Mejoras de ciberseguridad en infraestructuras

Para la gestión de las infraestructuras críticas, dada su complejidad, es importante contar con un marco que le permita realizar una mejora continua a su nivel de seguridad. El NIST (*National Institute of Standards and Technology*), en el año 2018, publicó el *Framework for Improving Critical Infrastructure Cybersecurity*, con el cual busca promover una adecuada gestión de los riesgos de la ciberseguridad en las organizaciones, adoptando las mejores prácticas de ISO, ITU, CIS, NIST, entre otros.

1. Estructura del marco NIST

El *framework* de NIST se encuentra compuesto por tres secciones, como se puede identificar en la figura No. 15,

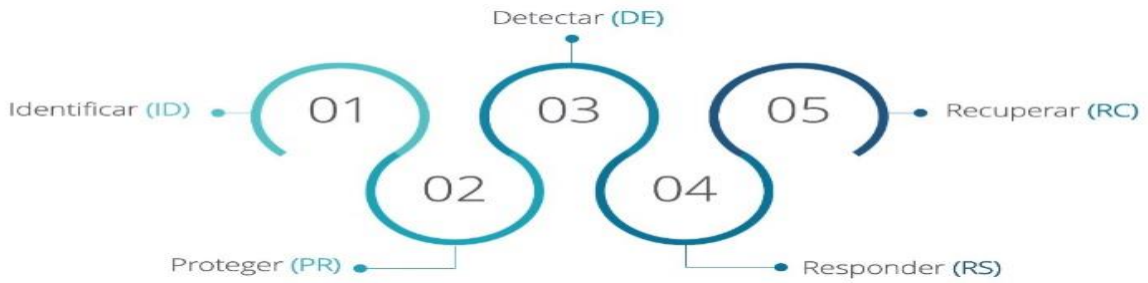
Figura 1. *Componentes del Framework de NIST*

Marco básico (Framework Core)	Niveles de implementación del marco (Framework Implementation Tiers)	Perfiles del marco (Framework Profiles)
Es un conjunto de actividades de ciberseguridad, resultados esperados y referencias aplicables que son comunes a los sectores de infraestructuras críticas, en términos de estándares de la industria, directrices y prácticas que permiten la comunicación de actividades de ciberseguridad y sus resultados a lo largo de la organización, desde el nivel ejecutivo hasta el de implementación/operación. El Framework Core consta de cinco funciones simultáneas y continuas: identificar, proteger, detectar, responder y recuperar.	Los niveles de implementación le permiten a la organización catalogarse en un umbral predefinido en función de las prácticas actuales de gestión de riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y misión del negocio y las restricciones de la propia empresa.	Los perfiles se emplean para describir el estado actual (Current Profile) y el estado objetivo (Target Profile) de determinadas actividades de ciberseguridad. El análisis diferencial entre perfiles permite la identificación de brechas que deberían ser gestionadas para cumplir con los objetivos de gestión de riesgos.

Así, el *Core* del *Framework* plantea acciones de ciberseguridad para las infraestructuras críticas.

Por otra parte, el núcleo del marco, propone cinco funciones básicas secuenciales, como se muestra a continuación.

Figura 2. *Funciones básicas del Framework de NIST*



De igual manera propone cuatro elementos que enmarcan las actividades y referentes para la aplicación del presente marco:

Figura 3. *Elementos que determinan las actividades a realizar*

Estas funciones y categorías se articulan para generar un modelo que permita gestionar la ciberseguridad en las organizaciones.

Figura 4. *Categoría de función y de identificadores únicos*

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Nota: recuperado de guía NIST

A medida que las organizaciones realizan su implementación, se puede determinar su nivel de acuerdo a la siguiente clasificación propuesta:

Figura 5. *Niveles de implementación*

NIVEL	TIPO	PROCESO DE GESTIÓN DE RIESGOS	PROGRAMA DE GESTIÓN INTEGRADA DE RIESGOS	PARTICIPACIÓN EXTERNA
1	PARCIAL	No se formalizan las prácticas organizativas de gestión de riesgos de ciberseguridad y se gestiona el riesgo de manera ad hoc ya veces reactiva.	Se conoce muy poco el riesgo de ciberseguridad a nivel organizativo y no se ha establecido un enfoque de gestión del riesgo de ciberseguridad en toda la organización.	Puede no tener los procesos establecidos para participar en la coordinación o colaboración con otras entidades.
2	RIESGO INFORMADO	Las prácticas de gestión de riesgos son aprobadas por la administración pero no pueden establecerse como políticas de toda la organización.	Se conoce el riesgo de ciberseguridad a nivel organizativo, pero no se ha establecido un enfoque a nivel de toda la organización	La organización conoce su papel en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente.
3	REPETIBLE	Las prácticas de gestión de riesgos de la organización son formalmente aprobadas y expresadas como políticas.	Existe un enfoque a nivel de toda la organización para gestionar el riesgo de la ciberseguridad.	La organización entiende sus dependencias y socios y recibe información que permite la colaboración y las decisiones de gestión basadas en el riesgo
5	ADAPTATIVO	La organización adapta sus prácticas de ciberseguridad basadas en las lecciones aprendidas y los indicadores predictivos	Existe un enfoque a nivel de toda la organización para gestionar el riesgo de ciberseguridad que utiliza políticas, procesos y procedimientos	la organización gestiona el riesgo y comparte activamente la información con los socios para garantizar que se distribuye información precisa para mejorar la ciberseguridad antes de que se produzca un evento

Nota: tomado de [| Tecnología | Actualidad | ESAN]

2. Implementación

El marco se puede implementar en cualquier organización, sin importar que no se esté en Los Estados Unidos. A continuación, revise los pasos básicos para su adopción.

Figura 6. *Pasos para la implementación de CSF en una organización*

Nota: Adaptado de: Guía NIST

- **Priorizar el alcance**: La organización debe identificar sus objetivos de negocios / misión y las prioridades organizacionales de alto nivel para tomar las decisiones estratégicas relacionadas con la implementación.
- **Orientar**. Identificar los sistemas y activos de información, así como los requerimientos normativos para la gestión del riesgo, identificando amenazas y vulnerabilidades a dichos activos.
- **Crea un perfil actual**. Se genera un perfil que represente el estado actual de la ciberseguridad en la organización.
- **Realizar una evaluación de riesgos**. Realiza el análisis de riesgos con el fin de determinar las acciones necesarias para gestionar la ciberseguridad.
- **Crea un perfil de destino**: Genera un nuevo perfil, estableciendo los resultados esperados de la gestión de la ciberseguridad.
- **Determinar, analizar y priorizar brechas**. Establece las acciones necesarias para reducir las brechas identificadas para la gestión de la ciberseguridad.
- **Implementar un plan de acción**. Aplica las acciones identificadas con el objetivo de reducir las brechas en ciberseguridad.