ESCUELA SUPERIOR
DE GUERRA
"General Rafael Reyes Prieto"
Colombia

SECURITY OPERATIONS – INCIDENT RESPONSE

CC Diego E. Cabuya Padilla
MY Sergio Baudin Cruz
MY Víctor A. López Salguero
CC Yerson A. Torres

DEFINICIONES:

SECURITY OPS – INCIDENT RESPONSE

AGENDA

01 Security Response

02 Incident Response

03 Bibliografía

Security Operations

- ☐ Prevention
  - Data Protection
    - Encryption, PKI, TLS
    - Data Loss Prevention (DLP)
    - Email Security
  - Network Security
    - Firewall, IDS/IPS, Proxy Filtering
    - VPN, Security Gateway
    - DDoS Protection
  - Application Security
    - Threat Modeling
    - Design Review
    - Secure Coding
    - Static Analysis
    - Web App Scanning
    - WAF, RASP
  - Endpoint Security
    - Anti-virus, Anti-malware
    - HIDS/HIPS, FIM
    - App Whitelisting
  - Secure Configurations
  - Active Defense
  - Patching
- ☐ Detection
  - Log Management/SIEM
  - Continuous Monitoring
  - Network Security Monitoring
  - NetFlow Analysis
  - Advanced Analytics
  - Threat Hunting
  - Penetration Testing
  - Red Team
  - Vulnerability Scanning
  - Human Sensor
  - Data Loss Prevention (DLP)
  - Security Operations Center (SOC)
  - Threat Intelligence
  - Threat Information Sharing
  - Industry Partnerships
- ☐ Response
  - Incident Handling Plan
  - Breach Preparation
  - Tabletop Exercises
  - Forensic Analysis
  - Crisis Management
  - Breach Communications

1

Security Operations

PREVENCIÓN

Prevención

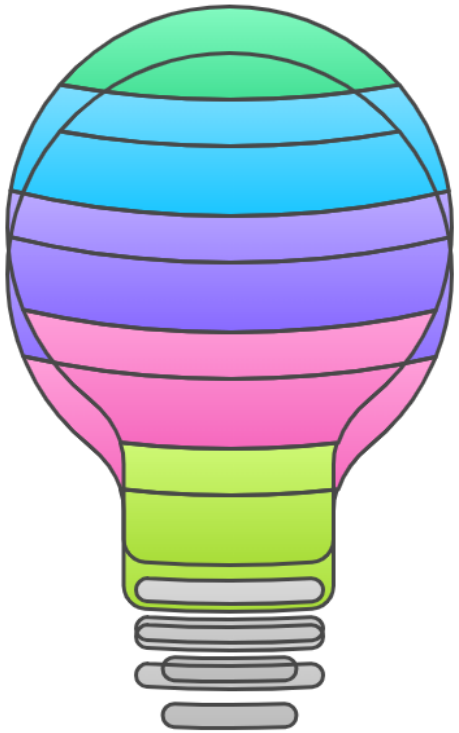
Implementa controles para evitar ataques

Seguridad de las Aplicaciones

Refuerza el código de software contra vulnerabilidades

Configuraciones Seguras

Establece estándares de seguridad en sistemas



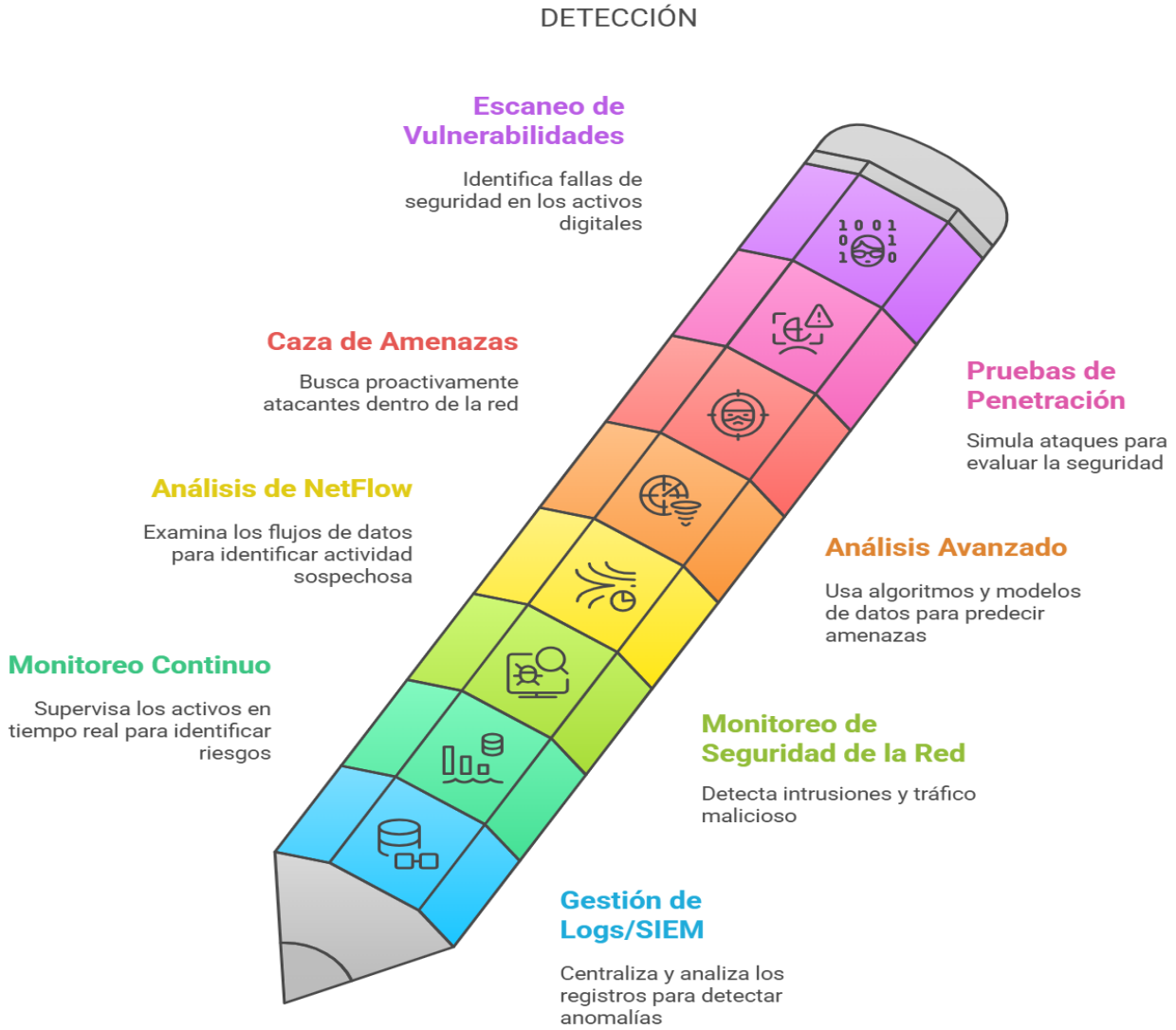
Seguridad de la Red

Protege la infraestructura con firewalls y VPNs

Seguridad de los Endpoints

Protege dispositivos contra malware y accesos no autorizados

01 Security Operations



RESPUESTAS

Comunicación en Caso de Brechas

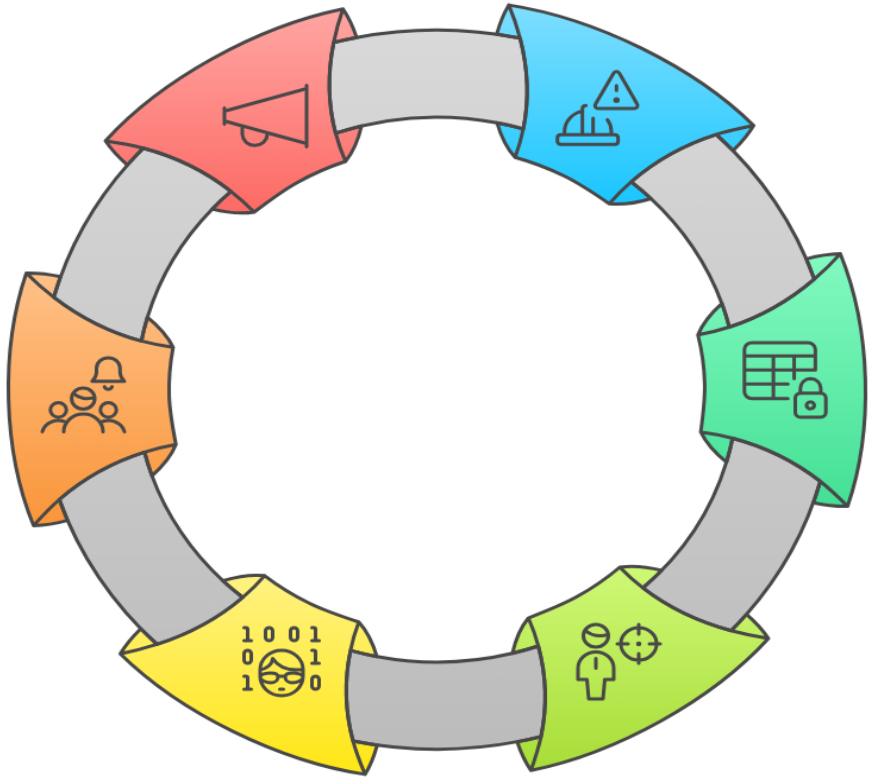
Maneja la divulgación de incidentes a las partes interesadas

Gestión de Crisis

Coordina la respuesta ante emergencias cibernéticas

Análisis Forense

Investiga incidentes para identificar causas y responsables



Plan de Manejo de Incidentes

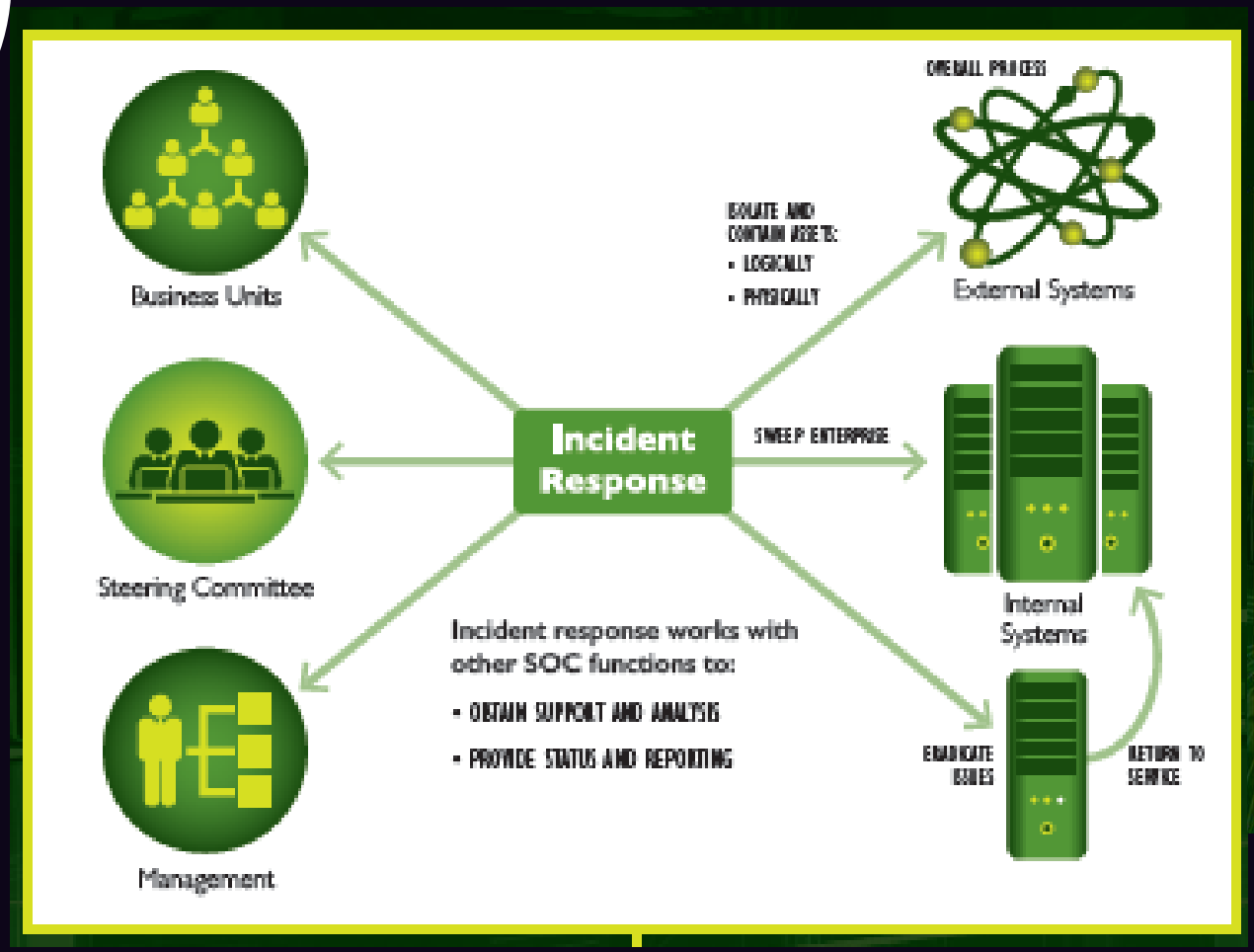
Define protocolos para responder a ataques

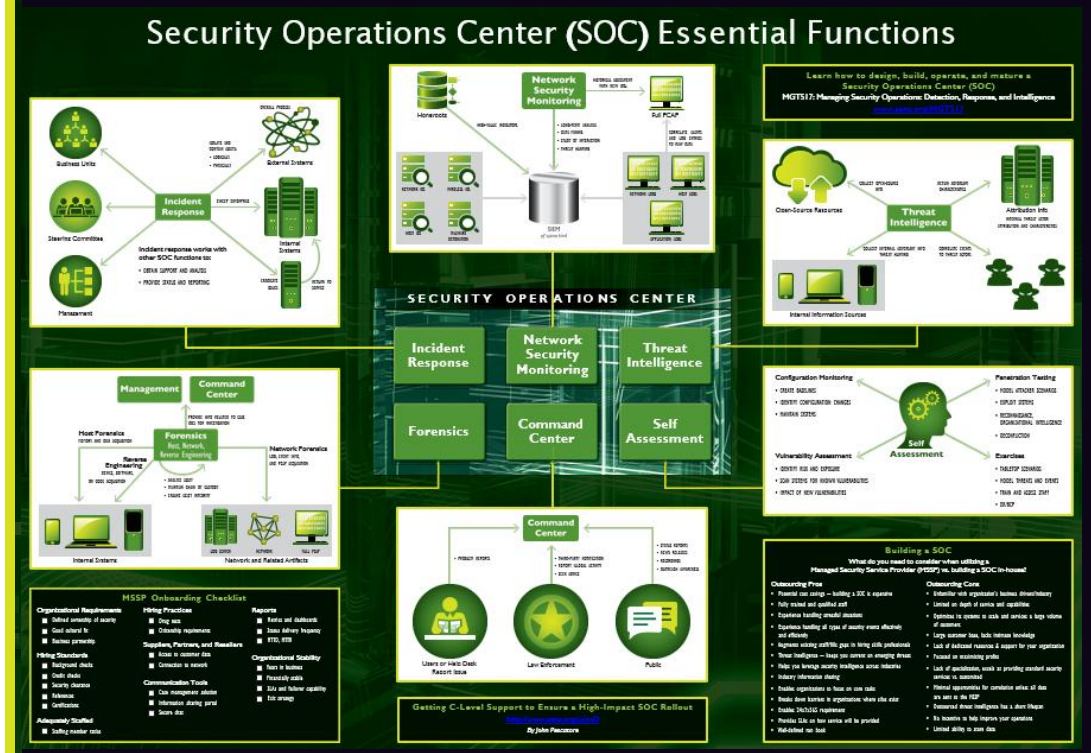
Preparación ante Brechas de Seguridad

Establece medidas para minimizar daños en caso de intrusión

Ejercicios de Simulación

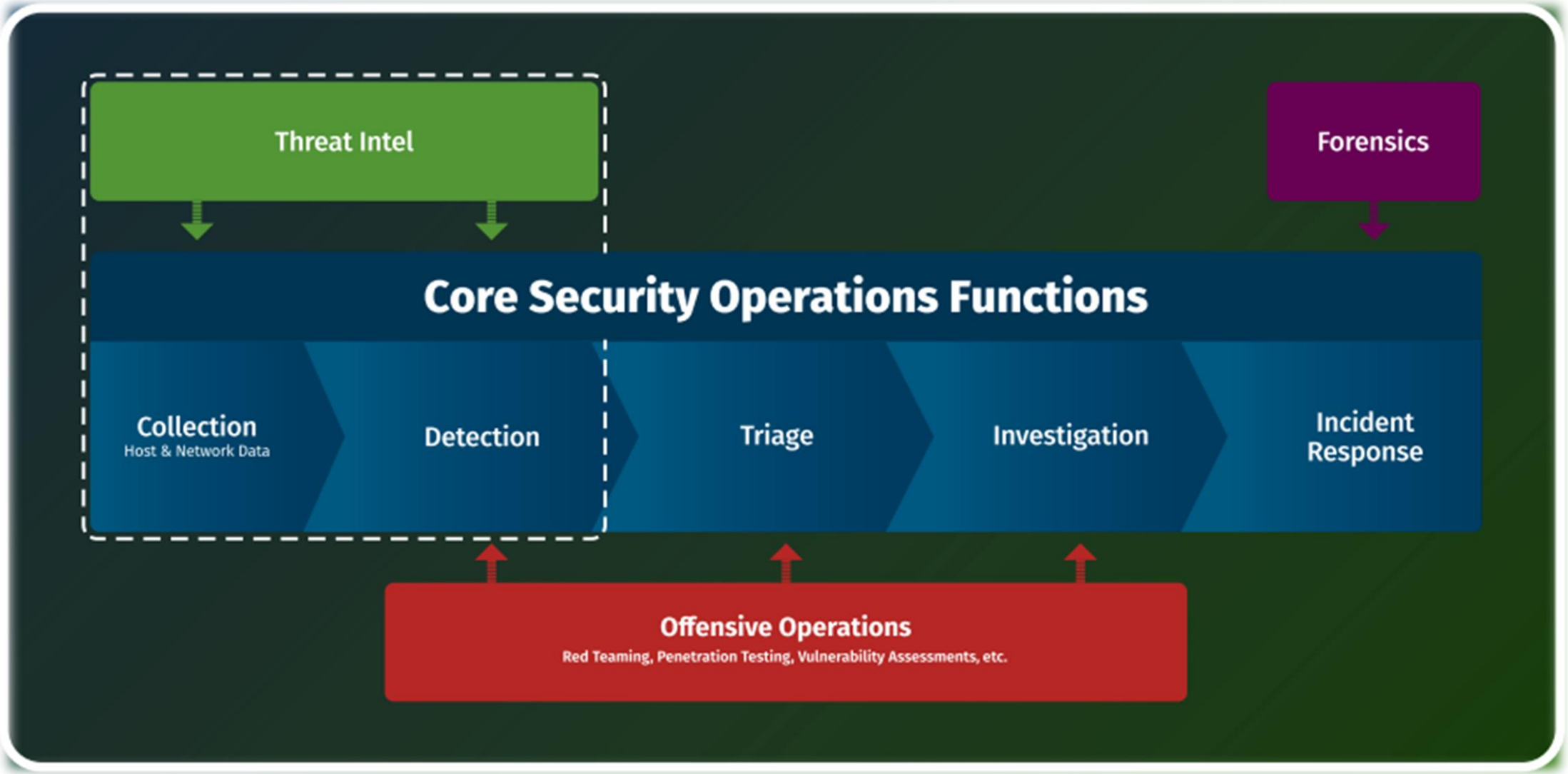
Entrena equipos con escenarios de ciberataques





2

Incident Response


Threat Intel
Forensics
Core Security Operations Functions
Collection
Host & Network Data
Detection
Triage
Investigation
Incident Response
Offensive Operations
Red Teaming, Penetration Testing, Vulnerability Assessments, etc.

COMPONENTES CLAVE I

Aislar Activos

Limitar la propagación de la amenaza

Contener Amenazas

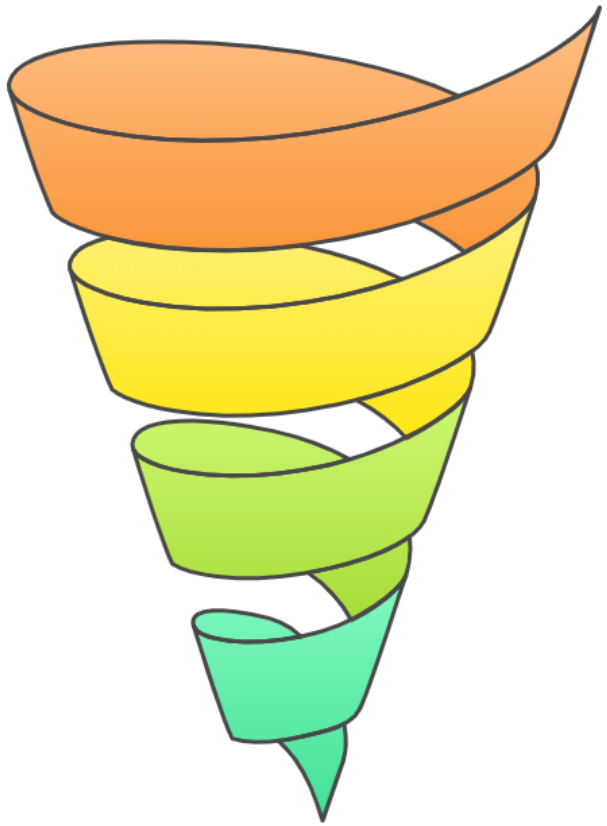
Implementar medidas de contención

Erradicar Problemas

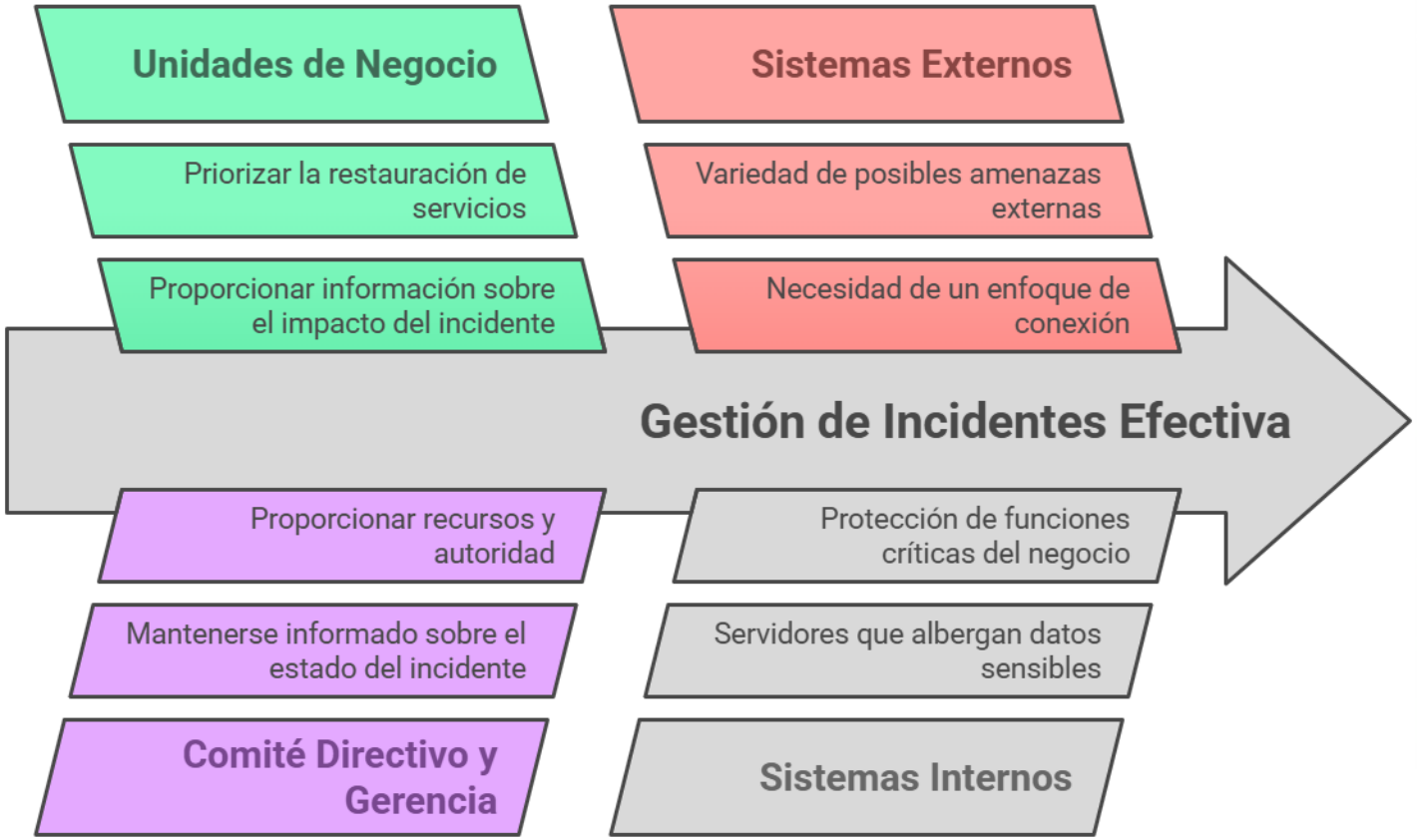
Eliminar amenazas completamente

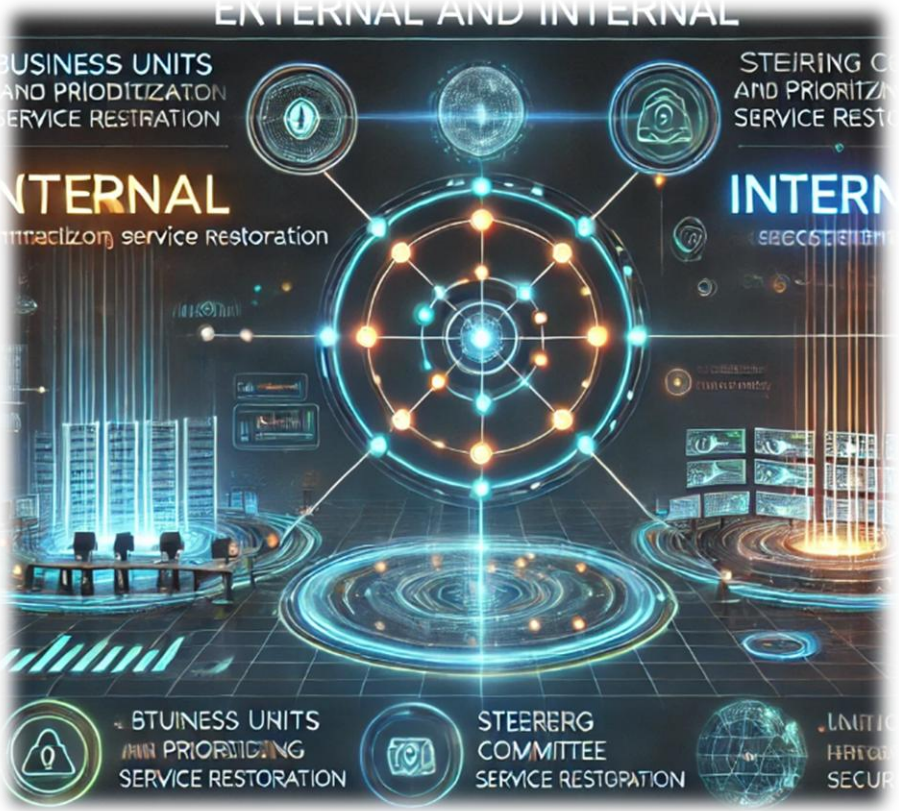
Retornar al Servicio

Restaurar operaciones normales



COMPONENTES CLAVE II





IMPLICACIONES PARA UN CISO

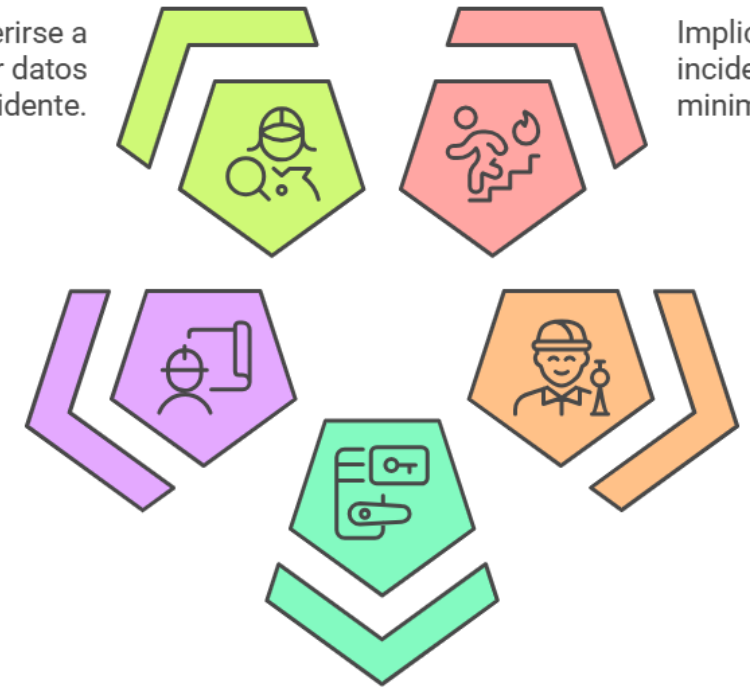
Elementos Clave para una Estrategia de Seguridad Integral

Cumplimiento y Forense

Abarca adherirse a regulaciones y analizar datos post-incidente.

Respuesta a Incidentes

Implica manejar y mitigar incidentes de seguridad para minimizar el impacto.



Arquitectura de Seguridad

Involucra diseñar sistemas y estructuras de seguridad robustos.

Monitoreo de Seguridad

Se centra en la vigilancia continua para detectar y responder a amenazas.

Protección de Datos

Asegura la confidencialidad, integridad y disponibilidad de los datos.

Referencias

SANS Institute. (2018). *Security Operations Center (SOC) Essential Functions*. SANS. Recuperado de https://www.sans.org

Hubbard, J. (2023). *Guide to security operations*. SANS Institute. https://www.sans.org/

DALL-E. (2025). *An infographic summarizing the key elements and activities needed to develop a cybersecurity strategy*. OpenAI.

DALL-E. (2025). *A comprehensive infographic representing a wider range of cybersecurity elements and activities*. OpenAI.

DALL-E. (2025). *An image depicting a group of professionals simulating the activities of a Chief Information Security Officer (CISO) in a modern cybersecurity operations setting*. OpenAI.

Preguntas

@EsdegCol

Escuela Superior de Guerra

Escuela Superior de Guerra

Escuela Superior de Guerra

www.esdegue.edu.co

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

Gracias

@EsdegCol

Escuela Superior de Guerra

Escuela Superior de Guerra

Escuela Superior de Guerra

www.esdegue.edu.co