CTIC UNI

# UNIVERSIDAD NACIONAL DE INGENIERÍA

## OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

### Programa de Iniciación Tecnológica PIT - 2025

# *CERTIFICADO*

**Otorgado a**

## RONY HAROLD CCENCHO TIPISMANA

**Por haber aprobado el curso de**

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

**Realizado del 05 de mayo al 18 de junio del presente, con una duración de 16 horas.**

Lima, julio de 2025

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

**N° Certificado: 017 - 0058893**

FIRMA DIGITAL

Firmado digitalmente por: BORJA ROSALES Ruben Arturo FAU 20169004359 hard
Motivo: En señal de conformidad
Fecha: 08/07/2025 09:36:53-0500

# UNIVERSIDAD NACIONAL DE INGENIERÍA

## OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

CTIC UNI

### Temario del Curso:

### CIBERSEGURIDAD: CYBERSOC (C|CS)

- 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).
- Detección de amenazas y respuesta ante incidentes (PARTE 1)
- Indicadores de compromiso
- Técnicas de detección
- Correlación de eventos en el SIEM.
- Reglas de detección (YARA, SIGMA).
- Detección de amenazas y respuesta ante Incidentes (PARTE 2)
- Impacto y probabilidad (matriz de criticidad).
- Creación de alertas en el SIEM.
- Gestión de incidentes
- Simulación de incidentes
- Análisis forense (PARTE 1)
- Introducción al Análisis Forense Digital
- Proceso de Análisis Forense
- Análisis forense (PARTE 2)
- Herramientas de Análisis Forense
- Análisis forense en casos reales
- Threat Intelligence
- Definición de Threat Intelligence
- Fuentes abiertas (OSINT)
- Ciclo de vida de Threat Intelligence
- Aplicación de Threat Intelligence

**Nota final:** **16 (Dieciseis)**

**N° Certificado: 017 - 0058893**