
SEGURIDAD
CERO
CURSO GRATIS
CIBERSEGURIDAD
Y NIST CSF


SEGURIDAD
CERO
Curso Oficial
LEAD CYBERSECURITY
PROFESSIONAL CERTIFICATE
50% OFF
Registro Aquí

https://www.seguridadcero.com.pe/

https://www.linkedin.com/company/seguridadcero/

http://www.youtube.com/c/SEGURIDADCERO

https://www.facebook.com/segu.cero

https://t.me/seguridadcero

Fernando Conislla

Experto en ciberseguridad

- +5 años de experiencia en servicios de ciberseguridad para entidades gubernamentales, bancarias, medios de pago, etc.
- Instructor en SEGURIDAD CERO e instructor Oficial Certiprof
- Expositor en eventos internacionales
- Master en gestión y dirección de la ciberseguridad
- Certificaciones internacionales CEH, CPTE, CSWAE, LCSPC

Jaime Moya

Experto en ciberseguridad

Especialista en Seguridad de la Información, certificado internacionalmente CISM, LCSPC, etc, con más de 10 años de experiencia generando valor en ciberseguridad y seguridad de la información para clientes de los sectores energético, consumo masivo, cooperativas, telecomunicaciones, educativo, petróleo & gas, auditorías, entre otros. Instructor Oficial Certiprof.

SEGURIDAD CERO

CertiProf® | Partner

SEGURIDAD CERO

CLASE 2
Conociendo NIST CSF

MARTES 25 AGOSTO

CRI	GTM	HND	MEX	PER
5:00 PM	5:00 PM	5:00 PM	6:00 PM	6:00 PM

COL	ECU	PAN	PRY	CHL
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM

BOL	VEN	DOM	ARG	URY
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM

SEGURIDAD CERO

Introducción al marco

SEGURIDAD CERO

Introducción al marco

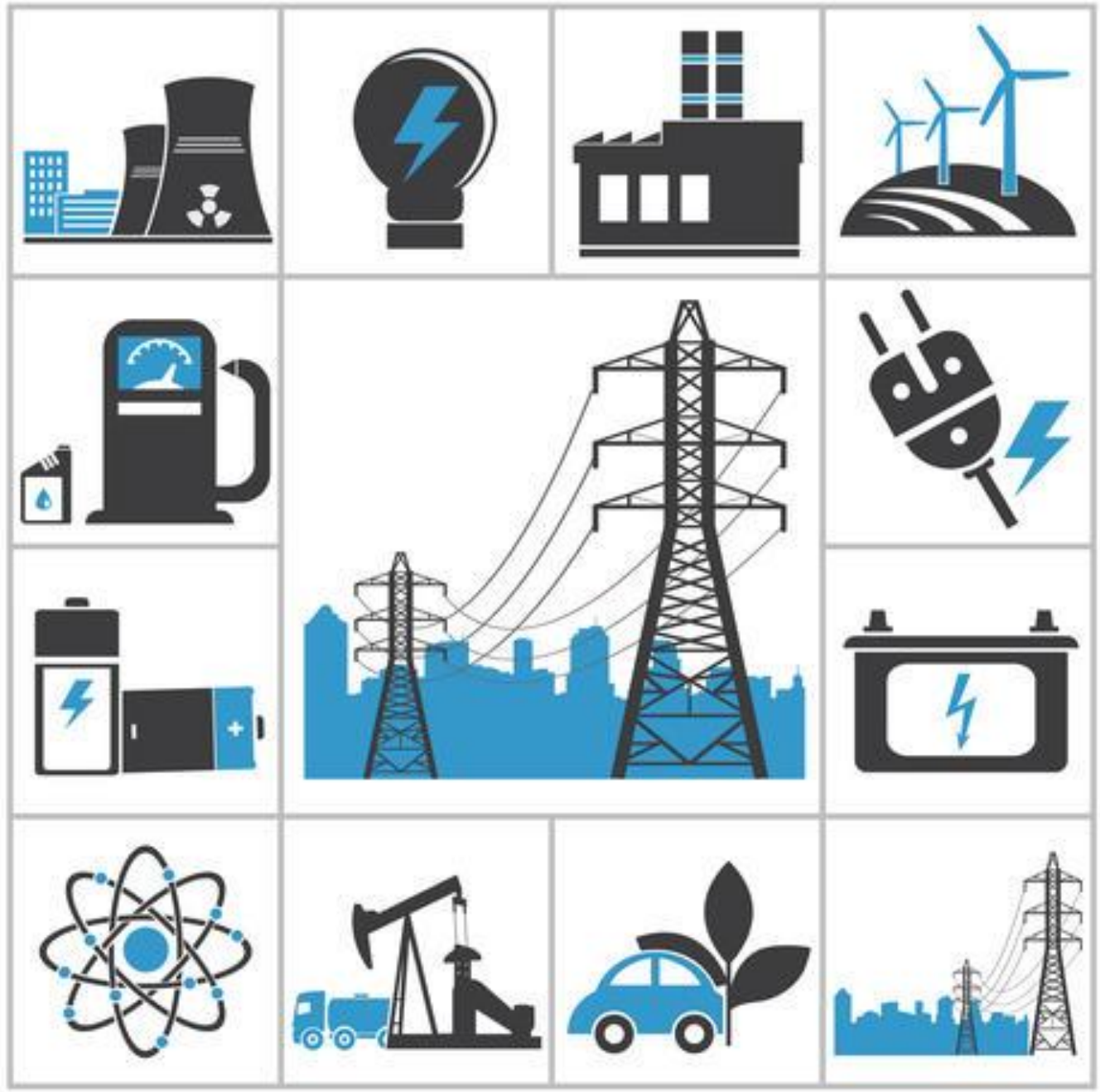
Los EEUU dependen del funcionamiento confiable de la infraestructura crítica. Las amenazas de seguridad cibernética explotan la mayor complejidad y conectividad de lo sistemas de infraestructura crítica, lo que pone en riesgo la seguridad de la nación, su economía, y la salud y seguridad pública.

Para fortalecer la capacidad de **recuperación de esta infraestructura**, la Ley de Mejora de la Ciberseguridad de 2014(CEA) actualizó el papel del Instituto Nacional de Estándares y Tecnología (NIST) para "facilitar y apoyar el desarrollo de "marcos de riesgo de ciberseguridad".

SEGURIDAD CERO

Introducción al marco

La infraestructura crítica se define en la Ley Patriótica de los EE.UU de 2001 como **"sistemas y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitador en la seguridad de la nación, la seguridad económica nacional, la salud y seguridad pública, o cualquier combinación de estos mismos".**



SEGURIDAD CERO

Introducción al marco

El Marco proporciona una taxonomía común y un mecanismo para que las organizaciones realicen lo siguiente:

- ✓ Describir su postura actual de seguridad cibernética
- ✓ Describir su objetivo deseado para seguridad cibernética
- ✓ Identificar y priorizar oportunidades de mejora dentro de contexto de un proceso continuo y repetible
- ✓ Evaluar el progreso hacia el objetivo deseado
- ✓ Comunicarse entre las partes interesadas internas y externas sobre el riesgo de seguridad cibernética

SEGURIDAD CERO

Descripción general del marco

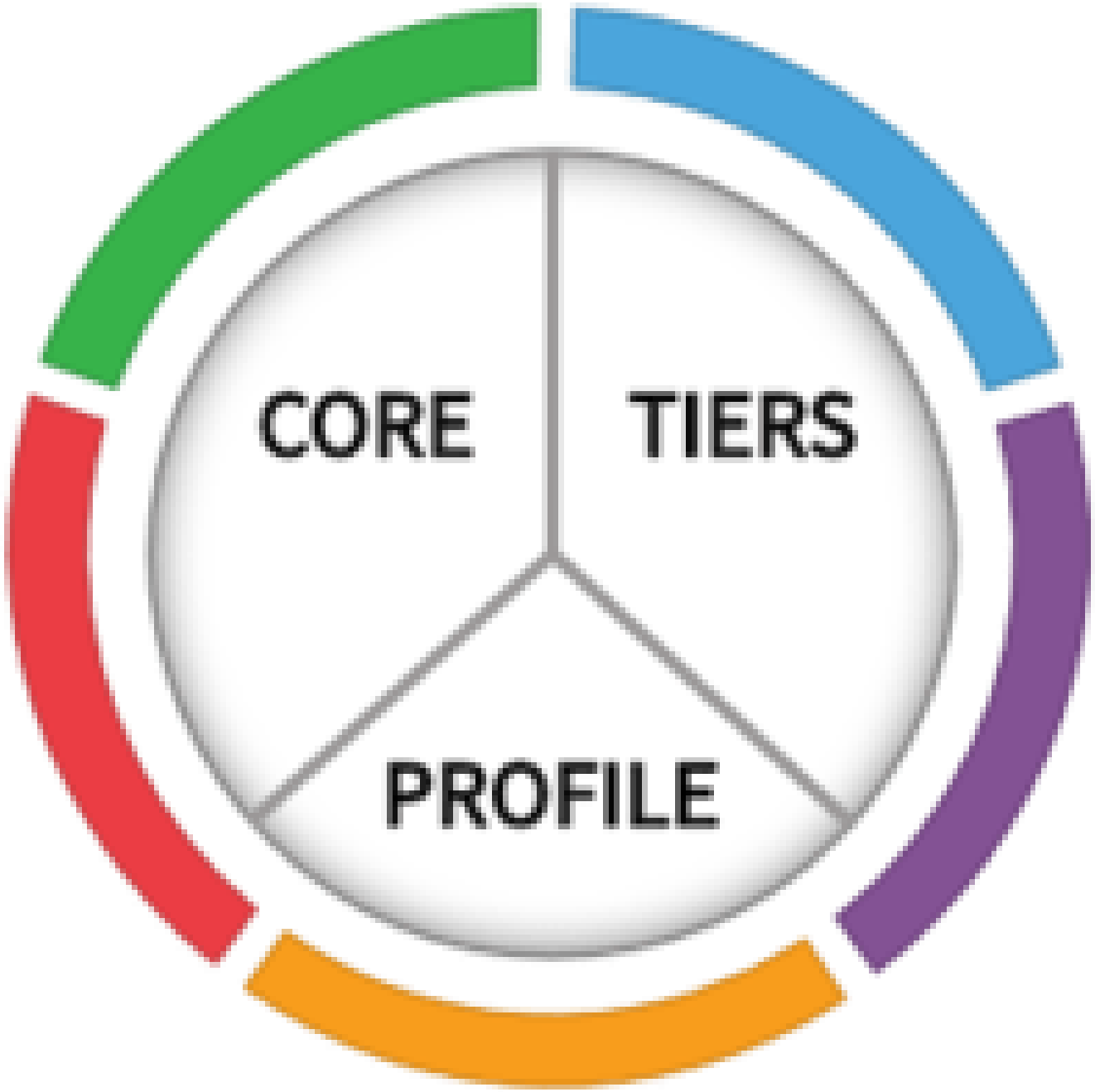
SEGURIDAD CERO

Descripción general del marco

El Marco es un enfoque basado en el riesgo para gestionar el riesgo de ciberseguridad, y se compone de tres partes:

- ✓ El núcleo del marco
- ✓ Los niveles de implementación del marco
- ✓ Los perfiles del marco

Cada componente del Marco refuerza la conexión entre los impulsores de negocio / misión y las actividades de ciberseguridad.


CORE
TIERS
PROFILE

SEGURIDAD CERO

Núcleo del marco


1
Identify
AM: Asset Management
BE: Business Environment
GV: Governance
RA: Risk Assesment
RM: Risk Management Strategy
2
Protect
AC: Access Control
AT: Awareness Training
DS: Data Security
IP: Information Protection
Processes and Procedures
PT: Pretective Technology
3
Detect
AE: Anomolies and Events
CM: Security Continuous Monitoring
DP: Detection Processes
4
Respond
RP: Response Planing
CO: Communications
AN: Analysis
MI: Mitigation
IM: Improvements
5
Recover
RP: Recovery Planning
IM: Improvements
CO: Communications
Cyber Security Framework

SEGURIDAD CERO

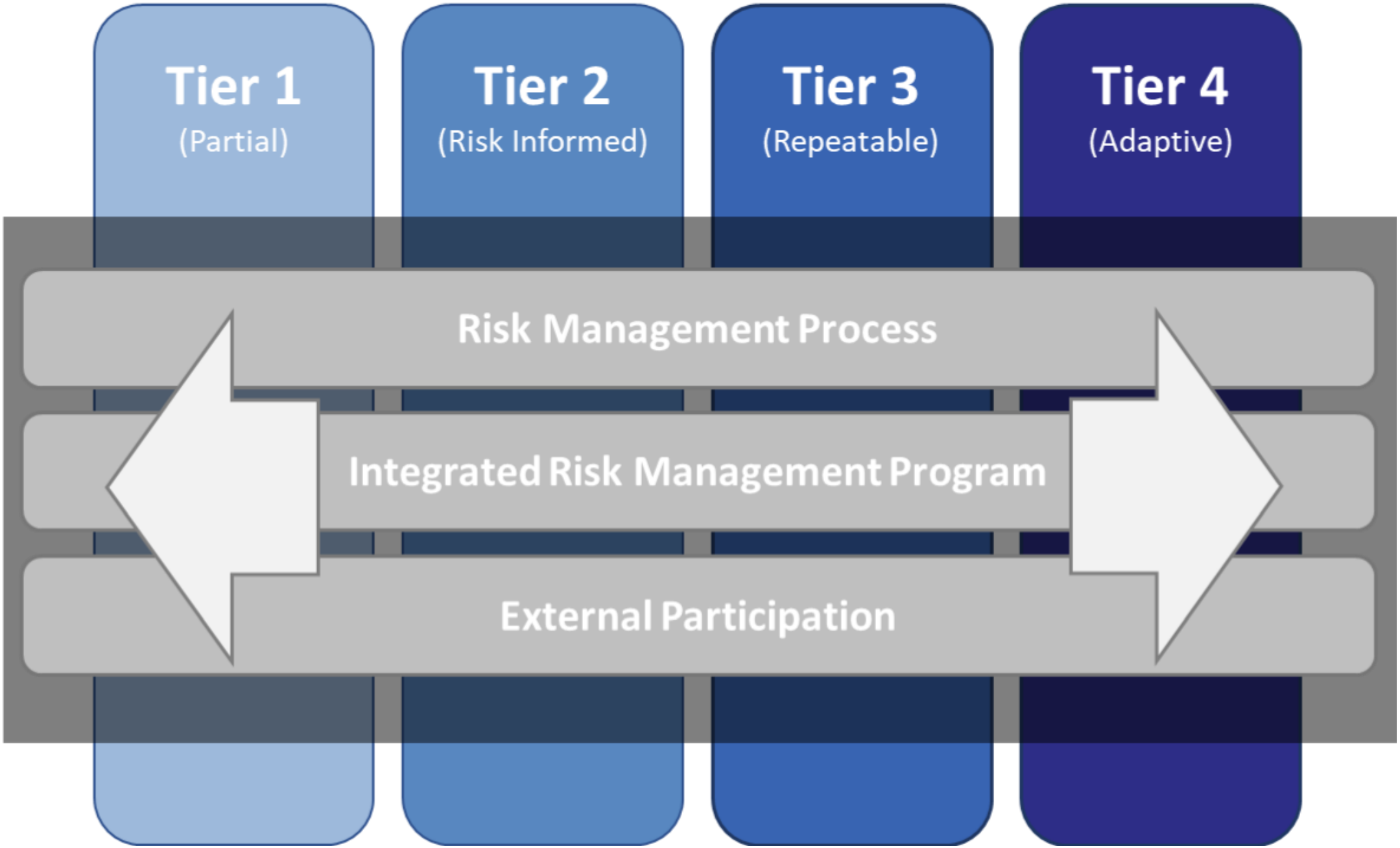
Núcleo del marco

El Núcleo del Marco proporciona un conjunto de actividades y resultados de ciberseguridad deseados utilizando un lenguaje común que es fácil de entender. El núcleo guía a las organizaciones en la gestión y reducción de sus riesgos de ciberseguridad de una manera que complementa los procesos existentes de ciberseguridad y gestión de riesgos de una organización.

El Núcleo del Marco consta de cinco Funciones simultáneas y continuas: ***Identificar, Proteger, Detectar, Responder y Recuperar***.

SEGURIDAD CERO

Niveles de Implementación del Marco


Tier 1
(Partial)
Tier 2
(Risk Informed)
Tier 3
(Repeatable)
Tier 4
(Adaptive)
Risk Management Process
Integrated Risk Management Program
External Participation

SEGURIDAD CERO

Niveles de implementación del marco

Los niveles de implementación del marco brindan un punto de referencia sobre como aborda y enfrenta una organización sus retos de ciberseguridad.

Existen diversos criterios para considerar a una organización en alguno de los niveles.

Los niveles son los siguientes: Parcial, Riesgo Informado, Repetible y adaptativo.

Nivel	Tipo	Proceso de gestión de riesgos	Programa de gestión integrada de riesgos	Participación externa
1	Parcial	Prácticas informales de riesgo, reactivo, enfoque de riesgo ad hoc	Conciencia institucional limitada, gestión de riesgos en su lugar pero irregular	Carece de procesos para coordinar y colaborar
2	Riesgo Informado	Práctica de gestión de riesgos aprobada, pero no en toda la organización, prioridades informadas por el objetivo por las partes interesadas y las decisiones de riesgo corporativo	La organización tiene conciencia del riesgo de ciberseguridad pero aún no tiene un enfoque institucionalizado	La organización no ha formalizado las capacidades para interactuar y compartir información
3	Repetible	Prácticas de gestión de riesgos aprobadas formalmente, expresadas como políticas actualizadas regularmente	Enfoque en toda la organización para gestionar el riesgo de ciberseguridad, las políticas, los procesos y los procedimientos son informados sobre el riesgo se definen e implementan según lo previsto	La organización comprende las dependencias y los socios, recibe información que permite la colaboración y las decisiones de respuesta basadas en el riesgo
4	Adaptativo	Se adapta según las lecciones aprendidas, mejora continua y respuesta oportuna	Enfoque del riesgo organizacional con conciencia situacional integrada en la cultura	Comparte activamente con socios para aprender y beneficiar la comunidad de manera proactiva

SEGURIDAD CERO

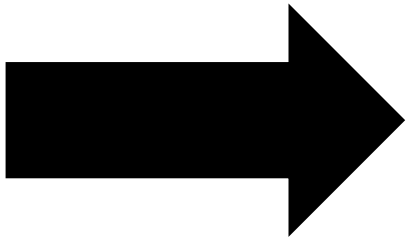
Perfiles del marco

SEGURIDAD CERO

Perfiles del marco

El Perfil del Marco ("Perfil") es la alineación de las Funciones, Categorías y Subcategorías con los requisitos empresariales, la tolerancia al riesgo y los recursos de la organización. Los Perfiles del Marco se pueden utilizar para describir el estado actual o el estado objetivo deseado de actividades específicas de seguridad cibernética. El Perfil Actual indica los resultados de seguridad cibernética que se están logrando actualmente. El Perfil Objetivo indica los resultados necesarios para alcanzar los objetivos de gestión de riesgos de seguridad cibernética deseados

Función	Perfil Actual
IDENTIFICAR (ID)	
PROTEGER (PR)	
DETECTAR (DE)	
RESPONDER (RS)	
RECUPERAR (RC)	



Función	Perfil Objetivo
IDENTIFICAR (ID)	
PROTEGER (PR)	
DETECTAR (DE)	
RESPONDER (RS)	
RECUPERAR (RC)	

SEGURIDAD CERO

Marco de gestión de riesgos de ciberseguridad

SEGURIDAD CERO

Gestión de riesgos de ciberseguridad

La gestión de riesgos es el proceso continuo de identificación, evaluación y respuesta al riesgo. Para gestionar el riesgo, las organizaciones deben comprender la probabilidad de que ocurra un evento y los posibles impactos resultantes. Con esta información, las organizaciones pueden determinar el nivel aceptable de riesgo para lograr sus objetivos organizacionales y pueden expresar esto como su tolerancia al riesgo.


Establecimiento del Contexto
Valoración de Riesgos
Identificación de Riesgos
Análisis de Riesgos
Evaluación de Riesgos
Tratamiento de Riesgos
Comunicación y consulta
Monitoreo y revisión

SEGURIDAD CERO

Preguntas

SEGURIDAD CERO

¿Cuáles son las funciones del marco?

a) Intensificar, Proteger, Detectar, Responder y Recuperar
b) Identificar, Proteger, Detectar, Atacar y Recuperar
C) Identificar, Proteger, Detectar, Responder y Recuperar
d) Implementar, Proteger, Defender, Resistir y Resiliencia

SEGURIDAD CERO

¿Cuáles son las funciones del marco?

a) Intensificar, Proteger, Detectar, Responder y Recuperar
b) Identificar, Proteger, Detectar, Atacar y Recuperar
C) Identificar, Proteger, Detectar, Responder y Recuperar
d) Implementar, Proteger, Defender, Resistir y Resiliencia

SEGURIDAD CERO

¿Cuáles son los niveles del marco?

a) De Parcial hasta Adaptativo
b) De Inicial hasta Avanzado
C) De Estándar hasta Final
d) De Inicial a Repetible

SEGURIDAD CERO

¿Cuáles son los niveles del marco?

a) De Parcial hasta Adaptativo
b) De Inicial hasta Avanzado
C) De Estándar hasta Final
d) De Inicial a Repetible

SEGURIDAD CERO

¿Cuál es el perfil al que apunta la organización?

a) Perfil Destino
b) Perfil Actual
C) Perfil NIST
d) Perfil Objetivo

SEGURIDAD CERO

¿Cuál es el perfil al que apunta la organización?

a) Perfil Destino
b) Perfil Actual
C) Perfil NIST
d) Perfil Objetivo


SEGURIDAD
CERO
Curso Oficial
LEAD CYBERSECURITY
PROFESSIONAL CERTIFICATE
50% OFF
Registro Aquí

https://www.seguridadcero.com.pe/

https://www.linkedin.com/company/seguridadcero/

http://www.youtube.com/c/SEGURIDADCERO

https://www.facebook.com/segu.cero

https://t.me/seguridadcero


SEGURIDAD
CERO
CURSO GRATIS
CIBERSEGURIDAD
Y NIST CSF