**Propuesta de tesis**

Este documento contiene una propuesta de tesis que está siendo ofrecida a los nuevos estudiantes de doctorado del Programa de Doctorado en Ciencias de la Computación por un profesor UNIR que es miembro del programa. Esperamos que la propuesta de investigación resulte de interés para algunos de los estudiantes que solicitan admisión al programa. Un estudiante de doctorado no tiene por qué atenerse a las propuestas publicadas, sino que tiene libertad para designar el tema de investigación del que tratará su tesis. Sin embargo, si durante el proceso de admisión designa una propuesta de tesis publicada, la Comisión Académica valorará esta petición de cara a la asignación de su director de tesis. Además, las propuestas de tesis se desarrollan dentro de grupos y líneas de investigación para la que disponemos de investigadores especializados, que además pueden tener ayudas económicas asociadas. Le recomendamos contactar con el profesor que publica la ayuda para obtener más información sobre esta propuesta.

**Datos de la propuesta**

|  |
| --- |
| **Título** |
| Implementación de las Políticas de seguridad informática en los sistemas productivos |
| **Línea de investigación1** |
| Ciberseguridad |
| **Breve descripción y objetivos** |
| **Breve Descripción**:  En un mundo cada vez más digitalizado, las organizaciones enfrentan desafíos crecientes en materia de seguridad informática. Las amenazas cibernéticas, como ataques de malware, filtración de datos y accesos no autorizados, ponen en riesgo la confidencialidad, integridad y disponibilidad de la información. Esta investigación tiene como propósito analizar, diseñar y optimizar políticas de seguridad informática que permitan proteger los activos digitales de las organizaciones. A través de un enfoque integral, se abordarán buenas prácticas, normas internacionales y estrategias efectivas que contribuyan a la gestión de riesgos y la mitigación de vulnerabilidades. Además, se evaluarán casos de estudio para identificar fortalezas y áreas de mejora en la implementación de políticas de seguridad.  **Objetivos:**  ***Objetivo General:***  Desarrollar políticas de seguridad informática robustas y efectivas que sean implementadas correctamente en los sistemas en producción. Ello permitirá la protección integral de los recursos tecnológicos y la información en entornos organizacionales.  ***Objetivos Específicos***:   1. Identificar amenazas y vulnerabilidades comunes: Analizar los principales riesgos de seguridad informática en distintos sectores productivos. 2. Diseñar políticas de seguridad efectivas: Elaborar lineamientos específicos que incluyan controles técnicos, administrativos y físicos. 3. Incorporar normativas internacionales: Integrar estándares reconocidos, como ISO/IEC 27001 y el RGPD, para garantizar el cumplimiento normativo. 4. Evaluar el impacto de políticas existentes: Realizar estudios de caso para identificar aciertos y fallas en la implementación de políticas de seguridad. 5. Desarrollar estrategias de concienciación: Proponer programas de capacitación que fomenten una cultura de ciberseguridad dentro de las organizaciones.   **Problema a resolver**  En el contexto actual de creciente digitalización y transformación digital, las organizaciones enfrentan múltiples desafíos en torno a la protección de sus sistemas productivos frente a ciberamenazas. Las políticas de seguridad informática adoptadas en muchos sectores productivos resultan insuficientes o ineficaces ante la evolución constante de los ataques cibernéticos, lo que genera vulnerabilidades críticas en la infraestructura tecnológica y pone en riesgo la continuidad operativa y la protección de la información sensible. A pesar de los esfuerzos realizados en la implementación de medidas de seguridad, persisten brechas significativas debido a la falta de actualización de políticas, la adopción incompleta de estándares internacionales y la baja concienciación en materia de ciberseguridad entre los empleados. Además, muchos entornos productivos carecen de un enfoque integral que contemple tanto controles técnicos como administrativos y físicos, lo que aumenta la exposición a incidentes que pueden tener consecuencias económicas, legales y reputacionales. Por lo tanto, el problema central que aborda esta propuesta es la necesidad de revisar y fortalecer las políticas de seguridad informática en los sistemas productivos, garantizando su efectividad frente a amenazas contemporáneas y su alineación con normativas internacionales reconocidas.  **Aportación técnica / ingenieril de la propuesta**  Esta propuesta representa un enfoque técnico integral para el fortalecimiento de la ciberseguridad en sistemas productivos, centrado en el desarrollo de políticas robustas y prácticas efectivas que reduzcan significativamente la vulnerabilidad ante ataques informáticos. La aportación técnica se materializa a través de los siguientes elementos:   1. Desarrollo de Modelos de Seguridad Personalizados: Se propondrán políticas ajustadas a las características específicas de cada entorno productivo, contemplando tanto la infraestructura tecnológica como el perfil de amenazas propias de cada sector. 2. Integración de Normas Internacionales: Se elaborarán guías prácticas que incorporen estándares internacionales como ISO/IEC 27001, NIST CSF y normativas de protección de datos (ej., RGPD), garantizando el cumplimiento legal y la adopción de mejores prácticas. 3. Metodologías de Evaluación de Vulnerabilidades: Se desarrollarán procedimientos para identificar y analizar vulnerabilidades específicas en sistemas productivos, utilizando técnicas de auditoría de seguridad y herramientas automatizadas de análisis de riesgos. 4. Estrategias de Gestión de Riesgos: Se implementarán métodos para la clasificación y priorización de riesgos, promoviendo una toma de decisiones fundamentada en datos que permita maximizar la resiliencia organizativa. 5. Programas de Capacitación en Ciberseguridad: Se diseñarán estrategias educativas para mejorar la conciencia de seguridad entre el personal, lo que permitirá reducir el factor humano como vector de ataque.   Al abordar estos aspectos técnicos de manera integral, esta propuesta contribuirá al establecimiento de un entorno seguro y resiliente frente a ciberamenazas, promoviendo la continuidad operativa y la protección de los activos críticos en sistemas productivos. |
| **Profesor que convoca la propuesta y dirección de contacto** |
| Dr. Sergio Mauricio Martinez Monterrubio. sergiomauricio.martinez@unir.net |
| **Información adicional sobre el profesor/organización que publica** |
| https://investigacion.unir.net/investigadores/818157/ |
| **Potenciales ayudas asociadas a la propuesta** |
|  |

1 Las líneas de investigación a las que están adscritos los miembros del Programa de Doctorado en Ciencias de la Computación están publicadas en la siguiente dirección web https://www.unir.net/ingenieria/doctorado-ingenieria-informatica/