ANEXO 1

FORMATO PARA LA PRESENTACIÓN DE PROYECTOS DE INVESTIGACIÓN CON EL FINANCIAMIENTO DEL FEDU

1. Título del proyecto

Ciberseguridad en la detección y respuestas a riesgos en las universidades de la ciudad de Juliaca

2. Área de Investigación

Área de investigación	Línea de Investigación	Disciplina OCDE
Ciencias de la ingeniería	Desarrollo, gestión, seguridad y auditoria de sistemas de información	Ingeniería y tecnología

3. Duración del proyecto (meses)

12 meses

4. Tipo de proyecto

Individual	X
Multidisciplinario	
Director de tesis pregrado	

4. Datos de los integrantes del proyecto

Apellidos y Nombres	TICONA YANQUI FIDEL ERNESTO
Escuela Profesional	INGENIERIA DE SISTEMAS
Celular	951765555
Correo Electrónico	fticona@unap.edu.pe

I. Título (El proyecto de tesis debe llevar un título que exprese en forma sintética su contenido, haciendo referencia en lo posible, al resultado final que se pretende lograr. Máx. palabras 25)

Ciberseguridad en la detección y respuestas a riesgos en las universidades de la ciudad de Juliaca

II. Resumen del Proyecto de Tesis (Debe ser suficientemente informativo, presentando -igual que un trabajo científico- una descripción de los principales puntos que se abordarán, objetivos, metodología y resultados que se esperan**)**

El trabajo de investigación surge de la necesidad de que muchas veces las organizaciones como las universidades sufren de ataques de ciberseguridad, lo cual ocasiona la perdida de información o simplemente el mal funcionamiento del sistema y estos problemas son originados por la falta de conocimiento de los ataques mediante las redes de comunicación o el internet, por lo cual en el trabajo

de investigación se tiene como objetivo reconocer las brechas en materia de ciberseguridad que están relacionadas con la detección y respuesta a los eventos de ciberseguridad en las universidades de la ciudad de Juliaca, el trabajo de investigación es de tipo es de tipo no experimental por que la investigación se concentra en el análisis de las variables de estudio (Hernández Sampieri, Fernández Collado, y Baptista Lucio 2014), también es de tipo transaccional descriptivo porque permite conocer las variables a través de una exploración inicial en un momento especifico de las variables (Horna, A. A. V. 2012). La población estará compuesta por los estudiantes, administrativos y personal docente de las Universidades de Juliaca, para la cual se tomará una muestra aleatoria simple con la finalidad de realizar la investigación. Además, con el presente trabajo de investigación se pretende desarrollar estrategias para evitar los ataques cibernéticos a los sistemas de las universidades de la ciudad de Juliaca.

III. Palabras claves (Keywords) (Colocadas en orden de importancia. Máx. palabras: cinco**)**

Ciberseguridad, esteganografía, owaps, Malware, Keylogger, ransomware, metasploit

IV. Justificación del proyecto (Describa el problema y su relevancia como objeto de investigación. Es importante una clara definición y delimitación del problema que abordará la investigación, ya que temas cuya definición es difusa o amplísima son difíciles de evaluar y desarrollar**)**

El presente trabajo de investigación se justifica debido a que existe la necesidad de proteger la información que se tiene en las universidades y la cual ayuda en la toma de decisiones a los directivos, también es importante mencionar que el internet es una tecnología que tiene muchas ventajas y también tiene una serie de riesgos potenciales en cuanto se refiere a la información.
Es importante que las universidades tomen en cuenta las vulnerabilidades a las que están inmersas debido al uso de redes de comunicación de información, mediante las cuales las personas inescrupulosas podrían vulnerar un sistema, mediante el uso de diferentes técnicas infiltración a la seguridad, como son los Keylogger, ransomware y otras técnicas para ingresar a sistemas y vulnerar su seguridad.
La información es lo mas valioso para las organizaciones y también es considerada como el mayor activo que esta pueda tener, debido a estas características es que en el presente trabajo de investigación se pretende detectar y dar respuesta a los diferentes ataques de seguridad que puede tener una universidad en la ciudad de Juliaca, de tal forma que se pueda desarrollar un plan de ciberseguridad para la organización.
Con el presente trabajo de investigación se beneficiarán las universidades, los directivos, estudiantes y personas que interactúan con la universidad de tal forma que se pueda evitar la vulneración de los sistemas que tienen estas universidades.

V. Antecedentes del proyecto (Incluya el estado actual del conocimiento en el ámbito nacional e internacional. La revisión bibliográfica debe incluir en lo posible artículos científicos actuales, para evidenciar el conocimiento existente y el aporte de la Tesis propuesta. Esto es importante para el futuro artículo que resultará como producto de este trabajo)

(Silva & Gallegos, 2019), En el trabajo de investigación denominado “Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SISC”, El presente trabajo de investigación tuvo por objetivos diagnosticar

el nivel de capacidad en la gestión de la ciberseguridad de la empresa, identificar las brechas para diseñar y proponer los controles claves para fortalecer la ciberseguridad y, por último, elaborar y proponer la hoja de ruta de implementación de los controles clave. Asimismo, se limitó el alcance a los aspectos relacionados a la detección y respuesta de eventos relacionados a la ciberseguridad. Finalmente, no es menos importante mencionar que el presente trabajo supuso un reto por el hecho de aplicar una metodología relativamente nueva dentro del fenómeno –también nuevo- de la ciberseguridad y cómo se le entiende en el marco del uso de la tecnología de la información en el mundo actual.

(Espina Suárez & Gomez Hormaza, 2021), En el trabajo de investigación Denominado "Mitigación de riesgos a través del uso de una arquitectura de ciberseguridad mediante modelamiento de amenazas en la implementación de sistemas de información basados en internet de las cosas", El presente trabajo busca proponer una arquitectura de ciberseguridad para la implementación de dispositivos que hacen uso del Internet Of Things (IoT). La arquitectura tiene una estructura de 3 capas: negocio, aplicaciones y tecnología, donde se describe componentes tales como políticas, servicios y nodos respectivamente. La arquitectura fue validada a través de un ambiente simulado de un sistema para el control y seguimiento del proceso de gestación de mujeres utilizando dispositivos wearables. Los resultados evidencian una reducción del índice de la probabilidad y el impacto de los riesgos en un 14.95% y 6.81% respectivamente.

(Aliaga Yupanqui, 2021), En la investigación titulada "Implementación de un Sistema de Ciberseguridad para la prevención de los Ataques Cibernéticos en la Empresa Radiadores Fortaleza, 2021.", el objetivo general de la presente investigación fue la realización de la implementación de un sistema de ciberseguridad que influye de manera positiva en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021. El modelo de implementación de ciberseguridad que se adoptó en la empresa fue el idóneo porque hay una mejora notable en la defensa de los ataques informáticos y una disminución de las vulnerabilidades que con lleva a un mejor desempeño de negocio de la empresa Radiadores Fortaleza.

(Bruderer Vega, 2019), En la investigación titulada "Diseño de un modelo de ciberseguridad para dispositivos móviles en el sector empresarial", Por esta razón para el presente proyecto de fin de carrera se recopilará información de los estándares de NIST y de la ISO 27032 para elaborar un modelo de ciberseguridad que permita establecer controles para proteger los dispositivos móviles y la información manejada por ellos. En la guía de implementación se encontrará las estructuras de gobierno sugeridas, una lista de amenazas de ciberseguridad para dispositivos móviles y el procedimiento que se seguirá para realizar una evaluación previa para determinar el estado actual de la seguridad de la organización y determinar los controles que faltan implementar para lograr el nivel de protección deseado. Además, al final de la guía se encontrará las actividades recomendadas para implementar controles asociados a las subcategorías. Este modelo ha sido validado a través del juicio experto y además este modelo ha participado en la 11th IADIS International Conference on Information System 2018 en Lisboa, Portugal. (Bruderer, Villena, Tupia, & Bruzza, 2018).

(Bohorquez Salcedo, 2021), En el trabajo de investigación denominado "Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020", tuvo como objetivo principal determinar la relación de la ciberseguridad con la gestión de tecnologías de información en la empresa I & T Electric, Lima - 2020. Para la prueba estadística inferencial de los datos se empleó el coeficiente de correlación Rho de Spearman. La investigación

concluye evidenciándose una correlación de nivel muy fuerte de 0,832 entre la variable Ciberseguridad y la variable Gestión de tecnología de información.

(Ormachea Montes, 2020), En el trabajo de investigación denominado “Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional”, el objetivo de esta investigación es proponer estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad nacional del Perú, 2019. Concluye que, en los indicadores referidos a cooperación regional, bilateral y multilateral, el Perú ha manifestado comportamientos disímiles. El Estado y la sociedad peruana aún transitan por los enfoques de la concientización y del desarrollo de las capacidades cibernéticas militares como indicadores prevalentes en el diseño de las políticas nacionales de ciberseguridad. Aun cuando el liderazgo descanse, en principio, en el Estado, la ciberseguridad constituye un compromiso social que demanda de articulación entre el sector público y el sector privado, lo que en el Perú aún no se concreta. En consecuencia, el diseño de la Estrategia Nacional de Ciberseguridad del Perú constituye una necesidad que demanda ser satisfecha.

(Muedas Higginson & Rojas Velásquez, 2019), El trabajo de investigación denominado “Modelo de madurez de seguridad de aplicaciones web ante ciberataques para clínicas de nivel 2”, El presente proyecto propone un modelo de madurez de seguridad de aplicaciones web ante ciberataques para clínicas de nivel 2 bajo la norma técnica del MINSA, orientada a mostrar las debilidades de las aplicaciones web y las mejoras que se puedan realizar en aspectos de seguridad. El proyecto permitió la implementación de mejoras por parte de las empresas clientes en sus plataformas web mediante la recomendación propuesta por la guía de mejora luego de haber realizado el pentesting propuesto.

(Pérez Navarro & Salcedo Jara, 2021) El trabajo de investigación denominado “Modelo de madurez en ciberseguridad para empresas que manejan datos de salud”, este trabajo se propone un modelo de madurez de capacidades que identifica el grado de fiabilidad de los elementos de Ciberseguridad y Privacidad aplicados al Sector Salud. Esto se realizó mediante la selección de modelos, frameworks y normativas, aumentando su complejidad mediante la integración de capacidades de privacidad y gestión de datos de salud. Los resultados obtenidos se compararon con los componentes originales del modelo para verificar que los componentes se integraron holísticamente. Además, se entregó un formulario de evaluación del modelo a la empresa cliente para comprobar el nivel de satisfacción con respecto al uso del modelo y sus componentes.

(Mansilla Pizarro, 2021) El trabajo de investigación denominado “Implementación de programas de cumplimiento en ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano”, el propósito es de entender la situación problemática planteada, se ha plasmado dentro del presente trabajo, los conceptos clave para lograr un mejor entendimiento del problema de la investigación, además de desarrollar la experiencia en otros países, hecho que además de mostrar la gravedad y el perjuicio ocasionado por un ciberataque, nos permite tener una idea más clara de los aspectos esenciales que pueden ser implementados en nuestro país. Finalmente, considerando que existe la necesidad de implementar un programa de cumplimiento en ciberseguridad en las entidades que forman parte del sistema financiera peruano y que a la fecha no existe ningún tipo de regulación nacional sobre el tema, se pone en consideración los aspectos mínimos que deberán ser implementados en las empresas que forman parte del sistema financiero como parte de la implementación de prácticas de buen gobierno corporativo.

(Cari Arevalo & Lombardi Sánchez, 2020) En el trabajo de investigación denominado “Diseño de una Arquitectura de ciberseguridad para los servicios de plataformas IoT en el área de TI dentro de la empresa Pacífico Seguros”, tiene por objetivo el diseño de una Arquitectura de ciberseguridad para los servicios de plataformas IoT en el área de TI dentro de la empresa Pacífico Seguros. Esta arquitectura se ha basado en el desarrollo del framework NIST alineado a estándares que permite garantizar la ciberseguridad de las plataformas IoT, para ello se ha logrado culminar cada brecha identificada en la evaluación del perfil actual y perfil objetivo mediante un plan de acción, lo cual ha sido alineado a los controles de los estándares ISO 27001 y la ISO 27032. Finalmente, al cubrir cada brecha se ha realizado un plan de recuperación de las plataformas IoT en caso de que sucediera algún evento cibernético que dañe la continuidad y operatividad de las plataformas.

(Taipe Domínguez, 2020) El trabajo de investigación denominado “La auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018”, El desarrollo de la presente investigación tuvo como objetivo analizar cómo el realizar una Auditoria de Seguridad Informática tiene implicancia en la Ciberseguridad en el Sector Público. En lo que refiere a los resultados, se puede señalar que los encuestados manifiestan que el realizar una Auditoria de seguridad informática si tiene implicancia en la Ciberseguridad en el Sector Público año 2018.

(Cáceda Rodríguez, 2021) en el trabajo de investigación denominado “Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación” el trabajo propone desarrollar un modelo dinámico como herramienta de gestión, basado en las técnicas de dinámica de sistemas con la finalidad de mejorar la toma de decisiones estratégicas en seguridad de las organizaciones. Como conclusión el modelo permite gestionar las vulnerabilidades y prevenir ataques bajo diversos escenarios, determinando a través de indicadores de alertas, ataques y vulnerabilidades, si la aplicación del modelo favorece los procesos y protección de los activos de las TIC.

VI. Hipótesis del trabajo (Es el aporte proyectado de la investigación en la solución del problema)

Mediante las brechas detectadas de ciberseguridad se logró dar respuesta a los ataques de seguridad concientizando a los usuarios de los peligros de las redes de comunicación.

VII. Objetivo general

Reconocer las brechas en materia de ciberseguridad que están relacionadas con la detección y respuesta a los eventos de ciberseguridad en las universidades de la ciudad de Juliaca.

VIII. Objetivos específicos

Recopilar la información pertinente para evaluar la capacidad de gestión de la ciberseguridad en las universidades de la ciudad de Juliaca

Analizar las brechas existentes en los procesos de detección y respuesta de incidentes de ciberseguridad en las universidades de la ciudad de Juliaca

Analizar los escenarios de riesgos específicos relacionados a la ciberseguridad

Diseñar y proponer los controles clave de gestión para fortalecer la ciberseguridad en referencia a las brechas identificadas en el diagnóstico ejecutado.

IX. Metodología de investigación (Describir el(los) método(s) científico(s) que se empleará(n) para alcanzar los objetivos específicos, en forma coherente a la hipótesis de la investigación. Sustentar, con base bibliográfica, la pertinencia del(los) método(s) en términos de la representatividad de la muestra y de los resultados que se esperan alcanzar. Incluir los análisis estadísticos a utilizar**)**

El trabajo de investigación es de tipo es de tipo no experimental por que la investigación se concentra en el análisis de las variables de estudio (Hernández Sampieri, Fernández Collado, y Baptista Lucio 2014), también es de tipo transaccional descriptivo porque permite conocer las variables a través de una exploración inicial en un momento especifico de las variables (Horna, A. A. V. 2012). La población estará compuesta por los estudiantes, administrativos y personal docente de las Universidades de Juliaca, para la cual se tomará una muestra aleatoria simple con la finalidad de realizar la investigación.

X. Referencias (Listar las citas bibliográficas con el estilo adecuado a su especialidad)

Aliaga Yupanqui, C. A. (2021). Implementación de un sistema de ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza, 2021. *Repositorio Institucional - UCV*. https://repositorio.ucv.edu.pe/handle/20.500.12692/70776

Bohorquez Salcedo, A. I. (2021). *Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020*. https://renati.sunedu.gob.pe/handle/sunedu/2978422

Cari Arevalo, M., & Lombardi Sánchez, J. A. (2020). Diseño de una arquitectura de ciberseguridad para los servicios de plataformas IoT en el área de TI dentro de la empresa Pacífico Seguros. *Universidad Tecnológica del Perú*. http://repositorio.utp.edu.pe/handle/20.500.12867/3585

Espina Suárez, E. A., & Gomez Hormaza, G. E. (2021). *Mitigación de riesgos a través del uso de una arquitectura de ciberseguridad mediante modelamiento de amenazas en la implementación de sistemas de información basados en internet de las cosas*. https://renati.sunedu.gob.pe/handle/sunedu/3006616

Hernández Sampieri, Roberto, Carlos Fernández Collado, y Pilar Baptista Lucio. 2014. Metodología de la investigación.

Horna, A. A. V. (2012). Desde la idea hasta la sustentación: 7 pasos para una tesis exitosa. Instituto de Investigación de la Facultad de Ciencias Administrativas y Recursos Humanos. Universidad de San Martín de Porres. Lima.

Mansilla Pizarro, D. (2021). *Implementación de programas de cumplimiento en ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano*. https://renati.sunedu.gob.pe/handle/sunedu/2666835

Muedas Higginson, A. C., & Rojas Velásquez, R. G. (2019). *Modelo de madurez de seguridad de aplicaciones web ante ciberataques para clínicas de nivel 2*. https://renati.sunedu.gob.pe/handle/sunedu/3003964

Ormachea Montes, J. F. (2020). *Estrategias Integradas de Ciberseguridad para el Fortalecimiento de la Seguridad Nacional*. https://renati.sunedu.gob.pe/handle/sunedu/1336266

Pérez Navarro, H. B., & Salcedo Jara, H. L. (2021). *Modelo de madurez en ciberseguridad para empresas que manejan datos de salud*. https://renati.sunedu.gob.pe/handle/sunedu/3004121

Silva, L. F. M., & Gallegos, G. R. V. (s. f.). *Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SISC*. 90.

Taipe Domínguez, D. I. (2020). La auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018. *Universidad Nacional de Piura*. http://repositorio.unp.edu.pe/handle/20.500.12676/2361

XI. Uso de los resultados y contribuciones del proyecto (Señalar el posible uso de los resultados y la contribución de los mismos)

El proyecto pretende dar a conocer los riesgos de ciberseguridad que están latentes en las universidades y de esta forma prevenir los ataques a la seguridad de información de estas organizaciones educativas, además permitirá la investigación a las universidades formular estrategias para contar con un plan de acción ante estos posibles ataques por parte de usuarios que pretendan ingresar al sistema de información que tienen las universidades

XII. Impactos esperados

i. Impactos en Ciencia y Tecnología

Mostrar las diferentes formas de ataque a las universidades por parte de personas que quieran vulnerar el sistema de información que estos tengan.

Desarrollar estrategias de ciberseguridad para mitigar la vulnerabilidad al sistema.

ii. Impactos económicos

Evitar gastos en el mantenimiento de los sistemas de información y la reparación de daños provocados por ataques al sistema

iii. Impactos sociales

Fomentar los riesgos a los que los usuarios están propensos en las redes de comunicación y los sistemas de información

iv. Impactos ambientales

Promover el uso adecuado de los sistemas de información y las redes de comunicación.

XIII. Recursos necesarios (Infraestructura, equipos y principales tecnologías en uso relacionadas con la temática del proyecto, señale medios y recursos para realizar el proyecto**)**

Recursos Humanos:
- Analista de seguridad (cantidad 1)
- Programador de sistemas (cantidad 1)

Recursos Físicos:
- Computadora i7 de decima generación (cantidad 1)
- Impresora HP Smart 410 (cantidad 1)
- Cartuchos de tinta (cantidad 1)

Recursos Lógicos:
- Sistema operativo Windows (cantidad 1)
- Sistema operativo Kali Linux (cantidad 1)
- Metasploit (cantidad 1)
- Jupyter (cantidad 1)
- Python (cantidad 1)

Recursos de Escritorio:
- Papeles (2 millares)
- Bolígrafos (una docena)
- Cuadernos (6 cuadernos)

Recurso económico:
- Inversión Inicial S/. 5 000 (seis mil nuevos soles)
- Inversión total S/. 9 350 (once mil cuatro cientos treinta nuevos soles)

XIV. Localización del proyecto (indicar donde se llevará a cabo el proyecto)

Departamento de Puno, Provincia de San Román, Distrito de Juliaca, Universidad Andina Néstor Cáceres Velásquez.

XV. Cronograma de actividades

Actividad	Trimestres											
	E	F	M	A	M	J	J	A	S	O	N	D
Elaboración de proyecto de investigación	X											
Revisión de literatura		X										
Recopilación de información			X	X								
Pruebas de ciberseguridad					X	X						
Planes para mitigar problemas de ciberseguridad							X	X				
Redacción del borrador de trabajo de investigación									X	X		

Presentación del informe final											X	X

XVI. Presupuesto

Descripción	Unidad de medida	Costo Unitario (S/.)	Cantidad	Costo total (S/.)
Analista de seguridad	1 persona	1000	3 meses	3000
Programador de sistemas	1 persona	1000	3 meses	3000
Computadora i7 de decima generación	1 computadora	2000	2000	2000
Impresora HP Smart 410	1 impresora	800	800	800
Cartuchos de tinta	1 Cantidad	200	200	200
Sistema operativo Kali Linux	1 permiso	100	100	100
Sistema operativo Windows	1 permiso	100	100	100
Software Python	1 permiso	50	50	50
Metasploit	1 permiso	50	50	50
Papeles	4 millares	50	50	50