CTIC UNI

# UNIVERSIDAD NACIONAL DE INGENIERÍA

## OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

### Programa de Iniciación Tecnológica PIT - 2025

# *CERTIFICADO*

**Otorgado a**

## GENESIS ELIZABETH ALARCON CONSEPCION

**Por haber aprobado el curso de**

**CIBERSEGURIDAD: CYBERSOC (C|CS)**

**Realizado del 15 de enero al 03 de febrero del presente, con una duración de 16 horas**

Lima, febrero de 2025

**Mag. Ing. Rubén Arturo Borja Rosales**
**JEFE OTI - UNI**

**N° Certificado: 017 - 0007459**

FIRMA DIGITAL

Firmado digitalmente por: BORJA ROSALES Ruben Arturo FAU 20169004359 hard
Motivo: En señal de conformidad
Fecha: 21/02/2025 17:09:40-0500

# UNIVERSIDAD NACIONAL DE INGENIERÍA

## OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

CTIC UNI

**Temario del Curso:**

### CIBERSEGURIDAD: CYBERSOC (C|CS)

1. Introducción al SOC y Seguridad Informática
   - Componentes básicos del SOC
   - Conceptos básicos de ciberseguridad
   - Configuración básica de un SIEM (ejemplo: Splunk o Elastic Security)
   - Análisis de logs básicos: eventos del sistema operativo o red (DNS, HTTP, logs de firewall)
2. Detección de amenazas y respuesta ante incidentes
   - Indicadores de compromiso
   - Técnicas de detección: Correlación de eventos en el SIEM. Reglas de detección (YARA, Sigma).
   - Impacto y probabilidad (matriz de criticidad)
   - Creación de alertas en el SIEM.
   - Gestión de incidentes
   - Simulación de incidentes
   - Introducción al Análisis Forense Digital
   - Proceso de Análisis Forense
   - Herramientas de Análisis Forense
   - Análisis Forense en Casos Reales
3. Threat Intelligence
   - Definición de Threat Intelligence
   - Fuentes Abiertas (OSINT)
   - Ciclo de vida de Threat Intelligence
   - Aplicación de Threat Intelligence

**Nota final:** **20 (Veinte)**

**N° Certificado: 017 - 0007459**