UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima - 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información

AUTOR:

Manrique Reyna, Victor Hugo (ORCID: 0000-0003-1753-4394)

ASESOR:

Dr. Martínez López, Edwin Alberto (ORCID: 0000-0002-0769-1181)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LIMA - PERÚ

2022

DEDICATORIA

dedico con todo mi corazón mi tesis a mi madre, que siempre me acompañado en todos mis caminos y me ha brindado su apoyo y su amor infinito en mis retos y sueños, a mis hermanos que siempre están ahí para apoyarme en todo y a todos mis grandes amigos que no dudaron en expresarme su apoyo.

AGRADECIMIENTO

Agradezco a mi Madre a mis hermanos a toda mi familia, por apoyarme en mis objetivos, gracias a mi universidad por permitirme convertir en un gran profesional, agradezco a mi asesor por su apoyo, a mis maestros a mis compañeros de estudios.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

RESUMEN

La presente investigación tiene como objetivo general proponer un modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un instituto superior tecnológico público, la investigación tiene enfoque cualitativo, el método de la investigación se basó en el paradigma interpretativo, el tipo de investigación fue aplicada y su diseño de investigación acción. Se consultó a tres especialistas en ciberseguridad, los cuales son expertos en el sector de educación superior se utilizó como técnicas de investigación, la entrevista semiestructurada, la observación y el análisis documental.

La implementación de la metodología de Ciberseguridad, permitirá mejorar aspectos de confidencialidad, integridad y disponibilidad en los sistemas de información, mediante controles, políticas y mecanismos de seguridad que deben ser aplicados basado en la Norma ISO/IEC27032 lo cual va permitir que el instituto de educación superior público pase a un nivel de trasformación digital, ser más eficiente sus servicios digitales, encuentre seguridad en su arquitectura, además de tener más status a nivel nacional educativo ya que los institutos públicos aun no lo realizan, ello brindara mayor prestigio a la institución mostrando la seguridad que posee de manera física como virtual.

Palabras clave: Ciberseguridad, ISO 27032, gestión de tecnología, instituto tecnológico.

ABSTRACT

The present research has the general objective of proposing a cybersecurity model to improve the management of information technology in a public higher technological institute, the research has a qualitative approach, the research method was based on the interpretive paradigm, the type of research was applied and its action research design. Three cybersecurity specialists were consulted, who are experts in the higher education sector, the semi-structured interview, observation and documentary analysis were used as investigation techniques.

The implementation of the Cybersecurity methodology will allow to improve aspects of confidentiality, integrity and availability in the information systems, through controls, policies and security mechanisms that must be applied based on the ISO / IEC27032 Standard, which will allow the institute of Public higher education go to a level of digital transformation, be more efficient your digital services, find security in your architecture, in addition to having more status at the national educational level since public institutes still do not do it, this will provide greater prestige to the institution showing the security that it possesses in a physical and virtual way.

Keywords: Cybersecurity, ISO 27032, technology management, technological institute.

I. INTRODUCCIÓN

En la actualidad las instituciones educativas no cuentan con una seguridad informática adecuada e incluso la mayoría no le da importancia ello, ya que consideran que por ser una empresa dedicada a la educación no está muy expuesta, pero hoy en día los hacker también apuntan al sector educativo puesto que cuentan con información de suma importancia de todos los recursos humanos que participan en esta, desde los directivos hasta los alumnos y postulantes además de material académico e investigaciones científicas, lo cual buscan obtener con fines maliciosos. El objetivo de la investigación es implementar una metodología de Ciberseguridad, que permita mejorar aspectos de seguridad, integridad, disponibilidad y confidencialidad en los sistemas de información de un instituto tecnológico público, mediante controles y mecanismos de seguridad que deben ser aplicados según la Norma ISO/IEC27032.

Según la OEA (2020) la pandemia mundial del COVID-19 ha marcado un punto de inflexión fundamental en nuestra senda mundial y nos ha vuelto dependiente de lo digital. Con la crisis se expuso la deficiencia estructural que la sociedad ha tenido que atravesar en diversos sistemas – como la educación, empleo, economía y salud -, además se destaca el rol de catalizar de la tecnología de manera cómo se enfrentó colectivamente la pandemia. Hasta principios de 2020, solo 12 países tenían aprobada su estrategia nacional de ciberseguridad (se dio el incremento en referencia a 5 que poseían este tipo de estrategia para el 2016), solo 10 países establecieron su organismo gubernamental central como el responsable de las gestiones de ciberseguridad.

El ciberespacio se puede describir como el entorno virtual, el cual no existe de manera física, sin embargo, es un complejo entorno o en el espacio resultante en el cual aparece el internet, adicional de los individuos, organización y actividad de diversos tipos de objetos tecnológicos además de red que se conecta a él. La seguridad cibernética o en el ciberespacio viene a ser la seguridad del mundo virtual ISO (2012). Puesto que la ciberseguridad está a cargo de la protección de información, conservando su integridad como disponibilidad de ella, dando confianza cuando hay interacción por parte del usuario con la información con el sistema distribuido en el ciberespacio.

Además, como indica Movistar (2020) toda entidad educativa tiene manejo de un numero grande de información personal tanto del personal docente como de alumnos, adicional a ella los documentos académicos, dato financiero, registro e historial académico, es por ello que se vuelve un estratégico blanco de los ciberdelincuentes quienes buscaran perjudicar la privacidad que tienen los individuos además de la integridad que tiene la información.

Según el último informe de Fortune Business Insights (2021) el tamaño del mercado de la ciberseguridad en 2020 fue de 153.160 millones de dólares, mostrando un crecimiento del 7,6% en comparación con el año anterior. Para 2021 se prevé un tamaño de mercado de 165.780 millones de dólares, y se prevé que crezca hasta los 366.100 millones de dólares en 2028 con una tasa de crecimiento anual compuesto (TCAC) del 12,0% durante el periodo 2021-2028.

A nivel nacional es más común ver como las organizaciones siguen sufriendo ataques del hacker, como indica Fortinet (2021), el Perú ha sido el 3er país con mayores ataques en América Latina, siguiendo a México y Brasil. Gran cantidad de delitos cibernéticos fueron realizados con “Ransomware”, el cual es un tipo de malware el cual va impedir al usuario a tener acceso al sistema o archivo personal.

La justificación de la presente investigación tiene como fin el poder realizar la propuesta de un Modelo de ciberseguridad que permita minimizar los riesgos de los procesos académicos del instituto superior tecnológico público, la institución académica no cuenta con un plan de ciberseguridad que pueda mitigar los ataques de los ciberdelicuentes y que pueda ocasionar caídas de las redes de comunicaciones, perdidas de información del base de datos y caídas de las aplicaciones. Es muy importante contar con una metodología de ciberseguridad que permita reducir el riesgo, amenaza y vulnerabilidad del sistema distribuido. Defendiendo los términos de la metodología de implementación teniendo cuidado con el proceso y sistema se deberá emplear por base la norma ISO 27032. Esta investigación se justifica de manera práctica, necesitando disminuir el riesgo y vulnerabilidad de la institución educativa, se puede disminuir el nivel por más mínimo que sea de riesgos o la vulnerabilidad de cual se puede ser víctima ante la fuga o ataque de información. Como consecuencia, la norma ISO 27032, mejorará el proceso y servicio informático bajo un modelo de ciberseguridad de manera adecuada y segura.

La investigación presente, define el problema general que nos insta en poder defenderlo y ponerlo en investigación para revisar y evidenciar los resultados concebidos, siendo el enunciado lo siguiente: ¿Cómo el modelo de ciberseguridad mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021?.Obteniendo los siguientes problemas específicos: ¿Cómo es la organización respeto al modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021?¿Cómo verificar el análisis de riesgos de un modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021? ¿Cómo el plan de acción de un modelo de ciberseguridad mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021?, ¿Cómo se implementa un modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021?

La presente investigación tiene como objetivo general: Proponer un modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021, las cuales establece los siguientes objetivos específicos: Describir la organización del modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021. determinar el análisis de riesgos del modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021. Determinar el plan de acción del modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021, e Implementar el modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021.

II. MARCO TEÓRICO

Se tiene por primer antecedente nacional relacionado con el tema a investigar, a Aliaga (2016) quien presento por objetivo en su tesis realizar el diseño de un Sistema de Gestión de Seguridad de Información (SGSI) basándose en las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005, adoptando como framework de negocios la actual versión de COBIT, en su metodología adoptó el ciclo de Deming como metodología, el cual se puede aplicar a todos los procesos que abarca el SGSI. Dicha metodología es más conocida por sus siglas en inglés como PDCA: Plan-Do-Check-Act. Obteniendo como resultado los modelamientos para los procesos del negocio los cuales forman parte de los objetivos de la tesis, concluyendo que no hay políticas ni controles que estén enfocados en la seguridad lo cual puede generar una grave consecuencia en los cumplimientos del objetivo de negocio, además de tener pérdidas aún mayores de las que la organización.

También, tenemos al autor Aliaga (2021) que en su tesis tuvo por objetivo realizar la implementación del sistema de ciberseguridad el cual influya positivamente para prevenir un ataque cibernético en la compañía radiadores en el 2021, Se obtiene como resultado que es correcto para los objetivos el indicador con nivel de activos, están alineados con el plan de toda la empresa el nivel de satisfacción por la parte interesada. Se concluyó que hay influencia positiva para prevenir un ataque cibernético en la empresa como objetivo general.

A nivel nacional también se encuentra a Vilcarromero y Vilchez (2018) en su tesis presentaron por objetivo proveer a la empresa del SOC un modelo de ciberseguridad para brindar una solución que permita implantar, operar, monitorear, revisar y mejorar los controles y políticas de Ciberseguridad, con la importancia de lograr ser un SOC de referencia y ser competitivo en el mercado local. Basándose en ISO 27032, esta brinda el marco de orientación la cual mejora el estado de ciberseguridad, utilizando el aspecto técnico y estratégico sobresaliente para la actividad. Se concluyó que con las perspectivas de riesgo y/o seguridad, tomando los marcos del NIST buscando la mejora de la ciberseguridad de la infraestructura critica, siendo este un importante factor para crear el valor para la compañía, también las ciberseguridades gestionadas en las áreas de servicio de seguridad son compromisos compartidos del nivel jerárquico en la empresa, es por esos que

se tiene que crear planes adecuados de implantaciones de esquema de ciberseguridad con adecuadas coordinaciones con toda área de la compañía.

En otro estudió tenemos al autor Vásquez (2017) quien plantea en su tesis por objetico la determinación de las gestiones de la ciberseguridad junto con las prevenciones de un ataque cibernético en la PYME del Perú, 2016. Se concluyó que la indiferencia de la Gerencia con temas de Ciberseguridad brinda por resultado la carencia de apoyos económicos a procesos de creaciones de medios de seguridad informática en las redes privadas, causando de esta manera que las organizaciones estén expuestas a riesgos asimismo mayores.Seclen (2016) analizo los factores que sufrió las implementaciones y nos da a tener en cuenta la importancia de su ejecución, el análisis concluye en poder realizar el uso adecuado y basarse en la mejora continua del (PDCA).

Encontramos además a Lombardi y Cari (2020) quienes presentaron como objetivo el diseño de las arquitecturas de ciberseguridad para el servicio de la plataforma IoT en el área de TI en la compañía Pacífico Seguros. Es por ello que se realizó los diseños de las arquitecturas de ciberseguridad para el servicio de la plataforma IoT, esta va permitir que se genere un positivo impacto el cual cubre la nueva necesidad de la empresa Pacifico Seguros, lo cual va garantizar el respaldo de los datos además de permitió alcanzar la expectativa solicitada de la seguridad de la información en la plataforma correspondiente. Concluyendo que por medio del análisis de la brecha se pudo visualizar las pocas gestiones de comunicaciones que se encuentran entre áreas y de forma reactiva las cuales afrontan el incidente previsto que se deriva al HelpDesk.–Finalmente logrando terminar las brechas identificadas en la evaluación de perfil objetivo y actual por medio del plan de acción, el cual se alineo con el control del estándar ISO 27032 y la ISO 27001.

El autor Cáceda (2021) en su tesis resalta la vulnerabilidad de la infraestructura tecnológica crítica generó una preocupación nacional muy grande en seguridad, los ciber-riesgos son consolidados en los panoramas de riesgo global. Además, el ataque cibernético conforme pasa los años sigue en aumento causando así que la ciberseguridad sea convertida en el riesgo más crítico del mundo. Basado en ello se realizó la propuesta de elaborar los modelos dinámicos como herramientas de gestiones, basándose en la técnica de dinámicas de sistema con las finalidades de optimizarlas toma de decisión estratégica en seguridad de la

empresa ,asimismo Jaiyen & Sornsuwit (2019) involucra el estudio y análisis de las redes computacionales a través de una secuencia de estándares, protocolos, métodos y demás herramientas que se tienen para poder minimizar las posibles amenaza hacia la infraestructura o la información circundante, por lo que se implica el software, el hardware y las redes de datos.

Según los autores Pretell y Blas (2020) en su tesis presento como objetivo la gestión de forma segura de los activos de una municipalidad, controlando el acceso al recurso informático de la municipalidad, definiendo la política del cifrado, estableció la seguridad ambiental y física en la municipalidad, estableció la seguridad en la operación de los negocios, estableciendo la seguridad en la telecomunicación del sistema de información. Siendo descriptivo simple su esquema de diseño, por metodología empleada estuvo basada en la utilización del control de seguridad de seguridad de manera operativa de la norma ISO 27002:2013, el cual va corresponder al modelo de seguridad de información.

Siguiendo a nivel nacional está Rivera (2019) quien en su tesis propuso por objetivo la metodología para las gestiones de riesgo de ciberseguridad y su consecuencia para prevenir el fraude en la empresa industrial del distrito Yanacancha. Siendo descriptivo el tipo de investigación ya que será sometido Teniendo por conclusión que la digital economía se basa en las digitalizaciones de información además de las infraestructuras de la TIC. Se integra por compañías las cuales brindan servicios y productos solo digitalmente, servicios y productos mixtos, compañías que producen un bien además de las prestaciones de servicio intensivo en TIC, conjuntamente con actividad definido por el termino comercio electrónico, además del segmento que es parte de la TIC el cual brindan soporte a los demás segmentos que se identifican (infraestructura lógica y física), también Bejarano, Rodríguez y Merseguer (2021) en su artículo indican que las organizaciones empresariales apoyan las operaciones diarias utilizando Tecnologías de la Información y la redes de datos. Sirven de base para tener una gestión controlada de recursos, servicios y objetivos comerciales, alineados con la misión de la organización. En este documento, revisamos los estándares y marcos para lograr la ciber resiliencia en las organizaciones, como el marco NIST, ENISA o estándares internacionales como ISO / IEC 27032, se visualizará un nuevo marco de

ciberresilencia, se logrará aprovechar el aprendizaje automático contribuye con la continuidad del negocio.

De acuerdo con Mendoza y Vega (2019) en su tesis presento por objetivo realizar el diagnostico de los niveles de capacidad en las gestiones de ciberseguridad de la empresa, reconocer la brecha para el diseño y propuesta del control clave el cual fortalecerá la ciberseguridad y para finalizar la elaboración y propuesta de la hoja de ruta de las implementaciones del control clave. Adicional a ello, limito el alcance al aspecto que se relaciona con la respuesta y detección del evento que se relaciona con ciberseguridad. Su investigación de tipo cualitativo. El trabajo fue de gran utilidad para las compañías que estaban centradas en la implementación de la solución tecnológica como las protecciones ante un ciberataque el cual desarrolle enfoques de procesos que puedan permitir optimizar la capacitad de responder y detectar un evento del ciberataque, asimismo Ganesan, Jajodia, Shah & Cam (2016) la ciberseguridad busca garantizar el mantenimiento y monitoreo de los servicios de seguridad de los activos de la organización, así como a los usuarios y su información, contra riesgos y amenazas

Para finalizar los antecedentes nacionales, tenemos a Lino (2021) planteo en su investigación lo importante que es el uso de la herramienta de seguridad informática para la gestión política de seguridad basándose en normas internacionales ISO, tener conocimiento de datos del servidor Firewall lo cual permite tener una barrera por medio de la cual va poder pasar el tráfico de red, se diseñó para que trabaje como filtro a nivel paquetes IP o también se podría trabajar en una sola capa de protocola más alta. Para guardar los datos de algún ataque a través del internet, hacer el filtro de página web prohibida que pueda atentar con la integridad de los adolescentes, niñas y niños, según la ley peruana 30254 lo que se buscaba era las revisiones sistemáticas de la literatura científica es que tuviera las documentaciones necesarias para las administraciones de las redes de dato seguro así como las gestiones de servidores Firewall Linux como herramientas de administraciones para las seguridades de la red organizacional. Esta búsqueda la realizó en la base de datos. Esta tesis necesito tener conocimiento sobre cuán importante es la seguridad informática en la red local y externa, permitió tener un mejor control de tráficos del paquete a través del permiso de acceso al usuario.

En el ámbito internacional encontramos en primer lugar a los autores Avellan y Zambrano (2019), ellos plantearon por objetivo la determinación de la ciberseguridad con el uso de la ISO 27032 – 2012 con la finalidad de tener conocimiento sobre el riesgo, amenaza y vulnerabilidad del sistema distribuido. Por medio de la metodología Análisis Modal de Fallos y Efectos (AMFE), pudo identificar y evaluar los niveles de riesgo para cada dominio de seguridad (informaciones, redes, aplicaciones), esto les permitió poder plantear más soluciones que se sugieran para la mejora sea de largo o corto plazo en el aspecto de confiabilidad, disponibilidad e integridad de los datos. Buscando alcanzar el objetivo, se aplicó la herramienta de escaneo de vulnerabilidad Acunetix, Nessus y Shodam en el sistema distribuido en la IES pública, mostro por resultado el reporte de distintas categorías de la vulnerabilidad que poseían estos sistemas, y estos al mismo tiempo brindo la recomendación para prevenir la inseguridad en el

Ciberespacio, Como solución los autores elaboraron un plan de acción el cual le pudo permitir a cada instituto un objeto de estudio, tomar acción para resguardar las integridades de su información, de igual manera Urcuqui, García & Osorio (2018) en su artículo indica lo posible que es reducir el nivel de riesgo de forma concreta y con ello logar la materialización de las amenazas y la reducción del impacto sin la importancia de realizar elevada inversión ni tener una gran estructura de personal. es necesario conocer y administrar de manera ordenada los riesgos que está sometido el sistema digital, considerar procesos efectivos y planificar, implantar los mecanismos de ciberseguridad.

También encontramos a los autores Montaro y Varona (2021) con su objetivo de hacer una propuesta del modelo dinámico para seguridad digital basándose en el estándar ISO para su subproceso de gestiones del recurso tecnológico en la Institución Universitaria Colegio Mayor del Cauca. Para su metodología se optó por el aporte teórico que tiene relación con el tema de la investigación, además, de generar cierta actividad que permite la construcción del diseño del modelo el que se va ajustar con el requerimiento y necesidad de una Institución de Educación Superior. Como resultado se tuvo el modelo que contribuyo en su plan que mejorara la seguridad de los datos brindándole integridad, disponibilidad, confidencialidad y protección de esta forma se pueda prevenir el riesgo además de identificar la posible amenaza de ciberseguridad, ala

ves Navarro, Urcuqui, García, & Osorio (2018) en su investigación científica menciona los niveles de seguridad en el ciberespacio se consigue instalando controles, que tengan políticas ordenadas, procesos, procedimientos y un mecanismo de acción entre hardware y software, los que deben ser alineados, implementados, supervisados y mejorados para cumplir las metas establecidos en la seguridad del ciberespacio.

Como también se tiene al autor Nacipucha (2019) quien en su tesis presento por objetivo el diseño del sistema para la gestión de la ciberseguridad de información por medio de la norma ISO/IEC 27001:2013 para la empresa ArteHogar S.A. en la ciudad de Guayaquil. En su diseño utilizó como método cuantitativo y cualitativo resaltando el objetivo que tiene el estudio. Las investigaciones cualitativas son características por el uso del texto, palabra, discurso, dibujo, grafico e imagen permitiendo comprender la social vida por medio del significado. Concluyendo que, por medio del estudio elaborado por la compañía en relación con la actual situación de su ciberseguridad, se pudo realizar los modelos de gestiones basándose en la Norma ISO27001:2013, con el fin de resguardar los datos que se encuentren expuestos, Para Jaime Romero (2018) indica que la ciberseguridad es una gestión de estrategia que cuenta con herramientas, políticas, estrategias de seguridad, salvaguardas, directrices, gestión de riesgos, acciones, formación, prácticas efectivas, seguros y tecnologías que puedan proteger la información de las entidades y al personal que interactúan en el ciberentorno.

Encontramos también al autor Vivanco (2019) presentando por objetivo la implementación de SIEM para poder detectar y mitigar un evento e incidente de seguridad en comandos de ciberdefensa de la FF.AA. la especificación técnica requerida por SIEM implementado fue revisada según la característica en base a la norma ISO 25000 en referencia a la evaluación de calidad de software. Al realizar la implementación se comprueba la hipótesis que se planteó la cual determina que el sistema SIEM pueda permitir la respuesta oportuna y detección automática de la amenaza tecnológica en tiempo real. Realizando una investigación con enfoque deductivo puesto que al iniciar se consultó la general información de diferentes fuentes estudiadas. Concluyendo que las metodologías PDCA fue empleada en el proyecto ya que se puede desarrollar, implementar, dar mantenimiento además de realizar la mejora continua de la seguridad existente en el COCIBER, por medio de

sus etapas se pudo emplear ciertas metodologías o norma ISO las cuales permiten asegurar que el sistema SIEM se implemente, analice y evalué de manera correcta.

También tenemos a Gumucio (2021) en su tesis tuvo por finalidad entregar la guía para el gerente de riesgo lista para su implementación de la gestión en ciberseguridad en Entidades de Intermediación Financiera, teniendo como base el Marco de Trabajo NIST (National Institute of Standards and Technology), es así como se pudo resolver el problema de enfrentar las incorporaciones de la gestión de riesgo cibernético en una entidad de intermediación financiera. El método que se utilizó en la guía integró el proceso que inicia en las bases del marco de trabajo NIST en su pilar inicial que es “identificar”. Por base practica se empleó la aplicada metodología en ese momento en las entidades de intermediación financiera boliviana, como caso de éxito además de ejemplo en ese país, permitiéndole además de gestionar el riesgo no financiero el poder aumentar el valor de la empresa ya que le permite resguardar su digital pilar como puntas de lanzas de sus estrategias de negocio, según Philco (2017) en su artículo menciona la diferencia del resto de los entornos donde se le combate al ciberataque, el ciberespacio tiene una dimensión física y virtual; entonces , cualquier peligro que suceda en la red del ciberespacio tiene consecuencia en el mundo físico y viceversa. Cuanto más se extienda el uso de internet o el metaverso (internet más allá del internet) se aumentará la dependencia a las infraestructuras físicas y tecnologías informáticas, el nivel de ataques a los entornos digitales se incrementará.

Continuando en el nivel internacional el autor Alfaro (2017) en su tesis indica como objetivo la propuesta de una metodología para las gestiones de riesgo para la tecnología de la información en la firma de costa rica Touche & Deloitte S.A. basándose en COBIT 5 ajustándose con la mejor práctica de la industria de tecnología de información, viendo el aspecto estratégico además de las gestiones de riesgo. Para el desarrollo se empleó un enfoque cualitativo. Concluyendo que las investigaciones que tienen relación con las gestiones de riesgo de TI que se desarrolló por la empresa además de analizarse al ser parte de la investigación, sin seguir los esquemas estandarizados en base con la metodología o procesos definidos. En lugar de ello se emplea los datos de distintos previos proyectos, buscando articular una solución, causando a veces presentar un error o inconsistencia en la entregada solución.

Se encuentra también a Aristizáb al (2019) quien planteo en su tesis realizar el diseño de un modelo de C2M2 buscando el establecimiento del marco en referencia para poder proteger la crítica infraestructura de las industrias manufactureras del sector textil, buscando la evaluación de madurez en seguridad del proceso, política, medida los cuales buscan reducir el impacto que podría ocasionar la vulnerabilidad propia del sistema de controles industriales (ICS), el sistema de control distribuido (DCS), el control lógico programable (PLC). Teniendo la adaptación de modelo C2M2 para las evaluaciones de la madurez en seguridad informática, pretendió determinar su nivel de madurez que tiene las gestiones del sistema SCADA en el sector textil, generando herramientas las cuales buscan la identificación, evaluación y calificación del elemento de seguridad los cuales pudieron ocasionar el riesgo de pérdida, no disponible o cambios que no hayan estado permitidos en los datos. Al momento de revisar este elemento de seguridad se desea la generación del informe, donde se podrá reconocer errores, riesgo y debilidad si lo hubiera, teniendo por finalidad que más adelante se pueda utilizar para fijar política, procedimiento o directiva que puedan aportar en el fortalecimiento de la seguridad informática en el sistema SCADA.

Además, esta Alfaro (2020) en su tesis planteo por objetivo realizar la estrategia de negocio para la ciberseguridad de entel s.a., permitiendo el incremento del ingreso además de poder participar en el mercado chileno, así pudo incrementar el valor de su negocio. A nivel global el mercado de seguridad digital posee un gran potencial de incremento, como aumento en las inversiones en TICs en los desarrollos de estrategia digital, a las preocupaciones de mitigación de riesgo de ciberataque, también por cumplimientos de normativa gubernamental exigida por el estado. Es por eso que la organización considera la seguridad informática como algo fundamental en la estratégica planificación. A pesar de ello, se presentan ciertos obstáculos para poder implementarlo con un recurso interno, limite en las inversiones, una gran demanda de personas con capacidades para el desarrollo, aspecto cultural, etc. Por resultado se estimó que Entel S.A. luego de 4 años podría duplicar el número de sus ingresos del servicio de la seguridad informática de 6.2 miles de millones de pesos que obtuvo en el 2018 podría tener 19.1 miles de millones para el 2023. Ala ves Royal (2018) en su artículo indica que la seguridad en la red digital (internet) debería ser una prioridad importante para todas la

empresas u organizaciones con presencia en los entornos digitales. Los hackers están constantemente buscando vulnerabilidades en las defensas que se colocan como protección; si la organización opta por renunciar y no dar importancia a la seguridad de la red de datos, pueden dañar gravemente su reputación, por lo que no se debe arriesgar más con las vulnerabilidades a los servicios tecnológicos

Contamos con Lara (2019) quien en su tesis por objetivo general propuso elaborar el diseño del modelo de seguridad de los datos, basándose en ISO 27001, NIST SP 800-30 e OSSTMMv3, para la Universidad Regional Autónoma de los Andes. Teniendo por finalidad el poder resolver el problema que se presentó con las gestiones de recursos, disponibilidad de información además de las gestiones administrativas de la entidad. Esta tesis mostro que los modelos se seguridad son una presentación oficial de un estándar, que conlleva un grupo de prácticas y reglas las cuales regularan como es el manejo, protección y distribución de información de una institución, especialmente los datos delicados.

Para finalizar a nivel internacional tenemos a García, Pérez y Rodríguez (2019) quienes plantean en su tesis el desarrollo de una guía para las gestiones de riesgo cibernético la cual pueda permitir la prevención, protección, detección, mitigación además de brindar respuesta frente al principal riesgo al cual se exponga una firma de auditoria en San Salvador. El estudio que se realizó fue cualitativo en su enfoque necesitando el procedimiento recurrente, interactivo, interpretativo, inductivo. Concluyendo que la falta de gestiones efectivas de riesgo cibernético en la firma de auditorías que se dedican al servicio de una externa auditoria, según la Oficina de Seguridad para las Redes Informáticas (2018) los servicios tecnológicos están sometidos a altos grados de amenazas de diversas formas, originadas tanto desde mismo entorno institución, como desde exterior, procedentes de gran variedad de fuentes. las amenazas físicas, como los accesos no autorizados, catástrofes naturales imprevistos, sabotajes, incendios, y accidentes.

Como indica Vilcarromero y Vílchez (2018) el problema y situación del Perú en referencia a la ciberseguridad indica que los encargados del protocolo de seguridad de la tecnología de la información de Estado de Oficina Nacional de Gobierno Electrónico, está a cargo del liderazgo del proyecto, normativo, y diferentes tareas que como gobierno electrónico se encarga de realizar el estado. Indica que, en Perú, en entidades estatales la ciberseguridad recién está en una

etapa muy temprana ya que recién inicia ,se avanzado muy poco en el aspecto de capacitaciones y organizaciones, ya que no hay propiamente una Agencia Nacional de Ciberseguridad, La Secretaría de Gobierno Digital (SeGDi) es el órgano alineado, que posee autoridad técnico normativa a nivel nacional, la cual tiene la responsabilidad de proponer y formular la política sectorial y nacional, plan nacional, norma, lineamiento y estrategia en materias de gobierno electrónico e informática. Además, es quien regula los sistemas nacionales de informática y otorga asistencias técnicas para las implementaciones del proceso de innovación tecnológica buscando que el estado se modernice coordinando con la Secretaría de Gestión Pública.

Es por ello que se necesita fijar la política para proteger los datos digitales, más aún sabiendo que hay entidades encargadas de telecomunicación, luz, agua, etc., y estas pueden verse perjudicadas por un ciberataque, viéndose perjudicados los clientes. Adicional a ello hay que resaltar que en nuestro país no hay política nacional acerca de la ciberseguridad, hasta el momento no se han dado problemas muy serios en esta área, es por ello que la mayoría de compañías no le dan tanta importancia a este tema, pero es muy importante que se tome toda medida preventiva. Además, el Ministerio de transporte y comunicaciones (2021) indica que la International Telecomunicación Unión (ITU) conceptualiza la Ciberseguridad como: grupo de seguros, practicas idóneas, formación, método de gestión de riesgo, directriz, cuidar la seguridad, conceptos de seguridad, política y herramienta tecnológica la cual se pueda usar para la protección del activo de la organización además del usuario en los entornos de ciberespacios. El modelo de ciberseguridad según la ISACA (2018) necesita al principio levantar información a través de la entrevista a usuarios de la empresa, buscando recoger datos y opinión de usuarios acerca de expectativa sobre las confiabilidades, integridad y disponibilidad del activo de información.

Los activos de la organización son datos claves para conocer el funcionamiento de los servicios de TI, de igual manera el análisis del riesgo viene a ser un trabajo de suma importancia cuando se tiene que definir iniciativa y proyecto para las mejoras en la seguridad de la información, brinda datos con valor además optimiza la seguridad de la organización mediante las subcategorías Activos, Amenazas, Vulnerabilidades, Impacto. De la misma forma el plan de acción

permitirá tener conocimiento, priorizar los lineamientos del negocio, mediante las subcategorías, Políticas, Roles, Métodos, Procesos, Controles y finalmente mediante la propuesta de implementación se logrará ser proactivo, resaltando la importancia del mecanismo de prevención en el ciberespacio las sub categorías, Controles de seguridad, Procedimientos de seguridad, Intercambio de información, Capacitación, monitoreo, Gestión de incidentes.

Según Gómez (2017) La ISO 27032 elaboró el Comité Técnico ISO/IEC JTC 1 encargados de la Tecnología de la Información, el Subcomité SC 27 por medio de la Técnica de Seguridad Informática, esta ISO posee el estándar que va garantizar la directriz de seguridad lo cual la empresa aseguró que “se brinde una general colaboración que se da entre diversas partes que tienen interés en disminuir el riesgo en internet”. Más claro la ISO 27032 brinda un marco de intercambiar datos, manejar un incidente, así como las coordinaciones que permiten ser más seguro el proceso, Como indica Gómez (2019) la gran cantidad de ataque que se dan en un sistema de infraestructura crítica y al impacto que este ataque se pueda dar en un contexto, en estados unidos, el 12 de febrero de 2013 el Presidente Barack Obama redactó la Orden Ejecutiva (EO) de Mejora de Ciberseguridad de Infraestructuras Críticas en donde se delegaba en el NIST (National Institute of Standards and Technology), Según Netcloud (2017) de las vulnerabilidades son muy diferentes. Pueden ser debido a fallas en la construcción del software, fallas de procedimientos o errores de configuración; los investigadores de seguridad han identificado que el comportamiento del ser humano tiene un rol fundamental las fallas de los sistemas tecnológicos.

Las instituciones educativas públicas se orientan a desarrollar ciencia, investigaciones, se crearon los institutos de educación superior tecnológica, escuelas de educación superior pedagógica y escuelas de educación superior tecnológica de todo el país. Las escuelas de educación superior (EES) son instituciones que son altamente especializada. Se clasifican de la siguiente, escuelas de educación superior pedagógica (EESP) y escuelas de educación superior tecnológica (EEST)MINEDU (2021)

III. METODOLOGÍA

El problema de la investigación que tiene el instituto superior es no contar con un modelo de ciberseguridad, que pueda ayudar a evitar riesgos, amenazas que cuentan su infraestructura y sus servicios de TI, contar con una respuesta inédita hacia una incidencia de ataque, esta investigación busca implantar un modelo de ciberseguridad que pueda contrarrestar cualquier amenaza hacia el campus universitario, el enfoque de la investigación es cualitativo ya que nos basamos en la observación de los expertos analizando su entorno y sus particularidades y su invaluable experiencias, según Hernández y Mendoza (2018) método cualitativo busca que los investigadores estudien hechos por ellos mismos y que confíen en investigaciones realizadas previas para que generaren teorías solidas a lo que se observa y se visualiza. Teniendo en cuenta la investigación se formuló en el paradigma interpretativo que busca profundizar los conocimiento a la ciberseguridad.

3.1. Tipo y diseño de investigación

Tipo de investigación

La investigación es de tipo aplicada, porque se basa en conocimientos científico y tecnológicos que busca implementar un modelo de ciberseguridad para mejorar la protección de los activos, se busca comprender la actualidad de los procesos del instituto superior, según Baena (2014) formula que la investigación aplicada tiene como rol principal estudiar temas enfocados a la acción, prioriza en poner en marcha teorías generales y estar comprometido a resolverlos.

Diseño de investigación

El trabajo de investigación, se utilizó el diseño de investigación acción, que busca ser muy eficiente en sus procesos a través de la implementación de una metodología de ciberseguridad que se va realizar, además de visualizar las mejoras en los lineamientos del instituto superior, siendo mucho más seguros contra las vulnerabilidades y los riesgos existentes, Se elaborara la investigación en los tres pasos observando, pensando y actuando. según Hernández, Fernández y Baptista (2014) la investigación acción participativa se concentra en brindar información para elaborar tomas de decisiones de proyectos, procesos y reformas estructurales, de

la misma forma los colaboradores deben participar en los procesos de modificar y ala ves mejorar la implementación de los resultados del estudio de investigación.

3.2. Categorías, Subcategorías y matriz de categorización

Los modelos de ciberseguridad pueden ser implementados en todo tipo de empresa que tenga alguna tecnología, ya que busca la protección de toda la información que las empresas puedan manejar, con la finalidad que estos datos se encuentren seguros y no al asecho de personas con malas intenciones que traten que acceder a ella. Con los objetivos de seguridad definidos. Se indica a continuación la lista de subcategorías del modelo alineadas a su categoría correspondiente:

Tabla 1

Categorías y subcategorías de la investigación

Categorías	Subcategorías
Activos de la Organización	▪ . Productos y servicios ▪ . Marco normativo de seguridad ▪ . Flujos de información de procesos ▪ . Técnicas de seguridad implementadas
Análisis de riesgos	▪ . Activos Críticos ▪ . Amenazas ▪ . Vulnerabilidades ▪ . Impacto y riesgos
Plan de acción	▪ . Políticas ▪ . Identificación de Roles ▪ . Métodos de implantación ▪ . Procesos ▪ . controles tecnológicos
Implementación	▪ . controles y políticas de seguridad ▪ . Procedimientos de seguridad ▪ . intercambio de información ▪ . capacitación ▪ . Gestión de incidentes

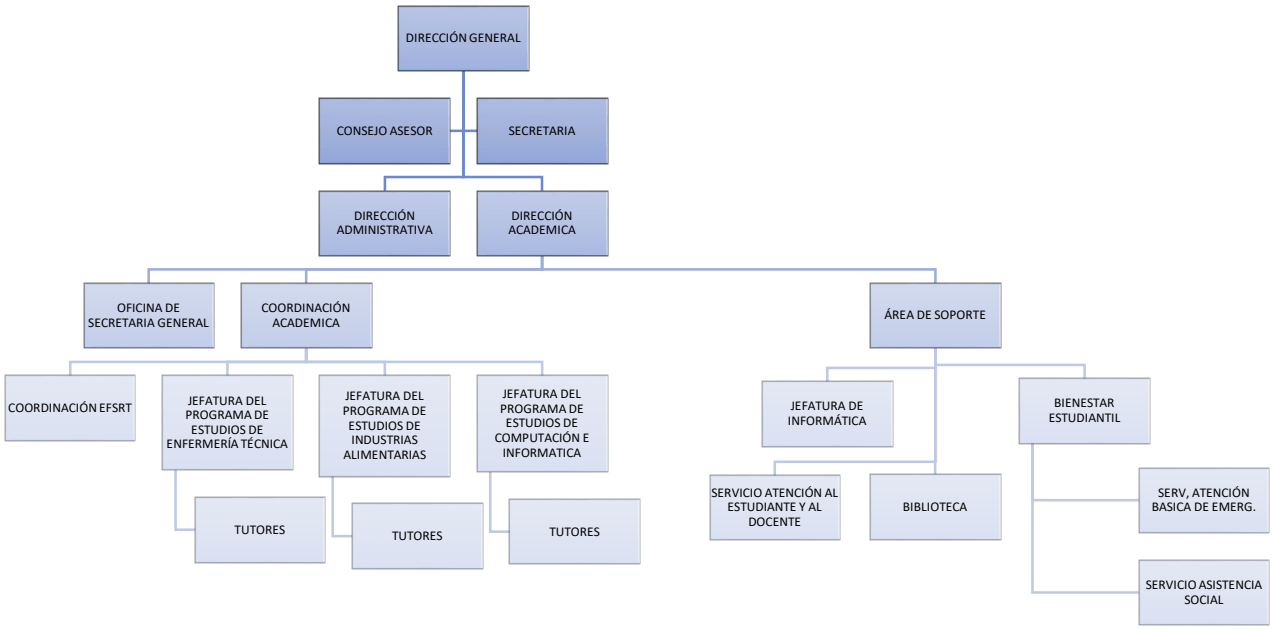
3.3. Escenario de estudio

El estudio de investigación se realizó en el departamento de tecnología de la institución ubicado en el distrito de Los olivos-Lima, se considera un lugar donde se puede recoger información que permita conocer y entender la realidad problemática de sus servicios tecnológicos y nos ayude alcanzar los objetivos de la investigación, y por lo tanto , se procedió a solicitar la autorización a la dirección general, la institución cuenta con áreas académicas y administrativas es muy importante implementar una metodología de ciberseguridad para reducir las vulnerabilidades de los servicios de TI.

.

Figura 1

Organigrama de IESTP Manuel Arévalo Cáceres



3.4. Participantes

La presente investigación se consultó a tres especialistas de tecnologías, los cuales son expertos en el sector de educación superior y laboran en el MINEDU, son elegidos para ser parte de la investigación, además son especialistas en la materia de ciberseguridad y cuentan con experiencia en los procesos de tecnológicos, la finalidad es poder observar ,describir los pasos de sus proceso y herramientas informáticas que utilizan para salvaguardar su infraestructura del sector de educación.

3.5. Técnicas e instrumentos de recolección de datos

Como menciona Hernández y Mendoza (2018) los métodos cualitativos, cuantitativos, la recolección de información es fundamental, pero su importancia no es medir las variables para inferencias y análisis estadísticos. La importancia de la investigación cualitativa es recolectar y obtener toda la información a profundidad sobre los usuarios, organismos, pueblos, condiciones o procesos. En la investigación de estudio se procedió a realizar la recolección de información del instituto superior, usando las técnicas de entrevista a profundidad como herramientas como la guía de entrevista semiestructurada, guía de observación estructurada ,se ha creado preguntas para proceder con el entrevista a los expertos además usaremos la observación con la finalidad de obtener datos del estado real de la institución y el comportamiento de los especialistas en su trabajo, la finalidad de poder analizar de manera individual, colectiva responder las preguntas lo cual nos da el punto inicio para la elaboración de la investigación.

3.6. Procedimientos

La elaboración del procedimiento que se realizó , fue utilizar los siguientes métodos, como, la entrevista a profundidad que se realizó a tres especialistas con amplia experiencia en ciberseguridad que laboran en la institución, también se elaboró una guía de entrevista, que nos permitió poder recoger la información de los especialistas ,también se realizó la observación, para identificar el comportamiento de los usuarios mediante la guía de observación y por lo último se realizó un análisis documental donde se identifica el problema general mediante un informe. Ala ves se procedió con la implementación de la metodología.

3.7. Rigor científico

En la presente investigación del trabajo se recolecto datos del instituto superior mediante entrevista a tres expertos del sector de educación ala ves se realizó una observación de los procesos administrativos y se extrajo información de los documentos relacionado a sus objetivos de trabajo a nivel tecnológico, dando credibilidad que los datos obtenidos son reales y auténticos. Cómo indica Guasmayan (2000) quien indica que la credibilidad es ser precisos en el procedimiento que se utiliza en la investigación y que se pueda confirmar que sea veraz. consistencia lógica es que se mantenga la coherencia al sustentar el desarrollo de la investigación, argumentos, sustentos, enunciados, los cuales deben guardar relación y tener cohesión. Ortiz y Mariño (2014)

3.8. Método de análisis de la información

La investigación usa el método inductivo, cómo se evalúan las características que se muestran en el comportamiento de los participantes, también puede utilizarse herramienta de las entrevistas semi estructuradas, identificando el problema general de nuestra investigación y la creación de las categorías de nuestra matriz. Y ala ves realizar el método llamado triangulación a las entrevistas realizadas para dar una valides a la información recolectada.

3.9. Aspectos éticos

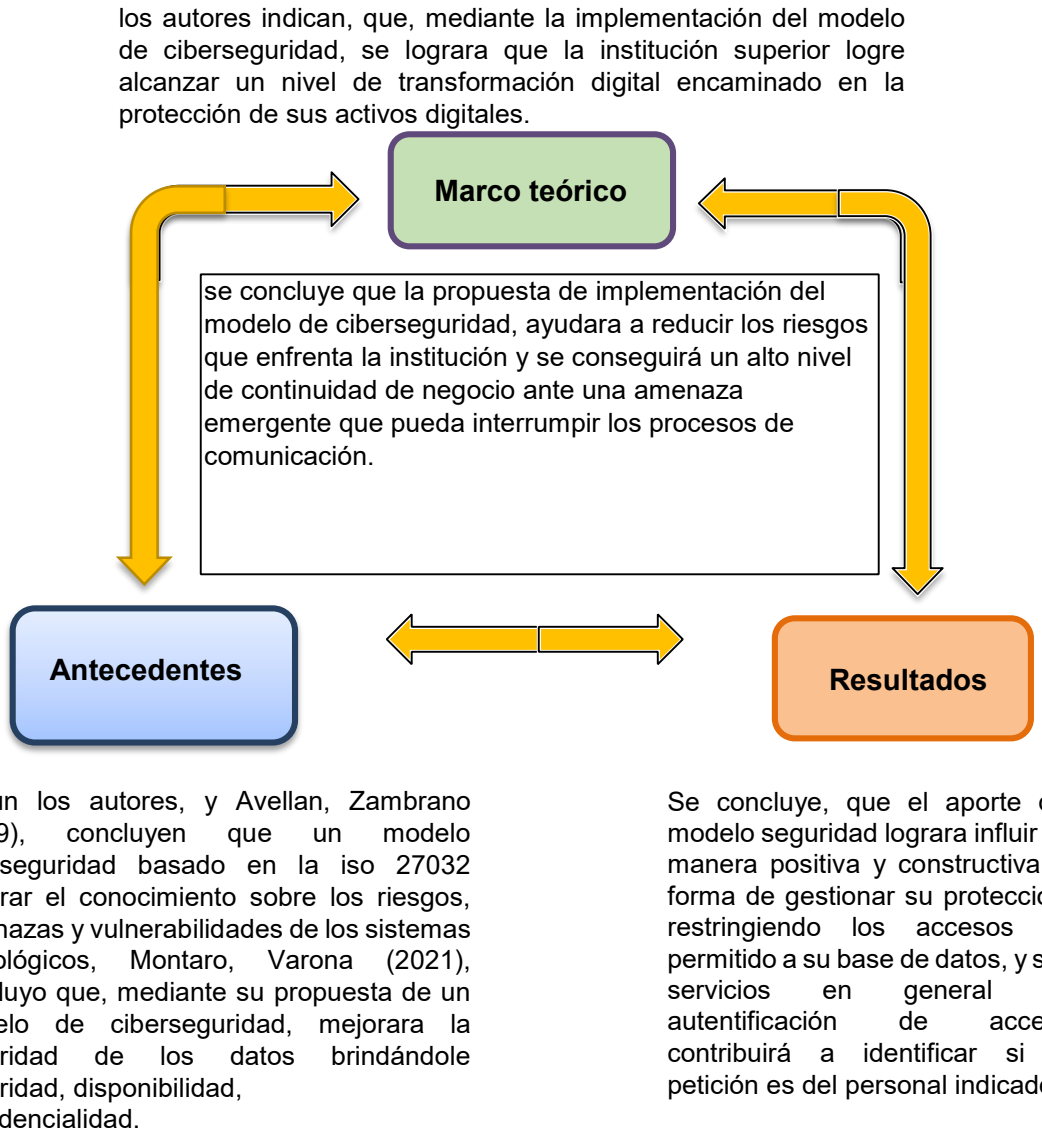
La investigación que se desarrolla es propia y original del investigador, quien respeta los lineamientos para los contenidos, se pasa por el turnitin solicitado para comprobar que no exista plagio ni algo inadecuado en la investigación. Se cita contenido de artículos, tesis y libros con el fin de respetar la autoría de cada material. El investigador utiliza la Resolución Rectoral N° 00089/2019 que corresponde a los lineamientos establecidos por la Universidad Cesar Vallejos, donde se puede observar la estructura de la tesis para posgrado, norma de redacción al estilo APA. También cuenta con anonimato de las personas entrevistadas, y con pleno consentimiento de ser entrevistados. De esta manera podrá alcanzar los objetivos que se planteó, logrando tener el resultado esperado

IV RESULTADOS Y DISCUSIÓN

Para la investigación realizada, se ha realizado con las técnicas de recolección de información, entrevista a profundidad, observación e análisis documental, y así poder obtener los resultados de los objetivo trazados.

Figura 2

Triangulación de antecedentes, marco teórico y los resultados.



Se concluye que la propuesta de implementación de modelo de ciberseguridad basado en la iso 27032 ayudara a reducir las vulnerabilidades, riesgos y amenazas de los sistemas tecnológicos, se lograra la continuidad de negocio ante una amenaza emergente, la institución tiene que entender que su personal debe estar altamente capacitado que se ajusten a las necesidades y retos que cada día se

integran en el mundo cibernético, las instituciones superiores deben integrar nuevos componentes dentro de sus programas curriculares como el Internet de las Cosas, comprensión de los Malware y mecanismos de defensa más actuales, así como el uso de la misma tecnología para brindar mejores experiencias en el proceso de enseñanza-aprendizaje, Beltrán & Martín (2015) Esto también necesita prácticas docentes que enfoquen su atención dentro de la dinámica estudiantil integrando la ciberseguridad de forma práctica, como el propuesto por Ribada-Pena et al. (2015), donde se usa un simulador de plataformas denominado DSBox con el fin de recrear algunas situaciones y posibles escenarios donde se pueden dar los ciberataques así como interactuar con las variables clave dentro de la dinámica de uso seguro de las redes y su respectiva defensa, promoviendo el conocimiento de una forma más interactiva y fácil de entender. Con el presente estudio se hace uso del análisis bibliométrico como una herramienta de gran ayuda para el reconocimiento del comportamiento que tiene un área específica, Arias-Ciro (2020), usando las tendencias encontradas como insumo para la discusión sobre las oportunidades que se encuentran en la educación en ciberseguridad. De esta manera, el estudio tiene como objetivo la divulgación de los resultados para futuras investigación o acciones dirigidas sobre las tendencias encontradas y los focos de atención que se pueden encontrar en el análisis sobre los temas alrededor de la ciberseguridad la metodología garantizara el alcance y mantendrá las propiedades intactas de los activos de la institución y de los usuarios contra los riesgos que se presente se menciona la descripción de los pilares que reguardan la protección de la información que se menciona en la tabla 2.

Tabla 2

Pilares de la protección de los activos

Pilares	Descripción
Disponibilidad	• Acceso y uso oportuno y confiable de la información por los usuarios autorizados.
Integridad	• Protección de la información para no ser alterada ni dañada.
Confidencialidad	• Ocultar la información confidencial no se divulgue a personas entidades o procesos no autorizados.
Autenticidad	• Se refiere a garantizar que el mensaje ha sido enviado por quien dice ser.

Figura 3

Triangulación de las entrevistas a profundidad.

Se concluye, la pregunta mencionada en el objetivo general de la propuesta de investigación ¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto? Especialistas entrevistados concluyeron que la metodología de ciberseguridad mejorará la protección del sistema de información a nivel del ciberespacio, con la implementación de las políticas y controles se podrá prevenir los ataques de los ciberdelicuentes y mitigar las amenazas a los equipos de sistemas de información mediante la buena práctica y con la continuidad del

negocio. Para la implementación de la propuesta de ciberseguridad es necesario elaborarlo en función de las fases de la metodología PDCA (Plan, Do, Check, Act)

Como apoyo de la metodología se implementará controles y políticas de ciberseguridad que se realizará mediante recolección de la información utilizando el marco de referencias como lo es COBIT, la cual permitirá identificar cada uno de los requerimientos y lineamientos definidos por la norma ISO 27032 para ser aplicada en la institución. Con respecto a la pregunta que se relaciona con el primer objetivo específico ¿Cómo es el funcionamiento de los activos? Se concluye que el especialista recomienda que es importante conocer el funcionamiento de los activos para lograr objetivos claros de ciberprotecion, conocer la magnitud del negocio y su alcance como menciona esto involucra el estudio y análisis de las redes computacionales a través de una secuencias de estándares de seguridad, lo que permitirá reducir los riesgos de la tecnologías emergentes la infraestructura juega un parte muy importante en soporta los servicios que se involucren el software, el hardware y las redes Jaiyen & Sornsuwit (2019) De esta manera la ciberseguridad busca garantizar el mantenimiento de los sistemas de los activos de la instituciones proteger a los trabajadores y su sistema de información propios del ciber entorno Ganesan, Jajodia, Shah & Cam (2016) Siguiendo las etapas, con respecto a la pregunta a nuestro segundo objetivo específico: ¿Cuál es la importancia de realizar el análisis de riesgos? Los entrevistados concluyeron que Se debe realizar regularmente pruebas de pentesting para evaluar el nivel de seguridad que se encuentra los equipos de sistemas. Ayudar identificar los riesgos y amenazas emergentes que surgen constantemente. La pregunta a nuestro tercer objetivo ¿Cómo elaborar el plan de acción para la gestión de la ciberseguridad? Los entrevistados concluyen Se debe realizar una elaboración eficaz de las políticas y controles que ayuden a mejorar los sistemas digitales y físico de la institución basado en las mejores prácticas.

Sin embargo, para que cualquier control, herramienta o proceso establecido para la seguridad del ciberespacio sea lo más segura posible, se debe realizar un buen proceso de análisis, identificación, priorización de posibles riesgos para establecer normas preventivas, correctivas de forma correcta. Continuando la pregunta que del cuarto objetivo específico: ¿Cómo implementar el sistema de ciberseguridad? Los entrevistados concluyeron que la implementación Mejorar todos los procesos

de seguridad basado en las buenas practicas donde las existencias de política y controles reducirán todas las incidencias que puedan dañar la institución.
concluyendo, con el quinto objetivo específico: ¿Cuál es la importancia del sistema de ciberseguridad? Los entrevistados concluyeron que es importante contar con modelo de ciberseguridad que nos permita proteger los activos, y estar a la vanguardia de los estándares más altos de seguridad. La Ciberseguridad ha dado un incremento importante en la última década, debido a que esta ha sido consecuencia de la frecuencia de ataques informáticos que llegan a colapsar plataformas gubernamentales, con trágicas consecuencias los mecanismos que nos ayudan a proteger la infraestructura tecnológica se mencionan en la tabla 3.

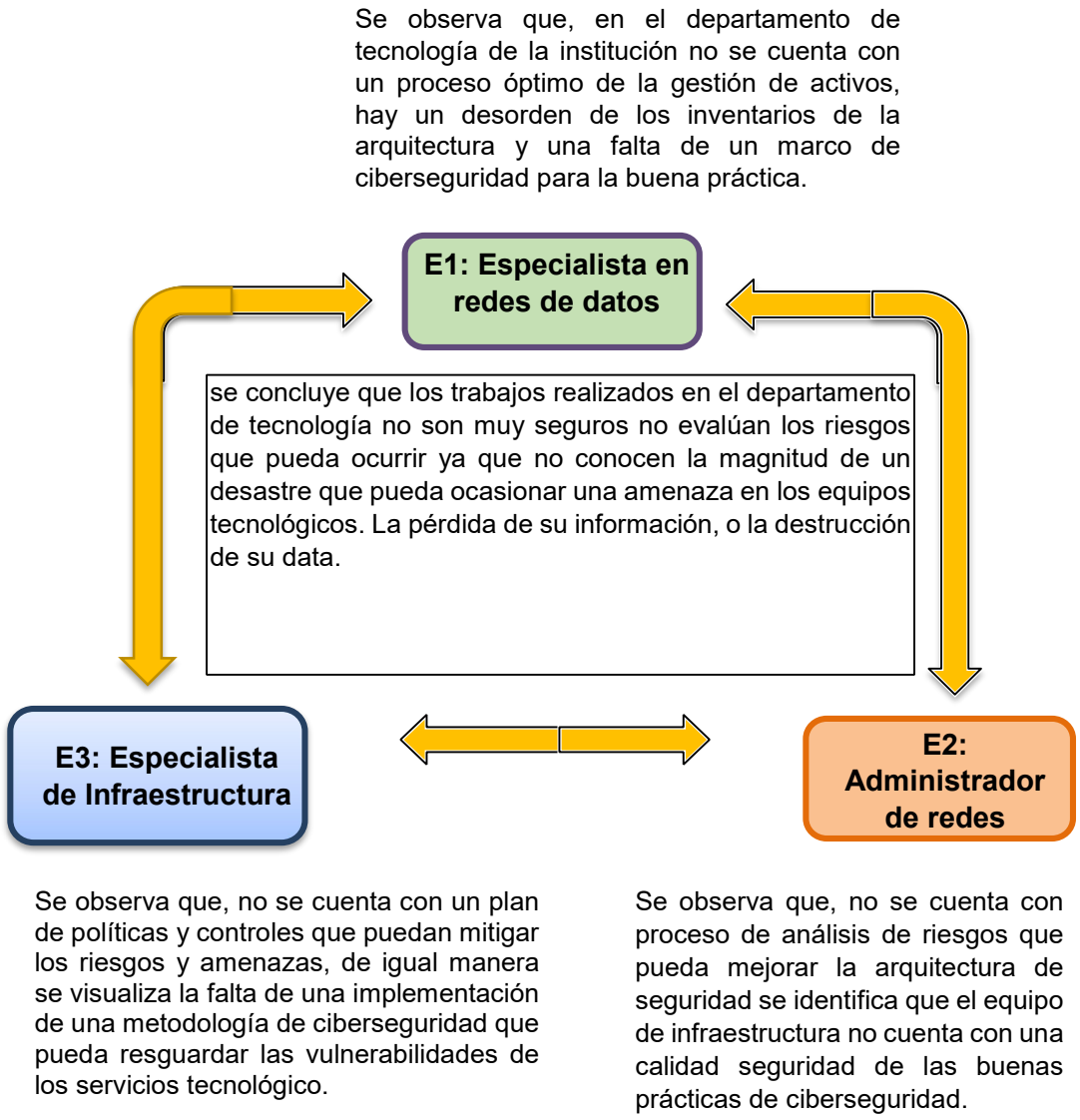
Tabla 3

Mecanismo de la ciberseguridad

Mecanismo	Descripción
Seguridad de la información	• Confidencialidad • Integridad • Disponibilidad
Seguridad de las aplicaciones	• Procesos • Componentes • Software • Resultados • Datos
Seguridad de la red	• Diseño • Implementación • Operación
Seguridad de internet	• Servicios en internet seguro • Redes • Disponibilidad de servicios • Fiabilidad de servicios
Seguridad en la infraestructura	• Datacenter • Condiciones ambientales • Acceso Físico • Sitios alternos

Figura 4

Triangulación de la observación de la unidad de estudio.



De los observado concluyo que los procesos de trabajo de área de tecnología de la institución no son muy seguros y no evalúan los riesgos que puedan ocurrir, ya que no conocen las amenazas que puedan ocurrir en los equipos tecnológicos, no existe un control de los accesos a los sistemas, ya que el usuario accede a equipos o paginas no autorizadas, los procesos y procedimientos de seguridad no se tienen los controles adecuados, no se cuenta con un estándar de seguridad que puedan contribuir a mejorar las buenas prácticas de ciberseguridad ,los administrativos no tienen conocimientos de la importancia de contar con políticas de seguridad

mediante ,la triangulación haces énfasis al objetivo general de la problemática de la investigación ¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto? Dándole una solución proponemos que la implementación de un modelo de ciberseguridad ,es una herramienta que permitirá ordenar información o darle diferentes tratamientos para interpretarlos de manera clara, sintética y práctica, a la vez que permitan dar una idea general de las diferentes fases o procesos que se llevan cabo para identificar, analizar y priorizar respectivamente cada una de las posibles vulnerabilidades y riesgo, de forma que el cumplimiento de las normas permita llevar un control preciso y esquematizado para posteriores mitigaciones de dichos impactos en la institución superior,

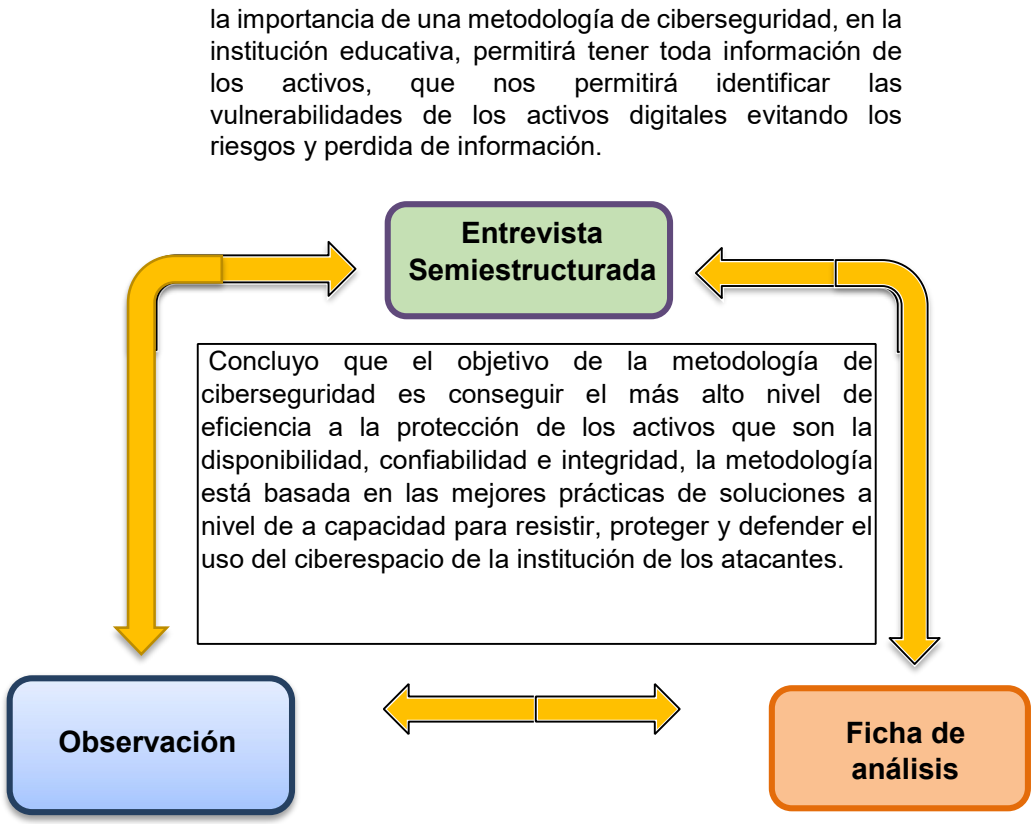
Tabla 4

Objetivos de la ciberseguridad

Objetivos
Proteger el ciberespacio
Gestión de crisis
Educación
Alertas sobre amenazas
Coordinación entre entidades

Figura 5

Triangulación de las técnicas utilizadas.



Se puede identificar lo importante que es contar con un modelo de ciberseguridad el objetivo de la metodología de ciberseguridad es conseguir el más alto nivel de eficiencia a la protección de los activos que son la disponibilidad, confiabilidad e integridad, la metodología está basada en las mejores prácticas de soluciones a nivel de a capacidad para resistir, proteger y defender el uso del ciberespacio de la institución de los atacantes.

Concluyendo a través de las técnicas utilizadas se entiende el valor que tiene el avance de la comunicación a través de la red de internet la transformación digital que implica tomar medidas preventivas, la institución superior no es ajena a estos cambios y se requiere un modelo de seguridad que este a la par con la evolución de las TI, adaptarla a todos los procesos del campus universitario.

Tabla 5

Ciclo de vida de un ataque

Ciclo de vida	Descripción
Preparación del ataque	• **Identificación y selección del objetivo**
Obtención de acceso	• **Explotación de vulnerabilidades**
Creación de persistencia	• **Escalacion de privilegios**
Ejecución de acciones	• **Selección y recolección**
Eliminación de rastros	• **Eliminación de rastro**

IV. CONCLUSIONES

PRIMERA:

El objetivo general, proponer un modelo de ciberseguridad que mejorará eficientemente la protección de los servicios del ciberespacio, sus procesos actuales y reducirá las amenazas a los activos digitales, mediante de las buenas practicas, y el apoyo de la dirección general la metodología tendrá un respaldo, uso e implementación.

SEGUNDA:

El primer objetivo específico, se describe que la organización del modelo de ciberseguridad mejorará la gestión de tecnología, mediante los procesos de la gestión de los activos para conocer la magnitud de los servicios digitales de la institución su alcance y proyección, el modelo de ciberseguridad está enfocado bajo la guía de fundamentos del PDCA y COBIT.

TERCERA:

Del segundo objetivo específico, se determina el análisis de riesgos del modelo de ciberseguridad, mediante la gestión de un reconocimiento y escaneo de los servicios digitales (PESTESTING) que permitirá evaluar y diagnosticar el nivel de seguridad del campus, asegurando la garantía del cumplimiento de la confiabilidad, disponibilidad e integridad de los activos digitales.

CUARTA:

El tercer objetivo específico, se determina el plan de acción del modelo de ciberseguridad, mediante la elaboración de controles y políticas de ciberseguridad se conseguirá procesos óptimos de salvaguardar la información que interactúa en la red del campus universitario.

QUINTA:

Del cuarto objetivo específico, se determina la implementación del modelo de ciberseguridad, mediante la creación de lineamientos de políticas basado en las buenas practicas, se logrará reducir las incidencias que pueda dañar los servicios digitales de la institución.

VI. RECOMENDACIONES

PRIMERA:

Se recomienda a la dirección general implementar el modelo y adoptar las directrices y controles que se provee la norma ISO 27032 para la seguridad de sus sistemas tecnológicos, de manera que forme parte de sus procesos para reducir las vulnerabilidades y amenazas, así evitar ataques a futuro.

SEGUNDA:

Se recomienda al especialista considerar el tipo o nivel de vulnerabilidad dentro del sistema distribuidos de comunicación, debido a que, si no controlan a tiempo, podrían llegar a materializarse y provocar ataques a los servicios digitales.

TERCERO:

Se recomienda al especialista realizar evaluaciones de riesgos mensualmente, para poder identificar las vulnerabilidades de los activos que se encuentra en la red o los servicios digitales y poder mitigar las amenazas emergentes.

CUARTA:

Se recomienda ejecutar auditorías internas con la finalidad de conocer las vulnerabilidades del sistema de seguridad y que procedimiento realizar para mitígalos.

QUINTA:

Se recomienda realizar capacitaciones de ciberseguridad a todas las áreas académicas del instituto superior, ya que de esta manera se reducirá las brechas de ataques de ingeniería social, los usuarios son una línea importante de información que debe ser protegida.

REFERENCIAS

Alfaro, J. (2017). Metodología Para La Gestión De Riesgos De Ti Basada En Cobit 5. Instituto Tecnológico De Costa Rica. Tesis De Licenciatura. Recuperado, De: Https://Bit.Ly/3se7rze

Alfaro, V. (2020). Estrategia De Negocio Para El Servicio De Ciberseguridad Entel S.A. Universidad De Chile. Tesis De Grado. Recuperado De: Https://Bit.Ly/3meq6jc

Aliaga, C. (2021). Implementación De Un Sistema De Ciberseguridad Para La Prevención De Los Ataques Cibernéticos En La Empresa Radiadores Fortaleza, 2021. Tesis De Maestría. Universidad Cesar Vallejo. Lima Perú Disponible En: Https://Bit.Ly/3p6o4ie

Aliaga, L. (2013). Diseño De Un Sistema De Gestión De Seguridad De Información Para Un Instituto Educativo. Tesis De Titulación. Pontificia Universidad Católica Del Perú. Lima, Perú. Disponible En: Https://Bit.Ly/3f89mlo

Arias-Ciro (2020), Estudio Bibliométrico De La Eficiencia Del Gasto Público En Educación Revista Cea 6(11)127-144 Https://Doi.Org/10.22430/24223182.1588

Aristizábal, J. (2019). Adaptación Del Modelo De Madurez En Ciberseguridad Basado En C2m2, Para La Industria Manufacturera Del Sector Textil Que Utiliza Sistemas Scada. Institución Universitaria De Colombia. Tesis De Grado. Recuperado De: Https://Bit.Ly/3ydqtei

Avellan, N. Y Zambrano, M. (2019). Ciberseguridad Y Su Aplicación En Las Instituciones De Educación Superior Públicas De Manabí. Escuela Superior Politécnica Agropecuaria De Manabí Manuel Félix López. Tesis De Maestría. Recuperado De: Https://Bit.Ly/32afdzx

Baena, G. (2014). Metodología De La Investigación Serie Integral Por Competencias Grupo Editorial Patria Recuperado De Https://Bit.Ly/2ajqfx8.

Ballestero, F. (2020). La Ciberseguridad En Tiempos Difíciles. Boletín Económico De Ice, 3122, Article 3122. Recuperado De: Https://Doi.Org/10.32796/Bice.2020.3122.6993

Bejarano, Rodriguez Y Merseguer (2021). A Vision For Improving Business Continuity Through Cyber-Resilience Mechanisms And Frameworks. Iberian Conference On Information Systems And Technologies, Cisti, (5). Https://Doi.Org/10.23919/Cisti52073.2021.9476324

Beltrán, M. Y Martín, I. (2015) Experiencias Actualizando La Asignatura De Seguridad Informática Para Los Grados De Ingeniería Informática. Actas De Las Primeras Jornadas Nacionales De Investigación En Ciberseguridad. Instituto Nacional De Seguridad, España. 176-181

Blas, W. Y Pretell, G. (2020). Modelo De Seguridad De La Información Para Mejorar La Gestión Informática En La Municipalidad Distrital De Florencia De Mora. Universidad Nacional De Trujillo. Tesis De Grado. Recuperado De: Https://Bit.Ly/3ydykbk

Caceda, C. (2021). Modelo Dinámico Para La Gestión De Seguridad De La Infraestructura De Las Tecnologías De Información Y Comunicación. Universidad Nacional Mayor De San Marcos. Tesis De Título. Recuperado De: Https://Bit.Ly/3e4uddl

Cari, M. Y Lombardi, J. (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. Tesis De Bachiller. Recuperado De: Https://Bit.Ly/3pglnsp

Carrillo, J., Et Al. (2020) Cybersecurity Process: Methodological Guide For Its Implementation. Risti - Revista Ibérica De Sistemas E Tecnologías De Información, Volumen 2020 (E29). Recuperado De: Https://Bit.Ly/3fcqxec

Carrillo, J., Et Al. (2019). Cybersecurity and Its Application in Higher Education Institutions. Risti - Revista Ibérica De Sistemas E tecnologías De Información, Volumen 2019, (E20). Recuperado De: Https://Goo.Gl/Tnzcbu

Fortune Business Insights (2021). Tecnologías Que Crecerán A Un Ritmo De Dos Dígitos Recuperado De: Https://Bit.Ly/32j4rjr

Fuentes, E. M. (2020). Ciberseguridad Y Su Importancia En El Sector Salud: La Experiencia De Madrid Digital. I+S: Revista De La Sociedad Española De Informática Y Salud, 139, 13-15, Fuente: Https://Bit.Ly/3seiqbu

Ganesan, R., Jajodia, S., Shah, A., & Cam, H. (2016). Dynamic Scheduling Of Cybersecurity Analysts For Minimizing Risk Using Reinforcement Learning. Acm Transactions On Intelligent Systems And Technology (Tist), 8(1), 1-4 Https://Dl.Acm.Org/Doi/10.1145/2882969

García, M., Pérez, Y. Y Rodriguez, Y. Guía De Gestión De Riesgos Cibernéticos Para Empresas Dedicadas A Brindar Servicios De Auditoria Externa En El Área Metropolitana De San Salvador. Universidad De El Salvador. Tesis De Licenciatura. Recuperado De: Https://Bit.Ly/3qfeluo

Gómez, G. (2019). ¿Qué Es El Cybersecurity Framework De Nist De Los Estados Unidos? Conexionesan. Perú. Disponible En: Https://Bit.Ly/3eapfiu

Guasmayán, R. (2000). (C. E. Magisterio, Ed.) Obtenido De Https://Bit.Ly/37r0lwm

Gumucio, J. (2021). Guía De Implementación De Un Programa De Gestión De Riesgos De Ciberseguridad En Entidades De Intermediación Financiera. Universidad De Chile. Tesis De Maestría. Recuperado De: Https://Bit.Ly/3se4zvv

Hernández, R., Fernández, C. Y Baptista, M. (2014). Metodología De La Investigación. (6ta.Ed.). México D.F., México. Recuperado De Https://Bit.Ly/2a1rwzf

Hernández, R. Y Mendoza, C. (2018). Metodología De La Investigación: Las Rutas Cuantitativa, Cualitativa Y Mixta. Ciudad De México, México: Edamsa Impresiones Recuperado de: https://bit.ly/3j4nxvz

Icontec. (2013). Norma Técnica Colombiana Ntc-Iso-Iec 27001 Técnicas De Seguridad Y Requisitos Para Un Sistema De Gestión De Seguridad De La Información Colombia. Disponible En: Https://Bit.Ly/3q57hqr

Isaca. (2018). Cobit 2019 - Introducción Y Metodología. Isaca. Recuperado De: Https://Bit.Ly/35b5rve

Jaiyen, S., & Sornsuwit, P. (2019). A New Incremental Decision Tree Learning For Cyber Security Based On Ilda And Mahalanobis Distance. Engineering Journal, 23(5),71-88 Recuperado De: Https://Bit.Ly/327sxzs

Romero, J. (2018). Conceptualización De Una Estrategia De Ciberseguridad Para La Seguridad Nacional De México. 28. Retrieved From https://Bit.Ly/3q724sa

Lara, E. (2019). Diseño De Un Modelo De Seguridad De La Información, Basado En Osstmmv3, Nist Sp 800-30 E Iso 27001, Para Centros De Educación: Caso De Estudio Universidad Regional Autónoma De Los Andes, Extensión Tulcán. Universidad Internacional Sek De Ecuador. Tesis Tesis De Maestría. Recuperado De: https://bit.ly/3h0odkt

Lee, S. (2018) Resiliency Of Mobile Os Security For Secure Personal Ubiquitous Computing. Personal And Ubiquitous Computing, Vol 22 (1). Https://Doi.Org/10.1007/S00779-017-1098-X

Lino, J. (2020). Herramientas Para Mejorar La Seguridad Informática En Ambientes De Cómputo En El Sector Educación: Una Revisión De La Literatura Científica. Universidad Privada Del Norte. Tesis De Grado. Recuperado De: Https://Bit.Ly/3p6xvtz

Mendoza, L. Y Vega, G. (2019). Evaluación De La Capacidad De Detección Y Respuesta A Riesgos De Ciberseguridad, Caso De La Empresa Sisc. Universidad Del Pacifico. Tesis De Maestría. Recuperado De: Https://Bit.Ly/3iyif5f

Minedu (2021). Institutos De Educación Superior. Recuperado De: Https://Bit.Ly/3minrkh

Ministerio De Transporte Y Comunicaciones (2021). Ciberseguridad. Perú. Recuperado De: Https://Bit.Ly/3sxretl

Montaro, F. Y Varon, M. (2017). Modelo Dinámico De Ciberseguridad Basado En Estándares Ios Para Ios Caso De Estudio: Subproceso De Gestión De Recursos Tecnológicos En Un Mayor. Institución Universitaria Tecnológico De Antioquia. Recuperado De: Https://Bit.Ly/3f8zqug

Movistar. (2020). El Sector Educativo También Sufre Los EfectosDe La Ciberseguridad.
Destino Negocio. México. Recuperado En: https://bit.ly/3mgcrih

Nacipucha, J. (2019). Análisis Y Diseño Para Un Modelo De Gestión De Seguridad De La Información Basados En Normas Iso/Iec 27001:2013 Para La Empresa Artehogar En La Ciudad De Guayaquil. Universidad De Guayaquil. Tesis De Titulo. Recuperado De: https://bit.ly/3ycykxs

Navarro, A., Urcuqui, C., García, M., & Osorio, J. (2018). Ciberseguridad: Un Enfoque Desde La Ciencia De Datos. In Universidad Icesi (Ed.), Ciberseguridad: Un Enfoque Desde La Ciencia De Datos (Primera Ed). https://doi.org/10.18046/eui/ee.4.2018

Netcloud Engineering. (2017). Netcloud Engineering. Retrieved From Disponible En: Https://Bit.Ly/32dihpq

Organización De Los Estados Americanos (2020). Reporte Ciberseguridad 2020: Riesgos, Avances Y El Camino A Seguir En América Latina Y El Caribe. Cybersegurityobservatory. Doi: http://dx.doi.org/10.18235/0002513

Ortiz, E., & Mariño, M. (2014). Una Comprensión Epistemológica De La Psicopedagogía. Revista De Epistemología De Ciencias Sociales, 22-30. Obtenido De https://bit.ly/2mikz37

Perú Sufrió Más De 4.700 Millones De Intentos De Ciberataques En El Primer Semestre. [22 De Setiembre De 2021]. El Comercio. Disponible En: https://bit.ly/3e8wfpi

Philco, L. (2017). Estudio Y Análisis De Ciberataques En América Latina, Su Influencia En Las Empresas Del Ecuador Y Propuesta De Políticas De Ciberseguridad. Disponible En: https://bit.ly/3mjqcqe

Ramió, J. (2015). Ciberseguridad: Un Nuevo Paradigma De La Seguridad Y Nuevos Retos En La Formación Especializada. Criptored, Intypedia, Crypt4you Y Thoth. Chile. Recuperado De: https://bit.ly/3mbt047

Reategui, A. (2019). Guia De Procedimientos Para La Elaboración De Trabajos De Investigación, Tesis Y Trabajos De Suficiencia Profesional En La Universidad Privada De La Selva Peruana. Universidad Privada De La Selva. Pag. 20. Recuperado De: https://bit.ly/327zvy0

Osri (Oficina De Seguridad Para Las Redes Informáticas Página). (2018). Metodología Para La Gestión De La Seguridad Informática (Pp. 1–68). Pp. 1–68. Retrieved From Https://Bit.Ly/3sxxic7

Ribadas-Pena, F. & Anido-Bande, R., Darriba-Bilbao, V. (2015) Repositorio De Actividades Autónomas Para La Docencia De Seguridad En Sistemas Informáticos. Universidad De Vigo. Recuperado De: https://bit.ly/3p7wa0x

Rivera, A. (2019). Riesgos De Ciberseguridad Y Sus Consecuencias En La Prevención De Fraudes En Las Empresas Industriales Del Distrito De Yanacancha – Pasco 2016. Universidad Nacional Daniel Alcides Carrión. Tesis De Maestría. Recuperado De: Https://Bit.Ly/3f95wj5

Rojal. (2018). La Ciberseguridad Se Posiciona En 2018 Como Uno De Los Requisitos Esenciales Del Diseño Web. Disponible En: https://bit.ly/3gty75r

Sancho, C. (2017). Ciberseguridad. Presentación Del Dossier. Urvio: Revista Latinoamericana De Estudios De Seguridad, 20, 8-15. Disponible En: https://doi.org/10.17141/urvio.20.2017.2859

Seclén Arana, J. A. (2016). Factores Que Afectan La Implementación Del Sistema De Gestión De Seguridad De La Información En Las Entidades Públicas Peruanas De Acuerdo A La Ntp-Iso/Iec 27001. (Tesis De Maestría,

Universidad Nacional Mayor De San Marcos) Disponible En: https://bit.ly/3p7b3du

Templeton (2011) Aspectos De Seguridad De La Seguridad De Los Dispositivos Ciberfísicos En Entornos De Asistencia. Serie De Actas De Conferencias Internacionales De Acm, (53). https://dl.acm.org/doi/10.1145/2141622.2141685

Vásquez, L. (2017). Gestión De La Ciberseguridad Y Prevención De Los Ataques Cibernéticos En Las Pymes Del Perú, 2016. Tesis De Bachiller. Universidad San Ignacio De Loyola. Lima, Perú. Disponible En: https://bit.ly/3q1xvfg

Vázquez, F. M. (2020). Ciberseguridad Y Estado Autonómico. Icade. Revista De La Facultad De Derecho, 109, 1-19. Recuperado De: https://doi.org/10.14422/icade.i109.y2020.001

Vilcarromero, L. Y Vilchez, E. (2018). Propuesta De Implementación De Un Modelo De Gestión De Ciberseguridad Para El Centro De Operaciones De Seguridad (Soc) De Una Empresa De Telecomunicaciones. Tesis De Maestría. Universidad Peruana De Ciencias Aplicadas. Lima, Perú. Disponible En: https://bit.ly/3mgwz4h

Vivanco, P. (2019) Implementación De Un Siem Para El Comando De Ciberdefensa Utilizando Herramientas De Código Abierto Bajo El Estándar Iso 27032. Universidad Tecnológica Israel. Tesis De Titulación. Recuperado De: https://bit.ly/3e5iwdz

Yupanqui, J. R. A., & Oré, S. B. (2017). Políticas De Seguridad De La Información: Revisión Sistemática De Las Teorías Que Explican Su Cumplimiento. Risti-Revista Ibérica De Sistemas E tecnología De Información, (25), 112-134.Recuperado https://bit.ly/3e3cwme

ANEXO 1

Matriz de categorización

Título: Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico Público, Lima-2021

Autor: Victor Hugo Manrique Reyna

Problema General	Objetivo General	Categorías	Subcategorías	Técnicas	Instrumentos
¿Cómo el modelo de ciberseguridad mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021?	Proponer un modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021	Activos de la organización	▪ Productos y servicios ▪ Marco normativo de seguridad ▪ flujos de información de procesos ▪ Técnicas de seguridad implementadas	Entrevista Semi estructurada	Guía de Entrevista
Problemas Específicos	**Objetivos Específicos:**				
¿Cómo es la organización respeto al modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021?	Describir la organización del modelo del ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021	Análisis de riesgos	▪ Activos críticos ▪ Amenazas ▪ Vulnerabilidades ▪ Impacto y riesgos		
¿Cómo verificar el análisis de riesgos de un modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021?	determinar el análisis de riesgos del modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021			Observación	Guía de observación
¿Cómo el plan de acción de un modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021?	Determinar el plan de acción del modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021	Plan de acción	▪ Políticas ▪ Identificación de Roles ▪ Métodos de implantación ▪ Procesos ▪ controles tecnológicos	Análisis documental	Ficha de análisis documental
¿Cómo se implementa un modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021?	Determinar la Implementación del modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima-2021	Implementación	▪ controles y políticas de seguridad ▪ Procedimientos de seguridad ▪ intercambio de información ▪ capacitación ▪ Gestión de incidentes		

Fuente: Gómez (2017)

Anexo 2

Instrumento de recolección de datos

Guía de entrevista semi estructurada

1. ¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto?
2. ¿Cómo es el funcionamiento de los activos?
    a. ¿Cuál es la relación de los productos y servicios?
    b. ¿En qué consiste el marco normativo de seguridad?
    c. ¿Cómo debe ser el flujo de información de procesos?
    d. ¿Qué Técnicas de seguridad se usa en instituto técnico?

3. ¿Cuál es la importancia de realizar el análisis de riesgos?
    a. ¿Verificar los Activos críticos?
    b. ¿Cómo verificar las Amenazas?
    c. ¿Cómo verificar las Vulnerabilidades?
    d. ¿Cómo verificar el Impacto y riesgos?

4. ¿Cómo elaborar el plan de acción para la gestión de la ciberseguridad?
    a. ¿Cómo se determinan las políticas?
    b. ¿Cómo se determina la Identificación de Roles?
    c. ¿Cómo se determina los métodos de implementación?
    d. ¿Cómo se determina los procesos?
    e. ¿cómo se determina los controles tecnológicos?

5. ¿Cómo implementar el sistema de ciberseguridad?
6. ¿Cuál es la importancia del sistema de ciberseguridad?
    a. ¿Qué controles y políticas de seguridad se deben tener?
    b. ¿Qué procedimientos de seguridad son los más adecuados?
    c. ¿Cómo realizar el intercambio de información?
    d. ¿Cuál es la importancia de la capacitación?
    e. ¿Qué estrategia se tiene para la gestión de incidentes?

Anexo 3:

Matriz de desgravación de la entrevista

N°	Preguntas	Entrevistado 1 – Especialista en redes de datos
1	¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto?	La metodología más adecuada para proteger los activos de la institución es la iso 27032 de ciberseguridad que permitirá asegurar la confidencialidad integridad y disponibilidad de los activos digitales de la institución, es una solución dinámica que permitirá prevenir todo tipo de riesgo y amenazas interno como externo, a mi experiencia el modelo de ciberseguridad ayudara mejorara todos los procesos de seguridad que se encuentra en el ciberespacio en las aplicaciones, base de datos y los entornos de red ,por lo que su uso reducirá los riesgos de los ataques y la perdida de la información o secuestros, y los más importante es que la metodología garantizaría la continuidad del negocio .
2	¿Cómo es el funcionamiento de los activos?	El funcionamiento de los activos consiste en identificar, analizar y conocer las técnicas y los procesos de los activos digitales de la institución sus funcionamiento y conocer que tan preparados están frente a los ataques de delincuentes cibernéticos, entender los productos y servicios que cuenta , verificar su normativa y documentación de seguridad, En la institución se priorizan los activos computacionales Los datos en general ya que cualquier dato es un activo importante para la institución ,y también es realizar un estudio en general de la institución desde el punto de vista de seguridad para poder saber todos los activos que se cuentan .uno de los activos más importantes es la base de datos donde se almacenan toda la información de los alumnos y docente.
3	¿Cuál es la importancia de realizar el análisis de riesgos?	La importancia de realizar un análisis es conocer las vulnerabilidad y amenazas de los activos de la institución los riesgos que se cuentan a diario. Realizar el análisis no permite evaluar la seguridad de la infraestructura de forma segura, el análisis nos ayuda a corregir el impacto y riesgo y estar prevenido frente a cualquier vulnerabilidad de los sistemas operativos, servicios y fallas de las aplicaciones, configuraciones incorrectas del técnico. En mi experiencia realizar una evaluación

		de riesgo son muy utilices para validar la eficacia de las configuraciones de seguridad de la institución. una buena práctica es contratar a un especialista para que realice Una auditoría interna como externa a las aplicaciones de la institución e identificar el nivel de seguridad que se encuentra.
4	¿Cómo elaborar el plan de acción para la gestión de la ciberseguridad?	En esta etapa se Permitirá conocer y documentar las priorización y medidas de políticas de ciberseguridad para implementar en la institución alineando las mejores prácticas más importante identificando roles que se debe asumir el personal para la correcto funcionamiento de la seguridad y determinar los procesos que deben alinear a la institución para la protección de sus activos de información que se encuentran en la red digital, el plan de acción es una fase muy importante del modelo ciberseguridad ya que no permitirá conocer los procesos afectados y determinar los controles tecnológicos que nos permitirán mitigar los riegos de los activos
5	¿Cómo implementar el sistema de ciberseguridad?	En esta etapa final ya conociendo el funcionamiento de los activos , los riesgos y su plan de acción, se ve debe crear existencia de políticas y procedimientos de seguridad en la institución ala ves crear marcos existentes para el intercambio de información entre la red de la institución, la capacitación al personal administrativo y docentes es una parte más importante para proteger la confiabilidad de la información, otro punto importante es la gestión de incidentes donde podemos tener mapeado y tomar medidas preventivas inmediatas para salvaguardar los activos. es muy importante seguir los lineamientos para la protección de los activos de información que se encuentran en el red de la institución, se podrá conocer e identificar los puntos clave en las cuales está más débil de tal medida que se pueda fortalecer mediante controles y mecanismos de prevención en los procesos de la información .
6	¿Cuál es la importancia del sistema de ciberseguridad?	Es de suma importancia contar con un sistema de ciberseguridad en la institución, para la protección de sus sistemas informáticos contra atacantes, ayuda a garantizar que la información privada permanezca privada, incluso cuando naveguemos

		a través de Internet. Al contar con un sistema de ciberseguridad la institución estaría a la vanguardia y los más altos estándares de seguridad.

N°	Preguntas	Entrevistado 2 – Administrador de redes
1	¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto?	Es muy importante para la institución educativa contar con un modelo de ciberseguridad para poder tener establecidos procedimientos de estándares de seguridad que mejoren el proceso de negocios. La metodología de la iso 27032 nos brinda un marco de ciberseguridad para mejora los lineamientos para identificar los riesgos a los cuales están expuestos en la red y que pueda llegar a afectar los activos de la institución nos brindara controles necesarios para implementar y asegurar de manera efectiva los diferentes activos de información.
2	¿Cómo es el funcionamiento de los activos?	En esta etapa es reconocer el funcionamiento de los activos de la institución educativa identificar el tamaño o la magnitud el tipo o modelo de negocio, su regularización bajo la cual debe regir los productos y servicios que brinda en la institución, entender el tipo de tecnología implementada los mecanismo de seguridad con los que se cuenta, entender como está constituida la institución saber todos sus procesos como revisar su normativa de seguridad ala ves recopilar y revisar las documentaciones de seguridad y por ultimo conocer las técnicas implementadas , mediante el reconociendo de la institución podemos saber los activos más importantes que se cuenta y poder realizar una análisis de riesgos y saber el nivel de seguridad que cuenta la institución educativa.
3	¿Cuál es la importancia de realizar el análisis de riesgos?	Es importante realizar un análisis de riesgos en la institución educativa porque permitirá realizará un diagnostico en la cual se identificará las vulnerabilidades de cada uno de los activos de información junto con su criticidad y como también el nivel de su exposición al riesgo respeto a su nivel de preparación frente a los ataques de los ciberdelicuentes. unos de los puntos más importantes es que nos ayudara a verificar los activos críticos, amenazas

		,vulnerabilidades , impacto, riesgo e identificar los responsables .
4	¿Cómo elaborar el plan de acción para la gestión de la ciberseguridad?	El plan de acción es identificar los puntos más importantes de la institución educativa para la elaboración de políticas de mejoras donde el personal de ti y en general toda la institución conozcan los métodos, controles y el proceso de resguardar y prevenir una fuga o daños a los sistemas de información, para que el plan de acción funcione de manera eficaz lo primero que tiene que hacer la institución es realizar un escaneo y verificación de todos los activos para poder entender donde se encuentra las vulnerabilidades de los sistemas de información, para poder elaborar políticas, roles, métodos procesos y controles.
5	¿Cómo implementar el sistema de ciberseguridad?	La implementación proporcionara directrices que mejorara la seguridad digital de la institución educativa mediante las buenas prácticas de resguardar y proteger la información y como se logra ese cometido mediante existencia y creación de políticas y controles de seguridad
6	¿Cuál es la importancia sistema de ciberseguridad?	La importancia de contar con un sistema de ciberseguridad En la institución ayudara a proteger los sistemas contra diversas amenazas que dañen los sistemas información, en mi experiencia uno de los ataques más comunes y peligros es el ramsomware que te secuestra la información y te pide un rescate por eso la importancia de contar con

		sistema de ciberseguridad que permita mitigar los riesgos y también que el personal de la institución educativa comprenda la importancia de contar con un sistema de prevención.

N°	Preguntas	Entrevistado 3 – Especialista de Infraestructura
1	¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto?	El modelo que mejoraría la estrategia de la seguridad seria Nist Cybersecurity Framework porque ayudaría a la institución a comprender sus procesos, gestionar y reducir sus riesgos y proteger sus redes y datos. Este modelo mejoraría a proporciona un lenguaje común entre el personal de ti y una estrategia de las mejores prácticas que ayudarían a mitigar los ataques de los ciberdelicuentes.
2	¿Cómo es el funcionamiento de los activos?	Es priorizar y determinar el alcance de todos los activos de la organización, identificar sus objetivos de negocio y las prioridades de alto nivel de la institución. Con esta información se puede determinar sus productos, servicios y su alcance al modelo ciberseguridad que serán abordados.
3	¿Cuál es la importancia de realizar el análisis de riesgos?	Ayudará a mejora a la institución a identificar los riegos emergentes teniendo en cuenta la verificación de las vulnerabilidades de los activos a nivel de red y aplicaciones, las amenazas de ataques de ciberdelicuentes de fuentes internas y externas para obtener una mejor compresión de las probabilidades y el impacto de los eventos. Es muy factible que el análisis de riegos se realice internamente realizando pruebas de ataques a los activos de la institución para verificar el estado de eficacia que se encuentra la seguridad , para poder mejorar los controles y políticas.
4	¿Cómo elaborar el plan de acción para la gestión de la ciberseguridad?	Para la elaboración de plan de acción se debe abordar la mejor estrategia y prácticas actuales de seguridad para lograr el objetivó, es importante que las acciones contemplen todos los puntos de la gobernanzas los procesos, políticas y procedimientos adecuados a la necesidad y realidad de la institución.

5	¿Cómo implementar el sistema de ciberseguridad?	La implementación se determinara mediante políticas de seguridad, controles y pasos específicos a seguir a fin de optimizar los procesos de intercambio de información y la respectivas coordinaciones para la gestión de los incidentes de seguridad de manera efectiva, fiable y eficiente
6	¿Cuál es la importancia sistema de ciberseguridad?	la importancia de contar con un sistema de ciberseguridad nos ayudara a reducir y prevenir un ataque de una persona no autorizada a nuestros activos ,nos proporcionara directrices para mejorar la seguridad mediante buenas prácticas y asegurar la información de las redes de internet y proteger las infraestructura de la entidad.

Anexo 4:

Matriz de codificación de la entrevista

N°	**Preguntas**	**Entrevistado 1 – Especialista en redes de datos**	**Entrevista 1 Codificada**
1	¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto?	La metodología más adecuada para proteger los activos de la institución es la iso 27032 de ciberseguridad que permitirá asegurar la confidencialidad integridad y disponibilidad de los activos digitales de la institución, es una solución dinámica que permitirá prevenir todo tipo de riesgo y amenazas interno como externo, a mi experiencia el modelo de ciberseguridad ayudara mejorara todos los procesos de seguridad que se encuentra en el ciberespacio en las aplicaciones, base de datos y los entornos de red ,por lo que su uso reducirá los riesgos de los ataques y la perdida de la información o secuestros, y los más	• Metodología Iso 27032 de ciberseguridad • Permitir la confiabilidad integridad y disponibilidad • Prevenir los riesgos y amenazas • Mejorar los procesos • Reducir los riesgos de los ataques y perdida de información • Continuidad de negocio

		importante es que la metodología garantizaría la continuidad del negocio .	
2	¿Cómo es el funcionamiento de los activos?	El funcionamiento de los activos consiste en identificar, analizar y conocer las técnicas y los procesos de los activos digitales de la institución sus funcionamiento y conocer que tan preparados están frente a los ataques de delincuentes cibernéticos, entender los productos y servicios que cuenta , verificar su normativa y documentación de seguridad, En la institución se priorizan los activos computacionales Los datos en general ya que cualquier dato es un activo importante para la institución ,y también es realizar un estudio en general de la institución desde el punto de vista de seguridad para poder saber todos los activos que se cuentan .uno de los activos más importantes es la base de datos donde se almacenan toda la información de los alumnos y docente.	• Identificar analizar y conocer las técnicas y procesos de los activos • Entender los productos y servicios • Verificar su normativa y documentación de seguridad • Priorizar los activos computacionales • Realizar un estudio general de los activos

3	¿Cuál es la importancia de realizar el análisis de riesgos?	La importancia de realizar un análisis es conocer las vulnerabilidad y amenazas de los activos de la institución los riesgos que se cuentan a diario. Realizar el análisis no permite evaluar la seguridad de la infraestructura de forma segura, el análisis nos ayuda a corregir el impacto y riesgo y estar prevenido frente a cualquier vulnerabilidad de los sistemas operativos, servicios y fallas de las aplicaciones, configuraciones incorrectas En mi experiencia realizar una evaluación de riesgo son muy utilices para validar la eficacia de las configuraciones de seguridad de la institución. una buena práctica es contratar a un especialista para que realice Una auditoria interna como externa a las aplicaciones de la institución e identificar el nivel de seguridad que se encuentra.	• Evaluar la seguridad de la infraestructura de forma segura • Corregir el impacto y riesgo de las vulnerabilidades • Validar la eficacia de las configuraciones • Una buena práctica es contratar un especialista • Identificar el nivel de seguridad que se encuentra
4	¿Cómo elaborar el plan de acción para la gestión de la ciberseguridad?	En esta etapa se Permitirá conocer y documentar las priorización y medidas de políticas de ciberseguridad para implementar en la institución alineando las mejores prácticas más importante identificando roles que se debe asumir el personal para la correcto funcionamiento de la seguridad y determinar los procesos que deben alinear a la institución para la protección de sus activos de	• Permitirá conocer las priorizaciones y medidas de políticas • Alineando las mejores practicas • Correcto funcionamiento de la seguridad • Procesos afectados que determinan los controles y

		información que se encuentran en la red digital, el plan de acción es una fase muy importante del modelo ciberseguridad ya que no permitirá conocer los procesos afectados y determinar los controles tecnológicos que nos permitirán mitigar los riegos de los activos.	permitirá mitigar los riesgos
5	¿Cómo implementar el sistema de ciberseguridad?	En esta etapa final ya conociendo el funcionamiento de los activos , los riesgos y su plan de acción, se ve debe crear existencia de políticas y procedimientos de seguridad en la institución ala ves crear marcos existentes para el intercambio de información entre la red de la institución, la capacitación al personal administrativo y docentes es una parte más importante para proteger la confiabilidad de la información, otro punto importante es la gestión de incidentes donde podemos tener mapeado y tomar medidas preventivas inmediatas para salvaguardar los activos. es muy importante seguir los lineamientos para la protección de los activos de información que se encuentran en el red de la institución, se podrá conocer e identificar los puntos clave en las cuales está más débil de tal medida que se pueda	• Crear existencia de políticas y procedimientos • Capacitaciones al personal administrativo y docente • Gestión de incidentes donde se tendrá mapeado y tomar medidas preventivas • Seguir los lineamientos para la protección de los activos

		fortalecer mediante controles y mecanismos de prevención en los procesos de la información .	
6	¿Cuál es la importancia del sistema de ciberseguridad?	Es de suma importancia contar con un sistema de ciberseguridad en la institución, para la protección de sus sistemas informáticos contra atacantes, ayuda a garantizar que la información privada permanezca privada, incluso cuando naveguemos a través de Internet. Al contar con un sistema de ciberseguridad la institución estaría a la vanguardia y los más altos estándares de seguridad.	• Garantizar que la información permanezca privada a través de la red • Estar a la vanguardia de los más altos estándares de seguridad

N°	**Preguntas**	**Entrevistado 2 – Administrador de redes**	**Entrevista 2 Codificada**
1	¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto?	Es muy importante para la institución educativa contar con un modelo de ciberseguridad para poder tener establecidos procedimientos de estándares de seguridad que mejoren el proceso de negocios. La metodología de la iso 27032 nos brinda un marco de ciberseguridad para mejora los lineamientos para identificar los riesgos a los cuales están expuestos en la red y que pueda llegar a afectar los activos de la institución nos brindara controles necesarios para implementar y asegurar de manera efectiva los diferentes activos de información.	• Tener establecidos procedimientos de estándares de seguridad que mejoren el proceso de negocios • Mejorar los lineamientos para identificar los riesgos • Asegurar de manera efectiva los diferentes activos

2	¿Cómo es el funcionamiento de los activos?	En esta etapa es reconocer el funcionamiento de los activos de la institución educativa identificar el tamaño o la magnitud el tipo o modelo de negocio, su regularización bajo la cual debe regir los productos y servicios que brinda en la institución, entender el tipo de tecnología implementada los mecanismo de seguridad con los que se cuenta, entender como está constituida la institución saber todos sus procesos como revisar su normativa de seguridad ala ves recopilar y revisar los documentaciones de seguridad y por ultimo conocer las técnicas implementadas , mediante el reconociendo de la institución podemos saber los activos más importantes que se cuenta y poder realizar una análisis de riesgos y saber el nivel de seguridad que cuenta la institución educativa.	• Identificar el tamaño o la magnitud del modelo de negocio • Entender el tipo de tecnología implementada, los mecanismos de seguridad • Entender como está constituida la institución y sus procesos • Revisar los documentos de seguridad, técnicas implementadas • Saber los activos más importantes y realizar un análisis de riesgos

3	¿Cuál es la importancia de realizar el análisis de riesgos?	Es importante realizar un análisis de riesgos en la institución educativa porque permitirá realizará un diagnostico en la cual se identificará las vulnerabilidades de cada uno de los activos de información junto con su criticidad y como también el nivel de su exposición al riesgo respeto a su nivel de preparación frente a los ataques de los ciberdelicuentes. unos de los puntos más importantes es que nos ayudara a verificar los activos críticos, amenazas ,vulnerabilidades , impacto, riesgo e identificar los responsables .	• Identificar las vulnerabilidades de los activos • Nivel de exposición al riesgo respeto a su nivel de preparación • Verificar los activos críticos
4	¿Cómo elaborar el plan de acción para la gestión de la ciberseguridad?	El plan de acción es identificar los puntos más importantes de la institución educativa para la elaboración de políticas de mejoras donde el personal de ti y en general toda la institución conozcan los métodos, controles y el proceso de resguardar y prevenir una fuga o daños a los sistemas de información, para que el plan de acción funcione de manera eficaz lo primero que tiene que hacer la institución es realizar un escaneo y verificación de todos los activos para poder entender donde se encuentra las vulnerabilidades de los sistemas de información, para poder elaborar políticas, roles, métodos procesos y controles.	• Elaboración de políticas de mejoras donde el personal de ti y en general conozcan los métodos • Realizar un escaneo y verificación de todos los activos donde poder verificar las vulnerabilidades • Elaborar políticas ,roles y métodos procesos y controles

5	¿Cómo implementar el sistema de ciberseguridad?	La implementación proporcionara directrices que mejorara la seguridad digital de la institución educativa mediante las buenas prácticas de resguardar y proteger la información y como se logra ese cometido mediante existencia y creación de políticas y controles de seguridad	• Proporcionará directrices que mejorará la seguridad digital • Buenas prácticas de resguardar y proteger la información • Existencia y creación de políticas y controles de seguridad
6	¿Cuál es la importancia del sistema de ciberseguridad?	La importancia de contar con un sistema de ciberseguridad En la institución ayudara a proteger los sistemas contra diversas amenazas que dañen los sistemas de información, en mi experiencia uno de los ataques más comunes y peligros es el ramsomware que te secuestra la información y te pide un rescate por eso la importancia de contar con un sistema de ciberseguridad que permita mitigar los riesgos y también que el personal de la institución comprenda la importancia de contar con un sistema de prevención.	• Proteger los sistemas contra diversas amenazas que dañes los sistemas de información • Que permita mitigar los riesgos • Contar con un sistema de prevención

N°	Preguntas	Entrevistado 3 – Especialista de Infraestructura	Entrevista 3 Codificada
1	¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto?	El modelo que mejoraría la estrategia de la seguridad seria Nist Cybersecurity Framework porque ayudaría a la institución a comprender sus procesos, gestionar y reducir sus riesgos y proteger sus redes y datos. Este modelo mejoraría a proporcionar un lenguaje común entre el personal de ti y una estrategia de las mejores prácticas que ayudarían a mitigar los ataques de los ciberdelicuentes.	• Ayudaría a la institución a comprender sus procesos • Proteger sus redes y datos • Mejoraría a proporcionar un lenguaje común entre el personal de TI • Una estrategia de las mejores prácticas
2	¿Cómo es el funcionamiento de los activos?	En esta etapa se priorizar y determinar el alcance de todos los activos de la institución educativa, identificar sus objetivos de negocio y las prioridades de alto nivel que cuenta. Con esta información se puede determinar sus productos, servicios y su alcance al modelo ciberseguridad que serán abordados y implementados .	• Se prioriza y determina el alcance de todo el activo • Identificar sus objetivos de negocio • Determinar sus productos y servicios
3	¿Cuál es la importancia de realizar el análisis de riesgos?	Es esta etapa el análisis de riesgos mejora a la institución a identificar los riegos emergentes teniendo en cuenta la verificación de las vulnerabilidades de los activos a nivel de red y aplicaciones, las amenazas de ataques de los ciberdelicuentes, de las fuentes internas y externas para obtener una mejor	• Mejorará a identificar los riesgos emergentes • Verificación de las vulnerabilidades de los activos • Mejor compresión de las probabilidades y

		compresión de las probabilidades y el impacto de los eventos. Es muy factible que el análisis de riegos se realice internamente realizando pruebas de ataques a los activos de la institución educativa para verificar el estado de eficacia que se encuentra la seguridad , para poder elaborar una documentación de mejorar los controles y políticas.	el impacto de los eventos • Muy factible que el análisis de riesgo se realice internamente • Verificar el estado de eficacia de la seguridad
4	¿Cómo elaborar el plan de acción para la gestión de la ciberseguridad?	En esta etapa ya conociendo el análisis de riesgo se podrá elaboración el plan de acción se debe abordar la mejores estrategia y prácticas actuales de seguridad para lograr el objetivó, es importante que las acciones contemplen todos los puntos de la gobernanzas los procesos, políticas y procedimientos adecuados a la necesidad y realidad de la institución educativa.	• Abordar las mejores estrategias y prácticas actuales de seguridad • Es importante que las acciones contemplen todos los puntos de la gobernanza de procesos
5	¿Cómo implementar el sistema de ciberseguridad?	La implementación es la etapa final se determinara mediante las creaciones de políticas de seguridad, controles y pasos específicos a seguir a fin de optimizar los procesos de intercambio de información y la respectivas coordinaciones para la gestión de los incidentes de seguridad de manera efectiva, fiable y eficiente para mejorar los procesos de la institución educativa	• Creaciones de políticas de seguridad y controles • Optimizar los procesos de intercambio de información • Coordinaciones para la gestión de los incidentes de seguridad de manera efectiva

6	¿Cuál es la importancia del sistema de ciberseguridad?	la importancia de contar con un sistema de ciberseguridad en la institución educativa nos ayudara a reducir y prevenir un ataque de una persona no autorizada a nuestros activos ,nos proporcionara directrices para mejorar la seguridad mediante buenas prácticas y asegurar la información de las redes de internet y proteger las infraestructura .	• Ayudará a reducir y prevenir un ataque de una persona no autorizada • Proporcionará directrices para mejorar la seguridad • Buenas prácticas y asegurar la información

Anexo 5

Matriz de entrevistados y conclusiones

N°	Pregunta	E_1 – Especialista en redes de datos	E_2 – Administrador de redes	E_3 – Especialista de Infraestructura	Similitud	Diferencias	Conclusión
1	¿Qué modelo de ciberseguridad mejoraría la gestión de tecnología de información en el instituto?	1. Metodología Iso 27032 de ciberseguridad 2. Permitir la confiabilidad integridad y disponibilidad 3. Prevenir los riesgos y amenazas 4. Mejorar los procesos 5. Reducir los riesgos de los ataques y perdida de información 6. Continuidad de negocio	a. Tener establecidos procedimientos de estándares de seguridad que mejoren el proceso de negocios b. Mejorar los lineamientos para identificar los riesgos c. Asegurar de manera efectiva los diferentes activos	I. Ayudaría a la institución a comprender sus procesos II. Proteger sus redes y datos III. Mejoraría a proporcionar un lenguaje común entre el personal de ti IV. Una estrategia de las mejores prácticas	E1, E2 E3: Coinciden que una metodología de ciberseguridad mejorara a identificar los riegos y las vulnerabilidades de la institución educativa, y así reducir los riegos y amenazas de los sistemas de informáticos.	E1: detalla que la metodología de ciberseguridad se centra en los tres pilares más importantes de la seguridad, confidencialidad, integridad y disponibilidad. E2: Adiciona que la metodología de ciberseguridad mejorara los estándares , lineamientos de seguridad para el correcto funcionamiento del negocio E3: Adiciona que la metodología	La metodología de ciberseguridad mejorará la protección del sistema de información a nivel del ciberespacio, con la implementación de las políticas y controles se podrá prevenir los ataques de los ciberdelicuentes y mitigar las amenazas a los equipos de sistemas de información mediante la buena práctica y continuar con la continuidad del negocio.

						brindara una mejor estrategia de las buenas prácticas de seguridad	

2	¿Cómo es el funcionamiento de los activos?	1. Identificar analizar y conocer las técnicas y procesos de los activos 2. Entender los productos y servicios 3. Verificar su normativa y documentación de seguridad 4. Priorizar los activos computacionales 5. Realizar un estudio general de los activos	a. Identificar el tamaño o la magnitud del modelo de negocio b. Entender el tipo de tecnología implementada, los mecanismos de seguridad c. Entender como está constituida la institución y sus procesos d. Revisar los documentos de seguridad, técnicas implementadas e. Saber los activos más importantes y realizar un análisis de riesgos	I. Se prioriza y determina el alcance de todo el activo II. Identificar sus objetivos de negocio III. Determinar sus productos y servicios	E1, E2 E3: Coinciden que en esta etapa de implantación es muy importante identificar todos los activos y servicios , a nivel físico y lógico , conocer la documentaciones seguridad que existe , sus técnicas, sus mecanismo de prevención .	E3: Considera que que es importante identificar los objetivos de negocios ,ya que nos ayudaría a mejorar la implementación de la metodología.	Es importante conocer el funcionamiento de los activos para lograr objetivos claros de ciberseguridad, conocer la magnitud del negocio y su alcance.

3	¿Cuál es la importancia de realizar el análisis de riesgos?	1. Evaluar la seguridad de la infraestructura de forma segura 2. Corregir el impacto y riesgo de las vulnerabilidades 3. Validar la eficacia de las configuraciones 4. Una buena práctica es contratar un especialista 5. Identificar el nivel de seguridad que se encuentra	a. Identificar las vulnerabilidades de los activos b. Nivel de exposición al riesgo respeto a su nivel de preparación c. Verificar los activos críticos	I. Mejorará a identificar los riesgos emergentes II. Verificación de las vulnerabilidades de los activos III. Mejor compresión de las probabilidades y el impacto de los eventos IV. Muy factible que el análisis de riesgo se realice internamente V. Verificar el estado de eficacia de la seguridad	E1, E2 E3: Coinciden que el análisis de riesgos ayudara a evaluar el nivel de seguridad que se encuentran los activos, identificar sus vulnerabilidades. Para poder mejorar la configuraciones de los equipos de seguridad.	E1: Manifiesta que es importante contratar a un especialista de seguridad para que evalué el nivel de seguridad que se encuentra los activos de información	Se debe realizar regularmente pruebas de pentesting para evaluar el nivel de seguridad que se encuentra los equipos de sistemas. Ayudar identificar los riesgos y amenazas emergentes que surgen constante mente.
4	¿Cómo elaborar el plan de acción para la gestión de la ciberseguridad?	1. Permitirá conocer las priorizaciones y medidas de políticas 2. Alineando las mejores practicas 3. Correcto funcionamiento	a. Elaboración de políticas de mejoras donde el personal de ti y en general conozcan los métodos b. Realizar un escaneo y verificación de todos los activos	I. Abordar las mejores estrategias y prácticas actuales de seguridad II. Es importante que las acciones contemplen todos los	E1, E2 E3: coinciden que la elaboración de políticas, controles y roles mejorar las acciones contra las amenazas y riegos de los sistemas de información. Y	E3: Agrega que abordar las mejores estrategias y prácticas de seguridad, mejorara el plan de acción de ciberseguridad.	Se debe realizar una elaboración eficaz de las políticas y controles que ayuden a mejorar los sistemas digitales y físico de la

		de la seguridad 4. Procesos afectados que determinan los controles y permitirá mitigar los riesgos	donde poder verificar las vulnerabilidades c. Elaborar políticas ,roles y métodos procesos y controles	puntos de la gobernanza de procesos	su correcto funcionamiento.		institución basado en las mejores prácticas.
5	¿Cómo implementar el sistema de ciberseguridad?	1. Crear existencia de políticas y procedimientos 2. Capacitaciones al personal administrativo y docente 3. Gestión de incidentes donde se tendrá mapeado y tomar medidas preventivas 4. Seguir los lineamientos para la protección de los activos	a. Proporcionará directrices que mejorará la seguridad digital b. Buenas prácticas de resguardar y proteger la información c. Existencia y creación de políticas y controles de seguridad	I. Creaciones de políticas de seguridad y controles II. Optimizar los procesos de intercambio de información III. Coordinaciones para la gestión de los incidentes de seguridad de manera efectiva	E1, E2 E3: coinciden en la existencia y creación de políticas y controles de seguridad basado en las buenas prácticas de guardar y proteger la información.	E1: Agrega que las capacitaciones al personal son muy importantes ya que contando con personal que conozcan la importancia de la seguridad ayudara a reducir los riesgos a los sistemas computacionales. E3: Agrega la importancia de la gestión de incidentes ya que mejorar la forma de responder a cualquier sistema vulnerado	La implementación Mejorar todos los procesos de seguridad basado en las buenas practicas donde las existencia de política y controles reducirán todas las incidencias que puedan dañar la institución.

						tomando soluciones de tratamiento de riesgos para una recuperación inmediata.	
6	¿Cuál es la importancia del sistema de ciberseguridad?	1. Garantizar que la información permanezca privada a través de la red 2. Estar a la vanguardia de los más altos estándares de seguridad	a. Proteger los sistemas contra diversas amenazas que dañes los sistemas de información b. Que permita mitigar los riesgos c. Contar con un sistema de prevención	I. Ayudará a reducir y prevenir un ataque de una persona no autorizada II. Proporcionará directrices para mejorar la seguridad	E1, E2, E3: Coinciden en la importancia de un sistema de ciberseguridad para garantizar que la información no sea alterada mientras viaja por la red.	E1: Agrega que contar con metodología de ciberseguridad actualizada ayudara a mejorar la eficacia de prevención de los ciberdelicuentes,	Es importante contar con modelo de ciberseguridad que nos permita proteger los activos ,y estar a la vanguardia de los estándares más altos de seguridad.

En conclusión, la propuesta de la metodología de ciberseguridad es de gran beneficio para la institución educativa, porque se podrá tener toda información de los activos basado en la iso 27032 que nos permitirá reducir las vulnerabilidades de los activos digitales evitando los riesgos y perdida de información y protegiendo a la institución de las amenazas de los ciberdelicuentes.

Anexo 6

Guía de Observación

Empresa:	Instituto superior publico
Ubicación:	Avenida Los Alisos Nº 950 - Urb. Carlos Cueto Fernándini Los Olivos - Lima - Perú
Área:	Departamento de Tecnología
Observador:	Victor Hugo Manrique Reyna

Redacción de lo observado sobre las (03) especialistas, donde E1: Especialista en redes de datos E2: Administrador de redes y E3: Especialista en infraestructura.

Se observa en la institución no cuenta con un proceso óptimo de la gestión de los Activos, se identifica que hay un desorden de los inventarios de la arquitectura de ti Evidenciando la falta de un marco de ciberseguridad.

Se observa que no se cuenta con un análisis de riesgos que pueda mejorar la arquitectura de seguridad de los equipos de ti, se identifica que los equipos como el servidor, las aplicaciones

web y el entorno de red de comunicaciones no cuentan con calidad de seguridad.

Se observa que tampoco hay un plan de elaboración de políticas y controles que puedan mitigar los riesgos y amenazas que puedan ocurrir en la institución, se evidencia la falta de un plan de acción de políticas que puedan capacitar a los administrativos, docentes y alumnos.

Se observa se no cuentan con una planificación para implementar un marco de ciberseguridad

La institución tiene un proceso de seguridad que no basta para poder proteger todos los activos, y los más importante proteger la información de los alumnos, se evidencia las vulnerabilidades que cuenta la institución.

De los observado concluyo que los procesos de trabajo de área de tecnología de la institución no son muy seguros no evalúan los riesgos que puedan ocurrir, ya que no conocen las amenazas que puedan ocurrir en los equipos tecnológicos, no existe un control de los accesos a los sistemas, ya que el usuario accede a equipos o paginas no autorizadas, los procesos y procedimientos de seguridad no se tienen los controles adecuados, no se cuenta con un estándar de seguridad que puedan contribuir a mejorar las buenas prácticas de ciberseguridad ,los administrativos no tienen conocimientos de la importancia de contar con políticas de seguridad.

Anexo 7:

Ficha de Análisis Documental

Empresa:	Instituto superior publico
Ubicación:	Avenida Los Alisos Nº 950 - Urb. Carlos Cueto Fernándini Los Olivos - Lima - Perú
Área:	Departamento de Tecnología
Observador:	Victor Hugo Manrique Reyna

El departamento de Tecnología del instituto , tienen a cargo distintas áreas administrativas y plataformas tecnológicas ,pero no son correctamente gestionados a nivel de seguridad , existe ausencia de políticas de ciberseguridad y el poco conocimiento que se tiene no son correctamente cumplidos por los administrativos de manera que se genera un alto riesgo de seguridad , los servicios de tecnología del instituto no son gestionados de manera adecuada, creando riesgos críticos y no se cuenta con una plan de acción donde se pueda registrar y controlar las incidencias que puedan suceder en el sistema web, en las redes de comunicación y la base de datos. se ha observado que no hay una capacitación al técnico de tecnología, cuando realizan soluciones a las incidencias con poco conocimiento, generando muchas más vulnerabilidades en los servicios tecnológicos.

En base a lo analizado, la metodología de la norma ISO 27032, aportará un marco metodológico y de buenas prácticas en la implementación de ciberseguridad en la institución, fijando políticas y controles que proporcionará procesos seguros, confiable, eficaz y eficiente de intercambio de información y respuestas a incidentes y se lograra la continuidad de los procesos académicos.

En conclusión, el departamento tecnológico ha sido poco eficiente a las soluciones de los servicios tecnológicos, por no contar con lineamiento de políticas de ciberseguridad, las aplicaciones, entorno de red y base de datos no cuentan con lineamientos de políticas, y no hay un nivel de medir los riesgos que afecten el funcionamiento de los servicios, no se cuenta con una planificación de salvaguardar y proteger los activos de la institución. Por lo cual, implementando la norma 27032

se logrará crear políticas ciberseguridad en todos los lineamientos de cada proceso de los servicios tecnológico, se podrá medir los riesgos y amenazas y su impacto que pueda ocasionar en la institución, creando confianza y seguridad en el entorno del ciberespacio.

Anexo 8

PROPUESTA

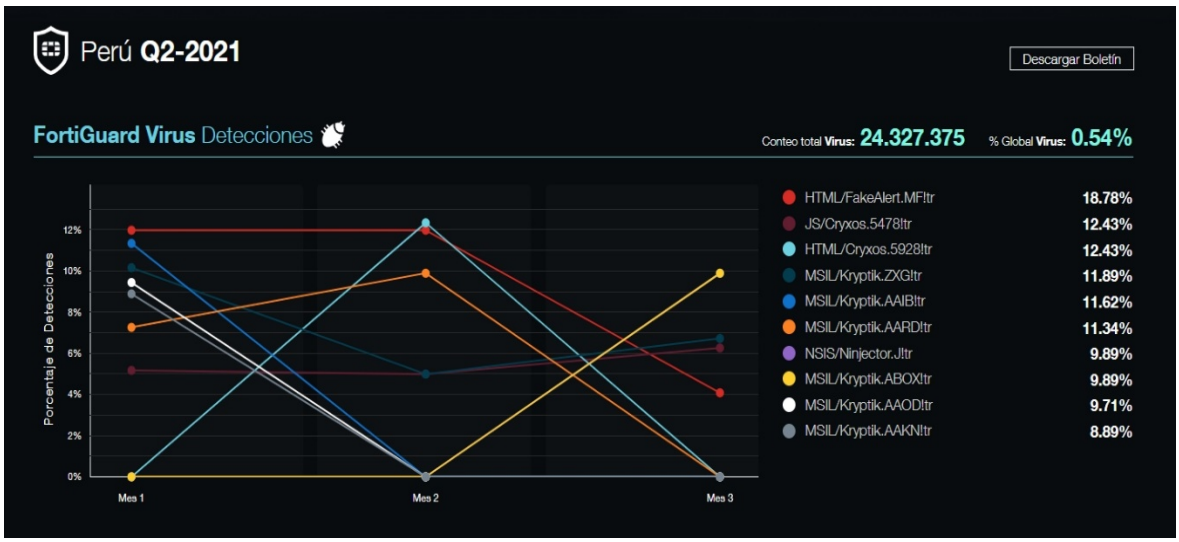
Implementar una metodología de Ciberseguridad en el instituto superior, tomando como base la norma ISO 27032 mediante la cual se pueda identificar cada uno de los factores que define la misma a fin de establecer las mejores prácticas para dar respuesta de manera efectiva a un incidente en el cual se vean comprometido y pueda llegar a ser críticos para la continuidad de los servicios tecnológicos. Partiendo de la premisa que la institución está expuesta a riesgos de diferentes formas a nivel de aplicaciones, entorno de red y base de datos.

Según el informe TI latín América (2021) un número creciente de dispositivos conectados, ha tenido una serie de impactos positivos en las instituciones de educación superior. Desde los servicios en la nube hasta Internet de las Cosas (IoT), los estudiantes y profesores ahora pueden mantenerse conectados mientras se encuentran fuera del aula para mejorar el aprendizaje y la investigación.

Sin embargo, todo este intercambio de información también ha abierto las puertas al aumento de la actividad cibercriminal dirigida a instituciones educativas.

Figura 5

ataques ciberneticos



Fuente: *TI latín América (2021)*

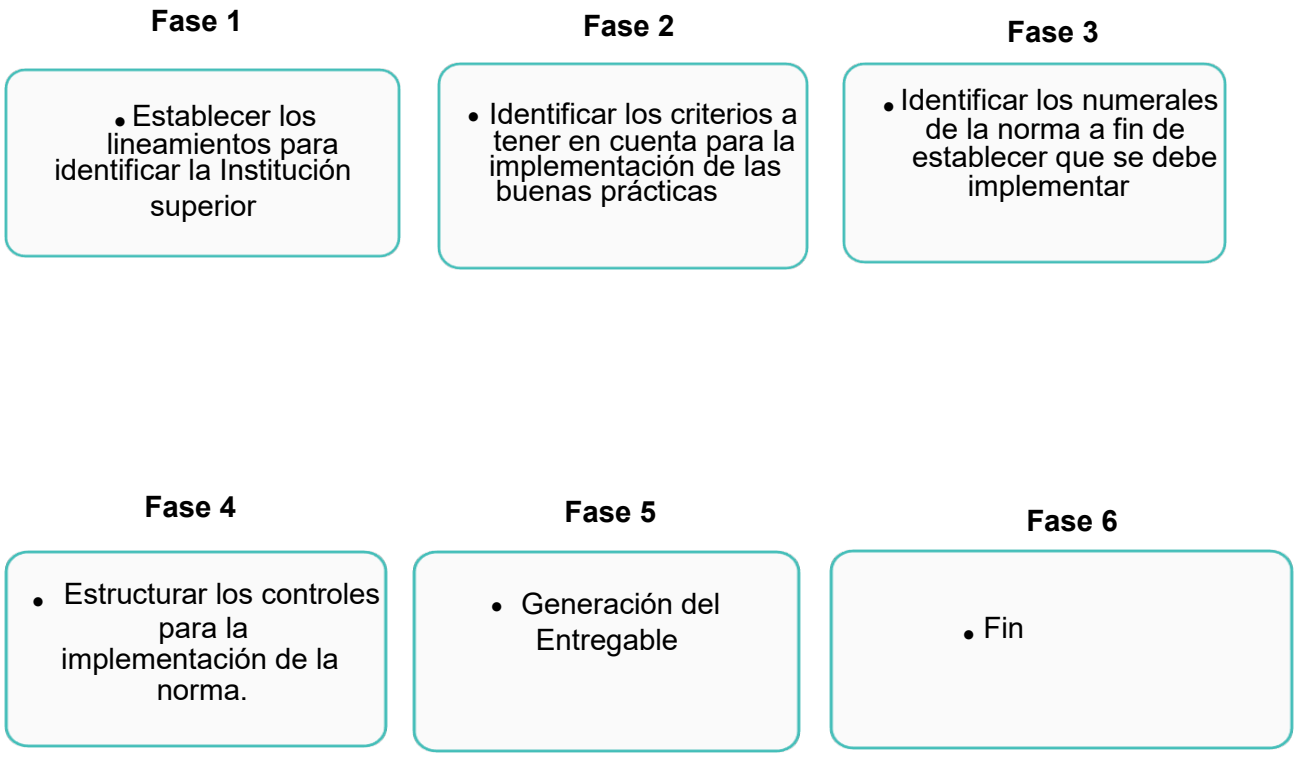
Solución Estimada:

Implementación:

El enfoque de la investigación es proporcionar una propuesta de un modelo de ciberseguridad donde se pretende realizar una recolección de información mediante el marco de referencia COBIT, que nos permitirá identificar los requerimientos de la institución y no ayudará a definir los lineamientos de la norma ISO 27032 para que sea aplicada.

Figura 6

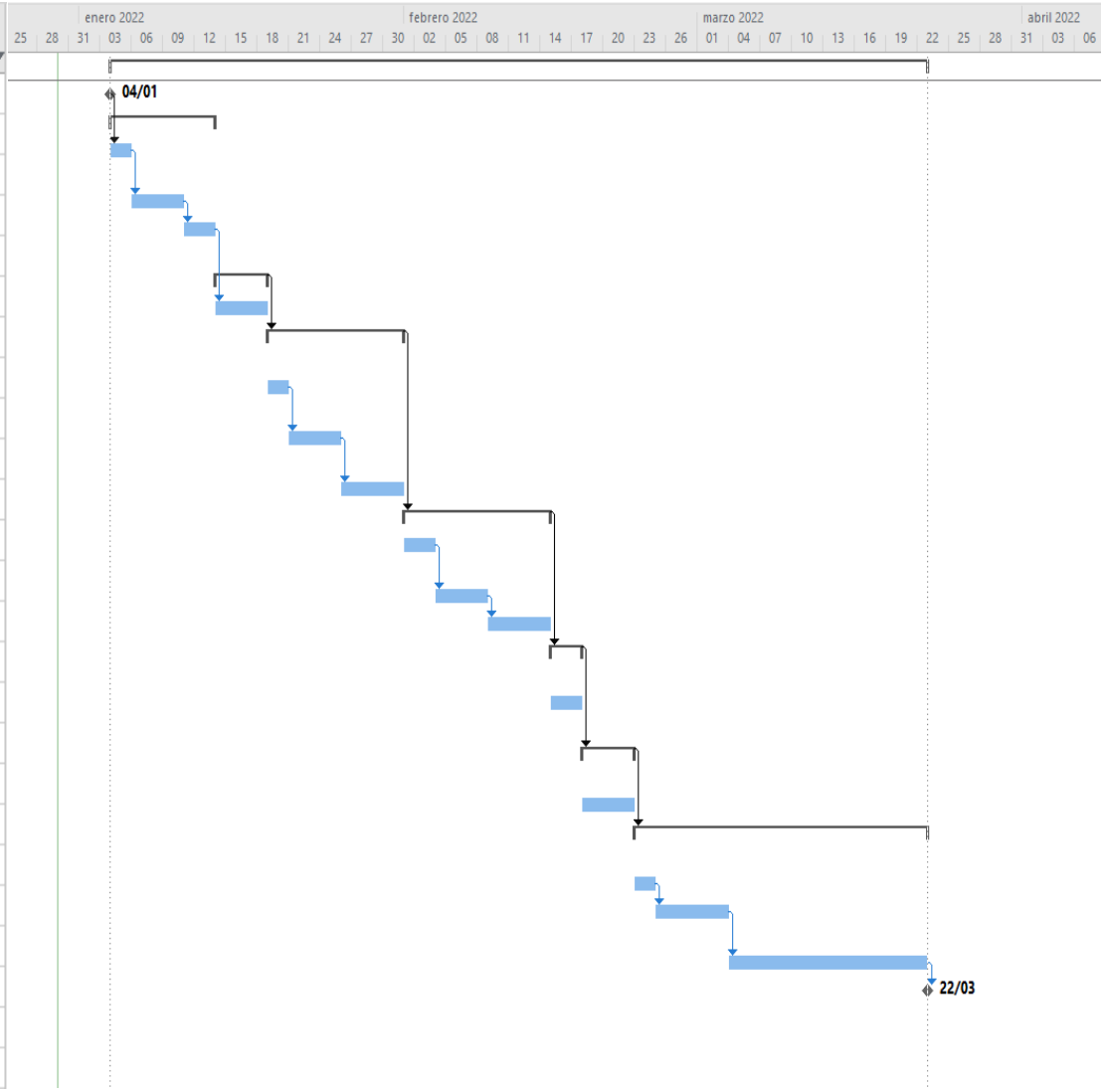
Faces de la implementacion



CRONOGRAMA DE ACTIVIDADES

DIAGRAMA DE GANTT

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**1 DESARROLLO DE PROYECTO**	**56 días**	**mar 04/01/22**	**mar 22/03/22**	
2	1.1 INICIO	0 días	mar 04/01/22	mar 04/01/22	
3	**1.2 Fase 1: PRIORIZACION**	**8 días**	**mar 04/01/22**	**jue 13/01/22**	
4	1.2.1 Identificar Situacion actual de la Institucion	2 días	mar 04/01/22	mié 05/01/22	2
5	1.2.2 Analisis de ciberseguridad	3 días	jue 06/01/22	lun 10/01/22	4
6	1.2.3 Identificar partes interesadas claves	3 días	mar 11/01/22	jue 13/01/22	5
7	**1.3 FASE 2: ORIENTACION**	**3 días**	**vie 14/01/22**	**mar 18/01/22**	
8	1.3.1 Recopilacion de datos	3 días	vie 14/01/22	mar 18/01/22	6
9	**1.4 FASE 3: DEFINICION DEL PERFIL ACTUAL**	**9 días**	**mié 19/01/22**	**lun 31/01/22**	**7**
10	1.4.1 Identificacion de nivel de madurez actual	2 días	mié 19/01/22	jue 20/01/22	
11	1.4.2 Identificacion de activos y sistemas	3 días	vie 21/01/22	mar 25/01/22	10
12	1.4.3 Analisis de las categorias	4 días	mié 26/01/22	lun 31/01/22	11
13	**1.5 FASE 4: ANALISIS DE RIESGOS**	**10 días**	**mar 01/02/22**	**lun 14/02/22**	**9**
14	1.5.1 Indetificacion de vulnerabilidades	3 días	mar 01/02/22	jue 03/02/22	
15	1.5.2 Deteccion de riesgos	3 días	vie 04/02/22	mar 08/02/22	14
16	1.5.3 Identificacion de amenazas	4 días	mié 09/02/22	lun 14/02/22	15
17	**1.6 FASES 5: DEFINICION DEL PERFIL OBJECTIVO**	**3 días**	**mar 15/02/22**	**jue 17/02/22**	**13**
18	1.6.1 Determinar nivel de madures del objectivo	3 días	mar 15/02/22	jue 17/02/22	
19	**1.7 FASE 6: DETERMINACION DE BRECHAS**	**3 días**	**vie 18/02/22**	**mar 22/02/22**	**17**
20	1.7.1 Identificacion de brechas	3 días	vie 18/02/22	mar 22/02/22	
21	**1.8 FASE 7: DISEÑO DE LA IMPLEMENTACION**	**20 días**	**mié 23/02/22**	**mar 22/03/22**	**19**
22	1.8.1 Culminacion de brechas	2 días	mié 23/02/22	jue 24/02/22	
23	1.8.2 Alineacion con el estandar de ciberseguridad	5 días	vie 25/02/22	jue 03/03/22	22
24	1.8.3 Diseño de la arquitectura	13 días	vie 04/03/22	mar 22/03/22	23
25	1.8.4 FIN	0 días	mar 22/03/22	mar 22/03/22	24



IMPLEMENTAR CONTROLES DE LA NORMA ISO 27032

Numerales ISO 27032

Numeral	Descripción
1	Alcance
2	Aplicabilidad
3	Referencias
4	Termino
5	Abreviaturas
6	Generalidades
7	Partes interesadas en el Ciberespacio
8	Activos en el Ciberespacio
9	Amenazas contra la seguridad del espacio
10	Roles de las partes interesadas en la ciberseguridad
11	Directrices para los interesados
12	Controles de Ciberseguridad
13	Marco del intercambio de información

Numeral	Descripción	Objetivo
1	Alcance	• Seguridad de la información • Seguridad de las redes • Seguridad de internet • Protección de la infraestructura crítica de información (CIIP)
	Aplicabilidad	• La ciberprotección, • El delito informático (cibercrimen) • La protección de la infraestructura crítica de información (CIIP) • La seguridad en internet • Los delitos relacionados con internet.
3	Referencia y Normativas	• Referencia la norma indica la ISO/IEC 27000, Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información.
4	Términos y definiciones	• La norma toma los términos y definiciones indicados en la ISO/IEC 27000.
5	Términos abreviados	• Describen las abreviaturas que se usan en los diferentes requerimientos que contiene la norma.
6	Generalidades	• Introducción • La naturaleza del Ciberespacio • La naturaleza de la ciberseguridad • Modelo general • Enfoque
7	Interesados en el ciberespacio	• Resumen • Consumidores • Proveedores • Resumen
8	Activos en el ciberespacio	• Bienes personales • Activos de la organización
9	Amenazas contra la seguridad del ciberespacio	• Amenazas • Agentes de la amaneza • Vulnerabilidades • Mecanismos de ataque

10	Roles de las partes interesadas en la ciberseguridad	• Función de los consumidores • Funciones de las organizaciones • Funciones de los proveedores
11	Directrices para los interesados	• Evaluación y tratamiento de los riesgos • Directrices para los consumidores • Directrices para organizaciones y proveedores de servicios • Controles de nivel de aplicación
12	Controles de ciberseguridad	• Protección del servidor • Controles para el usuario Final • Controles contra los ataques de ingeniería Social
13	Marco de intercambio y coordinación de la información	• Políticas • Métodos y procesos • Personas y organizaciones • Técnicas

UNIVERSIDAD CÉSAR VALLEJO

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

Lima, 13 de diciembre de 2021
Carta P. 1638-2021-UCV-VA-EPG-F01/J

Dr.
Mario Moreno Herrera
Director
IESTP Manuel Arévalo Cáceres

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a MANRIQUE REYNA, VICTOR HUGO; identificado con DNI N° 43657417 y con código de matrícula N° 7000608436; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un Instituto Superior Tecnológico público, Lima - 2021

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador MANRIQUE REYNA, VICTOR HUGO asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Ormeño Trinidad Vargas, MBA
Jefe (e)
Escuela de Posgrado
UCV FILIAL LIMA
CAMPUS LIMA NORTE

MINISTERIO DE EDUCACIÓN DIRECCIÓN MANUEL ARÉVALO CÁCERES

DR. MORENO HERRERA, MARIO FRANCISCO
DIRECTOR