

	UNIVERSIDAD DE CALDAS	
	FORMATO PARA CREACIÓN – MODIFICACIÓN DE ACTIVIDADES ACADÉMICAS	
	CÓDIGO: R-1202-P-DC-503	VERSIÓN: 3

PLAN INSTITUCIONAL DE ACTIVIDAD ACADÉMICA

I. IDENTIFICACIÓN

Facultad que ofrece la Actividad Académica:	CIENCIAS EXACTAS Y NATURALES		
Departamento que ofrece la Actividad Académica:	FÍSICA		
Nombre de la Actividad Académica:	CIBERSEGURIDAD EN ENTORNOS INDUSTRIALES		
Código de la Actividad Académica:			
Versión del Programa Institucional de la Actividad Académica (PIAA):	1		
Acta y fecha del Consejo de Facultad para: aprobación____ modificación____	Acta No. ____ Fecha: _____		
Programas a los que se le ofrece la Actividad Académica (incluye el componente de formación al cual pertenece):			
Actividad Académica abierta a la comunidad:	Si ____ No <u>X</u> __		
Tipo de actividad: Teórica ____ Teórico - Práctica <u>X</u> __ Práctica _____			
Horas teóricas:	32	Horas prácticas:	16
Horas presenciales:	48	Horas no presenciales:	96
Horas presenciales del docente:	48	Relación Presencial/No presencial:	1:1
Horas inasistencia con las que se reprueba:	5	Cupo máximo de estudiantes:	25
Habilitable (Si o No):	SI	Nota aprobatoria:	3
Créditos que otorga:	3	Duración en semanas:	16

Requisitos (escribir los códigos y el nombre de las actividades académicas que son requisitos, diferenciados por programas para el caso de una actividad académica polivalente):

II.JUSTIFICACIÓN: describe las razones por las cuales es importante la actividad académica desde la perspectiva del conocimiento, el objeto de formación del programa, el perfil profesional del egresado(s), y su lugar en el currículo.

La creciente interconexión de los sistemas de control industrial (ICS) y las tecnologías operativas (OT) con las redes de tecnología de la información (IT) en el marco de la Industria 4.0 y 5.0 ha incrementado exponencialmente la superficie de ataque y la vulnerabilidad de los entornos productivos a ciberamenazas. Un incidente de ciberseguridad en un entorno industrial puede tener consecuencias catastróficas, incluyendo la interrupción de la producción, daños a equipos costosos, riesgos para la seguridad de los operarios, impacto ambiental y pérdida de propiedad intelectual. Esta asignatura es esencial para que los especialistas en Industria 5.0 y Automatización Industrial comprendan los riesgos específicos de estos entornos, las normativas aplicables y las estrategias de defensa en profundidad necesarias para diseñar, implementar y mantener sistemas industriales seguros y resilientes, protegiendo la continuidad del negocio y la integridad de los activos críticos.

III.OBJETIVOS: describe en forma clara lo que se pretende con el desarrollo de la actividad académica.

Desarrollar competencias para identificar, analizar y mitigar los riesgos de ciberseguridad en sistemas de control industrial (ICS/OT), aplicando normativas, arquitecturas y tecnologías de protección específicas para garantizar la seguridad y resiliencia de los entornos industriales automatizados

2. Específicos:
 1. Identificar las principales amenazas y vulnerabilidades de ciberseguridad en entornos industriales conectados.
 2. Comprender los principios de protección de redes industriales y sistemas de control automatizado (SCADA, PLC, DCS).
 3. Aplicar estrategias de ciberseguridad y protocolos de seguridad en la gestión de redes IoT y dispositivos industriales conectados.
 4. Evaluar los marcos regulatorios y normativas de ciberseguridad en la industria y su implementación en sistemas industriales.
 5. Desarrollar planes de mitigación de riesgos y recuperación ante desastres cibernéticos en entornos industriales.

NOTA: en el caso que el Programa Institucional de la Actividad Académica (PIAA) se desarrolle por competencias, es necesario completar los siguientes aspectos, en lugar de objetivos:

IV.COMPETENCIAS: describe actuaciones integrales desde saber ser, el saber hacer y el saber conocer, para identificar, interpretar, argumentar y resolver problemas del contexto con idoneidad y ética.

1. Genéricas

- Pensamiento Crítico y Analítico: Capacidad para evaluar vulnerabilidades y el impacto potencial de ciberamenazas en sistemas industriales complejos.
- Resolución de Problemas Orientada a la Seguridad: Habilidad para desarrollar e implementar soluciones efectivas para prevenir, detectar y responder a incidentes de ciberseguridad en OT.
- Adaptabilidad Tecnológica: Disposición para aprender y aplicar nuevas tecnologías y metodologías de ciberseguridad en un campo en rápida evolución.
- Ética y Responsabilidad Profesional: Compromiso con la protección de activos críticos y la seguridad de las operaciones industriales, actuando con integridad.

2. Específicas

C1 (Ídem RA3 del programa): Implementar estrategias y medidas de ciberseguridad para proteger sistemas y datos en entornos industriales automatizados y conectados.

- (Sub-competencias específicas de la asignatura):
 - Identificar y clasificar amenazas y vulnerabilidades en sistemas ICS/OT.
 - Aplicar los principios de marcos normativos como ISA/IEC 62443 y NIST CSF en escenarios industriales.
 - Diseñar e implementar segmentación de red y controles de acceso en arquitecturas OT.
 - Configurar y gestionar tecnologías de defensa como firewalls industriales, IDS/IPS para OT.
 - Desarrollar y evaluar planes de respuesta a incidentes y de recuperación para sistemas OT.

COMPETENCIAS GENÉRICAS: describen el conjunto de conocimientos, habilidades, destrezas y actitudes que le permiten al egresado del programa interactuar en diversos contextos de la vida profesional.

COMPETENCIAS ESPECÍFICAS: describen los comportamientos observables que se relacionan directamente con la utilización de conceptos, teorías o habilidades, logrados con el desarrollo del contenido de la Actividad Académica.

V. RESULTADOS DE APRENDIZAJE (RA): cada asignatura debe contener resultados de aprendizaje particulares, siempre articulados con los generales de cada programa. Los RA de una asignatura pueden tributar a varios RA generales, y no necesariamente hay una relación uno a uno.

- **RA1 (Contribuye al RA1 del programa):** Analizar los principios de la Industria 5.0 y el rol de la ciberseguridad como tecnología clave para la resiliencia de entornos industriales específicos, identificando las particularidades de las amenazas en OT.

- **RA2 (Contribuye al RA2 y RA3 del programa):** Diseñar arquitecturas de red industrial seguras, aplicando estándares como ISA/IEC 62443 y seleccionando controles técnicos apropiados (firewalls, IDS/IPS para OT) para proteger la conectividad de sistemas IIoT y automatizados.
- **RA3 (Corresponde al RA3 del programa):** Implementar estrategias y medidas de ciberseguridad, incluyendo la configuración de herramientas de protección y el desarrollo de políticas, para proteger sistemas y datos en entornos industriales automatizados y conectados.
- **RA4 (Contribuye al RA4 del programa):** Utilizar herramientas de monitorización y análisis de eventos de seguridad (ej. SIEM básico) para la detección temprana de incidentes y la mejora de la postura de seguridad en procesos industriales.
- **RA5 (Contribuye al RA5 del programa):** Proponer planes de respuesta a incidentes y de continuidad del negocio específicos para entornos OT, considerando la colaboración humano-máquina en la gestión de la ciberseguridad y la sostenibilidad operativa.

/. **CONTENIDO:** describe los temas y subtemas que se desarrollarán en la actividad académica. Estos deben estar en perfecta coherencia con los objetivos, método y evaluación de la asignatura y con los perfiles de formación de los programas a los que se ofrece la actividad académica.

Módulo 1: Fundamentos de Ciberseguridad en Sistemas de Control Industrial (ICS/OT)

- Introducción a los ICS/OT: PLC, SCADA, DCS, IIoT.
- Diferencias y convergencia IT/OT en ciberseguridad.
- Panorama de amenazas: malware industrial (Stuxnet, Industroyer, Triton), ransomware, ataques a la cadena de suministro, amenazas internas.
- Vulnerabilidades comunes en protocolos industriales (Modbus, DNP3, S7, OPC).
- Impacto de los ciberataques en la seguridad física, la producción y el medio ambiente.
- Modelo Purdue de arquitectura de referencia para ICS.

Módulo 2: Marcos de Referencia, Normativas y Gestión de Riesgos en Ciberseguridad OT

- Estándar ISA/IEC 62443: Conceptos fundamentales, zonas y conductos, niveles de seguridad (SL), requisitos de seguridad.
- NIST Cybersecurity Framework (CSF) aplicado a OT.
- Análisis y gestión de riesgos en entornos OT: identificación de activos, evaluación de amenazas y vulnerabilidades, evaluación de impacto.
- Desarrollo de un Programa de Gestión de Ciberseguridad para OT (CSMS).
- Roles y responsabilidades en la ciberseguridad industrial.

Módulo 3: Controles Técnicos y Arquitecturas Seguras para OT

- Defensa en profundidad y arquitecturas de red OT seguras.
- Segmentación de red: firewalls industriales, data diodes, zonas desmilitarizadas (DMZ) industriales.
- Sistemas de Detección de Intrusiones (IDS) y Prevención de Intrusiones (IPS) para OT.

- Monitorización de la seguridad en OT: Network Security Monitoring (NSM), SIEM en OT.
- Hardening de dispositivos ICS: PLCs, HMIs, estaciones de ingeniería, servidores SCADA.
- Gestión segura de identidades y accesos (IAM) en OT: control de acceso basado en roles, gestión de contraseñas, autenticación multifactor.
- Seguridad en el acceso remoto y la gestión de proveedores.
- Protección de endpoints en el entorno industrial.
- Criptografía y su aplicación en protocolos industriales seguros (ej. OPC UA Security).

Módulo 4: Respuesta a Incidentes, Resiliencia y Futuro de la Ciberseguridad OT

- Plan de Respuesta a Incidentes de Ciberseguridad (CSIRP) para OT: preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas.
- Forense digital en entornos industriales (consideraciones especiales).
- Planes de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP) para OT.
- Cultura de ciberseguridad y programas de concienciación para personal de planta y de IT.
- Ciberseguridad en la cadena de suministro OT (Supply Chain Risk Management).
- Inteligencia de amenazas (Threat Intelligence) para OT.
- Aplicación de IA y Machine Learning en la ciberseguridad OT.
- Desafíos de la ciberseguridad en IIoT y la Industria 5.0.

- /.
- METODOLOGÍA:** describe las estrategias educativas, métodos, técnicas, herramientas y medios utilizados para el desarrollo del contenido, en coherencia con los objetivos o competencias.

- Clases Teórico-Expositivas Interactivas (Virtual Sincrónico Viernes / Presencial Sábado): Presentación de conceptos, marcos normativos, arquitecturas de referencia y tecnologías. Se utilizarán ejemplos reales, estudios de caso de incidentes y se promoverá la discusión sobre los desafíos actuales en ciberseguridad OT.
- Demostraciones y Talleres Prácticos (Presencial Sábado / Entornos Virtualizados):
- Configuración de reglas en firewalls (simulados o emulados).
- Uso de herramientas de análisis de tráfico de red (ej. Wireshark con dissectores para protocolos industriales) para identificar anomalías.
- Prácticas de hardening de sistemas operativos y aplicaciones comunes en OT (sobre máquinas virtuales).
- Simulación de ataques básicos y aplicación de contramedidas en laboratorios virtuales de ciberseguridad OT.
- Análisis de Casos de Estudio (Virtual Sincrónico / Presencial): Estudio en profundidad de incidentes de ciberseguridad industrial relevantes (ej. Ucrania

Power Grid, Oldsmar Water Plant), analizando el vector de ataque, las vulnerabilidades explotadas, el impacto y las lecciones aprendidas.

- Aprendizaje Basado en Problemas/Proyectos (Grupales, desarrollo continuo): Los estudiantes trabajarán en equipos para:
- Realizar una evaluación de riesgos simplificada para un escenario industrial propuesto.
- Diseñar una arquitectura de red segura aplicando principios de ISA/IEC 62443.
- Desarrollar un borrador de un plan de respuesta a incidentes para un sistema OT.
- Uso de Plataformas de Aprendizaje y Entornos Virtualizados: Se utilizará el Campus Virtual (Moodle) para materiales, foros, y se explorará el uso de plataformas de laboratorios virtuales (ej. Cyber Ranges si están disponibles, o entornos construidos con GNS3, Docker, máquinas virtuales con software SCADA/PLC de prueba).

I. **CRITERIOS GENERALES DE EVALUACIÓN:** describe las diferentes estrategias evaluativas, con valoraciones cuantitativas y reportes cualitativos, si son del caso, que se utilizarán para determinar si el estudiante ha cumplido con lo propuesto como objetivos o como competencias de la Actividad Académica. Ver reglamento estudiantil y política curricular.

- **Participación y Discusiones Técnicas (Virtual y Presencial): 15%**
 - Evaluación de la calidad de las contribuciones en debates sobre normativas, análisis de amenazas, y soluciones de seguridad.
- **Informes de Laboratorio y Talleres Prácticos (Individual/Grupal): 30%**
 - Calificación de los informes de prácticas de configuración de seguridad, análisis de tráfico, y ejercicios en entornos virtualizados, evaluando la correcta aplicación de técnicas y herramientas.
- **Análisis de Casos y Evaluación de Riesgos (Individual/Grupal): 25%**
 - Evaluación de la capacidad para analizar incidentes de ciberseguridad industrial, identificar causas raíz, y proponer medidas correctivas y preventivas. Evaluación de la aplicación de metodologías de análisis de riesgos a escenarios OT.
- **Proyecto Final Grupal (Propuesta de Solución de Ciberseguridad OT): 30%**
 - Desarrollo y presentación de un proyecto que aborde un desafío de ciberseguridad en un entorno industrial simulado o basado en un caso real (ej. diseño de arquitectura segura, plan de respuesta a incidentes detallado, evaluación de conformidad con ISA/IEC 62443 para un

sistema). Se evaluará la profundidad técnica, la aplicabilidad y la coherencia de la propuesta.

- I. **REFERENCIAS BIBLIOGRÁFICAS:** describe los textos guía, manuales, fuentes primarias, páginas de Internet, entre otras, que serán utilizadas para el desarrollo de la Actividad Académica.

- ISA/IEC 62443 Series of Standards. Security for industrial automation and control systems. ISA/IEC.
- NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (CSF).
- NIST SP 800-82 Rev. 2. (2015). Guide to Industrial Control Systems (ICS) Security.
- Langner, R. (2018). Robust Control System Networks: How to Achieve Reliable Control After Stuxnet. De Gruyter.
- Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
- Kim, D., & Solomon, M. G. (2016). Fundamentals of Information Systems Security. Jones & Bartlett Learning.
- Dragos Inc. Year in Review Reports y Resources. (dragos.com)
- SANS Institute. ICS Security Resources & Whitepapers. (sans.org/industrial-control-systems-security)
- Cybersecurity and Infrastructure Security Agency (CISA). ICS Advisories & Resources. (cisa.gov/ics)
- Artículos y blogs de expertos en ciberseguridad OT (ej. Dale Peterson, Joe Weiss).