DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)

Caso de estudio: BSD - Universidad de Chicago

Profesor
Juan Ignacio Iturbe A

Contexto

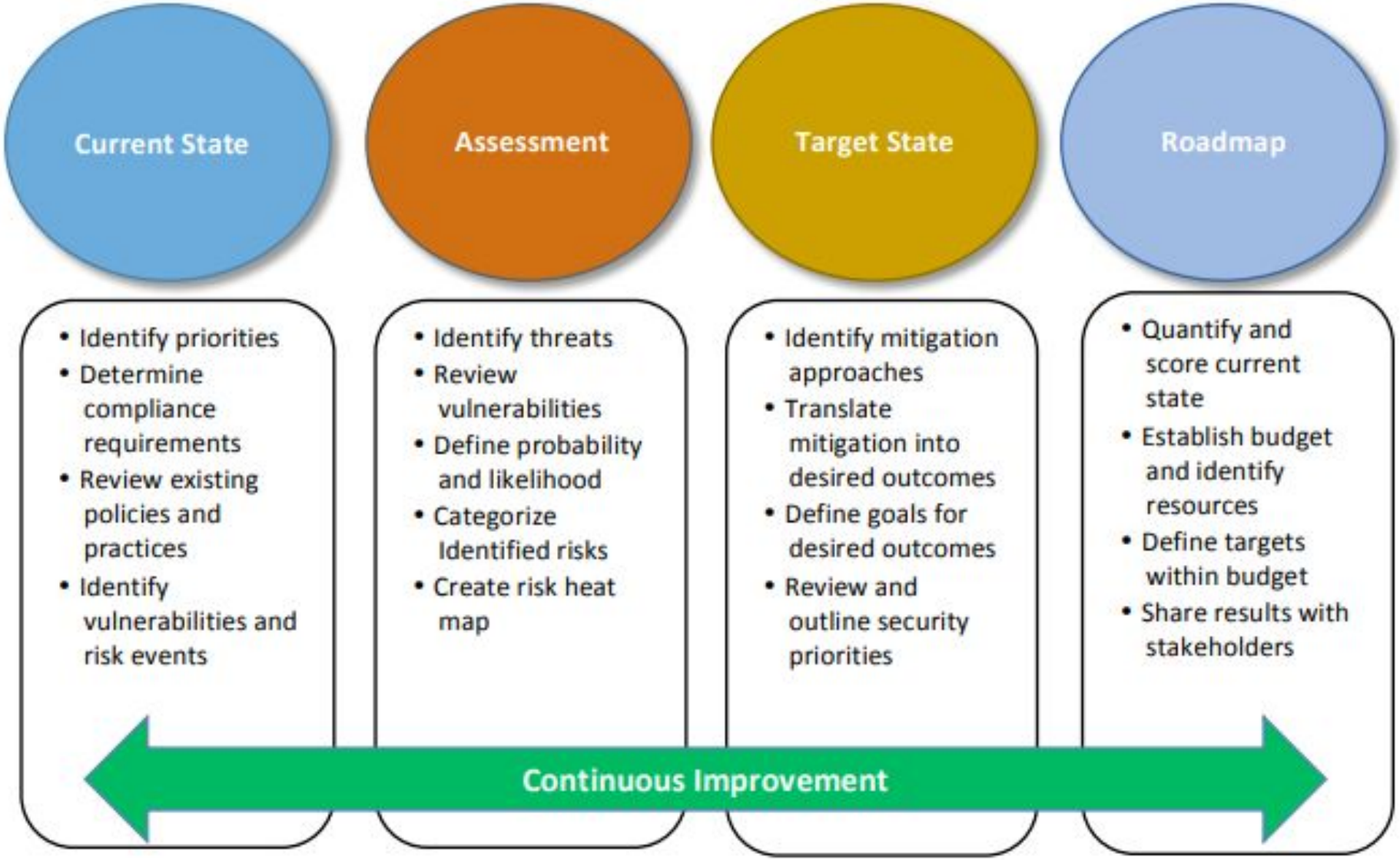
- La división de ciencias biológicas cuenta con 5000 personas contratadas entre académicos y administrativos en 23 Departamentos. Es la división más grande de la Universidad.
- Cuentan con un conjunto de tecnologías que habilitan a los académicos, administrativos y estudiantes avanzar en su investigación y educación.
- En 2014 se seleccionó el NIST CSF para la formulación de su programa de ciberseguridad.
- Estos esfuerzos fueron acompañados por la empresa G2 Inc.

THE UNIVERSITY OF CHICAGO BIOLOGICAL SCIENCES
AT THE FOREFRONT OF MEDICINE®

El desafío

- Modelo descentralizado utilizando administración local de TI específico para las necesidad de los Departamentos.
- Este modelo le provee agilidad a los departamentos. Sin embargo, 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.
  - Incremento en gastos de seguridad
  - Duplicación del esfuerzo.

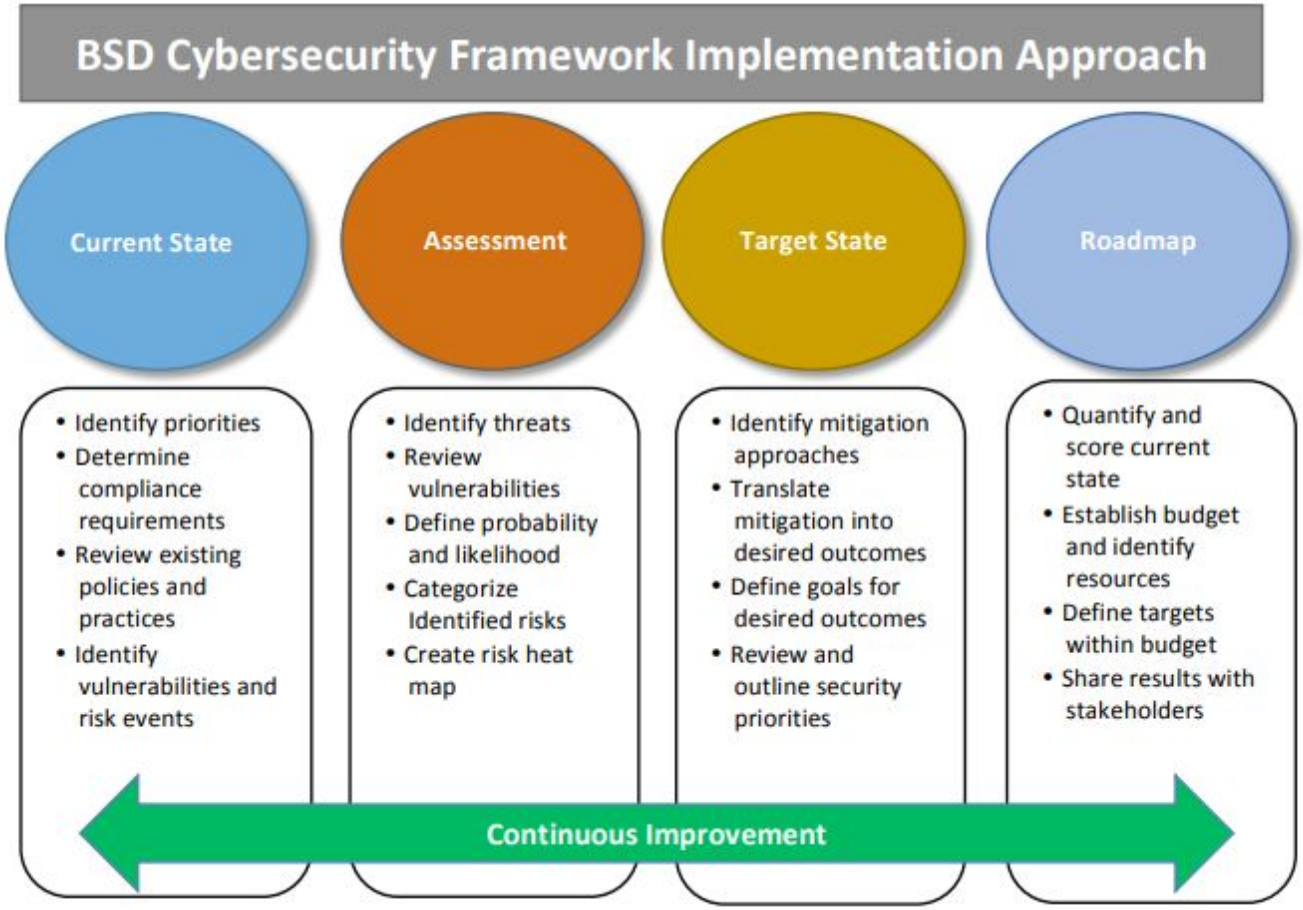
BSD Cybersecurity Framework Implementation Approach



Preguntas

1. ¿Cómo el equipo del BSD obtuvo información sobre la situación actual de la organización?
2. ¿Qué norma se utilizó para realizar la evaluación de riesgos? ¿Cómo se visualizó? ¿Qué tiene de importante esta visualización?
3. ¿Cómo se construyó el perfil objetivo? ¿En que se basó?
4. ¿Cómo se determinó el plan de actividades de ciberseguridad?
5. ¿Cómo se da seguimiento al plan de actividades y su mejora continua?
6. ¿Que beneficios se aprecian en la implementación del marco?

¿Cómo usar CSF NIST?



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.

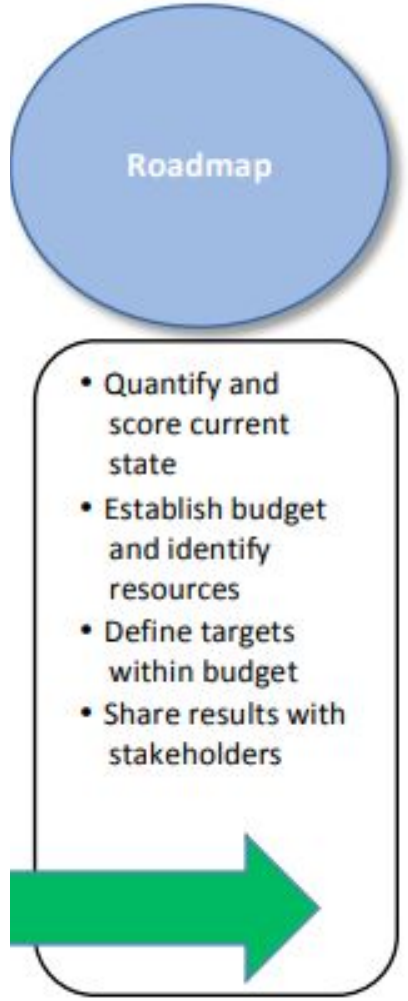
NIST CSF - Paso 2: Orientación

- 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.

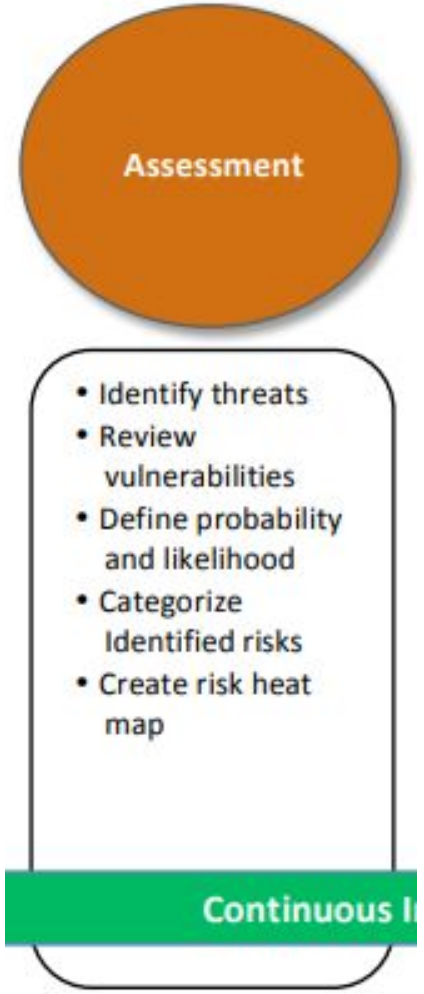
NIST CSF - Paso 3: Crear un perfil actual

- 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.



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.



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.

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**.

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.

Discusión

- ¿Cómo empezar a utilizar el NIST CSF en la Universidad?
- ¿Qué acercamiento usted utilizaría? ¿El del marco? ¿el del BSD? ¿otro?
- Acuerde con su grupo un plan de trabajo.

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?

Bibliografía

- https://www.nist.gov/cyberframework
- https://www.cisecurity.org/