DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

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.

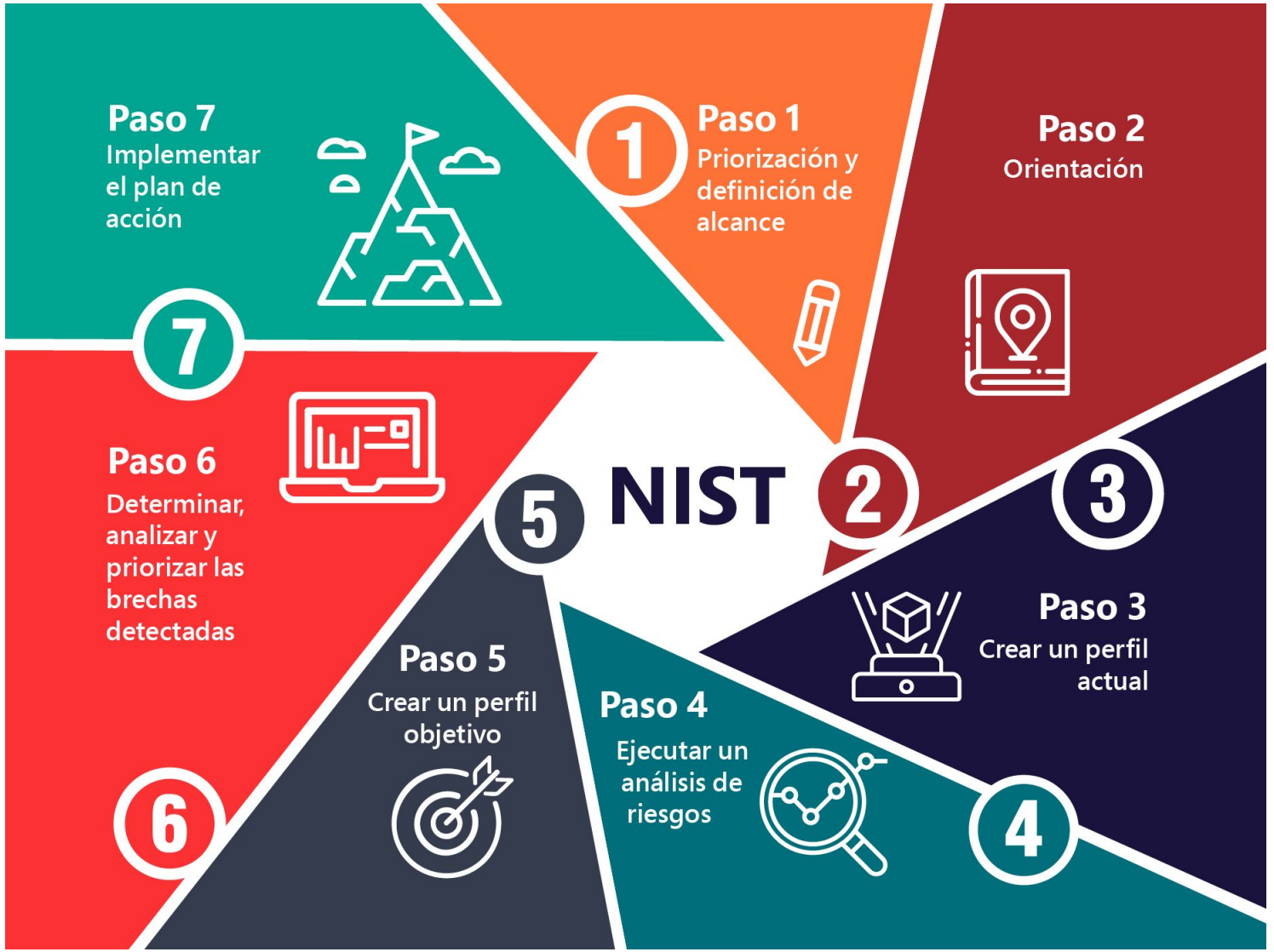
UNIVERSIDAD DE SANTIAGO DE CHILE

Organigrama USACH (Link)

El desafío

- Modelo descentralizado utilizando administración local de TI específico para las necesidad 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…


Paso 7
Implementar el plan de acción
7
1
Paso 1
Priorización y definición de alcance
Paso 2
Orientación
Paso 6
Determinar, analizar y priorizar las brechas detectadas
NIST
2
3
Paso 3
Crear un perfil actual
5
Paso 5
Crear un perfil objetivo
Paso 4
Ejecutar un análisis de riesgos
6
4

NIST CSF - Paso 4: Realizar una evaluación de riesgos

- Esta evaluación podría estar guiada por el **proceso de gestión de riesgos general** de la organización o actividades previas de evaluación de riesgos.
- La organización analiza el entorno operativo para discernir la **probabilidad** de un evento de ciberseguridad y el **impacto** que el evento podría tener en la organización.
- Es importante:
  - Identificar los riesgos emergentes
  - Utilizar información de amenazas de ciberseguridad de fuentes internas y externas
- Para obtener una mejor comprensión de la probabilidad y el impacto de los eventos de ciberseguridad.

Aplicación paso 4: Realizar una evaluación de riesgos

Recordar:

- Que el enunciado de la actividad indica la utilización de la ISO 31.000.
  - La evaluación de riesgos de la ISO 31.000 se encuentra en el punto 6.4 (pag. 19-21). De evidencia de cómo se alinea lo realizado por el grupo y la ISO.
- En el paso 2, se definió:
  - Evaluación de riesgos cualitativa.
  - Se deben mitigar aquellos riesgos extremos (esto implica un mapa de calor de los riesgos) y algunos riesgos deben ser extremos (al menos 3).
- Los activos y sistemas sobre los que se realiza la evaluación son los identificados en las etapas anteriores.
- Las probabilidades e impactos se deben justificar.
- Considere amenazas relacionadas con el levantamiento realizado en las etapas anteriores en las categorías asignadas.

Aplicación paso 4: Realizar una evaluación de riesgos

Impacto	Probabilidad				
	Muy Baja	Baja	Media	Alta	Muy Alta
Muy Alto	Medio	Medio	Alto	Extremo	Extremo
Alto	Bajo	Medio	Alto	Alto	Extremo
Medio	Bajo	Medio	Medio	Alto	Alto
Bajo	Muy Bajo	Bajo	Bajo	Medio	Alto
Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Medio	Medio

#	Activo comprometido	Vulnerabilidad	Amenaza	Agente de amenaza	Objetivo de ciberseguridad comprometido	Probabilidad	Impacto	Riesgo	Control	Probabilidad	Impacto	Riesgo residual
R1	Base de datos SIAC	Cliente SIAC sin inventariar que se encuentra en notebook personal del encargado de archivo de RC.	Suplantación del encargado de archivo RC para la modificación de la base de datos	Ex - estudiante enojado	Integridad	Alta	Muy Alto	Extremo	CIS 1.1 Establecer y mantener un detallado inventario de activos empresariales CIS1.2 Gestionar activos no autorizados A.8.1.2 Propiedad de los activos	Baja	Muy Alto	Medio

Mapa de riesgo

		Probabilidad				
Impacto		Muy Baja	Baja	Media	Alta	Muy Alta
	Muy Alto		R1 ← - - - - - - - - - - - -		R1	
	Alto					
	Medio					
	Bajo					
	Muy Bajo					

NIST CSF - Paso 5: Crear un perfil objetivo

- La organización crea un Perfil Objetivo que se centra en la evaluación de las Categorías y Subcategorías del Marco que describen los resultados deseados de ciberseguridad de la organización.
- Las organizaciones también pueden desarrollar sus propias Categorías adicionales y Subcategorías para tener en cuenta los riesgos únicos de la organización.
- La organización también puede **considerar** las **influencias** y los **requisitos** de las partes interesadas externas, como las entidades del sector, los clientes y los socios empresariales.
- El Perfil Objetivo debe reflejar adecuadamente los criterios dentro del Nivel de Implementación objetivo.

Aplicación del paso 5: Crear un perfil objetivo

- Recordar que nuestro perfil actual es **(Nivel 0)**.
- Debe estar alineado con la evaluación de riesgo anteriormente realizada.
- Podemos utilizar las preguntas desarrolladas anteriormente para determinar nuestro nivel futuro con los controles implementados.
  - Por ejemplo, con los controles propuestos podríamos llegar a un nivel 1.
  - Sin embargo, la organización puede querer o necesitar tener un nivel más elevado.
- La siguiente tabla se utiliza para identificar las metas organizacionales a corto plazo (Se basa en la del BSD).
- Establecer objetivos realistas puede ayudar a identificar prioridades y garantizar que el programa de seguridad cibernética de la organización madure como se esperaba.

Aplicación del paso 5: Crear un perfil objetivo

De acuerdo a la siguiente tabla y a nuestra situación actual, la organización plantea subir la categoría ID.AM a nivel 3 en 3 años.

Se plantean las siguientes metas:

- Nivel 1 en el primer año
- Nivel 2 en el segundo año
- Nivel 3 en el tercer año.

#	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.

NIST CSF - Paso 6: Determinar, analizar y priorizar brechas

- La organización **compara** el Perfil Actual y el Perfil Objetivo para determinar las brechas.
- Crea un plan de acción **priorizado** para abordar las brechas para lograr los resultados en el Perfil Objetivo.
- Luego, la organización determina los **recursos** necesarios para abordar las brechas, que incluyen los fondos y la fuerza laboral.
- El uso de Perfiles de esta manera alienta a la organización a tomar decisiones informadas sobre las actividades de ciberseguridad, respalda la gestión de riesgos y permite a la organización realizar **mejoras específicas y rentables**.

Aplicación paso 6: Determinar, analizar y priorizar brechas

- Tenemos que ID.AM:
  - Perfil actual: Nivel 0 - No comenzado
  - Perfil objetivo: Nivel 3 - Logrado
- Se plantean metas intermedias para conseguir el objetivo deseado en 3 años.
- Algunas puntos que pueden ayudar en el análisis:
  - ¿Qué debo hacer para subir mi nivel 0 a 1 en ID.AM?
  - ¿Cuál es el listado de actividades, compras de hardware y software que se deben realizar?
  - ¿Cuáles debo realizar el primer, segundo o tercer año? ¿Cómo lo se?

Recordemos: Madurez de los procesos
Personas

Nivel	Puntuación	Descripción
Inadecuado	0	- 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	- 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	- 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	- 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	- 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 .

Aplicación paso 6: Determinar, analizar y priorizar brechas

- Por ejemplo, recordemos (Personas):

Identificador	Función	Pregunta	Situación actual: **Inadecuado**	Primer año - Perfil Objetivo ID.AM: **No logrado**	Segundo año - Perfil Objetivo ID.AM: **Parcialmente logrado**	Tercer año - Perfil Objetivo ID.AM: **Logrado**
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)?		Implementación de controles: • CIS 1.1 Establecer y mantener un detallado inventario de activos empresariales Otras actividades: • Capacitar a los encargados del inventario en el proceso de inventario de activos	Definición del proceso de inventario. Contratar personal para labores de tecnología. Compra de software de gestión de inventario. Implementar software de gestión de inventario. Capacitar a las personas en el nuevo software de inventario y proceso. Personal se le asigna funciones asociadas en la medida de lo posible.	El personal prioriza, rastrea y hace inventario de los activos de TI sin ser asignado formalmente. Contratar personal para labores de ciberseguridad. Capacitación continua del capital humano en los procesos y tecnología de la organización. Auditoría de los procesos relacionados.

NIST CSF - Paso 7: Implementar el plan de acción

- La organización determina qué acciones tomar para abordar las brechas,
- Si las hay, identificadas en el paso anterior y luego ajusta sus prácticas actuales de ciberseguridad para lograr el Perfil Objetivo.
- Para proveer más dirección, el Marco identifica ejemplos de referencias informativas sobre las Categorías y Subcategorías.
- Son las organizaciones quienes deben determinar qué normas, directrices y prácticas funcionan mejor para sus necesidades.

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