



ESCUELA SUPERIOR  
DE GUERRA

“General Rafael Reyes Prieto”

Colombia

# Desafíos y Tendencias en la Identidad Digital para la Seguridad de las Infraestructuras Críticas en el Estado Colombiano

Electiva: Habilidades en Ciberseguridad

MY. Ramiro Alvarado  
MY. Rafael Martinez  
MY. Jaime Patiño

# AGENDA

00

Introducción y Contexto

01

Importancia de la  
identidad digital

02

Autenticación  
Y Autorización

03

Gestión de  
identidades y  
accesos

04

Privacidad y  
protección de  
datos

05

Amenazas  
internas

06

Resiliencia ante  
ciberataque

07

Tecnologías  
emergentes

08

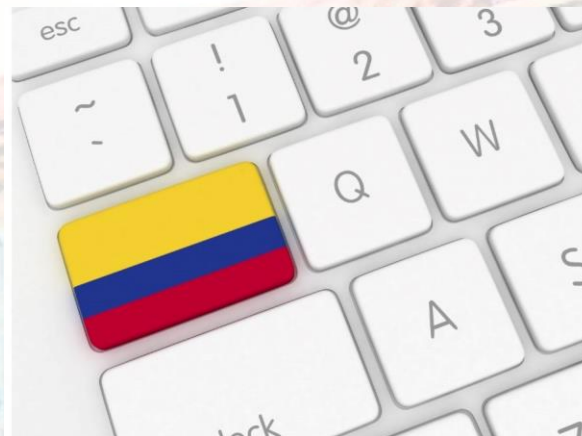
Desafíos  
especificos para  
Colombia

09

Conclusiones



## Introducción y Contexto



# Desafíos y Tendencias en la Identidad Digital para la Seguridad de las Infraestructuras Críticas en el Estado Colombiano



## 1

# Importancia de la identidad digital



**Importancia de la Identidad Digital:** La identidad digital es crucial para la seguridad de infraestructuras críticas, garantizando que solo usuarios autorizados tengan acceso a sistemas sensibles. La digitalización de sectores esenciales como energía, agua, telecomunicaciones y transporte ha incrementado la eficiencia, pero también la vulnerabilidad a ciberataques.

## 2

# Autenticación y Autorización

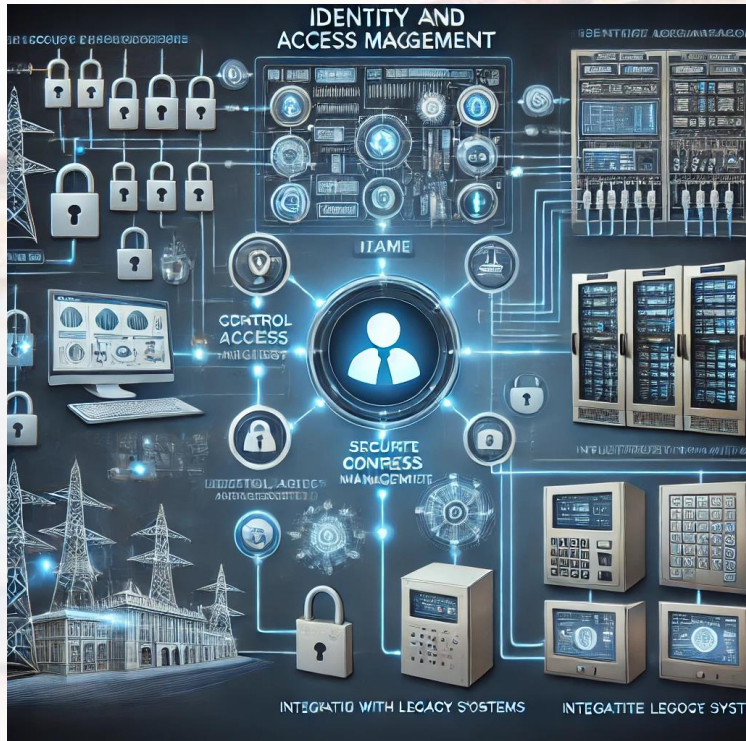


**Autenticación y Autorización:** Estos procesos son vitales para proteger sistemas sensibles. Métodos como la autenticación multifactor (MFA) y biometría mejoran la seguridad, aunque presentan desafíos en su implementación y aceptación por parte de los usuarios.



## 3

# Gestión de identidades y accesos



**Gestión de Identidades y Accesos (IAM):** La gestión efectiva requiere soluciones avanzadas y políticas robustas. Los desafíos incluyen la integración con sistemas heredados y la falta de estandarización.

## 4

# Privacidad y Protección de datos



**Privacidad y Protección de Datos:** Las organizaciones deben cumplir con la Ley de Protección de Datos Personales de Colombia (Ley 1581 de 2012) para evitar brechas de datos que pueden tener graves consecuencias.







## 6

# Resiliencia ante ciberataques



**Resiliencia ante Ciberataques:** La resiliencia cibernética es esencial para resistir y recuperarse de ciberataques. Estrategias de defensa en profundidad y colaboración entre el sector público y privado son cruciales.

# 7

## Tecnologías emergentes



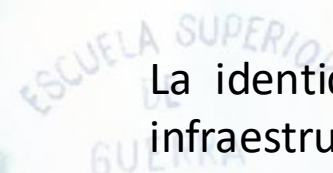
### Tecnologías Emergentes:

- **Blockchain:** Ofrece una solución segura y descentralizada para la gestión de identidades, aunque enfrenta desafíos como la escalabilidad.
- **Inteligencia Artificial (IA):** Puede mejorar la seguridad mediante la detección de patrones anómalos y la predicción de amenazas, pero también presenta riesgos como sesgos en los algoritmos.
- **Zero Trust Architecture (ZTA):** Este enfoque asume que todas las solicitudes de acceso son potencialmente maliciosas, verificando constantemente la autenticidad de cada solicitud.





# Conclusiones



La identidad digital es esencial para la seguridad de infraestructuras críticas en Colombia. Se necesitan enfoques multifacéticos y colaborativos para gestionar identidades digitales de manera segura. La adopción de tecnologías avanzadas y la implementación de políticas robustas mejorarán la resiliencia y seguridad frente a amenazas cibernéticas.





ESCUELA SUPERIOR  
DE GUERRA

"General Rafael Reyes Prieto"

Colombia

# Preguntas



Escuela Superior  
de Guerra



Escuela Superior  
de Guerra



@EsdegCol



Escuela Superior  
de Guerra



Esdeguecol





ESCUELA SUPERIOR  
DE GUERRA

“General Rafael Reyes Prieto”

Colombia



La ***Escuela Superior de Guerra “General Rafael Reyes Prieto”*** está certificada  
bajo las normas internacionales **ISO 9001:2015** e **ISO 21001:2018**.





Escuela Superior de Guerra  
"General Rafael Reyes Prieto"

Colombia

# Gracias



Escuela Superior  
de Guerra



Escuela Superior  
de Guerra



@EsdegCol



Escuela Superior  
de Guerra



Esdeguecol

