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

**PLAN INSTITUCIONAL DE ACTIVIDAD ACADÉMICA**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **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 \_X\_     No \_\_\_\_ | |
|  | | | | |
| Tipo de actividad:  Teórica \_\_X\_                 Teórico - Práctica \_\_\_                                     Práctica \_\_\_\_\_ | | | | |
| Horas teóricas: | 48 | Horas prácticas: | | N/A |
| Horas presenciales: | 48 | Horas no presenciales: | | 64 |
| Horas presenciales del docente: | 48 | Relación Presencial/No presencial: | | 1:2 |
| Horas inasistencia con las que se reprueba: | 5 | Cupo máximo de estudiantes: | | 40 |
| Habilitable (Si o No): | SI | Nota aprobatoria: | | 3 |
| Créditos que otorga: | 3 | Duración en semanas: | | 3 |
|  |  |  | |  |
| 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): | | | | |
|  | | | | |
|  | | | | |
| 1. **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 ciberseguridad es un elemento crítico en el contexto de la **Industria 5.0**, donde la interconexión de dispositivos mediante el **Internet de las Cosas (IoT)** y la integración de sistemas automatizados presentan nuevos desafíos de seguridad. A medida que las fábricas y sistemas industriales se digitalizan y automatizan, el riesgo de ataques cibernéticos y vulnerabilidades aumenta significativamente. Este curso tiene como objetivo preparar a los profesionales para identificar, prevenir y mitigar riesgos de ciberseguridad en entornos industriales, asegurando la protección de datos, redes, sistemas de control y dispositivos conectados. El conocimiento en ciberseguridad es esencial para garantizar la continuidad operativa, la integridad de los procesos automatizados, y la protección de la infraestructura crítica de las industrias. | | | | |
|  | | | | |
| 1. **OBJETIVOS**: describe en forma clara lo que se pretende con el desarrollo de la actividad académica. | | | | |
| Desarrollar en los estudiantes las competencias necesarias para identificar, gestionar y mitigar los riesgos de ciberseguridad en entornos industriales automatizados, garantizando la integridad, disponibilidad y confidencialidad de los sistemas de control y redes industriales. | | | | |
| 1. Específicos: 2. Identificar las principales amenazas y vulnerabilidades de ciberseguridad en entornos industriales conectados. 3. Comprender los principios de protección de redes industriales y sistemas de control automatizado (SCADA, PLC, DCS). 4. Aplicar estrategias de ciberseguridad y protocolos de seguridad en la gestión de redes IoT y dispositivos industriales conectados. 5. Evaluar los marcos regulatorios y normativas de ciberseguridad en la industria y su implementación en sistemas industriales. 6. 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:     1. **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  * Capacidad de resolución de problemas: Desarrollar habilidades para identificar y resolver problemas de ciberseguridad en entornos industriales complejos. * Pensamiento crítico: Analizar y evaluar los riesgos cibernéticos desde una perspectiva estratégica y técnica, implementando soluciones innovadoras. * Trabajo en equipo: Colaborar con equipos multidisciplinarios para diseñar e implementar políticas y medidas de seguridad cibernética. | | 1. Específicas  * Gestión de riesgos de ciberseguridad: Capacidad para evaluar y gestionar riesgos asociados a ciberataques en redes industriales y dispositivos conectados. * Implementación de soluciones de seguridad: Habilidad para implementar protocolos de seguridad en entornos de automatización industrial (IoT, SCADA, PLC). * Monitoreo y respuesta ante incidentes cibernéticos: Competencia para desarrollar estrategias de monitoreo, detección y respuesta ante ataques cibernéticos en tiempo real. * Cumplimiento normativo: Conocimiento sobre las regulaciones y normativas de ciberseguridad aplicadas a entornos industriales, garantizando el cumplimiento de estándares internacionales. |   **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. | | | | |
| 1. **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: Introducción a la Ciberseguridad en Entornos Industriales (10 horas)**   * Conceptos fundamentales de ciberseguridad en la Industria 5.0 * Principales amenazas y vulnerabilidades en sistemas industriales * Impacto de los ciberataques en la infraestructura crítica   **Módulo 2: Redes Industriales y Sistemas de Control Automatizado (14 horas)**   * Introducción a redes industriales: SCADA, PLC, DCS * Ciberseguridad en sistemas de automatización y control * Seguridad en dispositivos IoT conectados en la industria * Protocolos de seguridad y cifrado en redes industriales   **Módulo 3: Estrategias y Tecnologías de Ciberseguridad (12 horas)**   * Firewalls, detección de intrusiones y prevención de ataques * Seguridad en la nube aplicada a entornos industriales * Monitoreo y auditoría de redes industriales * Análisis de amenazas en tiempo real   **Módulo 4: Gestión de Incidentes y Recuperación (12 horas)**   * Planes de contingencia y recuperación ante desastres cibernéticos * Desarrollo de un plan de respuesta ante incidentes (IRP) * Evaluación y mitigación de riesgos en redes industriales * Cumplimiento normativo y estándares de ciberseguridad (ISO/IEC 27001, NIST) | | | | |
|  | | | | |
| 1. **METODOLOGÍA**: describe las estrategias educativas, métodos, técnicas, herramientas y medios utilizados para el desarrollo del contenido, en coherencia con los objetivos o competencias. | | | | |
| * Clases magistrales interactivas: Explicación de los conceptos y fundamentos de ciberseguridad, complementadas con estudios de casos prácticos de ataques en entornos industriales. * Estudio de casos reales: Análisis de ciberataques en redes industriales y evaluación de las medidas de respuesta aplicadas, permitiendo a los estudiantes comprender el impacto y las soluciones implementadas. * Talleres prácticos: Simulaciones de ataques cibernéticos y configuración de soluciones de seguridad en sistemas industriales conectados (redes SCADA, IoT). * Proyectos en equipo: Desarrollo de proyectos donde los estudiantes diseñen y apliquen políticas de ciberseguridad en un entorno industrial simulado, con evaluación de | | | | |
| 1. **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 en clases y talleres:** 20% Evaluación de la participación activa en las discusiones y simulaciones prácticas de ciberseguridad.  **Estudio de casos:** 25% Análisis crítico de casos reales de ciberseguridad industrial y presentación de soluciones propuestas.  **Talleres prácticos:** 25% Realización y entrega de talleres donde los estudiantes apliquen soluciones a problemas de seguridad en redes industriales.  **Proyecto final grupal:** 30% Desarrollo de un proyecto en equipo para implementar una política de ciberseguridad en un entorno industrial, evaluando los riesgos y diseñando medidas de protección. | | | | |
| 1. **REFERENCIAS BIBLIOGRÁFICAS:** describe los textos guía, manuales, fuentes primarias, páginas de Internet, entre otras, que serán utilizadas para el desarrollo de la Actividad Académica. | | | | |
|  | | | | |
|  | | | | |
| * Stallings, W. (2018). Cryptography and Network Security: Principles and Practice. Pearson. * Industrial Internet Consortium. (2016). Industrial Internet Security Framework. * Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication. * Green, J. (2020). IoT Security Issues: Securing Industrial Control Systems. Wiley. * Bayuk, J. (2012). Cybersecurity Policy Guidebook. John Wiley & Sons. | | | | |