Aprende más en
www.awssecuritylatam.com

Tema 3: Conceptos de control de acceso

CIBERSEGURIDAD DESDE CERO

Tercera clase: Sábado 13-Mayo

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

ABOUT ME

¿QUIÉN ESTÁ HABLANDO?
Rodrigo Elissamburu
Arquitecto de Soluciones / Desarrollador

LINKED IN

REPO

SLACK

TEMA 3
CONTROL DE ACCESO

Módulo 1: Fundamentos de control de acceso

¿Qué es un control de seguridad?

EN TÉRMINOS GENERALES

Protección o contramedida diseñada para preservar la CONFIDENCIALIDAD, INTEGRIDAD y DISPONIBILIDAD.

Son el corazón de un programa de seguridad de la información.

Consisten en:

- **Restringir el acceso a los sistemas de información y a los datos.**
- **Permitir el acceso adecuado al personal y los procesos autorizados.**

Acceso

SE BASA EN 3 ELEMENTOS

- **Sujeto: Iniciador de una solicitud de servicio (ACTIVO)**
- **Reglas: Instrucciones desarrolladas para permitir o denegar el acceso**
- **Objeto: Todo aquello a lo que se intenta acceder (PASIVO)**

Control Físico

Control Administrativo

LEY DE TRANSITO

Ley Nº 24.449

Principios Básicos. Coordinación Federal. Consejo Federal de Seguridad Vial Registro Nacional de Antecedentes del Tránsito. Usuario de la Vía Pública. Capacitación. Licencia de Conductor. Vía Pública. Vehículo. Modelos Nuevos. Parque Usado. Circulación. Reglas Generales. Reglas de Velocidad. Reglas para Vehículos de Transporte. Reglas para Casos Especiales. Accidentes. Bases para el Procedimiento. Principios Procesales. Medidas Cautelares. Recursos Judiciales. Régimen de Sanciones. Principios Generales. Sanciones. Extinción de Acciones y Sanciones. Norma supletoria. Disposiciones Transitorias y Complementarias.

Sancionada: Diciembre 23 de 1994.

Promulgada Parcialmente: Febrero 6 de 1995.

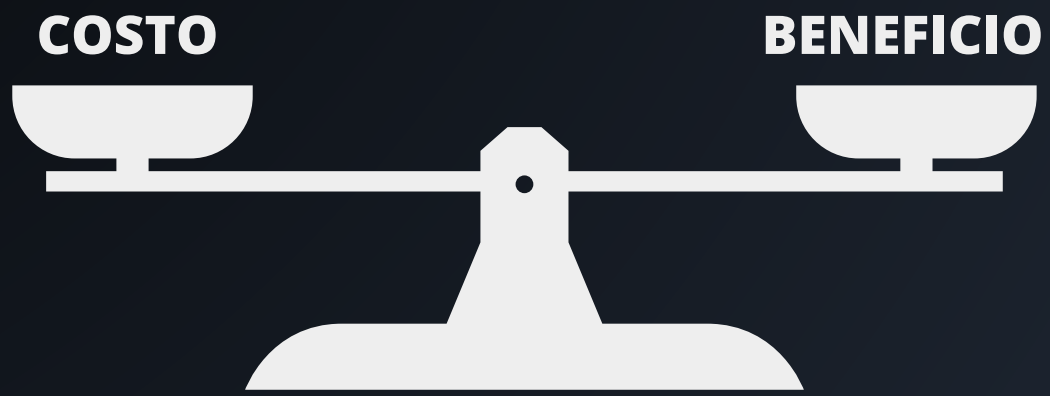
Ver Antecedentes Normativos

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc., sancionan con fuerza de Ley

Evaluación de los controles

La reducción del riesgo depende de la eficacia del control. Debe aplicarse a la situación actual y adaptarse a un entorno cambiante.

El costo de implantación de los controles debe estar en linea con el valor de lo que se protege.



Defensa en capas

Controles Físicos

Controles Técnicos/Lógicos

Controles Administrativos

Activos

Principio del menor privilegio

Permitir únicamente el acceso mínimo necesario para que los usuarios o programas cumplan su función.

Gestión de acceso privilegiado

Para los usuarios que requieran acceso privilegiados, una buena práctica es que sólo se usen los privilegios cuando es estrictamente necesario.

Cuentas privilegiadas

Cuentas con permisos superiores a los de los usuarios normales, como los gestores y administradores.

- **Administradores de sistemas**
- **Personal del servicio de asistencia o de soporte de TI**
- **Analistas de seguridad**

Medidas:

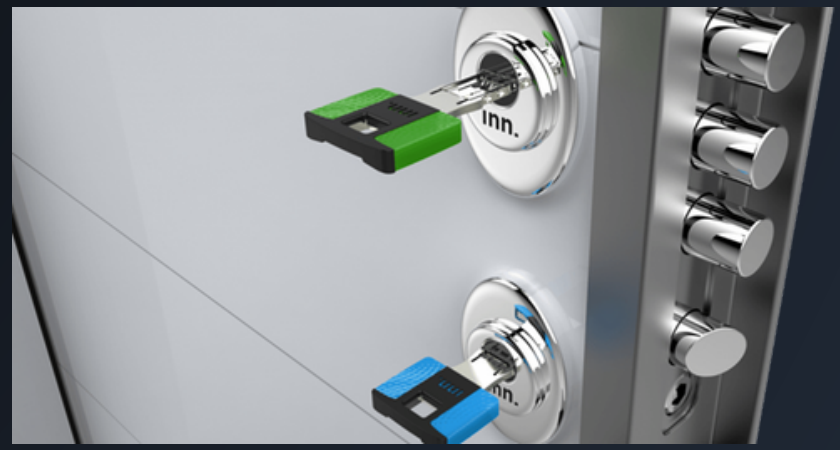
- **Registro detallado de acciones -> Disuasión y control administrativo**
- **Control de acceso mas estricto -> MFA / Limitación de horarios permitidos**
- **Verificación de confianza más profunda**
- **Mayor nivel de auditoría**

Segregación de funciones

Ninguna persona debe controlar toda una transacción de alto riesgo de principio a fin

¿Qué medidas se pueden tomar?
- **Separar una transacción de alto riesgo en partes**
- **Que cada parte dependa de una persona diferente**
- **Doble control**

¿Qué obtenemos con esto?
- **Evitar el fraude**
- **Detectar un error en el proceso**



Personal autorizado vs NO autorizado

¿Cómo se proveen los usuarios?

¿Cómo actuamos en cada caso?

- **Nuevos empleados**
- **Cambio de posición**
- **Renuncia/Despido**

Debemos evitar la fluencia de permisos o privilegios

Definir normas con las funciones estándar de los usuarios

TEMA 3
CONTROL DE ACCESO

Módulo 2: Control de Acceso Físico

¿Qué son los controles de acceso físico?

Los controles de acceso físico son elementos que se pueden tocar físicamente

¿Por qué tener controles de seguridad física?
Para proteger activos (físicos, salud del personal)

Tipos de controles de acceso físico

SISTEMAS DE ACREDITACIÓN Y ACCESO

DISEÑO MEDIOAMBIENTAL (CPTED)

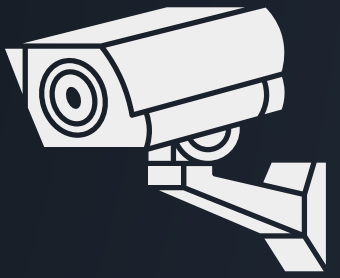
Crime Prevention Through Environmental Design

BIOMETRÍA

- **Registro**
  - **Fisiológico**
  - **Conductal**
- **Verificación**

Monitoreo/Supervisión - Ejemplos

CÁMARAS



- **Supervisan de forma centralizada**
- **Pueden ser un elemento disuasorio**
- **Si se graba, pueden aportar pruebas después de la actividad**

SISTEMAS DE ALARMA

- **Sensores que suelen instalarse en puertas y/o ventanas**
- **Alarmas de incendio**

Monitoreo/Supervisión - Ejemplos

GUARDIA DE SEGURIDAD

- **Control de seguridad física eficaz**
- **Pueden ser un elemento disuasorio**

REGISTROS

- **Hoja de registro mantenida por un guardia de seguridad**
- **Registros creados por un sistema electrónico que gestiona el acceso físico**
- **Conservar la información tanto tiempo cómo se requiera**
- **Si contienen datos confidenciales, deben protegerse contra la divulgación**

TEMA 3
CONTROL DE ACCESO

Módulo 3: Control de Acceso Lógico

¿Qué son los controles de acceso lógicos?

GENERALES

- **Son métodos electrónicos que impiden que alguien acceda a los sistemas, incluso a bienes o zonas tangibles.**

- **Contraseñas**
- **Biometría (implementada en un sistema, como un smartphone o un portátil)**
- **Lectores de credenciales/tokens conectados a un sistema**

Limitan quién puede obtener acceso lógico a un activo, incluso si la persona ya tiene acceso físico.

Control de acceso discrecional (DAC)

GENERALES

Un sujeto al que se le ha concedido acceso a la información puede hacer una o más de las siguientes cosas

- **Transmitir la información a otros sujetos u objetos**
- **Conceder sus privilegios a otros sujetos**
- **Modificar los atributos de seguridad de los sujetos, objetos, sistemas de información o componentes del sistema**
- **Elegir los atributos de seguridad que se asociarán a los objetos recién creados o revisados; y/o**
- **Modificar las normas que rigen el control de acceso; los controles de acceso obligatorios restringen esta capacidad.**

Control de acceso obligatorio (MAC)

GENERALES
Se aplica de manera uniforme a todos los sujetos y objetos dentro de los límites de un sistema de información

Sólo los administradores de seguridad pueden modificar cualquiera de las reglas de seguridad establecidas para los sujetos y objetos dentro del sistema.

El sujeto está restringido para:

- **Transmitir la información a sujetos u objetos no autorizados**
- **Conceder sus privilegios a otros sujetos**
- **Modificar uno o varios atributos de seguridad de las personas, los objetos, el sistema de información o los componentes del sistema.**
- **Elegir los atributos de seguridad que se asociarán a los objetos recién creados o modificados.**
- **Modificación de las reglas de control de acceso**

Control de acceso basado en roles (RBAC)

GENERALES
Se aplica de manera uniforme a todos los sujetos y objetos dentro de los límites de un sistema de información

Sólo los administradores de seguridad pueden modificar cualquiera de las reglas de seguridad establecidas para los sujetos y objetos dentro del sistema.

El sujeto está restringido para:

- **Transmitir la información a sujetos u objetos no autorizados**
- **Conceder sus privilegios a otros sujetos**
- **Modificar uno o varios atributos de seguridad de las personas, los objetos, el sistema de información o los componentes del sistema.**
- **Elegir los atributos de seguridad que se asociarán a los objetos recién creados o modificados.**
- **Modificación de las reglas de control de acceso**

MUCHAS GRACIAS

Ayúdame a seguir mejorando.
La encuesta es totalmente anónima.

No recopilo correo electronico.

QUIZZ