## **INSTITUTO POLITÉCNICO NACIONAL**

###### **ESCUELA SUPERIOR DE CÓMPUTO**

**IT Governance**

Profesora Jessie Paulina Guzmán Flores

Tarea 8: Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST)

**Grupo:** 3CM20 - Equipo 4

**Fecha de Entrega:** 8/Mayo/2022

**Integrantes:**

* Martínez Coronel Brayan Yosafat
* Ramírez Cotonieto Luis Fernando
* Sánchez Rojas Jesús Ubaldo

# Índice

[**Introducción**](#_t70btsdue1fh) **3**

[**Objetivos**](#_o00bt4wm3omi) **4**

[**¿Cuáles son los Objetivos del Marco de Trabajo de Ciberseguridad NIST?**](#_ykchfqqgta6b) **5**

[**¿En qué Estándares, Directrices y Mejores Prácticas está Basado?**](#_kvtroyh66oe6) **5**

[**¿Cómo es el Diseño de los 20 Controles de Ciberseguridad NIST?**](#_flvxmbaxnmy9) **6**

[**¿Cuáles son las cinco funciones fundamentales?**](#_jg1qze2mezl) **6**

[**¿Cuáles son las Acciones de Ciberdefensa para Mitigar Ataques?**](#_637f9ur5wyss) **7**

[**REFERENCIAS**](#_z0jfgnvimn9n) **12**

# Introducción

Por más de dos décadas, la internet y las tecnologías de la información conexas han impulsado innovaciones, crecimiento económico y mejoras sin precedentes en los servicios sociales. Muchos de estos beneficios potencian datos sobre personas que circulan por un ecosistema complejo. Por consiguiente, es posible que las personas no entiendan las consecuencias que podría acarrear para su privacidad la interacción con sistemas, productos y servicios. Al mismo tiempo, las organizaciones podrían no darse cuenta del alcance total de estas consecuencias para las personas, la sociedad o sus empresas; consecuencias que podrían afectar sus marcas, sus resultados finales y sus perspectivas de crecimiento futuras

Dado un aumento sostenido de la cantidad de incidentes de ciberseguridad en los EEUU, el presidente Barack Obama, el 12 de febrero de 2013, emite la orden ejecutiva 13636 en donde se encarga al Instituto de Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) el desarrollo del Marco de ciberseguridad para la protección de infraestructuras críticas, lo que hoy se conoce como el Cybersecurity Framework (CSF). EEUU identifica 16 sectores de infraestructuras críticas, estos son: químico; instalaciones comerciales; comunicaciones; fabricación crítica; presas/represas; base industrial de defensa; servicios de emergencia; energía; servicios financieros; comida y agricultura; instalaciones gubernamentales; salud y salud pública; tecnología de información; reactores nucleares, materiales y residuos; sistemas de transporte; sistemas de agua y aguas residuales.

# Objetivos

Con esta investigación se pretende:

* Comprender los objetivos del Marco de Trabajo de Ciberseguridad NIST
* Conocer los estándares, directrices y mejores prácticas en los que se baja el Marco de Trabajo de Ciberseguridad NIST
* Identificar las cinco funciones fundamentales del Marco
* Determinar las acciones de ciberdefensa para la mitigación de ataques
* Indagar sobre el diseño de los veinte controles del Marco

# ¿Cuáles son los Objetivos del Marco de Trabajo de Ciberseguridad NIST?

Las bases del Cyber Security Framework NIST fueron establecidas directamente en la Orden Ejecutiva 13636:

* Identificar estándares de seguridad y guías aplicables de forma transversal a todos los sectores de infraestructuras críticas.
* Establecer un lenguaje común para gestionar riesgos de ciberseguridad.
* Proveer un enfoque priorizado, flexible, repetible, neutral, basado en desempeño y efectivo en términos de coste-beneficio basado en las necesidades del negocio.
* Ayudar a los responsables y operadores de infraestructuras críticas a identificar, inventariar y gestionar riesgos informáticos.
* Establecer criterios para la definición de métricas para el control del desempeño en la implementación.
* Establecer controles para proteger la propiedad intelectual, la privacidad de los individuos y las libertades civiles cuando se ejecuten actividades de ciberseguridad.
* Identificar áreas de mejora que permitan ser gestionadas a través de colaboraciones futuras con sectores particulares y organizaciones orientadas al desarrollo de estándares.
* No introducir nuevos estándares cuando existan iniciativas ya desarrolladas que cubran los objetivos de la orden ejecutiva.

# ¿En qué Estándares, Directrices y Mejores Prácticas está Basado?

Framework Cyber Security NIST (Marco de Trabajo de Ciberseguridad NIST) está basado y/o hace referencia a los siguientes estándares, directrices y mejores prácticas:

* Control Objectives for Information and Related Technology (COBIT).
* Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC).
* ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.
* ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels.
* ISO/IEC 27001:2013, Information technology Security Techniques Information Security Management Systems Requirements.
* NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

# ¿Cómo es el Diseño de los 20 Controles de Ciberseguridad NIST?

El Framework de NIST, 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 nivel de implementación/operación.

# ¿Cuáles son las cinco funciones fundamentales?

En la versión del 2018, la cual es la versión 1.1, se pueden encontrar las siguientes cinco funciones:

**1. Identificar:** Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos, de acuerdo con su estrategia de administración de riesgos y sus necesidades comerciales.

**2. Proteger:** Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas.

**3. Detectar:** Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad.

**4. Responder**: Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado.

**5. Recuperar:** Identifica las actividades necesarias para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad.

# ¿Cuáles son las Acciones de Ciberdefensa para Mitigar Ataques?

| Número | Control | Objetivo |
| --- | --- | --- |
| CCS1 | Inventario de Dispositivos Autorizados y no Autorizados | Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red. |
| CCS2 | Inventario de Software Autorizado y no Autorizado | Gestionar activamente todo el software en los sistemas, de forma que solo se pueda instalar y ejecutar software autorizado. |
| CCS3 | Configuraciones Seguras de Software y Hardware para Dispositivos Móviles, Portátiles, Equipos de Escritorio y Servidores | Establecer una configuración base segura para dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables. |
| CCS4 | Proceso Continuo de Identificación Y Remediación de Vulnerabilidades | Disponer un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes. |
| CCS5 | Control sobre Privilegios Administrativos | Desarrollar procesos y utilizar herramientas para identificar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones. |
| CCS6 | Mantenimiento, Monitorización y Análisis de LOGs de Auditoría | Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque. |
| CCS7 | Protección del Correo Electrónico y del Navegador | Minimizar la posibilidad de que los atacantes manipulen a los empleados a través de su interacción con el correo electrónico y el navegador. |
| CCS8 | Defensas Contra el Malware Avanzado de Correo Electrónico y del Navegador | Evitar la instalación, difusión y ejecución de código malicioso en distintos puntos, al tiempo que se fomenta la automatización para permitir una actualización rápida en la defensa, recopilación de datos y la corrección. |
| CCS9 | Limitar y Controlar los Puertos de Red, Protocolos y Servicios | Gestionar el uso de puertos, protocolos y servicios en los dispositivos que tengan red para reducir las vulnerabilidades disponibles a los atacantes. |
| CCS10 | Capacidad de Recuperación de Datos | Disponer procesos, metodologías y herramientas adecuadas para respaldar la información crítica y realizar pruebas de recuperación. |
| CCS11 | Configuraciones Seguras de Dispositivos de Red (Firewalls, Routers y Switches) | Establecer una configuración base para los dispositivos de infraestructura de red, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables. |
| CCS12 | Defensa Perimetral | Desarrollar una estrategia para detectar, prevenir y corregir los flujos de transmisión de información entre redes de distintos niveles de seguridad (confianza). |
| CCS13 | Protección de los Datos | Disponer de procesos y herramientas adecuadas para prevenir la fuga de información, mitigar los efectos cuando se ha producido un incidente de fuga de información, y asegurar la confidencialidad e integridad de la información sensible. |
| CCS14 | Acceso Basado en la Necesidad de Conocer (Need to Know) | El acceso a los activos críticos debe realizarse de acuerdo a una definición formal de que personas, sistemas y aplicaciones tienen la necesidad y el derecho de acceso. Los procesos y herramientas utilizadas en el seguimiento, protección y corrección de estos accesos deben estar alineados con las definiciones. |
| CCS15 | Control de Acceso Wireless | Disponer de procesos y herramientas para garantizar una seguridad adecuada en las redes Wifi y en los sistemas clientes, incluyendo seguimiento y corrección de las medidas de seguridad. |
| CCS16 | Control y Monitorización de Cuentas de Sistema | Gestionar activamente el ciclo de vida de las cuentas de sistema y de aplicación (creación, uso, inactividad y borrado) para reducir su utilización por parte de un atacante. |
| CCS17 | Verificación de las Habilidades de Seguridad y Formación Adecuada | Identificar los conocimientos específicos, habilidades y capacidades necesarias en la organización para la defensa de los activos críticos de la compañía, y desarrollar y evaluar un plan para identificar gaps y remediar con políticas, formación y programas de sensibilización. |
| CCS18 | Seguridad en el Ciclo de Vida de las Aplicaciones | Gestionar el ciclo de vida de todas las aplicaciones, tanto las desarrolladas internamente como las de proveedores para prevenir, detectar y corregir vulnerabilidades técnicas. |
| CCS19 | Gestión y Respuesta a Incidentes | Proteger la información y la reputación de la organización desarrollando e implementando una infraestructura de respuesta a incidentes para detectar un ataque, contener el daño de forma efectiva, expulsar al atacante, y restaurar la integridad de los sistemas y la red. |
| CCS20 | Realizar Test de Penetración y Ejercicios de Ataque | Probar las defensas de la organización (tecnología, procesos y personas) mediante la simulación de un ataque, utilizando sus mismas acciones y objetivos. |

# Organizador Gráfico

# 

# Referencias

20 controles de ciberseguridad NIST: <https://netsecurechile.wordpress.com/2018/06/08/20-controles-ciberseguridad-nist/>

Ciberseguridad Marco NIST, Un abordaje integral de la Ciberseguridad: <https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf>

MARCO DE PRIVACIDAD DEL NIST: UNA HERRAMIENTA PARA MEJORAR LA PRIVACIDAD POR MEDIO DE LA GESTIÓN DE RIESGOS EMPRESARIALES, VERSIÓN 1.0 : <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932988>