Aprende más en
www.awssecuritylatam.com

Tema 1: Principios de seguridad

CIBERSEGURIDAD DESDE CERO

Inicio de clases: Sábado 29-Abril

10am **11am** **12pm**

OBJETIVOS DEL BOOTCAMP

GENERALES

- **Ayudar a quiénes buscan dar sus primeros pasos en CIBERSEGURIDAD.**
- **Entender los conceptos fundamentales que maneja un profesional de esta área.**
- **Este es un curso introductorio y abarcaremos solo 5 dominios de seguridad.**
- **Al finalizar, se hará entrega de un certificado de culminación, previa evaluación.**

ESPECÍFICOS

- **100% de este bootcamp estará alineado al CERTIFIED IN CYBERSECURITY del (ISC)²**
- **Obtener tu primera certificación GRATUITA y en ESPAÑOL de esta área**
- **Tener la preparación para los próximos BOOTCAMP de mayor nivel**

SLACK

ROADMAP

CIBERSEGURIDAD
DESDE CERO

29-04
Principios de seguridad

06-05
Respuesta ante incidentes y continuidad del negocio

13-05
Control de acceso

20-05
Seguridad de la red

27-05
Operaciones de seguridad

REPO

TEMA 1

PRINCIPIOS DE SEGURIDAD

Módulo 1: Aseguramiento de la seguridad

LA TRÍADA CIA

CONFIDENCIALIDAD

Permite el **acceso autorizado** a la información y, al mismo tiempo, **protege la información** de una divulgación indebida.

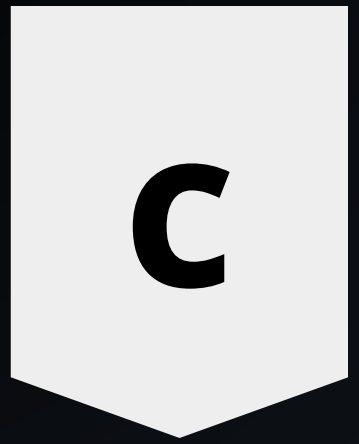
INTEGRIDAD

Es la **garantía** de que la información **no ha sido alterada** de manera **no autorizada.** Esta propiedad cubre los datos en almacenamiento, en procesamiento y en tránsito.

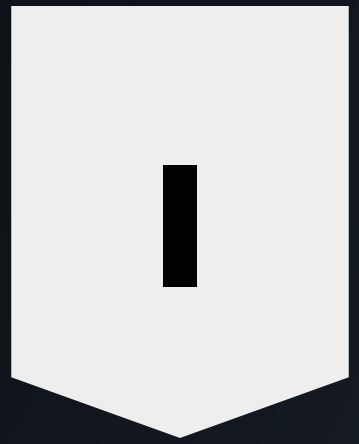
DISPONIBILIDAD

Permite que el **usuario autorizado pueda acceder** a los datos cuando los necesite, donde los necesite y en el formato en que los necesite.

TRÍADA CIA: DEEP DIVE



Información de identificación personal o PII, se refiere a cualquier dato con el que se puede identificar a una persona.
Otros término es **PHI:** Información de protección personal.



El concepto de integridad se aplica a no solo la información, **sino también** a los sistemas, organizaciones, incluso a las personas y sus acciones.

El profesional de seguridad debe **asegurarse en proporcionar los niveles adecuados** de disponibilidad ya que no significa que los datos o los sistemas esten el 100% del tiempo disponibles.

AUTENTICACIÓN

Se conoce como autenticación al proceso para probar la identidad de una persona comparando uno (SFA) o mas factores de identificación (MFA).

Existen tres métodos comunes de autenticación:

- **Algo que sabes: como contraseñas, pin o pregunta secreta.**
- **Algo que tienes: tokens físicos, tarjeta inteligentes, credenciales físicas.**
- **Algo que eres: biometría, características medibles.**

MÉTODOS DE AUTENTICACIÓN

Existen dos tipos de autenticación, usando uno solo de los métodos de autenticación mencionados anteriormente se conoce como autenticación de un solo factor (SFA). El otro tipo es cuando usas dos o más de estos metodos y a este tipo se le conoce como autenticación multifactor (MFA).

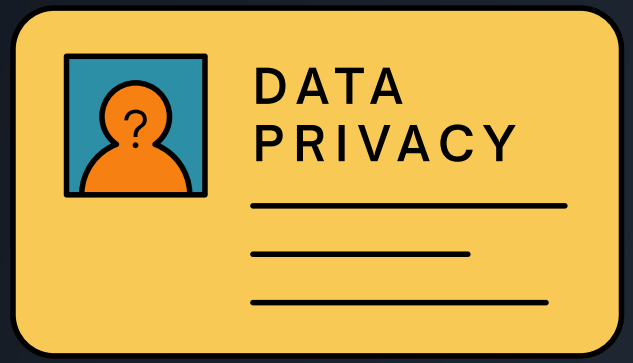
Una mejor práctica de seguridad es implementar como mínimo dos métodos comunes de autenticación:

- **Basado en el conocimiento**
- **Basado en token**
- **Basado en características**

NO REPUDIO Y PRIVACIDAD

No repudio es un término legal y se define como la protección contra un individuo que niega falsamente haber realizado una acción en particular. Brinda la capacidad de determinar si una persona realizó una acción con la información.

La privacidad es el derecho de un individuo a controlar la distribución de información sobre sí mismo.



TEMA 1

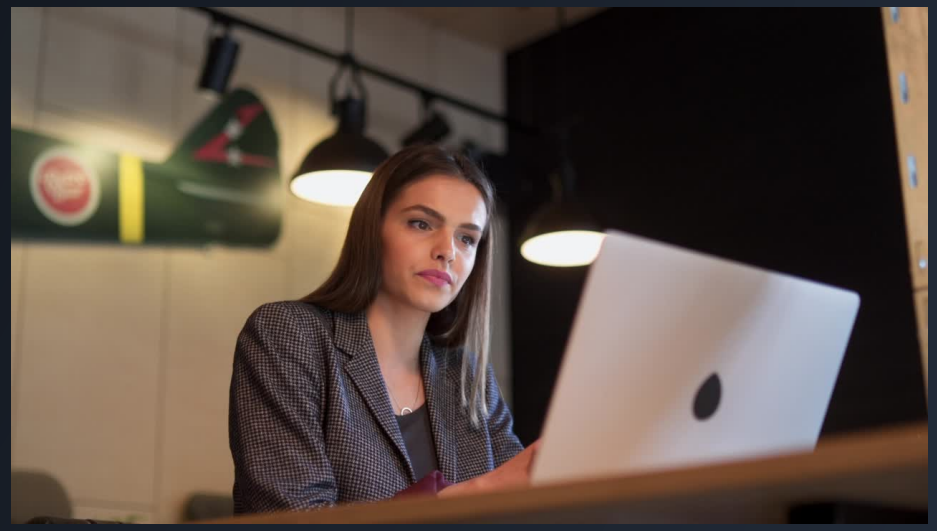
PRINCIPIOS DE SEGURIDAD

Módulo 2: Gestión de Riesgos

COMPRENDIENDO QUE SON LOS RIESGOS

Gestionar el riesgo es la principal tarea de un profesional de seguridad.

Es nuestro trabajo identificar, evaluar y administrar el riesgo para proteger nuestros activos.



Los riesgos pueden dividirse en dos categorias: riesgos internos y riesgos externos

Existen también los riesgos de multiples partes que se comparten entre varias org

EVALUACIÓN DEL RIESGO

Identificar el riesgo

Evaluar el riesgo

Amenaza y Vulnerabilidad

Una amenaza es una fuerza externa que pone en peligro la seguridad de sus datos.

Un vector de amenazas es el método que usa un atacante para llegar a su objetivo

Las vulnerabilidades son debilidades en sus controles de seguridad que una amenaza puede explotar.

EVALUACIÓN DEL RIESGO

Terremotos

Phishing

Huracanes

EVALUACIÓN DEL RIESGO

Impacto

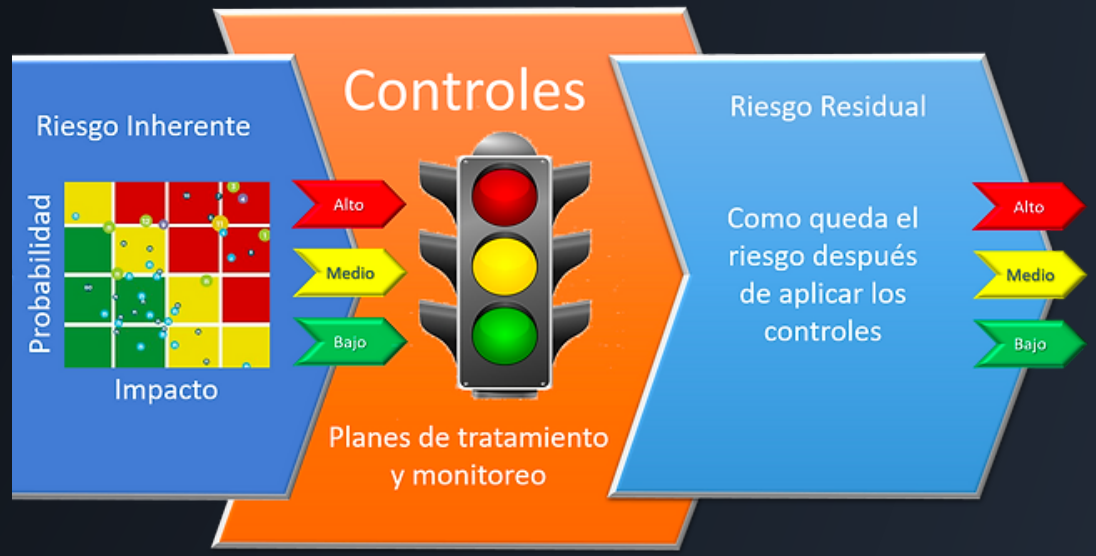
¿Qué tan severos serían los resultados si ocurriera el riesgo?

Probabilidad

¿Cuál es la probabilidad de que ocurra el riesgo?

	Insignificante 1	Menor 2	Significativo 3	Mayor 4	Severo 5
5 Casi seguro	Medio 5	Alto 10	Muy alto 15	Extremo 20	Extremo 25
4 Probable	Medio 4	Medio 8	Alto 12	Muy alto 16	Extremo 20
3 Moderado	Bajo 3	Medio 6	Medio 9	Alto 12	Muy alto 15
2 Poco probable	Muy bajo 2	Bajo 4	Medio 6	Medio 8	Alto 10
1 Raro	Muy bajo 1	Muy bajo 2	Bajo3	Medio 4	Medio 5

TRATAMIENTO DEL RIESGO



4 Maneras de gestionar los riesgos:

- **Evitar el Riesgo**
- **Transferir el riesgo**
- **Mitigar el riesgo**
- **Aceptar el riesgo**

Nivel inicial del Riesgo = Inherente
Despues de aplicar control = Residual
Nuevo riesgo = Control de riesgo

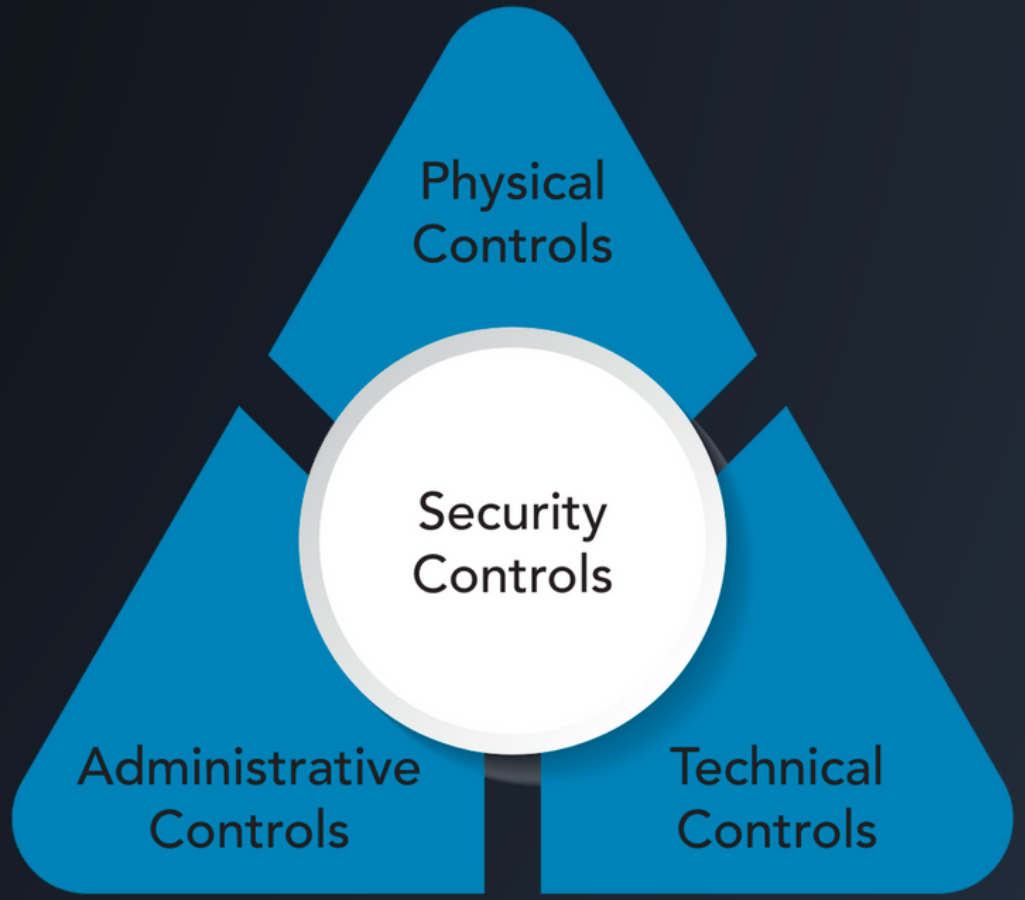
TEMA 1

PRINCIPIOS DE SEGURIDAD

Módulo 3: Controles de seguridad

¿QUÉ SON LOS CONTROLES DE SEGURIDAD?

Los controles de seguridad se refieren a los mecanismos físicos, técnicos y administrativos que actúan como contramedidas prescritas para un sistema de informacíon para proteger la triada CIA del sistema y su información. La implementación de controles debería reducir el riesgo a un nivel aceptable.



TEMA 1

PRINCIPIOS DE SEGURIDAD

Módulo 4: Gobierno de la seguridad

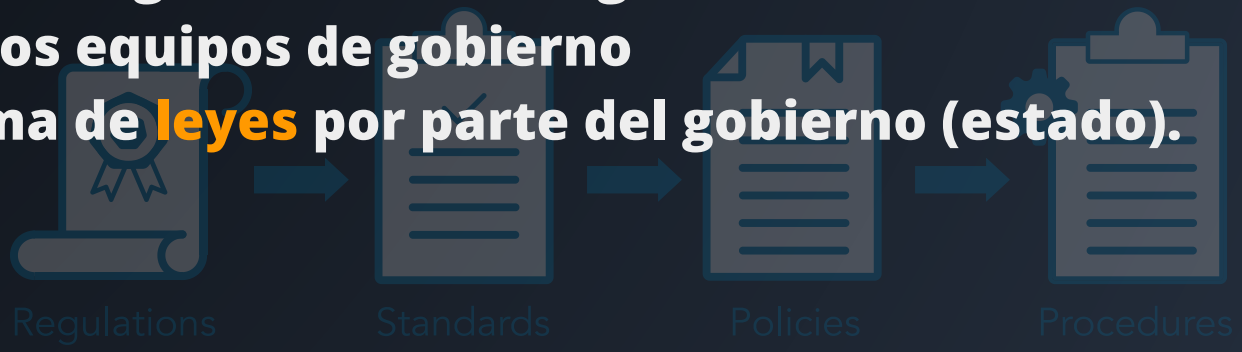
ELEMENTOS DE GOBERNANZA

Existen cuatros elementos de gobierno en la seguridad que hay que conocer:

- **Regulaciones y leyes**
- **Estándares**
- **Políticas**
- **Procedimientos**

¿Cómo se relacionan estos elementos?

- **Los procedimientos, son pasos detallados para completar una tarea.**
- **Las políticas son implementadas por el gobierno de la organización.**
- **Los estándares son utilizados por los equipos de gobierno**
- **Las regulaciones se emiten en forma de leyes por parte del gobierno (estado).**



REGULACIONES Y LEYES

Los gobiernos pueden imponer regulaciones y multas y sanciones a nivel nacional, regional y local.

Algunos ejemplos para conectar los conceptos con reglamentos reales:

La Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPPA) es un ejemplo de una ley que rige el uso de la informacion médica persona/protegida (PHI) en los Estados Unidos. La violación de la regla HIPAA conlleva la posibilidad de multas y/o encarcelamiento tanto para individuos como para empresas.

El Reglamento General de Protección de Datos (GDPR) fue promulgado por la Unión Europea (UE) para controlar el uso de la Información de Identificación Personal (PII) de sus habitantes y de la UE.

ESTÁNDARES, POLÍTICAS Y PROCEDIMIENTOS

Standards

Son utilizados como parte del programa de seguridad de sistemas de información, tanto como documentos de cumplimiento como avisos o pautas.

Policies

Se basa en las leyes aplicables y especifíca qué estándares y pautas seguirá la organización.

Procedures

Definen actividades explícitas y repetibles necesarias para realizar una tarea específica o un conjunto de tareas

- La **tríada CIA** esta compuesta por Confidencialidad, Integridad y Disponibilidad.
- El **control de acceso** tiene 3 pasos: identificación, autenticación y autorización.
- La **autenticación** tiene 3 métodos: basado en el conocimiento, token, y característica.
- El usuario tiene hasta 3 métodos para **autenticarse:** lo que sabe, tiene y es.
- Se conoce como MFA cuando se usa **2 métodos de autenticación diferentes.**
- La **privacidad de los datos** permite al usuario entender quién tiene su información y que uso le darán.
- **PII:** Información de Identificación Personal
- **PHI:** Información de Salud Protegida
- Un **Security Policy Framework** consta de 4 elementos: Políticas, Estándares, Guidelines y Procedimientos.
- **No repudio** evita que un individuo niegue falsamente una acción cometida.
- Existen 3 controles de seguridad: **físicos, técnicos y administrativos.**

Demuestra de qué estas hecho.
Es sin miedo al éxito.

No recopilo correo electronico.

QUIZZ

MUCHAS GRACIAS

Ayúdame a seguir mejorando.
La encuesta es totalmente anónima.

No recopilo correo electronico.

C S A T