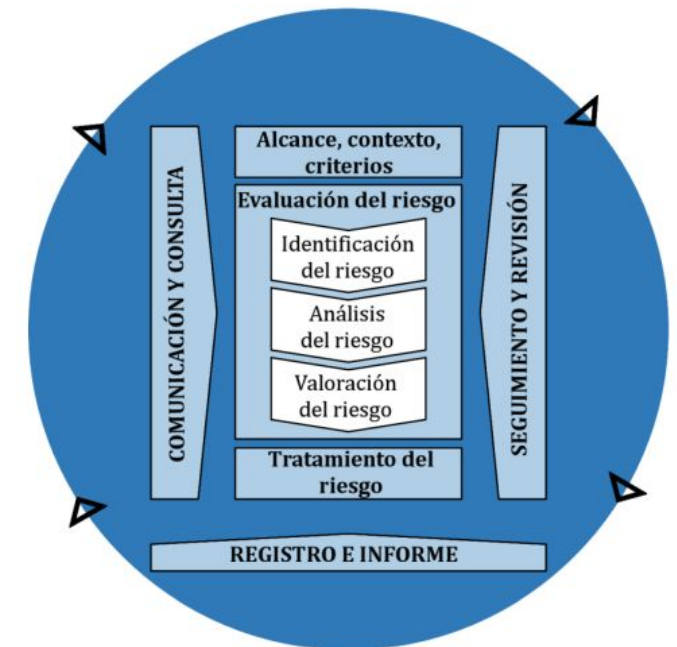


Figura 4 - Proceso

Aplicación paso 2: Orientación



- ¿Qué amenazas serían aplicables sobre los sistema?
 - Ej: Utilizar modelado de amenazas y STRIDE (a nivel de flujo de información, a nivel de acceso a los sistemas a través de la red).
- ¿Qué vulnerabilidades podría tener los sistema?
 - Ej: Sistemas desactualizados, control de acceso poco riguroso, cuentas de usuarios compartidas,





NIST CSF - Paso 3: Crear un perfil actual

- La organización desarrolla un Perfil Actual en que indica qué **resultados** de categoría y subcategoría del Núcleo del Marco se están logrando **actualmente**.
- Si se logra parcialmente un resultado, tomar nota de este hecho ayudará a respaldar los pasos posteriores al proporcionar información de referencia.

Revisemos una categoría

Función	Categoría	Subcategoría	Referencias informativas
IDENTIFICAR (ID)	Gestión de activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	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 ISA 62443-3-3:2013 SR 7.8 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 y terceros 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





¿Cómo identificamos el perfil actual de la categoría?

Función	Categoría	Subcategoría	Referencias informativas
IDENTIFICAR (ID)	Gestión de activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa	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 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5

Preguntas de ejemplo:

- Procesos
 - ¿Se tienen procesos para inventariar los activos físicos de la organización?
- Personas
 - ¿Las personas que participan en los procesos de inventario se encuentran capacitadas para ello?
- Tecnologías
 - ¿Se cuenta con un software centralizado para inventariar los activos físicos de la organización?

¿Desde donde nos podríamos basar para identificar preguntas de acuerdo a las buenas prácticas de la industria?



CIS CONTROL 01

Inventario y Control de los Activos Empresariales

SALVAGUARDAS

5

IG1

2/5

IG2

4/5












IG3

5/5

RESUMEN

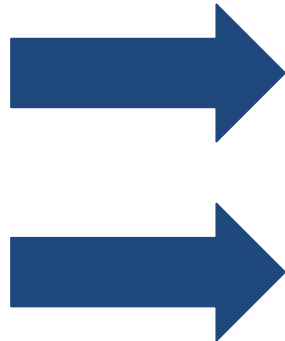
Gestione activamente (inventario, seguimiento y corrección) todos los activos de la empresa (dispositivos de usuarios finales, incluidos equipos portátiles y teléfonos móviles; dispositivos de red; Dispositivos no informáticos/Internet de las Cosas (IoT); y servidores) conectados a la infraestructura física, virtualmente, remotamente, y aquellos del ambiente de la nube, para conocer con precisión la totalidad de los activos que necesitan ser monitoreados y protegidos dentro de la empresa. Esto también apoyará la identificación de activos no autorizados y no administrados para eliminar o remediar.

Salvaguardas

SALVAGUARDA	TÍTULO DE SALVAGUARDA/DESCRIPCIÓN DE SALVAGUARDA	TIPO DE ACTIVO	FUNCIÓN DE SEGURIDAD	IG1	IG2	IG3
1.1	Establecer y Mantener un Detallado Inventario de Activos Empresariales Establecer y mantener un inventario preciso, detallado y actualizado de todos los activos de la empresa con el potencial de almacenar o procesar datos, para incluir: dispositivos de usuarios finales (incluidos portátiles y móviles), dispositivos de red, no informáticos IoT y servidores. Asegúrese de que el inventario registre la dirección de red (si es estática), la dirección de la máquina, el propietario del activo de datos, el departamento de cada activo y si el activo ha sido aprobado para conectarse a la red. Para los dispositivos móviles de usuario final, las herramientas tipo MDM pueden admitir este proceso, cuando corresponda. Este inventario incluye activos conectados a la infraestructura física, virtual, remotamente y aquellos de entornos de la nube. Adicionalmente, incluye activos que están conectados regularmente a la infraestructura de red de la empresa, incluso si no están bajo el control de la empresa. Revisar y actualizar el inventario de todos los activos de la empresa cada dos años o con mayor frecuencia.	Dispositivos	Identificar			
1.2	Gestionar Activos no Autorizados Asegúrese de que exista un proceso para abordar los activos no autorizados semanalmente. La empresa puede optar por eliminar el activo de la red, negar que el activo se conecte de forma remota a la red o poner en cuarentena el activo.	Dispositivos	Responder			
1.3	Utilice una herramienta de descubrimiento activo Utilice una herramienta de descubrimiento activa para identificar activos conectados a la red empresarial. Configure la herramienta de descubrimiento activo para ejecutar diariamente o con más frecuencia.	Dispositivos	Detectar			
1.4	Utilice el registro de la configuración de dinámica de host (DHCP) para actualizar el inventario de activos Utilice el registro DHCP en todos los servidores o las herramientas de administración de direcciones de protocolo de internet (IP) para actualizar el inventario de activos de la empresa. Revise y use los registros para actualizar semanalmente el inventario de activos de la empresa o con mayor frecuencia.	Dispositivos	Identificar			
1.5	Utilice una herramienta de descubrimiento de activos pasivo Utilice una herramienta de descubrimiento pasivo para identificar activos conectados a la red empresarial. Revise y utilice escaneos para actualizar el inventario de activos de la empresa al menos semanalmente o con más frecuencia.	Dispositivos	Detectar			



ISO 27001:2013



A.8 Gestión de activos		
A.8.1 Responsabilidad sobre los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		
A.8.1.1	Inventario de activos	<i>Control</i> La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
A.8.1.2	Propiedad de los activos	<i>Control</i> Todos los activos que figuran en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	<i>Control</i> Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.
A.8.1.4	Devolución de activos	<i>Control</i> Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

BAI09 Gestionar los Activos		Área: Administración Dominio: Construir, Adquirir e Implantar
Descripción del Proceso		
Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.		
Declaración del Propósito del Proceso		
Contabilización de todos los activos de TI y optimización del valor proporcionado por estos activos.		
El proceso apoya la consecución de un conjunto de objetivos primarios relacionados con las TI:		
Metas TI	Métricas Relacionadas	
06 Transparencia de los costes, beneficios y riesgo de las TI	<ul style="list-style-type: none"> • Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados. • Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI. 	
11 Optimización de activos, recursos y capacidades de TI	<ul style="list-style-type: none"> • Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las evaluaciones • Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI 	
Objetivos y Métricas del Proceso		
Meta del Proceso	Métricas Relacionadas	
1. Las licencias cumplen y están alineadas con las necesidades del negocio.	<ul style="list-style-type: none"> • Porcentaje de licencias usadas respecto a licencias pagadas 	
2. Los activos se mantienen en condiciones óptimas.	<ul style="list-style-type: none"> • Número de activos no utilizados • Comparativa de costes • Número de activos obsoletos 	

Matriz RACI BAI09																												
Prácticas Clave de Gestión																												
</																												

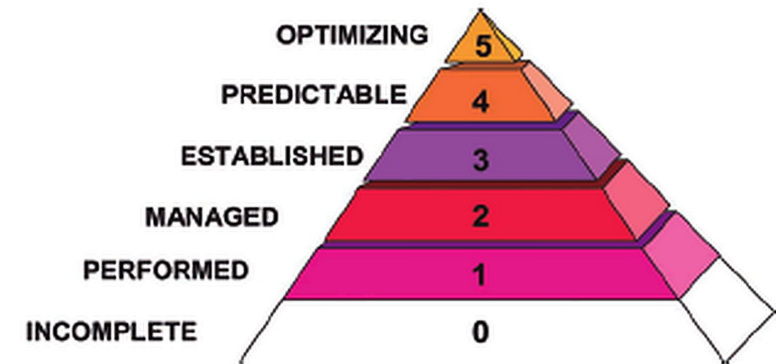
BAI09 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
BAI09.01 Identificar y registrar los activos actuales. Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera.	BAI03.04	Actualizaciones al inventario de activos	Registro de activos	AP006.01 BAI10.03
	BAI10.02	Repositorio de configuración	Resultados de comprobaciones físicas de inventario	BAI10.03 BAI10.04 DSS05.03
			Resultados de revisiones de adecuación al objetivo	AP002.02
Actividades				
1. Identificar todos los activos en propiedad en un registro que indique el estado actual. Mantener su alineación con los procesos de gestión de cambios y de la configuración, el sistema de gestión de la configuración y los registros contables financieros.				
2. Identificar los requisitos legales, reglamentarios o contractuales que deben ser abordados en la gestión de los activos.				
3. Verificar la existencia de todos los activos en propiedad mediante la realización periódica de controles de inventario físicos y lógicos y su conciliación, incluyendo la utilización de herramientas software de descubrimiento.				
4. Comprobar que los activos se adecuan a sus objetivos (p.ej., están en condiciones útiles).				
5. Determinar de forma regular si cada activo continúa proporcionando valor y, si es así, estimar la vida útil prevista de dicha validez.				
6. Asegurar la contabilización de todos los activos.				
Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
BAI09.02 Gestionar Activos Críticos. Identificar los activos que son críticos en la provisión de capacidad de servicio y dar los pasos para maximizar su fiabilidad y disponibilidad para apoyar las necesidades del negocio.			Comunicación de tiempo de inactividad planificado para mantenimiento	AP008.04
			Contratos de mantenimiento	Interno
Actividades				
1. Identificar los activos que son críticos en la provisión de la capacidad del servicio refiriéndose a los requisitos en las definiciones de servicio, ANSs y el sistema de gestión de la configuración.				
2. Supervisar el rendimiento de los activos críticos examinando las tendencias de incidentes y, en caso necesario, tomar medidas para reparar o reemplazar.				
3. De forma regular, considerar el riesgo de fallo o necesidad del reemplazo de cada activo crítico.				
4. Mantener la resiliencia de los activos críticos mediante la aplicación de un mantenimiento preventivo regular, de supervisión del rendimiento y, si fuera necesario, proporcionando alternativas y/o activos adicionales para reducir la probabilidad de fallo.				
5. Establecer un plan de mantenimiento preventivo para todo el hardware, considerando un análisis coste-beneficio, recomendaciones del proveedor, el riesgo de interrupción del servicio, personal cualificado y otros factores relevantes.				
6. Establecer contratos de mantenimiento que impliquen el acceso de terceros a las instalaciones de TI de la organización para actividades in situ y fuera del sitio (p. ej. externalización). Establecer contratos formales de servicio que contengan o se refieran a todas las condiciones de seguridad necesarias, incluidos los procedimientos de autorización de acceso, para garantizar el cumplimiento de las políticas y estándares de seguridad de la organización.				
7. Comunicar a los clientes y los usuarios afectados el impacto esperado (p. ej., las restricciones de rendimiento) de las actividades de mantenimiento.				
8. Asegurar que los servicios de acceso remoto y perfiles de usuario (u otros medios utilizados para el mantenimiento o diagnóstico) están activos sólo cuando sea necesario.				
9. Incorporar el tiempo de inactividad previsto en general en el calendario de producción, y programar las actividades de mantenimiento para minimizar el impacto adverso en los procesos de negocio.				

Madurez de los procesos

Personas



Nivel	Puntuación	Descripción
Inadecuado	0	<ul style="list-style-type: none"> - La actividad no se puede realizar debido a que el personal tiene habilidades limitadas. - La actividad no se puede realizar debido a la falta de disponibilidad de personal. - Ningún personal es responsable de completar la actividad .
Carente	1	<ul style="list-style-type: none"> - El personal actual tiene habilidades limitadas que solo les permiten realizar una pequeña parte de las actividades - El personal realiza las actividades en la medida en que tienen disponibilidad, pero requiere muchos recursos y le restan responsabilidades.
Adecuado	2	<ul style="list-style-type: none"> - El personal actual tiene las habilidades para realizar la mayoría de las responsabilidades asociadas con la actividad - El personal realiza las actividades en la medida en que tienen disponibilidad, pero requiere muchos recursos y le restan responsabilidades.
Informal	3	<ul style="list-style-type: none"> - La mayoría de las responsabilidades asociadas con la actividad se pueden realizar con la cantidad actual de personal y base de conocimientos sin una carga significativa. - El personal es responsable de realizar la actividad sin ser asignado formalmente .
Formal	4	<ul style="list-style-type: none"> - El personal tiene habilidades y experiencia suficientes para completar la actividad en su totalidad con poca carga. - El personal ha sido explícitamente designado roles y responsabilidades para completar la actividad .



- De acuerdo la ISO 15504 (SPICE) para evaluar la madurez de los procesos

Madurez de los procesos

Procesos



Nivel	Puntuación	Descripción
Sin proceso	0	- Las tareas asociadas a esta actividad no se realizan.
Ad-Hoc	1	- No hay documentación asociada a la actividad. - Las tareas asociadas con esta actividad se realizan de manera ad hoc .
Definido	2	- Existe alguna documentación escrita para abordar la actividad. - la documentación solo se implementa parcialmente o se sigue en la práctica .
Repetible	3	- Existe documentación apropiada para abordar la actividad. - La actividad se realiza principalmente de acuerdo con la documentación.
Formal	4	- Existe la documentación adecuada para abordar la actividad y se alinea con la política y los estándares de la organización - la actividad se realiza de acuerdo con la política y estándares de la organización

Madurez de los procesos

Tecnología



Title	Score	Description
Indisponible	0	- La tecnología apropiada requerida para realizar esta actividad no está disponible dentro del departamento.
No coincidente	1	- El propósito principal de la tecnología que se utiliza para completar la actividad no es el propósito previsto.
Limitado	2	<ul style="list-style-type: none"> - La tecnología es capaz y está configurada para realizar algunas de las actividades requeridas. - Hay una infraestructura limitada, capacidad de computación o licencias de software disponibles para el departamento para realizar la actividad requerida .
Aceptable	3	<ul style="list-style-type: none"> - La tecnología es capaz y está configurada para realizar la mayor parte de la actividad requerida. - Hay suficiente infraestructura, capacidad de computación y licencias de software disponibles para el departamento para realizar la actividad requerida .
Óptimo	4	<ul style="list-style-type: none"> - La actividad se puede completar en su totalidad con la tecnología. - La función principal de la tecnología es realizar la actividad requerida. - Hay una amplia infraestructura, capacidad de computación y licencias de software disponibles para el departamento para realizar la actividad requerida .

ID.AM



- Reconocer cuales son los dispositivos, el software y los recursos del entorno ayuda a identificar posibles incidentes de seguridad antes de que se exploten.
- Todos los días se descubren nuevas vulnerabilidades para una amplia variedad de dispositivos.
- Comprender los activos dentro del entorno garantiza que el equipo TI pueda parchear los sistemas vulnerables a medida que se descubren nuevas vulnerabilidades y garantiza que el punto de contacto adecuado pueda ser informado según sea necesario.



Ejemplo para ID.AM (Personas)

Personas

Identificador	Función	Pregunta	Respuesta
ID.AM.Pe-1	Identificar	¿Cuál es el nivel del personal de TI de su departamento para priorizar, rastrear e inventariar los activos de TI (incluidos los dispositivos físicos, el software)?	Inadecuado



Ejemplo para ID.AM (Procesos)

Procesos

Identificador	Función	Pregunta	Respuesta
ID.AM.Pr-1	Identificar	¿Cuál es el nivel de la organización para priorizar, rastrear e inventariar activos de TI (incluidos dispositivos físicos, software?	Ad-hoc



Ejemplo para ID.AM (Tecnología)

Tecnología

Identificador	Función	Pregunta	Respuesta
ID.AM.Tech-1	Identificar	¿Cuál es el nivel de los recursos tecnológicos de su organización para rastrear e inventariar los activos de TI y su importancia (incluidos los dispositivos físicos, el software)?	No coincidente



Aplicación Paso 3: Crear un perfil actual

- A modo de ejemplo se calculará la categoría en función de las preguntas que se tienen actualmente.
- Esto se debería hacer de acuerdo al diagnóstico completo de la situación actual en la categoría ID.AM

Función	Categoría	Subcategoría
IDENTIFICAR (ID)	Gestión de activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	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 y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.



Aplicación Paso 3: Crear un perfil actual

- De acuerdo a las respuestas podríamos decir que nuestro perfil actual en la categoría ID.AM es **“No comenzado” (Nivel 0)**.
- Definitivamente, hay que mejorar, pero eso lo veremos más adelante.

#	Evaluación	Definición
0	No comenzado	No se ha iniciado ningún progreso para lograr los resultados de la hoja de ruta definidos a partir del perfil del estado objetivo.
1	No logrado	Hay poca evidencia o ninguna evidencia del logro de los resultados definidos en el perfil de estado objetivo.
2	Parcialmente logrado	Existe cierta evidencia de un enfoque y algún logro de los resultados definidos en el perfil del estado objetivo. Algunos aspectos de las actividades requeridas para lograr el perfil de estado objetivo pueden no estar completamente definidos.
3	Logrado	Existe evidencia de un enfoque sistemático y un logro significativo de los resultados definidos en el perfil del estado objetivo. Pueden existir algunas debilidades en el proceso para lograr el resultado deseado.
4	Completamente logrado	Existe evidencia de un enfoque completo y sistemático y un logro completo de los resultados definidos en el perfil del estado objetivo. No existen debilidades significativas en el proceso para lograr el resultado deseado.



Actividad en clase

- Desarrolle un conjunto de preguntas de acuerdo al ID.AM-2.
- Al menos una pregunta basada en los CIS Controls y otra basada en la ISO 27.001:2013.
- Considere los siguientes aspectos: procesos, personas y tecnologías.



Bibliografía

- <https://www.nist.gov/cyberframework>
- <https://www.cisecurity.org/>
- https://www.usach.cl/sites/default/files/field/uploaded_files/Aprueba%20reglamento%20general%20de%20regimen%20de%20estudios%20de%20pregrado%20Res.2563.pdf
- Estudio de caso BSD - Universidad de Chicago