



CURSO GRATIS **CIBERSEGURIDAD** **Y NIST CSF**

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

CLASE 3

Componentes de NIST CSF

MIÉRCOLES 26 AGOSTO

CRI 5:00 PM 	GTM 5:00 PM 	HND 5:00 PM 	MEX 6:00 PM 	PER 6:00 PM 
COL 6:00 PM 	ECU 6:00 PM 	PAN 6:00 PM 	PRY 7:00 PM 	CHL 7:00 PM 
BOL 7:00 PM 	VEN 7:00 PM 	DOM 7:00 PM 	ARG 8:00 PM 	URY 8:00 PM 

Núcleo del Marco

Núcleo del Marco

El Núcleo del Marco proporciona un conjunto de actividades para lograr resultados específicos de seguridad cibernética y hace referencia a ejemplos de orientación en cómo lograr dichos resultados. El Núcleo no es una lista de verificación de las acciones a realizar. Este presenta los resultados clave de seguridad cibernética identificados por las partes interesadas como útiles para gestionar el riesgo. El Núcleo consta de cuatro elementos: **Funciones, Categorías, Subcategorías y Referencias Informativas de seguridad cibernética.**

Función	Categorías	SubCategorías	Referencias Informativas
IDENTIFICAR (ID)			
PROTEGER (PR)			
DETECTAR (DE)			
RESPONDER (RS)			
RECUPERAR (RC)			

Funciones

Funciones

Las **Funciones** organizan actividades básicas de seguridad cibernética en su nivel más alto. Estas funciones son Identificar, Proteger, Detectar, Responder y Recuperar. Estas ayudan a una organización a expresar su gestión del riesgo de seguridad cibernética organizando información, habilitando decisiones de gestión de riesgos, abordando amenazas y mejorando el aprender de actividades previas.



Función	Categorías	SubCategorías	Referencias Informativas
IDENTIFICAR (ID)			
PROTEGER (PR)			
DETECTAR (DE)			
RESPONDER (RS)			
RECUPERAR (RC)			

Identificar

La función de identificar ayuda a desarrollar una comprensión organizacional de la gestión del riesgo de ciberseguridad para sistemas, personas, activos, datos y capacidades.

Ejemplos de Resultados:

- Identificar activos físicos y de software para establecer un programa de gestión de activos.
- Identificar políticas de ciberseguridad para definir un programa de gobernanza.
- Identificar una estrategia de gestión de riesgos para la organización.

Proteger

Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos. La función Proteger admite la capacidad de **limitar o contener** el impacto de un posible evento de seguridad cibernética.

Ejemplos de Resultados:

- Gestión de identidad y control de acceso
- Conciencia y entrenamiento
- Seguridad de datos
- Procesos y procedimientos de protección de la información
- Mantenimiento y Tecnología de protección

Detectar

Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética.

La Función Detectar permite el **descubrimiento oportuno de eventos de seguridad cibernética**.

Ejemplos de Resultados:

- Anomalías y eventos.
- Monitoreo continuo de seguridad y Procesos de detección.

Responder

La función de respuesta desarrolla e implementa actividades apropiadas para **tomar medidas con respecto a un incidente de seguridad cibernética detectado.**

La función Responder admite la capacidad de contener el impacto de un posible incidente de ciberseguridad

Ejemplos de Resultados:

- Asegurar que los procesos de planificación de respuesta se ejecuten durante y después de un incidente.
- Gestión de comunicaciones durante y después de un evento.
- Analizando la efectividad de las actividades de respuesta.

Recuperar

La función Recuperar desarrolla e implementa actividades apropiadas para **mantener planes de resiliencia y restaurar cualquier capacidad o servicio** que se haya visto afectado debido a un incidente de ciberseguridad.

La función Recuperar admite la recuperación oportuna a las operaciones normales para reducir el impacto de un incidente de seguridad cibernética

Ejemplos de Resultados:

- Asegurar que la organización implemente los procesos y procedimientos de Planificación de Recuperación.
- Implementando mejoras basadas en las lecciones aprendidas.
- Coordinar las comunicaciones durante las actividades de recuperación

Categorías

Función	Categorías	SubCategorías	Referencias Informativas
IDENTIFICAR (ID)			
PROTEGER (PR)			
DETECTAR (DE)			
RESPONDER (RS)			
RECUPERAR (RC)			

Categorías

Las **Categorías** son las subdivisiones de una Función en grupos de resultados de seguridad cibernética estrechamente vinculados a las necesidades programáticas y actividades particulares. Los ejemplos de categorías incluyen "Gestión de activos", "Gestión de identidad y control de acceso" y "Procesos de detección".

Función	Identificador	Categorías
IDENTIFICAR (ID)	ID.AM	Gestión de Activos
	ID.BE	Entorno de negocio
	ID.GV	Gobierno
	ID.RA	Gestión de Riesgos
	ID.RM	Estrategia de gestión de riesgos

Función	Identificador	Categorías
PROTEGER (PR)	PR.AC	Control de acceso
	PR.AT	Sensibilización y formación
	PR.DS	Seguridad de los datos
	PR.IP	Procesos y procedimientos de protección de la información
	PR.MA	Mantenimiento
	PR.PT	Tecnología de protección

Función	Identificador	Categorías
DETECTAR (DE)	DE.AE	Anomalías y eventos
	DE.CM	Monitoreo continuo de seguridad
	DE.DP	Procesos de detección

Función	Identificador	Categorías
RESPONDER (RS)	RS.RP	Planificación de respuesta
	RS.CO	Comunicaciones
	RS.AN	Análisis
	RS.MI	Mitigación
	RS.IM	Mejoras

Función	Identificador	Categorías
RECUPERAR (RC)	RC.RP	Planificación de recuperación
	RC.IM	Mejoras
	RC.CO	Comunicación

Subcategorías

Función	Categorías	SubCategorías	Referencias Informativas
IDENTIFICAR (ID)	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>
PROTEGER (PR)	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>
DETECTAR (DE)	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>
RESPONDER (RS)	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>
RECUPERAR (RC)	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>	<hr/> <hr/> <hr/>

subcategorías

Las **Subcategorías** dividen aún más una Categoría en resultados específicos de actividades técnicas o de gestión. Proporcionan un conjunto de resultados que, aunque no son exhaustivos, ayudan a respaldar el logro de los resultados en cada Categoría. Algunos ejemplos de subcategorías incluyen "Los sistemas de información externos se catalogan", "Los datos en reposo se protegen". "y"La necesidad del sistema de gestión de información se invierte".

Función	ID	Categorías	ID	SubCategorías
IDENTIFICAR (ID)	ID.AM	Gestión de Activos	ID.AM-1	Los dispositivos y sistemas físicos dentro de la organización están inventariados.
			ID.AM-2	Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.
			ID.AM-3	La comunicación organizacional y los flujos de datos están mapeados
			ID.AM-4	Los sistemas de información externos están catalogados
			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.
			ID.AM-6	Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados

Referencias informativas

Referencias informativas

Las **Referencias Informativas** son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada Subcategoría. Las referencias informativas presentadas en el Núcleo del Marco son ilustrativas y no exhaustivas. Se basan en la orientación intersectorial a la que se hace referencia con más frecuencia durante el proceso de desarrollo del Marco."

Función	ID	Categorías	ID	SubCategorías	Referencias Informativas
IDENTIFICAR (ID)	ID.AM Gestión de Activos		ID.AM-1	Los dispositivos y sistemas físicos dentro de la organización están inventariados.	<ul style="list-style-type: none"> · 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.	<ul style="list-style-type: none"> · 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	<ul style="list-style-type: none"> · 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	<ul style="list-style-type: none"> · 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.	<ul style="list-style-type: none"> · 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	<ul style="list-style-type: none"> · 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

Documento	Referencia
NIST 800-53	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
CIS CSC	https://www.cisecurity.org/controls/
COBIT 5	http://www.isaca.org/cobit/pages/default.aspx
ISA 62443 (All)	https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-in-numerical-order/
ISO/IEC 27001	https://www.iso.org/isoiec-27001-information-security.html

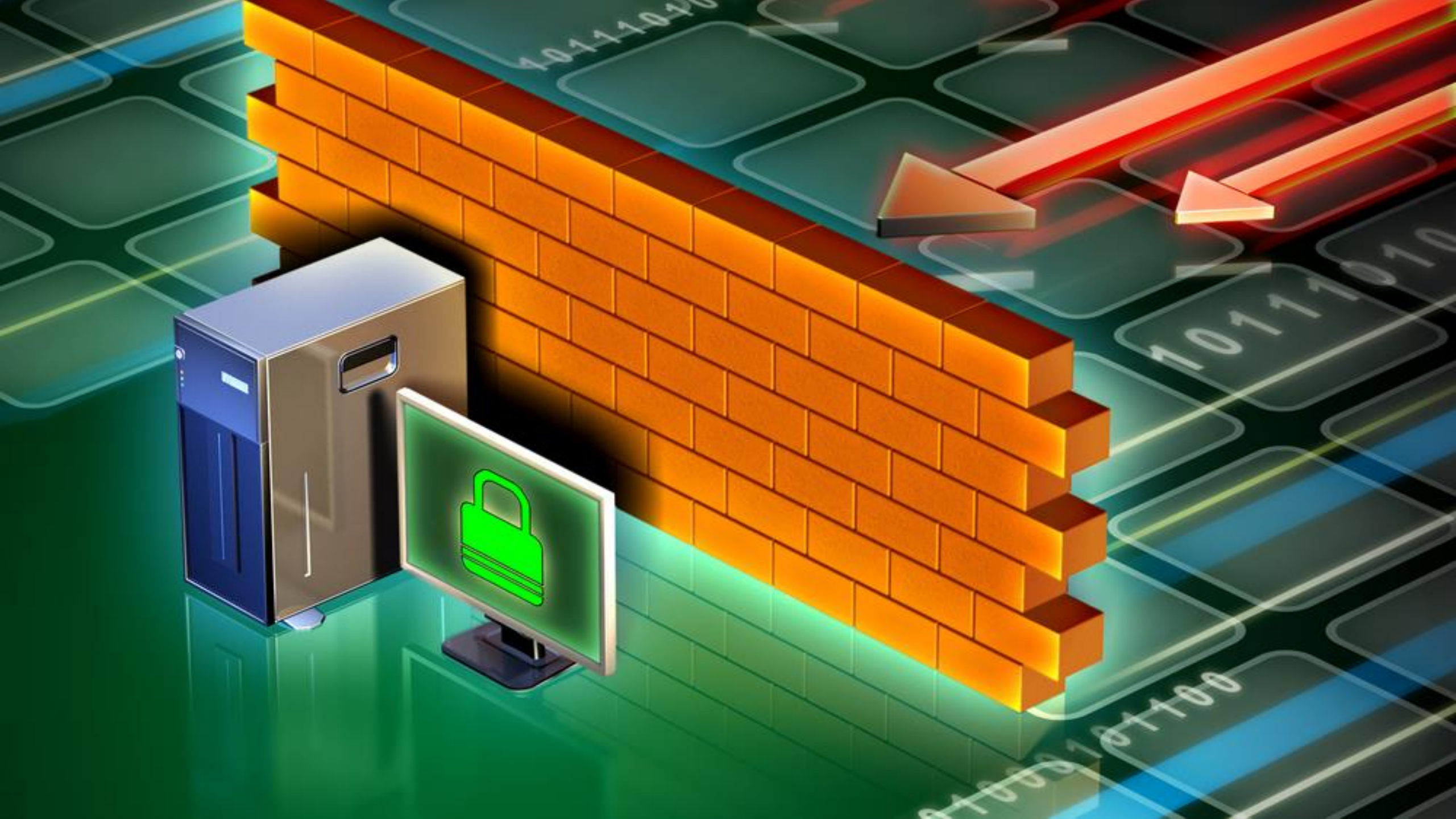
¿Cuál es la función
relacionada?



IDS
IPS



DETECTAR





PROTEGER

The image is a conceptual illustration of digital security. It features a prominent orange brick wall that acts as a barrier. To the left of the wall stands a blue and silver server tower. In front of the wall is a computer monitor displaying a glowing green padlock icon. The background is a dark green surface with glowing blue and yellow lines, and binary code (0s and 1s) is visible. Two large, glowing red arrows point towards the wall from the right side. A black rectangular box with a red border is centered over the wall, containing the word 'PROTEGER' in white capital letters.



Oops...



We're sorry, our website is down.
We're working on it.





Oops...



RECUPERAR


We're sorry, our website is down.
We're working on it.








CAPTCHA BANK

Securing your online presence


 [Captcha Settings](#)


 [General Settings](#)


 [Logs](#)


 [Other Settings](#)


 [Security Settings](#)


 [Blockage Settings](#)


 [Block / Unblock IP Addresses](#)


 [Block / Unblock IP Ranges](#)

 [Block / Unblock Countries](#)

 [Feature Requests](#)

 [System Information](#)

 [Error Logs](#)

 [Licensing](#)

Get Started

[Watch Captcha Bank Video!](#)

[or read documentation here](#)

User Guide

[Documentation](#)

[Support Question!](#)

[Contact Us](#)

More Actions

[Rate Us!](#)

[Our Other Products](#)

[Our Other Services](#)

[Home](#) [Captcha Bank](#) > [Security Settings](#) > [Block / Unblock IP Addresses](#)

Block / Unblock IP Addresses

IP Address :  *

121.163.26.28

Blocked For :  *

12 Hours

Comments : 

Blocked...

Get Started

[Watch Captcha Bank Video!](#)

[or read documentation here](#)

User Guide

[Documentation](#)

[Support Question!](#)

[Contact Us](#)

More Actions

[Rate Us!](#)

[Our Other Products](#)

[Our Other Services](#)

🏠 [Captcha Bank](#) > [Security Settings](#) > [Block / Unblock IP Addresses](#)

🌐 Block / Unblock

RESPONDER

IP Address : ? *

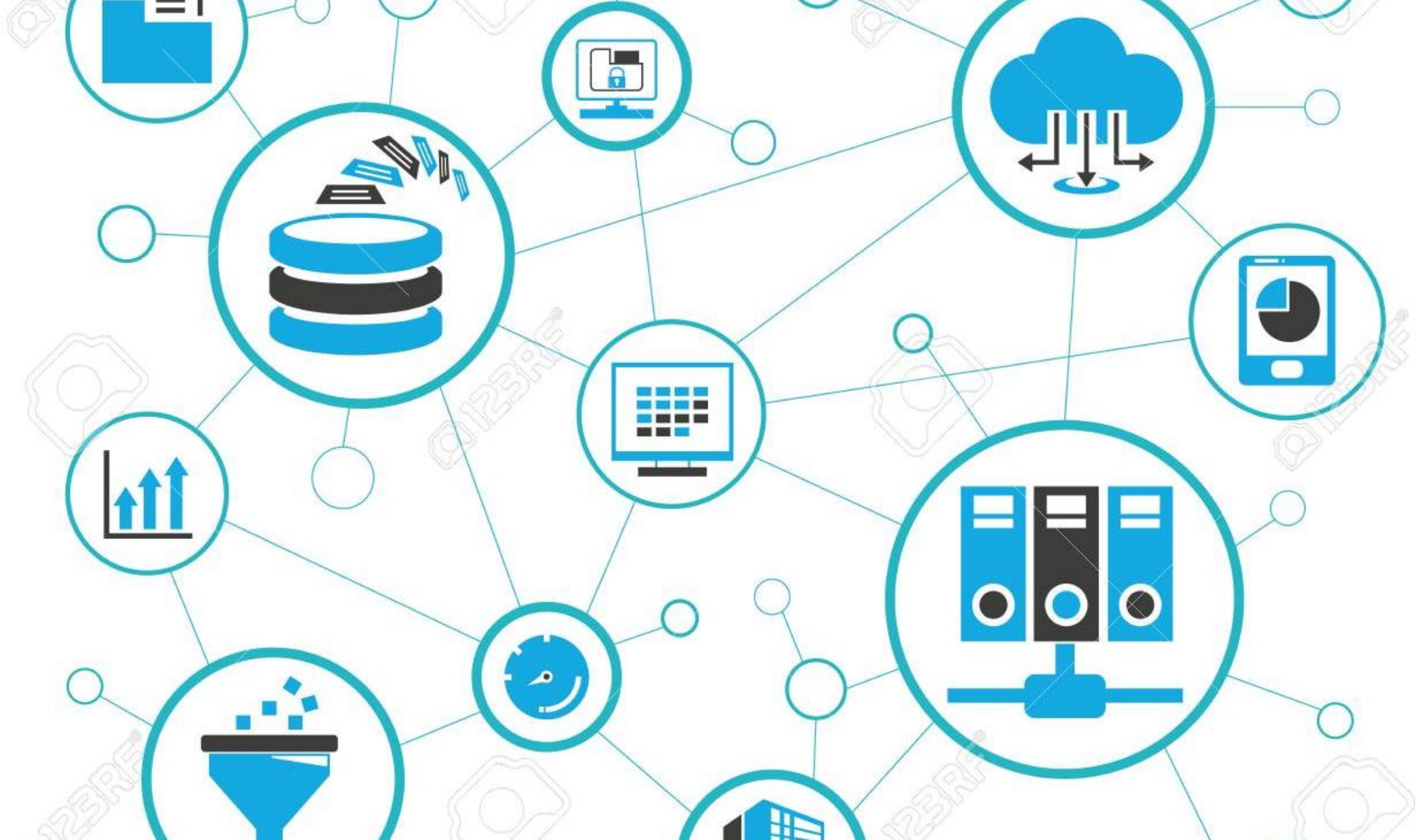
121.163.26.28

Blocked For : ? *

12 Hours

Comments : ?

Blocked...





IDENTIFICAR

Preguntas

¿Cuáles son las referencias del marco?

- a) NIST 800-53, CIS CSC, COBIT 5, ISA 62443, ISO 27001
- b) NIST 800-53, CIS CSC, COBIT 5, ITIL, ISO 27032
- c) NIST 800-53, ISO 22301, COBIT 4.1, ISA 62443, ISO 27001
- d) NIST 800-53, ISO 2000, ITIL, ISA 62443, ISO 27001

¿Cuáles son las referencias del marco?

- a) **NIST 800-53, CIS CSC, COBIT 5, ISA 62443, ISO 27001**
- b) NIST 800-53, CIS CSC, COBIT 5, ITIL, ISO 27032
- c) NIST 800-53, ISO 22301, COBIT 4.1, ISA 62443, ISO 27001
- d) NIST 800-53, ISO 2000, ITIL, ISA 62443, ISO 27001

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>



CURSO GRATIS **CIBERSEGURIDAD** **Y NIST CSF**