Un marco para mejorar la ciberseguridad de la infraestructura crítica

Julio 2023

Máster Michael Lee Vargas
CYBERSECURITY ASSISTANT – U.S. EMBASSY
ITILv4 CERTIFIED - NIST-CSF LEAD IMPLEMENTER
LeeML2@state.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Objetivos:

Ofrecer un breve panorama de los riesgos de ciberseguridad más importantes en LATAM y C.R.

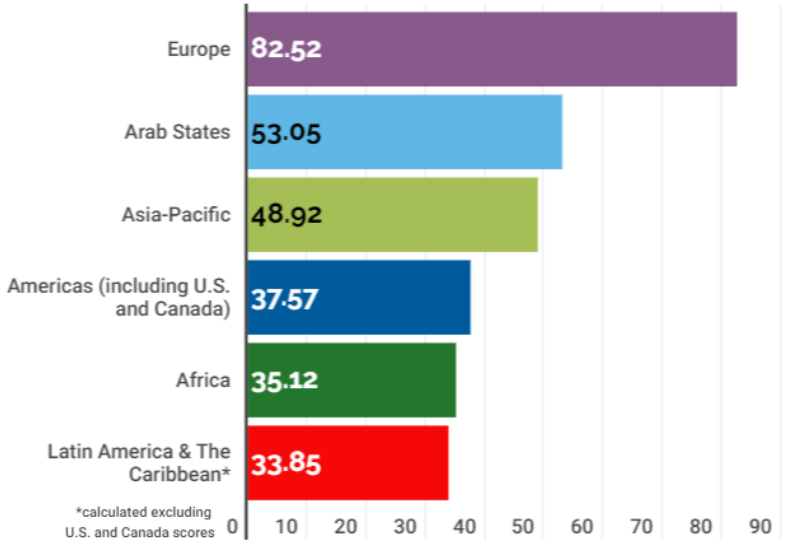
Dialogar sobre la importancia de las normas y buenas prácticas en ciberseguridad.

Ofrecer recursos para la implementación del NIST CSF 1.1.

Contexto (1)
Latin America, the low hanging fruit.

Latin America scores the lowest among world regions in commitment to cybersecurity measures.

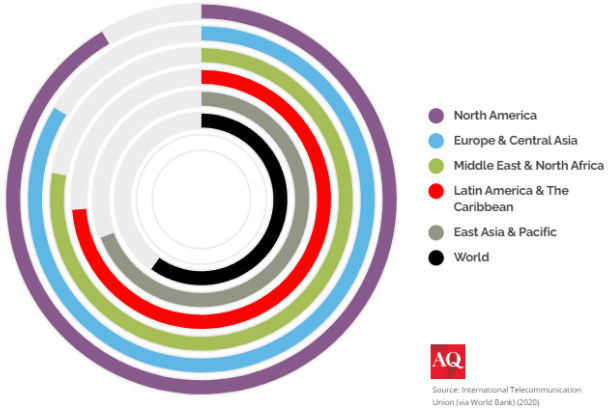
Regional averages based on 2020 ITU Global Cybersecurity Index



Note: Index measures the types of cybersecurity commitments countries have made and how widely they've been implemented. Source: International Telecommunication Union Global Cybersecurity Index (2020)

The region is very online...

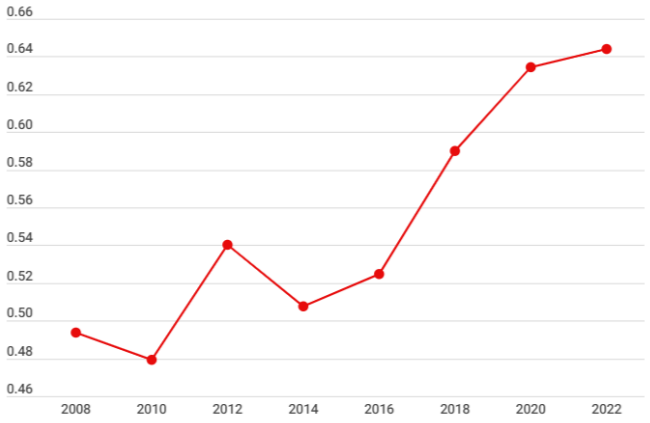
Share of population using internet



Source: International Telecommunication Union (via World Bank) (2020)

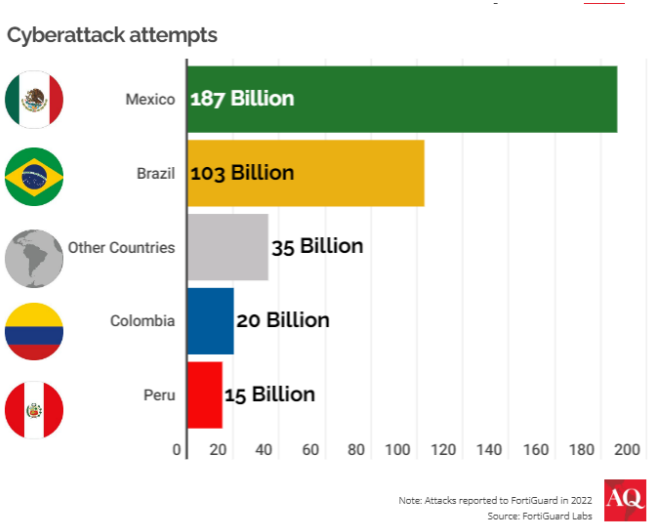
...and governments and services are increasingly digitized.

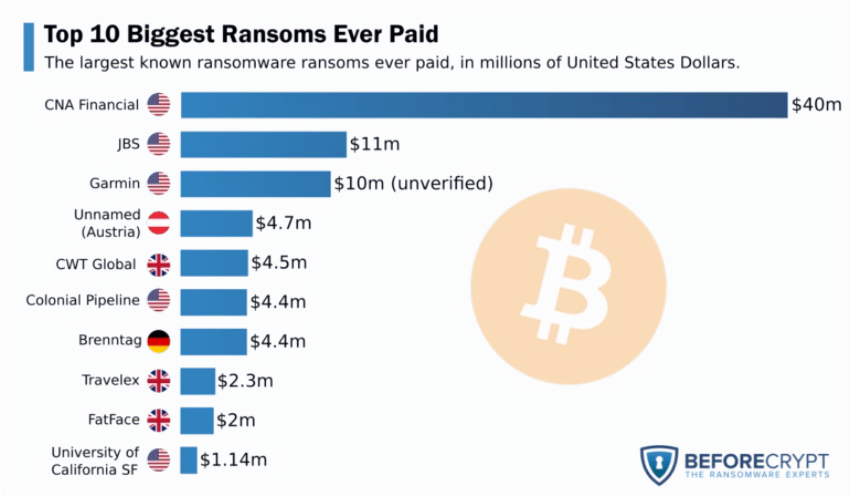
The Americas' average e-government scores

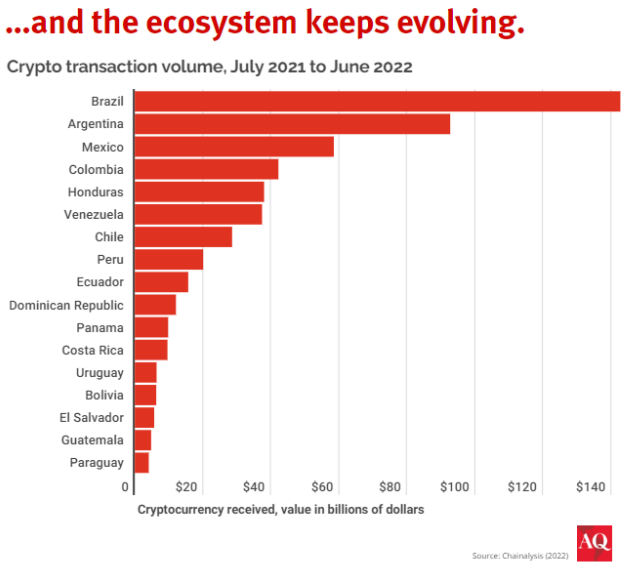


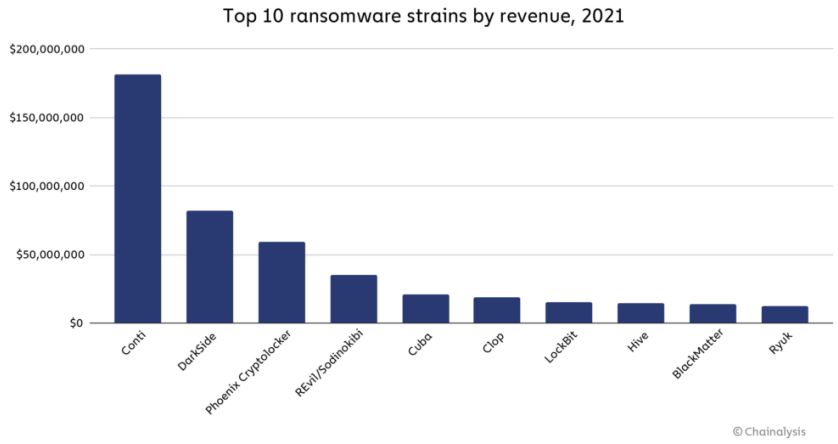
Note: Survey measures e-government effectiveness in the delivery of public services. Source: United Nations E-Government Survey (2022)

Contexto (2)


Cyberattack attempts
Mexico
187 Billion
Brazil
103 Billion
Other Countries
35 Billion
Colombia
20 Billion
Peru
15 Billion
0
20
40
60
80
100
120
140
160
180
200
Note: Attacks reported to FortiGuard in 2022
Source: FortiGuard Labs
AQ

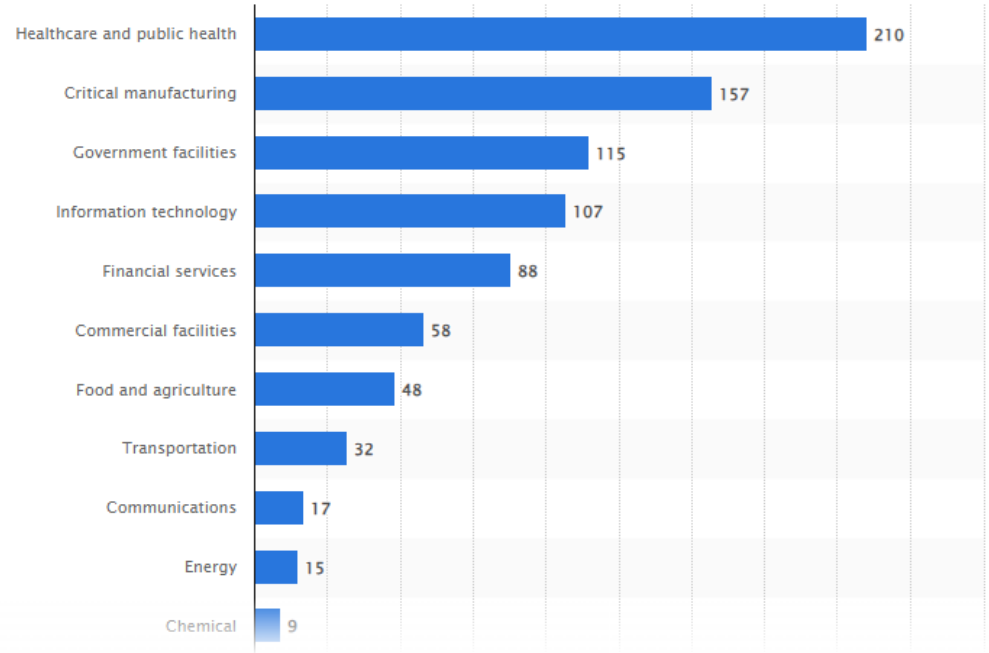

Top 10 Biggest Ransoms Ever Paid
The largest known ransomware ransoms ever paid, in millions of United States Dollars.
CNA Financial
$40m
JBS
$11m
Garmin
$10m (unverified)
Unnamed (Austria)
$4.7m
CWT Global
$4.5m
Colonial Pipeline
$4.4m
Brenntag
$4.4m
Travelex
$2.3m
FatFace
$2m
University of California SF
$1.14m
BEFORECRYPT
THE RANSOMWARE EXPERTS


...and the ecosystem keeps evolving.
Crypto transaction volume, July 2021 to June 2022
Brazil
Argentina
Mexico
Colombia
Honduras
Venezuela
Chile
Peru
Ecuador
Dominican Republic
Panama
Costa Rica
Uruguay
Bolivia
El Salvador
Guatemala
Paraguay
0
$20
$40
$60
$80
$100
$120
$140
Cryptocurrency received, value in billions of dollars
Source: Chainalysis (2022)
AQ


Top 10 ransomware strains by revenue, 2021
$200,000,000
$150,000,000
$100,000,000
$50,000,000
$0
Conti
DarkSide
Phoenix Cryptolocker
REvil/Sodinokibi
Cuba
Clop
LockBit
Hive
BlackMatter
Ryuk
© Chainalysis

Contexto (3) Sectores más atacados.

Sectors most targeted by ransomware attacks worldwide in 2022, by number of complaints



⊕ Expand statistic

DOWNLOAD

PDF XLS PNG PPT

Sources
- Show sources information
- Show publisher information
- Use Ask Statista Research Service

Release date
March 2023

Region
Worldwide

Survey time period
2022

Special properties
number of comlaints received by Internet Crime Complaint Center (IC3)

Citation formats
- View options

Contexto (4) Ciberataques en Costa Rica.

National Institute of Standards and Technology

Sobre el NIST

- Agencia del Departamento de Comercio de Estados Unidos.
- Su misión es desarrollar y promover la medición, los estándares y la tecnología para aumentar la productividad, facilitar el comercio y mejorar la calidad de vida.
- Fundada por el Congreso de EE.UU. en 1901.

¿Por qué el NIST?

- Historial de cooperación con el sector privado.
- Experiencia en el manejo de asuntos críticos con lineamientos basados en el consenso y no en la imposición.
- Desde el 2013 al 2018, el CSF fue desarrollado con la participación del gobierno, la industria y la ciudadanía.

Contexto del NIST-CSF

Para la ciberseguridad de infraestructura crítica

12 de febrero de 2013

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

Executive Order 13636

18 de diciembre de 2014

"…on an ongoing basis, facilitate and support the development of a ***voluntary***, ***consensus-based***, ***industry-led*** *set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure"*

Cybersecurity Enhancement Act

Contexto del NIST-CSF

Para la ciberseguridad de infraestructura crítica

La orden ejecutiva 14028 del 12 de Mayo de 2021 buscaba:

- Asegurarse que los proveedores de TI compartieran información sobre violaciones a la ciberseguridad.
- *Modernizar e implementar estándares como Zero Trust Architecture, MFA, encryption, supply chain security, etc.*
- *Creó un Cyber Safety Review Board, con representantes del sector público y privado con la autoridad de analizar y hacer recomendaciones después de un incidente mayor de ciberseguridad. Esto está inspirado en el National Transportation Safety Board conocido por sus investigaciones de tragedias aéreas.*
- *La EO impulsó la habilidad de detectar ciberactividad maliciosa en las redes federales gracias a una amplia implementación de un Sistema de detección y respuesta (EDR)*

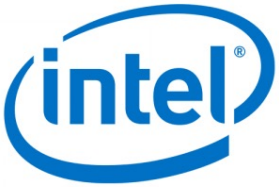
MAY 12, 2021

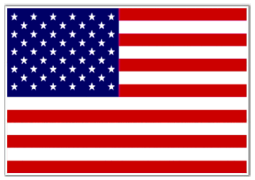
Executive Order on Improving the Nation's Cybersecurity

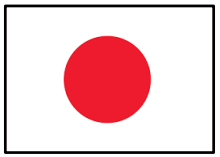
BRIEFING ROOM ▸ PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Usuarios del CSF

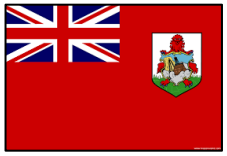






AT&T

NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION



Versiones 1.0 y 1.1 son compatibles

Para la ciberseguridad de infraestructura crítica

- Adiciones, incluyendo nuevas categorías y subcategorías, no invalidan los resultados ni usos de la V1.0

Component	Version 1.0	Version 1.1	Comments
Functions	5	5	
Categories	22	23	• Agregó una nueva categoría en ID.SC – Supply Chain
Subcategories	98	108	• Agregó 5 subcategorías en ID.SC • Agregó 2 subcategorías en PR.AC • Agregó 1 subcategoría en PR.DS, PR.PT, RS.AN • Clarificó algunos textos
Informative References	5	5	

Aspectos claves del NIST CSF

- Está escrito en un lenguaje sencillo y accesible.
- Es voluntario y gratuito.
- Es autocertificado, sin certificación externa. ISO 27001 ofrece una certificación reconocida a nivel mundial después de una auditoría de terceros llamados organismos de certificación.
- Es adaptable a muchos países, tecnologías, sectores y usos.
- No propone parámetros de riesgo (p.ej. complejidad de claves).
- Ofrece un catálogo de resultados de ciberseguridad.
- Trabaja en conjunto con estándares como ISO, COBIT, etc.
- No reemplaza procesos actuales.
- Permite que las buenas prácticas se conviertan en estándares.
- Se puede actualizar a medida que cambia la tecnología y las amenazas.
- Evoluciona más rápido que la regulación y la legislación.
- Mejora junto a los implementadores.

Componentes del CSF

¿Qué hacemos?
Prácticas, resultados de ciberseguridad y controles (referencias informativas que permiten la comunicación de riesgos cibernéticos en la organización.

¿Cuán bien lo hacemos?
Describe el grado de madurez en que una organización gestiona las prácticas y controles de ciberseguridad.

¿Dónde estamos y hacia dónde vamos?
Alinea estándares de la industria y buenas prácticas con el Framework Core en un escenario de implementación. Prioriza y mide tomando en cuenta las necesidades de la organización.

¿Certificación externa?

- NIST no tiene planes para desarrollar un sistema de certificación externo, sin embargo, la International Standards Organization (ISO) junto con la International Electrotechnical Commission (IEC) publicaron ISO/IEC TS 27110: Information Technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines, que provee un camino para integrar el CSF con un sistema completo de gestión de la seguridad de la información ISO 27001 (Information security management systems).

Core

Un catálogo de resultados en ciberseguridad

	Function
¿Qué procesos y recursos necesitan protección?	**Identify**
¿Qué protecciones están disponibles?	**Protect**
¿Cómo detectamos los incidentes?	**Detect**
¿Cómo contenemos el impacto de los incidentes?	**Respond**
¿Cómo nos restauramos después de un incidente?	**Recover**

- Fácil de entender
- Aplica a escenarios diferentes
- Ofrece una perspectiva amplia
- Implica la prevención y la reacción

Dentro de las funciones hay categorías

¿Qué procesos y recursos necesitan protección?

¿Qué protecciones están disponibles?

¿Cómo detectamos los incidentes?

¿Cómo contenemos el impacto de los incidentes?

¿Cómo nos restauramos después de un incidente?

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management, Authentication and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Niveles de implementación (Tiers)

NIST IMPLEMENTATION TIERS

TIER 1

PARTIAL IMPLEMENTATION

Your organization has an ad-hoc and reactive cybersecurity posture. You may have little awareness of organizational risk and any plans implemented are often done inconsistently.

TIER 2

RISK INFORMED

Your organization may be approving cybersecurity measures, but implementation is still piecemeal. You are aware of risks, have plans, and have the proper resources to protect yourselves but haven't quite gotten to a proactive point.

TIER 3

REPEATABLE

Your organization has implemented NIST standards company-wide and are able to repeatedly respond to crises. Policy is consistently applied, and employees are informed of risks.

TIER 4

ADAPTIVE

Your organization has total adoption of the NIST standard. You aren't just prepared to respond to threats, you proactively detect threats and predict issues based on current trends and your IT architecture.

Core – Example

Componentes del CSF

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

Core – Example

Componentes del CSF

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

Core – Example

Cybersecurity Framework Component

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15

1.1

Profiles

Adaptación del CSF

- Ayudan a conectar las funciones, categorías y subcategorías con los requerimientos de negocio, tolerancia a riesgos y recursos.

- Ayuda a identificar oportunidades de mejora.
- Ayuda a tener un punto de partida (Current Profile versus Target Profile).
- Ejemplos: https://www.nist.gov/cyberframework/examples-framework-profiles

Framework Seven Step Process

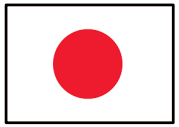
Gap Analysis Using Framework Profiles

- **Step 1:** Prioritize and Scope
  - Implementation Tiers may be used to express varying risk tolerances[1.1]
- **Step 2:** Orient
- **Step 3:** Create a Current Profile
- **Step 4:** Conduct a Risk Assessment
- **Step 5:** Create a Target Profile
  - When used in conjunction with an Implementation Tier, characteristics of the Tier level should be reflected in the desired cybersecurity outcomes[1.1]
- **Step 6:** Determine, Analyze, and Prioritize Gaps
- **Step 7:** Implementation Action Plan

Uso Internacional

Framework for Improving Critical Infrastructure Cybersecurity

- Japanese translation by Information-technology Promotion Agency
- Italian adaptation within Italy's National Framework for Cybersecurity
- Hebrew adaptation by Government of Israel
- Bermuda uses it within government and recommends it to industry
- Uruguay government is currently on Version 3.1 of their adaptation
- Focus of International Organization for Standardization & International Electrotechnical Commission



The Framework Web Site

www.nist.gov/cyberframework

NIST Search NIST NIST MENU

CYBERSECURITY FRAMEWORK

Helping organizations to better understand and improve their management of cybersecurity risk

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources +
- Newsroom +

Credit: N. Hanacek/NIST

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

LATEST UPDATES

- Registration is now available for an upcoming Webcast providing an overview of Framework Version 1.1, hosted by NIST on April 27th.

Self-Help Web Materials

www.nist.gov/cyberframework

Self-Help Web Materials

www.nist.gov/cyberframework

Resources

https://www.nist.gov/cyberframework/framework-resources-0

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources +
- Newsroom +

Framework Resources

General Resources sorted by User Group:

- Critical Infrastructure
- Small and Medium Business
- International
- Federal
- State Local Tribal Territorial Governments
- Academia
- Assessments & Auditing
- General

Over 150 Unique Resources for Your Understanding and Use!

Recursos

https://www.nist.gov/cyberframework/

Texas, Department of Information Resources

- Aligned Agency Security Plans with Framework
- Aligned Product and Service Vendor Requirements with Framework

North Dakota, Information Technology Department

- Allocated Roles & Responsibilities using Framework
- Adopted the Framework into their Security Operation Strategy

Houston, Greater Houston Partnership

- Integrated Framework into their Cybersecurity Guide
- Offer On-Line Framework Self-Assessment

National Association of State CIOs

- 2 out of 3 CIOs from the 2015 NASCIO Awards cited Framework as a part of their award-winning strategy

Uruguay

- Marco de Ciberseguridad de la Agencia de Gobierno Electrónico y Sociedad de la Información y Conocimiento

Resources

https://www.nist.gov/cyberframework/framework-resources-0

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources +
- Newsroom +

Framework Resources

NIST Special Publications

Computer Security Resource Center
800 Series @ csrc.nist.gov

National Cybersecurity Center of Excellence
1800 Series @ nccoe.nist.gov

Over 150 Unique Resources for Your Understanding and Use!

Formas para ayudar

Acciones recomendadas

- Cree y comparta sus avances con otros en la sección Resources en coordinación con NIST
  - Adapte el framework a su sector, país o comunidad.
  - Publique su perfil en la página del NIST.
- Comparta su historias de éxito de la implementación del CSF.
- Abogue por la implementación de marcos, estándares y buenas prácticas de ciberseguridad.
- Envíe ideas al NIST.
- Celebre el mes de la ciberseguridad en Octubre de cada año.

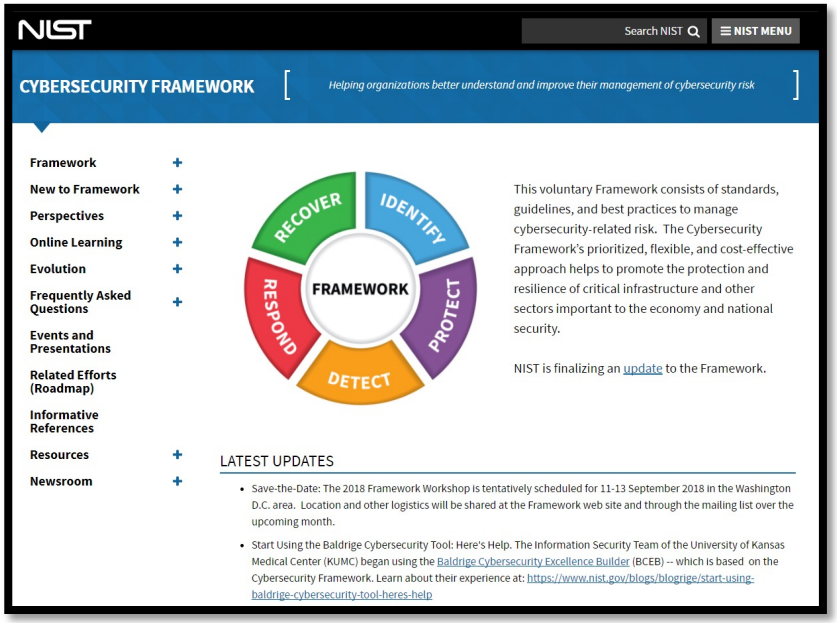
cyberframework@nist.gov

Recursos

- Framework for Improving Critical Infrastructure Cybersecurity and related news and information:
  - www.nist.gov/cyberframework

- Additional cybersecurity resources:
  - http://csrc.nist.gov/

- Questions, comments, ideas:
  - Leeml2@state.gov
  - cyberframework@nist.gov



"Si dispusiera de ocho horas para cortar un árbol, emplearía seis en afilar el hacha”
- Abraham Lincoln

“Lo que no se puede medir no se puede controlar;
lo que no se puede controlar no se puede gestionar;
lo que no se puede gestionar no se puede mejorar.”
-Peter Drucker

Preguntas o comentarios: