**Logotipo

Descripción generada automáticamenteUNIVERSIDAD TÉCNICA DEL NORTE**

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

**CARRERA DE SOFTWARE**

**ANTEPROYECTO DE TRABAJO DE INTEGRACIÓN CURRICULAR**

**DATOS GENERALES**

|  |  |
| --- | --- |
| 1. TEMA: Desarrollo de un sistema de seguimiento del proceso del control interno de compras públicas de la empresa AIRMAXTELECOM S.A aplicando Practicas de codificación Segura OWASP (*Open Web Application Security Project*) Top Ten. | |
| 1. ÁREA / LÍNEA DE INVESTIGACIÓN:   Línea de Investigación Carrera de Software: Desarrollo, aplicación de software y cyber security (seguridad cibernética).  Sublínea de Investigación Carrera de Software: Ingeniería de Software y Seguridad Informática. | |
| 1. ENTIDAD QUE AUSPICIA:   Ing. Andres Benavides. | |
| 1. DIRECTOR DE TRABAJO DE TITULACIÓN:   Director: Ing. Mauricio Rea  Especialista: . | |
| 1. PERTINENCIA DEL PROYECTO:   Desarrollo de una aplicación web aplicando Practicas de codificación Segura OWASP (*Open Web Application Security Project*). | |
| 1. AUTOR: Sr. Salazar Anrango Mario Andrés   DIRECCIÓN: El Tejar - Ibarra  TELÉFONO: 0994532438  CORREO ELECTRÓNICO: [masalazara@utn.edu.ec](mailto:masalazara@utn.edu.ec), [mariosalazar.ms.10@gmail.com](mailto:mariosalazar.ms.10@gmail.com) | |
| 1. DURACIÓN (Estimado): 6 meses | |
| 1. INVESTIGACIÓN: Nueva ([X]) Continuación ([ ]) | |
| 1. PRESUPUESTO (Estimado): $ 1.200,00 | |
| PARA USO DEL CONSEJO ACADÉMICO | |
| FECHA DE ENTREGA: | FECHA DE REVISIÓN: |
| APROBADO: SI ( ) NO ( ) | FECHA DE APROBACIÓN: |
| OBSERVACIONES: | |
|  | |

**Logotipo

Descripción generada automáticamente UNIVERSIDAD TÉCNICA DEL NORTE**Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

**CARRERA DE SOFTWARE**

**PLAN DEL ANTEPROYECTO DE TRABAJO DE INTEGRACIÓN CURRICULAR**

|  |  |
| --- | --- |
| **Propuesto por:**  Ing. Andrés Benavides | **Áreas Técnicas del Tema:**   * Ingeniería del Software * Ingeniería Web * Seguridad Informática |
| **Director sugerido:**  [nombre del director sugerido] | **Fecha:**  26/09/2024 |

|  |
| --- |
| 1. **Tema**   Desarrollo de un sistema de seguimiento del proceso del control interno de compras públicas de la empresa AIRMAXTELECOM S.A aplicando Practicas de codificación Segura OWASP (*Open Web Application Security Project*) Top Ten. |
| 1. **Planteamiento del Problema**   Actualmente las vulnerabilidades y ataques cibernéticos existen a gran escala a diferentes sitios web, según (García, 2024) en 2023 se identificaron aproximadamente 28778 vulnerabilidades en las aplicaciones web, es decir son propensos a ataques cibernéticos, esto significa que los desarrolladores de software no aplicaron o no se enfocaron en el desarrollo con buenas prácticas en el proceso de desarrollo del sistema.  Los activos más importantes de una organización empresarial son los datos e información que se manipula en diferentes procesos, no obstante, se encuentran expuestos a vulnerabilidades y ataques cibernéticos por el hecho de que no se aplica un protocolo de desarrollo de software en los sistemas, que garantice la seguridad de la información. Según el Foro Económico mundial(World  Economic Forum, 2023) tan solo el 4% de las organizaciones se encuentran con la protección ante los ataques, además, cabe recalcar que el 74% las vulnerabilidades y la inseguridad de la información son por factores del error humano.  En 2021 los ataques cibernéticos a los sitios web tanto en procesos públicos y privados se situaron en el quinto lugar como uno de los riesgos más altos, y con la posibilidad que para el 2025 se duplique los ataques cibernéticos de IT. De acuerdo con (Norman, 2024)el 78 % de los expertos en la seguridad de la Tecnologías de la Información carecen de protección pese a las inversiones que se realizan, el 62.7 % de las empresas tienden a creer que un factor de aumento de los ataques fue debido a la pandemia COVID-19 (Henríquez et al., 2021).  Con el inicio de la pandemia a causa del COVID-19, muchas organizaciones cambiaron a un modelo de trabajo remoto, el cual hizo depender de sistemas basados en internet. Esta dependencia dejo un espacio abierto para los hackers y se produjo un aumento en los ciber ataques, las principales vulnerabilidades y amenazas en los sitios web son: ataques de inyección SQL, programación Cross-Site (XSS), ataque de fuerza bruta a las credenciales, ataques DoS/DDoS, redirecciones y reenvíos no validos (Bommaraju, 22022).  En América Latina aproximadamente el 56 % de los ciberataques están dirigidos a países como Brasil, México, Colombia y Ecuador, estos ataques están destinados a las entidades bancarias, a los sectores y áreas del gobierno y finanzas, teniendo como un resultado de 7160 ataques por día, llevando a un promedio de 5 intentos por minuto (Bianchi, 2024). por otra parte, Appgate (Redacción Portal ERP Latam, 2024) en un estudio realizado en 2023 menciona que los ataques cibernéticos crecen en un 60% en América Latina, estos estudios realizados son con el informe anual de Fraud Beat Report.  Los analistas del Centro de Operaciones de Seguridad (SOC) de Appgate monitorearon las tendencias en 2023, revelando que el 74% de los incidentes de fraude se originaron por ataques de phishing, convirtiéndose en la técnica más utilizada por los ciberdelincuentes. El segundo tipo de ataque más frecuente fue el uso no autorizado de marcas registradas, representando el 17% de los casos. Por último, la divulgación de información constituyó el 9% del total de los incidentes registrados (Appgate, 2023), en la Figura 1 se muestra los 3 ataques principales:  A red circle with numbers and text  Description automatically generated  Figura 1: Top 3 Attacks Types in 2023 según (Appgate, 2023).  En el ámbito local, en Ecuador, se han registrado 3.183 delitos informáticos entre 2020 y julio de 2022. Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay son las provincias más afectadas. La estafa en línea es el delito más frecuente, impulsado por el mayor acceso a Internet y redes sociales, con el 79,21% de la población conectada (El Comercio, 2022). Este panorama de creciente ciberdelincuencia ha puesto de relieve la necesidad de proteger la información sensible en los procesos de contratación y compras públicas.  Para afrontar de manera efectiva las vulnerabilidades y amenazas es durante el proceso de desarrollo de software y todo su ciclo de vida a través de buenas prácticas de programación que recomienda OWASP (*Open Web Application Security Project*), teniendo en cuenta las 10 vulnerabilidades más frecuentes que sufren las aplicaciones según (Van Der Stock et al., 2024), así como también, realizar procesos de análisis y evaluación de riesgos.  En la actualidad, la empresa AIRMAXTELECOM S.A. no cuenta con un sistema de control interno para gestionar las compras públicas, lo que genera riesgos operativos y de seguridad. La información que se maneja en estos procesos incluye datos sensibles que podrían ser vulnerables a accesos no autorizados o ataques externos si no se implementan medidas de protección adecuadas. Un sistema eficiente de control y seguimiento del proceso de compras públicas permitirá:   * Centralizar la gestión de compras y optimizar los procedimientos internos. * Proteger la información sensible mediante la implementación de prácticas de desarrollo seguro OWASP. * Prevenir pérdidas financieras y fraudes ocasionados por vulnerabilidades en los sistemas actuales.   La integridad, confidencialidad y disponibilidad de la información son elementos clave para garantizar la continuidad operativa de AIRMAXTELECOM S.A. Implementar un sistema con arquitectura limpia y prácticas de codificación segura permitirá establecer controles efectivos para minimizar riesgos, aumentar la eficiencia operativa, y asegurar que los procesos se alineen con los estándares de seguridad internacionales.  La relevancia de garantizar la seguridad en los procesos de compras públicas en Ecuador ha sido resaltada por iniciativas como la capacitación organizada por el Servicio Nacional de Contratación Pública (SERCOP), enfocada en la prevención de delitos informáticos. Este tipo de delitos, como la apropiación fraudulenta por medios electrónicos, no solo vulneran la integridad de la información, sino que también afectan la transparencia de los procesos públicos. La adopción de herramientas y prácticas de seguridad es fundamental para evitar amenazas que comprometan los sistemas de contratación. La implementación de un sistema de control interno seguro en empresas como AIRMAXTELECOM S.A., que maneja información sensible, permitirá prevenir estos riesgos y alinearse con los estándares de protección promovidos por instituciones gubernamentales, garantizando así la confidencialidad, integridad y disponibilidad de los datos manejados (SERCOP, 2021).  La importancia de fortalecer los sistemas de control en los procesos de compras públicas se evidencia en las acciones del Servicio Nacional de Contratación Pública (SERCOP), que, en 2022 y 2023, presentó 43 denuncias y 10 nuevas acusaciones por presuntos delitos, como falsificación de documentos, sobreprecio y ataques a la integridad de los sistemas informáticos. Estas denuncias subrayan la necesidad de asegurar la transparencia e integridad en la contratación pública y de cumplir con la normativa vigente para evitar actos de corrupción que comprometen los recursos públicos y la eficiencia del Estado (SERCOP, 2023). Por ello, implementar un sistema de control interno seguro en la empresa Airmax Telecom Soluciones Tecnológicas S.A. no solo mitigará riesgos, sino que también alineará la gestión con los principios de transparencia promovidos por las instituciones nacionales.  Dada esta realidad, AIRMAXTELECOM S.A. se beneficiaría al implementar un sistema de control interno que refuerce la seguridad de sus procesos de contratación pública, asegurando así la confidencialidad, integridad y disponibilidad de la información, en cumplimiento con los estándares internacionales de seguridad y transparencia.  En la siguiente Figura 2 se puede observar el árbol de problemas de la ausencia de un sistema automatizado de control para el proceso de compras públicas:    Figura : Árbol de problemas |
| 1. **Objetivos**  Objetivo General Desarrollar un sistema de seguimiento del proceso de control interno de compras públicas de la empresa AIRMAXTELECOM S.A., aplicando Practicas de Codificación Segura OWASP para garantizar la integridad, confidencialidad y disponibilidad de la información. Objetivos Específicos Realizar una investigación descriptiva de los procesos de compras públicas, Arquitectura Limpia y las Prácticas de Codificación Segura OWASP.  Diseñar e implementar un sistema seguro de control de compras públicas mediante una arquitectura limpia, basado en las prácticas de codificación segura OWASP.  Evaluar la efectividad del sistema de control y seguimiento utilizando herramientas que provee OWASP para verificar que las medidas de seguridad, autentificación, protección contra vulnerabilidades y cifrado cumplan con los estándares de OWASP. |
| 1. **Alcance**   El objetivo principal de este proyecto es mitigar las vulnerabilidades ante ataques cibernéticos mediante el desarrollo de un sistema de control y seguimiento para los procesos de compras públicas de la empresa Airmax Telecom Soluciones Tecnológicas S.A. El sistema aplicará buenas prácticas de programación OWASP, centrándose en tres puntos específicos que son los siguientes:  **A01:2021 - Pérdida de Control de Acceso:** Esta categoría menciona que representa el mayor riesgo en aplicaciones web, lo que evidencia su relevancia para cualquier sistema crítico, como el que desarrollo en este proyecto. La alta frecuencia de ocurrencias (318.000) y el hecho de que el 3,81% de las aplicaciones evaluadas presenten al menos una debilidad en esta área refuerzan la necesidad de implementar controles estrictos de acceso en el sistema de control interno (Van Der Stock et al., 2024).  **A02:2021 - Fallas Criptográficas:** Esta categoría es fundamental, ya que la correcta implementación de mecanismos criptográficos es crucial para garantizar la confidencialidad de la información en procesos de compras públicas. La exposición de datos confidenciales sigue siendo una amenaza latente, y el enfoque en fallas de criptografía permite mitigar riesgos relacionados con el compromiso del sistema, alineándose con los principios de OWASP a aplicarse.  **A03:2021 - Inyección:** La elección de esta categoría se debe a que las inyecciones, especialmente SQL, siguen siendo una amenaza relevante en sistemas que manejan grandes volúmenes de datos. Según OWASP, el 94% de las aplicaciones probadas han presentado vulnerabilidades de este tipo, esto demuestra la importancia de proteger el sistema contra inyecciones, evitando así posibles accesos no autorizados o manipulación maliciosa de datos sensibles en el contexto del proceso de compras públicas de AIRMAXTELECOM S.A.  Para llevar a cabo este proyecto, se llevará a cabo durante 6 fases:  **Fase 1:** Análisis de los procesos de compras públicas y levantamiento de requisitos.  El propósito de esta fase es identificar las necesidades del sistema y las áreas de automatización en el proceso actual, por ende, para cumplir este propósito se llevará actividades de revisión documentos normativos y procedimientos internos mediante entrevistas y reuniones con los stakeholders. Además, se realiza el levantamiento de los requerimientos funcionales y no funcionales donde el entregable de esta fase es el documento de especificación de requisitos con casos de uso y flujos del proceso.  **Fase 2:** Diseño de la arquitectura del sistema y modelo de datos.  Esta fase tiene como objetivo definir la estructura del sistema y el manejo eficiente de la información mediante el diseño de la arquitectura del sistema y el diseño del modelo de datos. La arquitectura para aplicarse es la Arquitectura Limpia (Clean Architecture) para separar las capas del sistema (controladores, servicios, repositorios) y así, facilitar la escalabilidad y mantenibilidad del proyecto, Prácticas de Codificación Segura OWASP y se realizara la definición de las tablas y las relaciones entre entidades (ERD), en esta fase los entregables son la documentación de la arquitectura del sistema y el diagrama de modelado de datos.  **Fase 3:** Desarrollo de los módulos funcionales y de seguridad.  Esta fase tiene el propósito de desarrollar las funcionalidades del sistema identificados garantizando la seguridad y rendimiento, los módulos principales a realizar son: el módulo de seguridad y el módulo de control y seguimiento de las compras públicas utilizando las herramientas de Spring Boot para el backend de los servicios de Seguimiento y Autentificación, NodeJS para el servicio de notificaciones, React para el frontend. Los entregables de esta fase es el prototipo del sistema con los módulos funcionales y de seguridad.  **Fase 4:** Pruebas y evaluación de la efectividad del sistema.  El propósito de esta etapa es asegurar que el sistema funcione correctamente y que las medidas de seguridad implementadas sean efectivas. Las actividades para realizar son las pruebas funcionales, pruebas de seguridad y pruebas de rendimiento; validando cada módulo para asegurar que cumpla con los requisitos, simulando ataques para detectar vulnerabilidades y hacer uso de herramientas de pruebas de rendimiento. El entregable de esta fase es un informe detallado del resultado de las pruebas y sus acciones correctivas.  **Fase 5:** Implementación de los módulos funcionales y de seguridad.  El objetivo en esta fase es poner en funcionamiento el sistema en un entorno de producción mediante la instalación en los servidores de la empresa, migración de los datos, verificación post implementación para comprobar que todo funcione correctamente en el entorno real, por consiguiente, los entregables para esta fase es el sistema y validado en el entorno de producción.  **Fase 6:** Capacitación a los usuarios y entrega final.  En la fase final tiene el propósito de asegurar que los usuarios puedan usar el sistema de manera eficiente mediante actividades de capacitación o entrenamiento para el personal operativo y los administradores del sistema, además se entregara el manual del usuario final y la documentación técnica para el departamento de TI (Tecnologías de la Información), el entregable final es el sistema en producción y usuarios capacitados para su uso.  En el desarrollo de la aplicación web se utilizará las siguientes herramientas que se muestra en la Figura 2:  A diagram of a computer program  Description automatically generated with medium confidence  Figura : Esquema del alcance del proyecto   1. **Metodología**   En el desarrollo de este proyecto se utilizarán diferentes tipologías de investigación. La investigación documental se empleará para recopilar información sobre cómo es el proceso de control y seguimiento de compras públicas. Se realizará una investigación descriptiva para analizar en detalle los procedimientos actuales y principalmente las Buenas Prácticas de Codificación de OWASP. Asimismo, se aplicará una investigación cuantitativa para procesar los resultados obtenidos tras implementar OWASP Top Ten. Finalmente, se realizará una investigación aplicada para representar los resultados y asegurar el correcto funcionamiento del sistema, garantizando la mantenibilidad, escalabilidad y seguridad de la información frente a posibles ataques que puedan comprometer el rendimiento y la integridad de los usuarios.  Para cumplir con el primer objetivo, se llevará a cabo un estudio y revisión sobre los procesos de control y seguimiento de las compras públicas en la empresa Airmax Telecom Soluciones Tecnológicas S.A., así como la aplicación de las Buenas Prácticas de Codificación de OWASP. La metodología utilizada será la Revisión Sistemática de Literatura (SLR) para recopilar, analizar y describir múltiples trabajos de investigación de forma sistemática.  Para alcanzar el segundo objetivo, se desarrollará una aplicación web (frontend) utilizando la metodología de desarrollo en cascada. Esta aplicación permitirá gestionar el control y seguimiento del proceso de compras públicas de la Empresa Airmax Telecom Soluciones Tecnológicas S.A, el mismo que tendrá la protección y seguridad ante las vulnerabilidades y ataques por terceros cumpliendo con los estándares según OWASP Top Ten. Además, se aplicarán técnicas de demostración práctica para ejemplos del funcionamiento del sistema, así como la descripción y explicación del proceso de desarrollo y seguridad aplicada.  Para lograr el cuarto objetivo, se evaluará la efectividad de control y seguimiento mediante estudio de casos reales o ejemplos prácticos de como el sistema resuelve las situaciones, también mediante el uso de herramientas como OWASP SAP para verificar las medidas de seguridad, autentificación y protección ante vulnerabilidades para garantizar los estándares de OWASP.  En la Figura 6 se muestra el esquema de la metodología de investigación:A diagram of a diagram  Description automatically generated  Figura : Esquema de la metodología de investigación |
| 1. **Justificación**   El desarrollo de este proyecto es esencial para optimizar y asegurar los procesos de control interno de compras públicas en la empresa Airmax Telecom Soluciones Tecnológicas S.A. Actualmente, la ausencia de un sistema eficaz existe vulnerabilidades que ponen en riesgo la integridad, disponibilidad y confidencialidad de la información, afectando la toma de decisiones y el cumplimiento normativo.  En un entorno cada vez más digitalizado, la automatización y control de procesos críticos es fundamental para mejorar la eficiencia operativa y reducir los errores manuales. Además, la adopción de prácticas de codificación segura OWASP responde a la necesidad de proteger la información frente a amenazas cibernéticas, garantizando que los datos sensibles se gestionen de manera segura.  Este proyecto también promoverá mantenibilidad y escalabilidad mediante la aplicación de Arquitectura Limpia (Clean Architecture) y los principios SOLID, facilitando futuras mejoras y la adaptación a los cambios organizacionales o normativos. Desde una perspectiva social y alineada con los Objetivos de Desarrollo Sostenible (ODS), el proyecto contribuye al ODS 9: Industria, Innovación e Infraestructura, al incorporar tecnología moderna para fortalecer los procesos empresariales. Además, fomenta la transparencia y eficiencia en las compras públicas, promoviendo la confianza tanto interna como externa hacia la empresa. En particular, el proyecto se enfoca en la meta 9.1 del ODS, en desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad para apoyar el desarrollo económico y el bienestar humano (United Nations, 2023).  En resumen, la implementación de este sistema no solo permitirá controlar, gestionar y dar seguimiento efectivo a las compras públicas, sino que también garantizará que los procesos sean seguros, eficientes y preparados para enfrentar los desafíos tecnológicos actuales y futuros.  **Justificación Tecnológica**  El desarrollo de este proyecto se fundamenta en la necesidad de adoptar soluciones tecnológicas robustas y modernas que permian optimizar los procesos de control interno de compras públicas en la Empresa Airmax Telecom Soluciones Tecnológicas S.A, motivando a la innovación en el desarrollo de software. Al aplicar tecnologías de diceno como la Arquitectura Limpia (Clean Architecture) nos permite un sistema modular que facilita el mantenimiento, la escalabilidad y la incorporación de futuras mejoras sin la necesidad de afectar las funcionalidades ya existentes.  Al hacer la Aplicación de Practicas OWASP Top 10 con respecto a la seguridad, la incorporación de estándares internacionales fortalece la protección contra vulnerabilidades comunes como inyecciones SQL, cross-site scripting (XSS) y problemas de autentificación, junto con la implementación de mecanismos de cifrados de encriptación y control de acceso asegura la confidencialidad de los datos, mientras que el control de acceso garantiza que solo los usuarios autorizados interactúen con información sensible, es decir, la ciberseguridad es fundamental para evitar ataques y proteger la integridad de los datos durante el ciclo de compras (Villamagua, 2023).  En conclusión, la justificación tecnológica de este proyecto radica en la necesidad de adoptar soluciones no solo que optimicen los procesos de control, sino que también aseguren eficiencia, seguridad y capacidad de crecimiento a futuro. El uso de prácticas modernas de desarrollo y estándares de seguridad OWASP garantiza un sistema sostenible y alineado con las demandas de la tecnología actual.  **Justificación Organizacional**  El sistema web permitirá un seguimiento más eficiente en el proceso de compras públicas, evitando retrasos y aportando en la toma de decisiones mediante la optimización de los procesos internos, así también, la automatización del control interno reduce los riesgos de errores humanos en la gestión de control y seguimiento, asegurando un flujo constante y monitoreo de actividades  **Justificación Social.**  El desarrollo e implementación de un sistema de control en el proceso de compras públicas aplicando Buenas Prácticas de Codificación OWASP se debe a la importancia de la transparencia en la gestión pública, garantiza la confianza de los usuarios y promueve a la protección y seguridad de información sensible, evitando posibles vulneraciones que podrían afectar a los ciudadanos y proveedores que interactúan con la entidad.  **Justificación Académica**  El desarrollo del proyecto permitirá validar la efectividad e importancia de aplicar las Buenas Prácticas de Codificación OWASP, Arquitectura Limpia y principios SOLID en sistemas reales, por ende, este trabajo podría servir como una guía para proyectos futuros en el ámbito de seguridad de la información y desarrollo de software seguro, modular y mantenible, siendo una referencia para futuras investigaciones.  **Justificación Legal**  En el ámbito legal es fundamental que un sistema garantice el cumplimiento de regulaciones, ya que la implementación del sistema asegura que la organización cumpla con las normativas vigentes relacionadas con la protección de datos sensibles; un sistema eficiente ayuda a detectar y evitar prácticas corruptas o mal usos de los recursos públicos mediante la prevención de actos ilícitos, por consiguiente, al cumplir con los estándares de ciberseguridad, se reduce el riesgo de incumplimientos normativos y sanciones.  **Riesgos**  A continuación, en la Tabla 1. se describe los diferentes tipos de riesgos existentes y las respectivas estrategias de mitigación para el proceso de desarrollo del proyecto:   |  |  |  | | --- | --- | --- | | **Nro.** | **Riesgo** | **Estrategia de Mitigación** | | **R1** | No conocer a fondo los ataques cibernéticos a información sensible. | Estudiar y realizar una investigación de las vulnerabilidades más comunes en los sistemas. | | **R2** | Falta de experiencia en nuevas tecnologías pueden generar retrasos. | Capacitación acerca del uso de las tecnologías y realizar pruebas piloto. | | **R3** | Cambios constantes en los requisitos pueden generar confusión y retrasos. | Realizar reuniones claras del levantamiento de requisitos con los stakeholders desde el inicio. | | **R4** | Falta de compromiso del equipo o stakeholders. | Mantener una comunicación y revisión contante de los avances a los stakeholders. | | **R5** | Asignación excesiva de tareas puede llevar a un desgaste y afectar a la continuidad. | Distribuir las actividades de manera realista en concordancia a las actividades del desarrollador. | | **R6** | Resistencia al cambio podría hacer inviable el uso del sistema. | Involucrar a los usuarios en el proceso y brindar capacitación adecuada. |   En la Figura. 7 se representa la matriz de riesgos:  A chart with different colored squares  Description automatically generated  Figura : Matriz de Riesgos |
| 1. **Contexto**  |  |  |  | | --- | --- | --- | | Contexto local, nacional e internacional en base a tesis, trabajos o investigaciones realizadas: | | | | **INVESTIGACIÓN** | **ENLACE** | **APORTE** | | **Contexto:** Local  Título de la investigación y cita |  |  | | **Contexto:** Local  Título de la investigación y cita |  |  | | **Contexto:** Nacional  Título de la investigación y cita |  |  | | **Contexto:** Nacional  Título de la investigación y cita |  |  | | **Contexto:** Internacional  Título de la investigación y cita |  |  | | **Contexto:** Internacional  Título de la investigación y cita |  |  | |
| 1. **Contenidos** [Es una guía para la preparación del trabajo escrito, del contenido mismo del proyecto. En el formulario para la presentación del Plan del Proyecto, se exige consignar al menos los capítulos que contendrá el reporte escrito, los que deben tener íntima relación con los objetivos específicos. Cualquier cambio posterior en el temario, que no afecte los objetivos y alcance del proyecto, deberá comunicarse por escrito y recibir la aprobación del Coordinador de Carrera]   **INTRODUCCIÓN**  Antecedentes  Situación actual  Planteamiento del Problema  Objetivos  Alcance y Metodología  Justificación y Riesgos  Contexto  **CAPÍTULO I: MARCO TEÓRICO**   * 1. Tema 1.   2. Tema 2.   3. Tema 3.   4. Tema 4.   **CAPÍTULO II: DESARROLLO**   * 1. Tema 1.   2. Tema 2.   3. Tema 3.   4. Tema 4.   **CAPÍTULO III: RESULTADOS**   * 1. Tema 1.   2. Tema 2.   3. Tema 3.   4. Tema 4.   **CONCLUSIONES Y RECOMENDACIONES**  Conclusiones  Recomendaciones  **REFERENCIAS Y BIBLIOGRAFÍA**  Bibliografía  **ANEXOS** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Cronograma de Actividades.** [Se deben señalar las diferentes etapas o actividades del proyecto y el tiempo estimado para cada una de ellas. Mediante la gráfica de Gantt se establece una relación entre actividad y tiempo de ejecución.] | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Nro. | Nombre de tarea | Duración | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | | MES 5 | | | | MES 6 | | | | |
| 1 | Tema: Título del trabajo de grado | **días** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | **INTRODUCCIÓN** | **12 días** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Antecedente | 2 días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Situación actual | 2 días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Planteamiento del Problema | 2 días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | Objetivos | 2 días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | Alcance y Metodología | 2 días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 8 | Justificación y Riesgos | 1 día |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 9 | Contexto | 1 día |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 | **CAPÍTULO I: MARCO TEÓRICO** | **20 días** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11 | 1.1 Tema 1. | 5 días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12 | 1.2 Tema 2. | 5 días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 13 | 1.3 Tema 3. | 5 días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 14 | 1.4 Tema 4. | 5 días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 15 | **CAPÍTULO II: DESARROLLO** | **∑n días** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 16 | 2.1 Tema 1. | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 17 | 2.2 Tema 2. | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 18 | 2.3 Tema 3. | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 19 | 2.4 Tema 4. | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 20 | **CAPÍTULO III: RESULTADOS** | **∑n días** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 21 | 3.1 Tema 1. | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 22 | 3.2 Tema 2. | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 23 | 3.3 Tema 3. | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 24 | 3.4 Tema 4. | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 25 | **CONCLUSIONES Y RECOMENDACIONES** | **∑n días** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 26 | Conclusiones | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 27 | Recomendaciones | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 28 | **REFERENCIAS Y BIBLIOGRAFÍA** | **∑n días** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 29 | Bibliografía | n días |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 30 | **ANEXOS** | **∑n días** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Presupuesto** [Detallar el presupuesto a ser utilizado y de existir el financiamiento explicar si es personal o de alguna institución o empresa auspiciante. Anexar carta de auspicio económico de la entidad requirente.]  |  |  | | --- | --- | | **DESCRIPCION** | **COSTO ESTIMADO** | | HARDWARE |  | |  | $0.000,00 | |  | $0.000,00 | | SOFTWARE |  | |  | $0.000,00 | |  | $0.000,00 | | TALENTO HUMANO |  | |  | $0.000,00 | |  | $0.000,00 | | MATERIALES DE OFICINA |  | |  | $0.000,00 | |  | $0.000,00 | | INVESTIGACION |  | |  | $0.000,00 | |  | $0.000,00 | | **SUBTOTAL** | **$0.000,00** | | **10% IMPREVISTOS** | **$0.000,00** | | **TOTAL** | **$0.000,00** |  1. **Bibliografía.**   Appgate. (2023). *Fraud Beat Annual Report 2023*.  Bianchi, T. (2024, May 22). *Most targeted countries by cyber attacks Latin America 2020 | Statista*. https://www.statista.com/statistics/818412/latin-american-countries-highest-share-cyber-attacks/  Bommaraju, C. (22022, May 16). *Las 5 principales vulnerabilidades y amenazas de los sitios web que debemos tener en cuenta durante la pandemia*. https://www.nisum.com/es/nisum-knows/top-5-website-vulnerabilities-and-threats-to-look-out-for-during-the-pandemic  El Comercio. (2022, July 25). *3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020 - El Comercio*. https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html  García, J. (2024, March 14). *Estadísticas de Ciberseguridad: Pronóstico para el 2024*. https://www.deltaprotect.com/blog/estadisticas-de-ciberseguridad-pronostico-2024  Henríquez, B., Guzmán, P., Gutiérrez, N., & Tiznado, V. (2021). *Status of the Remote Work Cybersecurity Landscape*.  Norman, G. (2024, May 13). *30 Computer Security Statistics*. https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica  Redacción Portal ERP Latam. (2024, May 23). *Preocupación empresarial en Latam por ciberataques: Appgate | Latam*. https://latam.portalerp.com/preocupacion-empresarial-en-latam-por-ciberataques-appgate  SERCOP. (2021). *El combate a los delitos informáticos es parte de la estrategia de transparencia en la compra pública – Servicio Nacional de Contratación Pública*. https://portal.compraspublicas.gob.ec/sercop/el-combate-a-los-delitos-informaticos-es-parte-de-la-estrategia-de-transparencia-en-la-compra-publica/  SERCOP. (2023). *SERCOP presentó 10 nuevas denuncias por posibles delitos en procesos de contratación pública – Servicio Nacional de Contratación Pública*. https://portal.compraspublicas.gob.ec/sercop/sercop-presento-10-nuevas-denuncias-por-posibles-delitos-en-procesos-de-contratacion-publica/  United Nations. (2023, August). *Infrastructure and Industrialization - United Nations Sustainable Development*. https://www.un.org/sustainabledevelopment/infrastructure-industrialization/  Van Der Stock, A., Glass, B., Smithline, N., & Gigler, T. (2024). *OWASP Top Ten | OWASP Foundation*. https://owasp.org/www-project-top-ten/  Villamagua, F. (2023). *ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO ANÁLISIS, DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL FORTALECIMIENTO DE VULNERABILIDADES E INTEGRIDAD DE APLICACIONES WEB ACADÉMICAS JIMMY FERNANDO RAMÍREZ MÁRQUEZ*.  World  Economic Forum. (2023). *State of the  Connected World 2023 Edition*. |

|  |  |  |
| --- | --- | --- |
| DIRECTOR DE TRABAJO DE TITULACIÓN |  | ASESOR DE TRABAJO DE TITULACIÓN |
| Nombre Director  [C.I. \_director] |  | [Nombre Asesor]  [cédula\_Asesor] |

|  |  |
| --- | --- |
|  | ESTUDIANTE Sr. Mario Andrés Salazar Anrango  1003938477 |