UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

MAESTRÍA EN INFORMÁTICA

TESIS

SEGURIDAD INFORMÁTICA EN LA PLATAFORMA VIRTUAL DEL VICERRECTORADO DE INVESTIGACIÓN DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO DE PUNO - 2019

PRESENTADA POR:

EDSON DENIS ZANABRIA TICONA

PARA OPTAR EL GRADO ACADÉMICO DE:

MAESTRO EN INFORMÁTICA

CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

PUNO, PERÚ

2023

NOMBRE DEL TRABAJO

SEGURIDAD INFORMÁTICA EN LA PLAT AFORMA VIRTUAL DEL VICERRECTORA DO DE INVESTIGACIÓN DE LA UNIVERSI DAD

AUTOR

EDSON DENIS ZANABRIA TICONA

RECUENTO DE PALABRAS

20734 Words

RECUENTO DE CARACTERES

115746 Characters

RECUENTO DE PÁGINAS

91 Pages

TAMAÑO DEL ARCHIVO

1.9MB

FECHA DE ENTREGA

Dec 11, 2023 6:24 PM GMT-5

FECHA DEL INFORME

Dec 11, 2023 6:25 PM GMT-5

12% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base c

- 11% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr
- 6% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 12 palabras)

Dr. Jose P. Titolipa
DNI 08347804

Ing. Jared Luque Coila
ESTADISTICO E INFORMATICO
CIP. 116625

UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

MAESTRÍA EN INFORMÁTICA

TESIS

SEGURIDAD INFORMÁTICA EN LA PLATAFORMA VIRTUAL DEL VICERRECTORADO DE INVESTIGACIÓN DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO DE PUNO - 2019

PRESENTADA POR:

EDSON DENIS ZANABRIA TICONA

PARA OPTAR EL GRADO ACADÉMICO DE:

MAESTRO EN INFORMÁTICA

CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

APROBADA POR EL JURADO SIGUIENTE:

PRESIDENTE

.....

Dr. BERNABÉ CANQUI FLORES

PRIMER MIEMBRO

.....

Dr. SAMUEL DONATO PEREZ QUISPE

SEGUNDO MIEMBRO

.....

M.Sc. CHARLES IGNACIO MENDOZA MOLLOCONDO

ASESOR DE TESIS

.....

Dr. JOSÉ PAFILO TITO LIPA

Puno, 09 de enero de 2023

ÁREA: Auditoría Informática.
TEMA: Seguridad informática en la plataforma virtual del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno - 2019.
LÍNEA: Seguridad Informática.

DEDICATORIA

Dedico el presente trabajo de investigación a mis seres queridos más cercanos, a mi prometida Maricielo, quien con su amor, optimismo, sentido de responsabilidad, me enseña que para lograr nuestros objetivos la constancia y la disciplina son fundamentales, por incentivarme y motivarme a seguir adelante, por florecer nuestro amor en Massielita, motivo más grande en nuestras vidas, a mi abuelita Asunta quien con su cariño y su constante atención me demuestra la resiliencia que se debe tener para lograr nuestras metas, a mi madre Leonarda Victoria mi soporte emocional, por inspirarme a seguir estudiando y especializándome; a mi padre Fidel por enseñarme que la perseverancia y el trabajo constante son importantes para lograr nuestros objetivos, por motivarme con su esfuerzo y optimismo, por demostrarme su cariño con trabajo constante.

AGRADECIMIENTOS

En primera instancia agradecer a Dios, que guía nuestros caminos y hace posible nuestros éxitos, agradecimientos especiales a mis padres, quienes son el principal motor de motivación, a mi asesor Dr. José Tito L. por guiar con sus conocimientos y experiencia este trabajo de investigación. A los ingenieros que laboran en el Vicerrectorado de investigación, quienes colaboraron con la ejecución de la presente investigación y por último agradecer a la Universidad Nacional del Altiplano Puno por la formación que nos brinda y las oportunidades que nos abre.

ÍNDICE GENERAL

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

CAPÍTULO III

MATERIALES Y MÉTODOS

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

RESUMEN

En la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno en 2019, se planteó la hipótesis de la existencia de una probabilidad de riesgo en la seguridad informática, en relación a la ocurrencia de amenazas e impacto en daños. El principal objetivo de esta investigación fue determinar el nivel de riesgo en seguridad informática mediante políticas y estándares ISO 17799, bajo un diseño descriptivo transversal-exploratorio, lo que permitió la implementación de procesos y procedimientos seguros en el manejo y seguridad de la información. Los resultados generales de esta investigación mostraron que el 40,6 % de los ítems observados tenían un alto impacto, y la probabilidad de ocurrencia fue de nivel medio; en seguridad informática, esto representa un alto riesgo en el manejo de la información. También se observó que el 68,6 % de los ítems con alta probabilidad de ocurrencia tuvieron un alto impacto en el nivel de seguridad, los cuales serán reforzados en base a los hallazgos. En conclusión, se determinó que el nivel de riesgo en seguridad informática en la plataforma del Vicerrectorado de Investigación fue alto, de acuerdo con los activos que podrían verse comprometidos en caso de nuevos ataques a la seguridad informática.

Palabras clave: análisis de riesgos, ISO 17799, SGSI, seguridad de la información, seguridad informática.

ABSTRACT

On the platform of the Vice president for Research of the National University of the Altiplano of Puno in 2019, the hypothesis is raised, there is a probability of information security risk of threat occurrence and damage impact. The main objective of this research was to determine the level of information security risk through ISO 17799 policies and standards, under the exploratory transactional descriptive design that allowed the implementation of safe processes and procedures in terms of information management and security. The results of this investigation in a general analysis showed that 40.6% of the items observed are of high impact and the probability of occurrence was medium, in computer security this represents a high risk in the handling of information, it is also observed that the 68.6% of items in terms of the probability of high occurrence had a high impact on the level of security, that will be reinforced based on the findings. In conclusion, it was determined that the level of computer security risk in the platform of the investigation Vice president was high, according to the assets that are compromised if new attacks on computer security occur. Keywords: Risk analysis, ISO 17799, ISMS, information security, computer security occur.

Keywords: computer security, information security, ISMS, ISO 17799, risk análisis.

Dra. Ruth F. Boza Condorena
DOCENTE - UNA

INTRODUCCIÓN

Cuando hablamos de seguridad, podemos atribuirle múltiples significados, dependiendo del contexto en el que se utilice, lo que lo convierte en un término ambiguo e impreciso. En un sentido general, puede entenderse como un conjunto de técnicas diseñadas para prevenir, proteger y garantizar la integridad de todas las cosas consideradas vulnerables al robo, la pérdida o el daño. Si lo consideramos en el contexto de la tecnología de la información, podemos definirlo como un conjunto de normas, planes y acciones que aseguran la prestación de servicios y la protección de la información contenida en los sistemas informáticos. En este sentido, la información se convierte en el elemento primordial a proteger dentro de las redes organizacionales. Estas redes se enfrentan a amenazas informáticas procedentes de diversas fuentes, incluyendo aquellas provocadas por el ser humano, como el espionaje industrial, el sabotaje, los virus informáticos, los ataques o la piratería electrónica.

Hoy en día, experimentamos un fuerte auge en el ámbito de la seguridad informática, con la constante evolución de nuevas plataformas y cambios en las herramientas informáticas existentes. Esta dinámica se traduce en la continua aparición de amenazas y vulnerabilidades que afectan a los sistemas informáticos. La posibilidad de interconexión a través de Internet ha abierto amplios horizontes que permiten a las empresas aumentar su productividad y expandirse más allá de las fronteras nacionales, al mismo tiempo que conlleva nuevos y significativos riesgos para los sistemas de información de las organizaciones.

Para administrar adecuadamente la seguridad informática dentro de una organización y hacer frente a las amenazas mencionadas anteriormente, es fundamental contar con un sólido plan de seguridad informática. En este plan se definen la planificación, el diseño y la implementación de un modelo de seguridad con el objetivo de fomentar una cultura de seguridad en toda la organización. Esto implica prescindir de un plan de seguridad independiente, ya que debe estar en consonancia con las políticas de seguridad basadas en las necesidades de la institución. Este plan servirá para proteger la información y los activos de la organización, garantizando la confidencialidad, integridad y disponibilidad de los datos. Además, todos los colaboradores de la organización deben asumir la responsabilidad y el compromiso de cumplir dichas políticas. De esta manera, las políticas de seguridad informática se convierten en herramientas para establecer procedimientos

que los miembros de la organización deben seguir, al mismo tiempo que se hacen conscientes de la importancia y la sensibilidad de la información y de los servicios críticos que permiten el desarrollo y la continuidad de la organización.

El objetivo principal de la seguridad informática es reducir el riesgo y respaldar las operaciones comerciales. Para lograrlo, debe abarcar las siguientes áreas: seguridad del personal, seguridad de la información, seguridad de las comunicaciones y seguridad de los sistemas. Para que sea efectiva, la seguridad debe integrarse en los procesos comerciales en lugar de limitarse a aplicaciones técnicas específicas. Es importante destacar que no existe una solución de seguridad que pueda cubrir por completo todos los posibles riesgos, ni es completamente infalible. Por lo tanto, es esencial estar preparado y dispuesto a reaccionar rápidamente ante cualquier posibilidad imprevista, ya que las amenazas que deben enfrentarse y las vulnerabilidades potenciales que deben considerarse cambian constantemente.

En la presente investigación se aborda el nivel de riesgo de seguridad informática en la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno, basándonos en los estándares de auditoría ISO 17799. Estos estándares proporcionan pautas para determinar el nivel de seguridad informática de la organización en cuestión. La presente tesis forma parte de la línea de investigación en teoría de sistemas y administración de sistemas dentro del área de sistemas, computación e informática.

Dentro de la investigación, desarrollaremos en el Capítulo I la revisión de literatura. En este capítulo extraeremos antecedentes a nivel internacional, nacional y local que fundamenten la viabilidad de la presente investigación. También se llevará a cabo la recopilación de las bases teóricas de distintos autores que ayudarán a respaldar la estructura de la investigación.

En el Capítulo II, Planteamiento del problema, analizaremos el problema y sus diversos factores, evaluando su viabilidad. Esto nos ayudará a determinar los objetivos e hipótesis de la investigación.

En el Capítulo III, Materiales y métodos, se explicará el método de investigación en función de los objetivos y las variables de la investigación.

En el Capítulo IV, Resultados y discusión, se presentarán los resultados obtenidos mediante el estándar ISO 17799. Se analizarán los activos con los que cuenta la organización, la probabilidad de ocurrencia y el impacto que podría ocasionar cuando se produzca. En este capítulo, también se llevará a cabo la discusión y se presentarán las conclusiones a las que se ha llegado.

CAPÍTULO I
REVISIÓN DE LITERATURA

1.1. Marco teórico

En esta sección se presentan los fundamentos teóricos que ayudarán a sustentar el problema de investigación, considerando las variables objeto de estudio, siendo entre las más importantes:

1.1.1. Seguridad informática

La seguridad es una característica de cualquier sistema, ya sea computarizado o no, que indica que el sistema está libre de peligros, daños o riesgos que puedan comprometer la confiabilidad de la información. Si bien es difícil lograr la infalibilidad en sistemas operativos o redes informáticas, según la mayoría de los expertos en el campo, es preferible utilizar el término 'fiabilidad' en lugar de 'seguridad'. Por lo tanto, hablamos de sistemas fiables en lugar de sistemas seguros (Romero *et al.*, 2018).

Mantener un sistema seguro incluye básicamente tres aspectos: confidencialidad, integridad y disponibilidad (Romero *et al.*, 2018).

1.1.2. Valor de los activos

La seguridad informática se refiere a la protección de los elementos que valoramos, conocidos como activos, en una computadora o sistema informático. Existen diversos tipos de activos, que incluyen hardware, software, datos, personas, procesos o combinaciones de estos. Para determinar qué debemos proteger, primero debemos identificar qué tiene valor y para quién. Los equipos informáticos, desde hardware y complementos hasta accesorios, son sin duda una ventaja. Dado que gran parte del hardware informático es inútil sin programas, el software también se

considera un activo. Estos últimos incluyen sistemas operativos, utilidades y aplicaciones como procesadores de texto, reproductores multimedia o controladores de correo electrónico, o incluso programas que usted mismo cree. Aunque gran parte del hardware y el software están disponibles en el mercado (no están diseñados específicamente) y son fácilmente reemplazables, la singularidad y el valor de una computadora reside en su contenido: fotografías, música, artículos, correo electrónico, documentos electrónicos, proyectos, calendarios, información, correos electrónicos anotados. -libros, información de contacto, código creado por el usuario y más. Por lo tanto, los datos de su computadora también se consideran un activo. A diferencia de la mayoría del hardware y software, los datos pueden ser difíciles o imposibles de recrear o reemplazar. Después de identificar los activos a proteger, determinamos su valor. A menudo tomamos decisiones basadas en valores, incluso cuando no somos conscientes de ello. Por ejemplo, cuando va a nadar, puede dejar una botella de agua y una toalla en la playa, pero no su billetera ni su teléfono celular. La diferencia radica en el valor de los activos. El valor de un activo depende de la perspectiva del propietario o usuario del activo y puede ser independiente del costo monetario. Una foto de un familiar puede tener un valor significativo para usted, aunque su costo en términos de papel y tinta sea mínimo. Sin embargo, podría carecer de valor para un amigo o compañero. El valor de otros artículos puede depender del costo de reposición; algunos datos de la computadora son difíciles o imposibles de reemplazar. Por ejemplo, una foto tuya y de tus amigos en una fiesta podría no haber costado nada, pero su valor es incalculable porque no existe otra copia. En cambio, un DVD de tu película favorita podría haber representado un gasto significativo, pero es reemplazable en caso de pérdida o daño. Del mismo modo, el valor de nuestros valiosos activos puede cambiar con el tiempo, como en los planes para una nueva línea de productos que tiene el mayor valor antes del lanzamiento, pero disminuye significativamente una vez que el producto se introduce en el mercado. Bajo ciertos criterios determinados por el usuario podemos asignar un valor a nuestros activos, dependiendo de su capacidad de recuperación, importancia, valor sentimental u valor en el tiempo, dependiendo para quien puede resultar valioso (Pfleeger *et al.*, 2015)

1.1.3. Pruebas de seguridad

Es el aspecto más crucial de las pruebas de penetración. La seguridad representa un proceso, no un producto, y se puede entender como una metodología más que un producto. Otro elemento importante para considerar en nuestra discusión es que las pruebas de seguridad deben tener en cuenta las áreas clave de un modelo de seguridad. Un ejemplo de esto incluye: autentificación, autorización, confidencialidad, integridad, disponibilidad, no repudio. Cada uno de estos elementos debe ser considerado al proteger un entorno organizacional. Cada área en sí misma abarca diversas subáreas que también deben considerarse al construir un entorno seguro en su arquitectura. La conclusión es que, al realizar pruebas de seguridad, es esencial abordar cada una de estas áreas (Cardwell, 2014).

1.1.4. Confidencialidad

La confidencialidad es la cualidad que debe tener un documento o archivo para que pueda ser comprendido únicamente por individuos o sistemas autorizados con los debidos permisos. De esta manera, se considera que el documento es confidencial solo si una persona o entidad autorizada puede entender el contenido, ya sea por ser una persona instruida o acreditada. En el caso de una comunicación escrita, esto evita que personas no autorizadas intercepten y accedan al mensaje (Costa-Santos, 2014).

1.1.5. Integridad

Según Costa-Santos (2014), la integridad es una característica que posee un archivo o mensaje cuando no han sido modificados y que, además, permite verificar que el documento original no ha sido manipulado. Cuando se aplica en bases de datos, se refiere a la correspondencia que existe entre los registros y los hechos reflejados.

1.1.6. Disponibilidad

Según Costa-Santos (2014), el término “disponibilidad” está relacionado con la capacidad de los usuarios autorizados, o procesos, para acceder a servicios, datos o sistemas y utilizarlos cuando sea necesario. También hace referencia a la seguridad de cualquier dato que se pueda restaurar. En otras palabras, se busca prevenir la pérdida de información o el bloqueo causado por ataques maliciosos, fallos accidentales o circunstancias imprevistas o de fuerza mayor.

1.1.7. Autenticación

La verificación de identidad es una situación en la que es posible verificar quién preparó el documento. Desde el momento en que el individuo es considerado una persona autorizada, la comprobación de identidad se aplica a la validación de acceso. Es decir, cuando el usuario puede proporcionar alguna forma de verificar que la persona es quien dice ser, se realizará la verificación de identidad. La autentificación en los sistemas informáticos se suele realizar a través del nombre de usuario registrado y la clave de acceso (Costa-Santos, 2014).

1.1.8. Autorización

A menudo, el concepto de autorización es pasado por alto, ya que se da por sentado y no forma parte de algunos modelos de seguridad. Aunque algunos enfoques prescinden de él, se prefiere incluirlo en la mayoría de los modelos de prueba. La autorización es esencial, ya que determina cómo asignamos los derechos y permisos para acceder a un recurso, y es crucial asegurar su integridad. La autorización posibilita la coexistencia de distintos tipos de usuarios con niveles de privilegios separados dentro de un sistema (Cardwell, 2014).

1.1.9. No repudio

La afirmación de no repudio establece que un remitente no puede negar el envío de algo; por lo tanto, suele ser el aspecto con el que se enfrentan más problemas. Es crucial comprender que los sistemas informáticos han sido comprometidos en numerosas ocasiones, y la práctica de la negación no es un concepto nuevo. Dada esta realidad, la declaración que asegura "podemos garantizar el origen de una transmisión desde un ordenador específico por parte de una persona determinada"

no es completamente precisa. Sin conocer el estado de seguridad del equipo y considerando la posibilidad de compromisos, dicha afirmación podría ser precisa. Sin embargo, hacer esta afirmación en las redes actuales resulta extremadamente desafiante. La presencia de una máquina comprometida anula fácilmente la teoría de que "puedes garantizar el remitente". No exploraremos cada componente de seguridad en profundidad aquí, ya que esto va más allá del alcance de nuestro objetivo. La idea principal que queremos transmitir es que las pruebas de seguridad implican analizar cada componente de la seguridad, evaluar el riesgo asociado con ellos para una organización y luego mitigar ese riesgo (Cardwell, 2014).

1.1.10. Control de acceso

El control de acceso representa el núcleo tradicional de la seguridad informática, donde la ingeniería de seguridad se fusiona con la informática. Su función primordial es supervisar qué entidades principales, como personas, procesos y máquinas, tienen acceso a recursos específicos dentro del sistema. Esto implica determinar qué archivos pueden ser leídos, qué programas pueden ejecutarse y cómo se comparten datos entre diferentes entidades principales. El control de acceso opera en diversos niveles, abarcando la aplicación de software, capas intermedias, sistema operativo y hardware (Anderson, 2008).

1.1.11. ISO 17799

Según Rodríguez *et al.* (2012), el estándar ISO 17799 es una normalización internacional que brinda asesoramiento sobre la gestión de la seguridad de la información a los responsables de iniciar, implementar o mantener el buen funcionamiento organizacional. ISO 17799 define la información como un activo valioso para una organización, por lo tanto, debe protegerse adecuadamente estos recursos y garantizar la continuidad del negocio, minimizar el daño a la organización y maximizar el retorno de la inversión y la oportunidad comercial.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar estándares dentro de una organización y ser una práctica eficaz de gestión de la seguridad.

1.1.12. Vulnerabilidades informáticas

González-Perez *et al.* (2013) definen las vulnerabilidades como aquellos puntos de posible ataque a un sistema, lo que expone la información de tal manera que puede ser alterada, perdiendo su integridad. Estas vulnerabilidades pueden manifestarse en el software, hardware, configuraciones deficientes o en el manejo inadecuado de contraseñas por parte del personal encargado.

Un fallo de seguridad se refiere a una debilidad en un sistema que podría permitir a un usuario malintencionado afectar la integridad, disponibilidad o confidencialidad de la infraestructura en cuestión (González-Perez *et al.*, 2013).

1.1.13. Vulnerabilidades físicas

Según Romero *et al.* (2018), la vulnerabilidad se refiere a una debilidad que afecta físicamente la infraestructura de una organización y puede considerarse como un indicador de riesgo. Por ejemplo, si la organización se encuentra en una zona de alto riesgo sísmico, esta podría tener una vulnerabilidad significativa, ya que estaría expuesta a daños en caso de un terremoto, lo que afectaría la prestación de sus servicios. Es fundamental detectar y considerar esta posible fuente de problemas. Del mismo modo, si la organización se ubica en una zona propensa a inundaciones, también enfrenta otro tipo de vulnerabilidad.

Otra debilidad física se relaciona con el control de acceso. En muchos casos, aunque se tenga acceso a la infraestructura crítica, no se cuenta con un control adecuado sobre el ingreso, lo que significa que cualquiera podría abrir la puerta y entrar. Esto representa un riesgo significativo para la organización, ya que cualquier usuario podría insertar un dispositivo USB y copiar información o infectar los sistemas.

1.1.14. Vulnerabilidades lógicas

Según Romero *et al.* (2018), las vulnerabilidades son aquellas que afectan la infraestructura y la operatividad de los sistemas. Estas pueden dividirse en tres categorías principales: vulnerabilidades de configuración, vulnerabilidades de actualización y vulnerabilidades de desarrollo. Las vulnerabilidades de configuración se relacionan con la configuración del sistema operativo, configuraciones por defecto del sistema o incluso de algunas aplicaciones del servidor que se encuentren expuestas. En muchos casos, las vulnerabilidades de configuración también pueden estar relacionadas con la gestión deficiente de los firewalls y la infraestructura perimetral. Las vulnerabilidades de actualización se refieren a situaciones en las que las empresas no mantienen actualizados sus sistemas, lo que puede dar lugar a la aparición de fallos que deben ser tenidos en cuenta.

Por último, las debilidades de desarrollo involucran aspectos como inyecciones de código en SQL, Cross Site Scripting, entre otros. La naturaleza de estas debilidades varía según el tipo de aplicación y la validación de datos involucrada.

1.1.15. Medición de la vulnerabilidad

El Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. ha creado un protocolo para la clasificación y evaluación estandarizada del contenido de seguridad en sistemas de software, con el objetivo de "normalizar la manera en que se identifica y cataloga la vulnerabilidad de seguridad y la información de configuración". Este protocolo se denomina protocolo de automatización de contenidos de seguridad (S'CAP) y comprende los siguientes seis componentes: Vulnerabilidades y Exposiciones Comunes (CVE), Enumerador de Configuración Común (CCE), Enumerador de Plataforma Común (CPE), Sistema Común de Puntuación de Vulnerabilidad (CVSS), Formato de Descripción de Lista de Verificación de Configuración Extensible (XCCDF) y Lenguaje Abierto de Evaluación y Vulnerabilidad (OVAL) (Kostopoulos, 2013).

1.1.16. Depuración y análisis de vulnerabilidades

Es muy difícil y poco probable crear programas sin errores. Ya sea para corregir o aprovechar estos errores, la aplicación extensiva de herramientas y técnicas de depuración es la mejor manera de entender qué algo salió mal. Los depuradores permiten a los investigadores inspeccionar y controlar la ejecución de programas, formular hipótesis, verificar datos, atrapar estados interesantes o incluso modificar el comportamiento en tiempo de ejecución. En la industria de la seguridad de la información, los depuradores son fundamentales para analizar las vulnerabilidades y evaluar cuán severos son los problemas (Drake *et al.*, 2014).

1.1.17. Políticas de seguridad de la información

Es un medio de comunicación con los usuarios y los gerentes. La PSI (Política de Seguridad de la Información) establece las pautas de respuesta y los comportamientos del personal en el manejo de los recursos y servicios informáticos más relevantes de la organización. No debe confundirse con una descripción técnica de seguridad ni con una normativa legal que regule las conductas de los operadores. Más bien, es una documentación que especifica lo que se debe proteger y por qué, junto con los procedimientos basados en buenas prácticas. Cada PSI es consciente del personal, y este debe detallar el uso y las limitaciones de los recursos y servicios críticos de la compañía (Anthros, 2012).

Según Rodríguez & Ribón (2017), son un medio que también debe ofrecer pautas comprensibles sobre porque tomar ciertas decisiones y explicar la importancia de los recursos. De la misma forma, deberán establecer los objetivos de la organización con respecto a la seguridad y determinar la autoridad responsable de los correctivos o sanciones que corresponden.

1.1.18. Detección de intrusos mediante estadísticas

En redes que incorporan análisis estadístico, es factible implementar un método computacionalmente eficiente para identificar pequeñas anomalías, particularmente subgrafos en gráficos expansivos que evolucionan a lo largo del tiempo. La complejidad radica en la detección de intrusos en redes informáticas de gran escala, de millones de eventos de comunicación diarios. Cada interacción observada, que constituye series temporales de comunicaciones entre pares de computadoras en la red, se modela mediante el empleo de modelos de Markov observados y ocultos. Estos modelos establecen referencias de comportamiento para la detección de anomalías, capturando patrones inusuales, a menudo asociados con actividades humanas, que son prevalentes en un amplio conjunto de conexiones. A pesar de que las anomalías en conexiones individuales son frecuentes, las intrusiones buscadas en la red implican anomalías concurrentes en múltiples conexiones adyacentes. Se evidencia que las conexiones adyacentes son mayormente independientes y que la probabilidad de un subgrafo con múltiples conexiones coincidentes se evalúa mediante modelos de conexiones individuales. Se presenta un novedoso método de análisis estadístico en el que se examinan subgrafos con tamaños y formas específicos, como estrellas externas y rutas de 3 nodos. Se confirma que la identificación de estas formas fundamentales es suficiente para reconocer adecuadamente anomalías de diversas tipologías, tanto en entornos simulados como en situaciones reales. Sin embargo, es viable emplear otros métodos estadísticos para evaluar el nivel de ciberseguridad en una infraestructura, ya sea virtual o física (Adams & Heard, 2014).

1.1.19. Modos de ataques en seguridad informática

La ciberdelincuencia puede surgir de dos fuentes primordiales:

Ataques Internos:

Los ataques internos se perfilan como el riesgo cibernético más peligroso que enfrentan las organizaciones en la actualidad, ya que pueden subsistir sin ser detectados durante un periodo prolongado. Estos ataques se desencadenan cuando existe un abuso de confianza por parte de empleados u otras personas, como ex empleados, terceros, contratistas externos o socios comerciales, que desempeñan funciones dentro de la organización objetivo y cuentan con acceso legítimo a sus sistemas informáticos e información asociada a sus prácticas y medidas de ciberseguridad. En esta categoría se incluye el espionaje económico (Hassan, 2019).

Ataques Externos:

Este tipo de ataque proviene de fuera de la organización objetivo y generalmente es llevado a cabo por hackers especializados. Dichos ataques representan las amenazas más significativas para las organizaciones a nivel global. Un hacker con intenciones maliciosas podría intentar infiltrarse en el sistema de la organización objetivo desde redes informáticas situadas en otro país con el fin de obtener acceso no autorizado. En algunas instancias, los atacantes externos adquieren información confidencial de un colaborador interno (empleado insatisfecho) dentro de la empresa objetivo, quien suministra detalles sobre los sistemas de seguridad para facilitar el acceso ilegítimo (Hassan, 2019).

1.1.20. Caracterización de amenazas

La probabilidad de cualquier tipo de evento o comportamiento que podría causar daño a un elemento del sistema o afectar a un activo identificado se define como el riesgo. Se recomienda consultar el historial de tales amenazas, ya que la lista de estas amenazas está asociada para identificar el tipo de peligro al que se enfrentan los activos y los riesgos a los que están expuestos (Pinzón-Parada, 2017).

1.1.21. Amenazas en la nube

Las plataformas en la nube son ventajosas, aunque no están exentas de riesgos. Se distancian significativamente del concepto de la computadora personal que surgió en los años ochenta y que transformó la industria. En el hogar, las computadoras personales fueron concebidas como entidades privadas, simplemente otro dispositivo independiente, similar a una aspiradora o una cafetera eléctrica. Una computadora personal representaba una posesión privada, donde los dueños tenían control absoluto sobre los accesos. Al adquirir software, este se instalaba en las computadoras de manera semejante a la compra de un electrodoméstico nuevo para el hogar. Tanto el software como el electrodoméstico pertenecían al usuario. Cualquier persona que deseara utilizar el software o el electrodoméstico necesitaba obtener permiso del propietario para ingresar a su hogar. Acceder sin autorización a una computadora personal privada era considerado como un allanamiento de morada y estaba sujeto a intervención policial. Con el tiempo, las redes, especialmente Internet, conectaron las computadoras domésticas con el mundo exterior. La aparición de computadoras portátiles, teléfonos inteligentes y tabletas permitió a los usuarios liberarse de las máquinas de escritorio y utilizar sus dispositivos fuera del hogar. En la actualidad, a través de estas redes, diversas computadoras individuales acceden a recursos ubicados en nubes físicamente distantes. Este modelo proporciona beneficios sustanciales. A pesar de que nuestros dispositivos actuales son considerablemente más potentes que sus predecesores de hace una o dos décadas, nuestras expectativas de rendimiento han superado su capacidad intrínseca. Por ejemplo, las computadoras portátiles contemporáneas suelen tener unidades de disco de varios terabytes, y la conectividad inalámbrica a Internet es tan ubicua que rara vez representa un inconveniente. En la actualidad, utilizamos teléfonos inteligentes, tabletas y computadoras portátiles, además de las tradicionales computadoras de escritorio, y todas están conectadas a diversas nubes, cada una de las cuales ofrece servicios que serían difíciles de replicar utilizando recursos locales propios. Si bien las nubes han mejorado la utilidad y el valor de entretenimiento de nuestros dispositivos personales, también han introducido ciertos riesgos. Actualmente, existen diversas amenazas a la seguridad y preocupaciones que no se pueden abordar fácilmente con enfoques policiales convencionales (Waschke, 2017).

1.1.22. Analizando el impacto

Según Pinzón (2017), es necesario analizar el impacto, el cual está relacionado con la pérdida de integridad, disponibilidad o confidencialidad, y su efecto en la misión, evaluando la importancia y la sensibilidad de los activos o datos. El impacto se puede medir como la explotación de una vulnerabilidad que puede afectar las operaciones, la economía e incluso la imagen de una empresa. En algunos casos, el impacto es intangible. Dependiendo de consideraciones que pueden evaluarse cualitativa o cuantitativamente, se recomienda el segundo enfoque, ya que proporciona mediciones cuantificables que permiten realizar análisis de costo-beneficio.

1.1.23. Determinando el riesgo

Establecer la probabilidad de que un potencial punto vulnerable pueda afectar la operación del sistema o perjudicar algún pilar de seguridad. Para la determinación del riesgo, se divide en tres niveles: Alto, si una observación o hallazgo se define como de gran peligro, se requiere urgente, una acción correctiva. Los sistemas existentes pueden continuar operando, pero los planes de enmienda deben desarrollarse lo antes posible. Medio, si una observación se clasifica como riesgo moderado, se requiere una operación correctiva y se debe implementar un plan para incorporar estas tareas dentro de un tiempo razonable. Bajo, si una observación se describe como de mínimo de inseguridad, el sistema debe determinar si aún se requiere una labor correctiva o decidir aceptar las posibles consecuencias (Pinzón-Parada, 2017).

1.1.24. El elemento humano en la seguridad informática

La investigación científica es, por naturaleza, una actividad inherentemente humana. Incluso en disciplinas donde los humanos no son el foco directo de estudio, como suele suceder en campos como la biología o la psicología, son los seres humanos quienes lideran todas las investigaciones científicas, incluyendo el ámbito específico de la ciberseguridad. La importancia destacada de los roles humanos en la ciencia de la ciberseguridad y el concepto fundamental de reconocimiento del sesgo humano en la ciencia surgen a raíz de los roles que desempeñan en esta disciplina. Los individuos contribuyen a la ciencia de la ciberseguridad de al menos cuatro maneras: como desarrolladores y diseñadores, cuyas funciones son cruciales en el pensamiento y la ejecución científica dentro del ámbito de la ciberseguridad; como usuarios y consumidores, a menudo considerados el eslabón más vulnerable en la cadena de seguridad cibernética; como orquestadores y profesionales, encargados de salvaguardar redes, datos o usuarios, tomando decisiones estratégicas para alcanzar los objetivos deseados; y como adversarios activos, siendo impredecibles y difíciles de rastrear, lo que les permite ocultarse eficientemente en línea y abandonar ataques específicos antes de que los defensores tengan la oportunidad de detectarlos. Las investigaciones científicas exploran estas diversas dimensiones de la interacción humana con la ciberseguridad (Dykstra, 2016).

1.1.25. Contramedidas defensivas

Proteger un recurso en Internet es sumamente desafiante debido a la exposición al acceso público a nivel global, junto con la dificultad de garantizar el servicio a usuarios confiables de manera rentable en términos de seguridad. Es esencial integrar la seguridad en todas las etapas del ciclo de vida de cualquier entidad orientada al público, en lugar de considerar la seguridad como un aspecto secundario. Este enfoque no solo disminuirá el riesgo de amenazas contra el servicio, sino que también puede resultar menos costoso abordarlo en caso de un incidente cibernético. Kali Linux destaca como una herramienta principal en pruebas de penetración, útil para identificar las vulnerabilidades de los sistemas frente a posibles ataques. En lugar de dirigir ataques hacia un objetivo, se recomienda llevar a cabo pruebas de penetración en los propios activos de red para

identificar posibles debilidades antes de que un individuo malintencionado las aproveche. Es crucial tener un conocimiento interno profundo de nuestras infraestructuras y comprender sus puntos débiles. La ventaja radica en entender lo que está ocurriendo, permitiendo tomar medidas extremas sin activar alarmas. Por lo general, los hackers evitan exponerse, reduciendo así sus opciones de ataque. La estrategia de sigilo implica paciencia, un contacto mínimo con el objetivo y una cuidadosa planificación. La administración debe aprovechar su capacidad para invertir adecuadamente en tiempo y recursos para la seguridad, antes de que terceros inviertan más recursos en eludirla (Muniz & Lakhani, 2013).

1.1.26. Auditoria informática

Según Castello (2017), es un control, llevado a cabo por un grupo ajeno del sistema a auditar, con el propósito de obtener información relevante para examinar el normal funcionamiento del sistema bajo análisis. La acción de auditar es efectuar el control y realizar la revisión de un acontecimiento pasado. Es decir, es observar lo que ocurrió en una entidad y contrastarlo con normas antes predefinidas.

Según Hernández-Hernández (1993), es un proceso formal ejecutado por especialistas del área de auditoría, que se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de informática en la organización se lleven a cabo de una manera oportuna y eficiente.

1.2. Antecedentes

La seguridad informática es motivo de preocupación para todas las instituciones que gestionan su información a través de medios tecnológicos. Es importante tener en cuenta que estos sistemas pueden ser vulnerables y susceptibles de alteraciones que podrían causar graves perjuicios a la institución. Varios autores han propuesto métodos destinados a mejorar estas deficiencias y a concienciar a la población en general sobre la importancia de la seguridad informática. Los estudios utilizados como antecedentes en investigaciones previas muestran que los autores han expresado lo siguiente:

1.2.1. Internacional

Amasifuen-Shupingagua (2015) indica que "La auditoría en la organización es un elemento de monitoreo que permite llevar a cabo la revisión y evaluación de los controles, sistemas y procedimientos de informática. Además, es de vital importancia para el buen desempeño de las infraestructuras de información."

Calderón-Alvarado (2017) concluye que los recursos de administración de riesgos para la ciberseguridad "ayudan al área de infraestructura a tener un registro y control de los usuarios de red, respaldan al administrador de red para llevar a cabo su trabajo de manera eficaz, y preparan a la organización para futuras auditorías internas o externas.

Romero-Fuentes (2011) manifiesta que "La Seguridad Informática se basa, principalmente, en la efectiva administración de los permisos de acceso a los recursos informáticos, fundamentada en la identificación, autenticación y autorización de accesos, así como en políticas de seguridad".

Dioppe-Arellano (2015) alude, acerca de las amenazas en los sistemas, "Es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas".

Arenas-Villanueva & De-Los-Santos-Mendoza (2017) manifiestan que "OSSIM proporciona información útil, relevante y oportuna. Esto se debe a que cuenta con un motor de correlación (tanto lógica como cruzada) que genera eventos de mayor prioridad y fiabilidad, reduciendo así los falsos positivos y los falsos negativos. Esto permite al administrador tomar las decisiones correctas en relación a los eventos detectados en la red. OSSIM por su siglas en ingles "Open Source Security Information Management" es una herramienta SIEM, por sus siglas en ingles "Security Information and Event Management" de código abierto muy valiosa, que no solo implementa algunos controles de la ISO 27001 y PCI DSS, sino que también permite la integración con el marco de referencia COBIT 5, proporcionando un sistema de gestión de seguridad de la información alineado con los objetivos de seguridad propuestos en el caso de estudio".

Alcantára-Flores (2015), menciona, "Con la guía de implementación, se logró aumentar el nivel de seguridad en las aplicaciones informáticas de la institución policial. Esto se reflejó en el aumento de políticas de seguridad que se pusieron en marcha y que beneficiaron a la institución, contribuyendo a mejorar su nivel de seguridad".

Taco-Arias & Gamarra-Ramirez (2014), alega que, "El empleo de firmas digitales, encriptación asimétrica y protocolos SSL ha permitido implementar un sistema web que incremente la seguridad de los documentos digitales, con el cual se protege la integridad de los documentos después de ser firmados, se identifica de forma fehaciente a los autores y se evita el no repudio de los firmantes".

Plaza-Torres (2014) dice, "Se define los tipos de ataques informáticos, describiendo los métodos y herramientas que el atacante emplea para vulnerar un sistema. Se muestra la importancia de la seguridad información, permitiendo tomar conciencia de la importancia de la información como un activo más de una organización, permitiendo prevenir ataques utilizando mecanismos de defensa antes mencionados mediante el ejemplo práctico, las vulnerabilidades que hay en un sistema operativo, así mismo que hacer para contrarrestar estos ataques".

Pozo-Zulueta *et al.* (2009) refiere, "Para evaluar el aporte que traería la utilización del procedimiento se encuestaron 7 expertos del grupo seguridad, de los

encuestados, 2 evaluaron el procedimiento de regular (Suficientemente bueno con reservas) y los 5 restantes lo evaluaron de bueno (Aplicable con resultados destacados). Este procedimiento además de ser utilizado por testeadores de poca experiencia, también puede emplearse en equipos de desarrollo que deseen evaluar las vulnerabilidades de las aplicaciones web que construyen.

Analizando estos datos puede concluirse que el procedimiento es útil para los testadores porque después de su uso la cantidad de no conformidades o vulnerabilidades encontradas se asemejan más a las vulnerabilidades explotadas".

Benites-Barreiro *et al.* (2016) concluyen que, "Deshabilitar la difusión del SSID y el filtrado de direcciones MAC son métodos simples de eludir. La seguridad WEP está obsoleta. Se puede obtener una contraseña WEP con herramientas sencillas en pocos minutos. Una contraseña compleja con WPA logra que ataques de diccionario pierda sus posibilidades de éxito. Un ataque de fuerza bruta a esta tecnología sería poco práctico debido al tiempo que requiere. La autenticación del servidor por parte del cliente también es importante, ya que ayuda a prevenir ataques de AP falsos. Los certificados digitales como alternativa al uso de contraseñas nos ofrecen un método de autenticación mucho más seguro, pero su adopción se ha limitado debido a la complejidad de su implementación".

López-Alvarez (2015) manifiesta que, "Después de realizado el análisis de la información obtenida, se puede confirmar que, ninguna aplicación web es perfectamente segura y libre de ataques, pero con el uso de técnicas o test de intrusión, Pentesting, como herramientas de Hackeo Ético, todas esas vulnerabilidades pueden ser superadas, evitando los ataques que socavan la integridad y fiabilidad de los datos que se manejan".

Carbajal-Romero (2013) elabora una guía para implementar el sistema informático, en la cual se menciona que “Las tecnologías de la información y comunicaciones deben tener en cuenta estándares o buenas prácticas internacionales, como COBIT e ISO/IEC 27002, que permitan desarrollar un marco propio adaptable a la realidad de cada entidad perteneciente al sector público peruano”.

Ramírez-Reyes (2002) refiere, “La auditoría informática permite a la entidad pública buscar los medios para alcanzar los estándares internacionales en el uso adecuado de las tecnologías de información, con miras a una certificación. La auditoría informática pone al descubierto, si los esfuerzos están correctamente orientados a controlar los riesgos de mayor impacto y a redireccionar aquellos esfuerzos orientados a áreas que no representan riesgos para la entidad”.

Sabillón & Cano-M (2019) implementa un modelo general de auditoria en ciberseguridad, “Los resultados de este estudio muestran que, las auditorías de ciberseguridad realizadas por dominios pueden ser muy efectivas al evaluar los controles y las respuestas a las amenazas cibernéticas. El CSAM (Modelo de Auditoría de Ciberseguridad) no es exclusivo en una industria, sector u organización. Por el contrario, el modelo se puede utilizar para planificar, ejecutar y verificar auditorías de ciberseguridad en cualquier organización o país. El CSAM ha sido diseñado para realizar auditorías de ciberseguridad parciales o completas en dominios específicos, múltiples o auditoría integral”.

Socarrás & Santana (2019) alega que, “El número de potenciales problemas de seguridad y sus riesgos asociados, aumenta con el crecimiento de la complejidad y la conectividad de los SCI con redes externas. La salvaguarda de los mismos debe ser tenida en cuenta durante la etapa de proyecto y propician utilizar las soluciones tanto de hardware como de software del vendedor del SCI”.

1.2.2. Nacional

Cruz-Saavedra (2014) pudo identificar a través de la auditoria penetration testing el impacto de un fallo de seguridad, que perjudicaría directamente a la integridad de la información en un 40% del daño ocurrido, así como un 26% a la integridad de la información y un 34% a la disponibilidad de la información. El impacto de esta penetración llevó al control parcial de los sistemas por parte del atacante a la empresa de Data Business, Trujillo, y a la vez la posibilidad de obtener una gran cantidad de información sobre ellos, incluyendo contraseñas de acceso al servidor, carpetas compartidas, correos y todo mediante la explotación de puertos vulnerables.

Campos-Muñoz & Rios-Damián (2016) “Se ha logrado implantar un sistema de gestión de la seguridad de la información y un sistema para gestión de riesgos operativos relacionados con tecnología de información para la caja Sipán, cuyos resultados de sus evaluaciones están ayudando a encauzar y determinar una adecuada acción gerencial, la definición de prioridades para gestionar los riesgos de seguridad de la información y la implantación de los controles seleccionados para protegerse contra dichos riesgos. Los procedimientos metodológicos y requisitos de estos sistemas cumplen con las normatividades de la SBS para estos casos: Circular Nº G-140-2009: Gestión de la seguridad de la información y Resolución S.B.S. N° 2116-2009: Reglamento para la gestión del riesgo operacional”.

Diaz-Limary (2018) dice, “Obtuvo una correlación R de Pearson moderada de 0.640, significativa al 1% (0.009), por lo tanto, con ello se acepta la hipótesis que establece que la auditoría informática se relaciona significativamente con la seguridad de la información en el área de sistemas de la caja de Santa, Chimbote 2018”.

Tarrillo-Clavo & Correa-Cubas (2013) determinan que, “Se pudo evidenciar que la Municipalidad de Lambayeque carece de políticas y controles eficientes en cuanto a: la seguridad de la red, resguardo de la información y manejo de los riesgos a los que está expuesta. Se demostró que existe la factibilidad técnica, económica y operativa para realizar la metodología en sistemas de gestión de seguridad de la información”.

Aguilar-Portilla & De-La-Cruz-Ramos (2015) refieren que, “La implementación de la solución de hacking ético mejora a seguridad en la infraestructura informática de la caja municipal de Sullana – agencia Chimbote, ya que se adelanta a posibles fallas o problemas de seguridad, previniendo desarrollar controles de seguridad con lo cual optimizan los sistemas físicos y lógicos de la entidad”.

1.2.3. Local

Sanchez-Mamani & Huirse-Cruz (2017) indican que, “Tras la instalación y ejecución del prototipo de software en el servidor, se pudo determinar que si es posible controlar ese tipo de vulnerabilidad a través de un guardián estenográfico que bloquea las transacciones en un en la oficina de tecnología informática de la Universidad Nacional del Altiplano 2015 en un 98.5% lo cual es aceptable”.

Puma (2017) manifiesta que, “la implementación del proceso de auditoría de seguridad de la información basado en la norma ISO/IEC 27002 fue exitosa, reduciendo el costo de la auditoría de seguridad de la información realizada en Puno caja los Andes en el año 2016. El proceso facilita que los auditores internos cuenten con las herramientas, lineamientos técnicos, planes de prueba, procesos de retención de documentos de trabajo, hojas de tiempo, reportes y estructuras sistemáticas para ejecutar auditorías de seguridad de la información; también desde el diagnóstico del análisis situacional. En conclusión, al establecer un proceso, ayuda a comprender cómo funciona y tener en cuenta la experiencia que los empleados deben mejorar en las actividades del proceso implementado”.

Aro-Maquera (2021) dice que, “Se realizó la auditoria informática usando las metodologías COBIT 5, mediante ello se encontró que esta es apropiada para evaluar la gestión del sistema de información y que permitieron tener un diagnóstico sobre la situación actual de la oficina de informática y tecnología de la Municipalidad distrital de Pilcuyo. Si bien se confirmó que existía problemas con la dotación de personal de las oficinas de TI, también se observó que no había un proceso para permitir la selección de trabajadores debido a la falta de profesionales calificados con conocimientos en el área. Asimismo, se ha verificado que la asignación de roles y actividades del personal no es suficiente para que este realice adecuadamente las funciones anteriores”.

Cruz-Saavedra (2014) manifiesta, “Se pudo identificar a través de la auditoria penetration testing el impacto de un fallo de seguridad, que perjudicaría directamente a la integridad de la información en un 40% del daño ocurrido, así como un 26% a la integridad de la información y un 34% a la disponibilidad de la información. Los impactos que causó esta penetración, tuvieron como consecuencia el control de forma parcial de los sistemas de informáticos por parte del atacante y también el atacante pudo obtener información de la empresa, incluyendo claves de acceso a los servidores, carpetas compartidas, correos electrónicos y todo mediante la explotación de puertos vulnerables”.

Machicao-Mollocondo (2019) manifiesta que, “De acuerdo al resultado de análisis de peligros de la seguridad de la información respecto a los activos primordiales de la oficina de tecnologías de información Universidad Nacional del Altiplano Puno, existen 12 riesgos de nivel alto, 28 riesgos de nivel medio, también presentan 151 riesgos de nivel bajo, siendo estos varios los criterios respecto a las amenazas que se puedan vulnerar afectando así, la información que administra la oficina de tecnologías de la información, representando hoy en día un activo primordial y principal, al cual se debe garantizar su confidencialidad, integridad y disponibilidad”.

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

2.1. Identificación del problema

Hoy en día, las universidades están experimentando cambios extremadamente turbulentos. Su base de sustento se ha desplazado desde el entorno empresarial tradicional hacia recursos humanos, técnicos, financieros, académicos y un entorno en el que la gestión descentralizada ha llegado al punto de la virtualización.

En este sentido, el Vicerrectorado de Investigación de la Universidad Nacional del Altiplano está implementando una variedad de sistemas con servicios que permiten a sus usuarios realizar sus trámites de forma flexible y virtual. Esto nos lleva a considerar la importancia de asegurar la disponibilidad de los sistemas que ofrece, así como los problemas que pueden causar a los usuarios si estos sistemas no están disponibles.

Con el aumento de los servicios prestados, se destaca la necesidad de respaldar la integridad de la información. En la mayoría de los casos, este aspecto se pasa por alto, pero debería ser uno de los aspectos más cruciales de la seguridad informática.

Algunas entidades del sector público carecen de inversión, conciencia e interés en la implementación de ciberseguridad. El obstáculo principal en relación al tema económico que implica la ejecución de ciertas medidas de seguridad es que las organizaciones no priorizan asignar grandes presupuestos a la seguridad informática, ya que creen que estos fondos no afectarán la productividad ni las ganancias.

Debido a restricciones presupuestarias en nuestro entorno, a menudo se recurre a versiones de prueba o a soluciones de software de seguridad implementadas ilegalmente como primera opción. Sin embargo, estas soluciones pueden poner en riesgo la información de la institución, ya que estos softwares suelen ser modificados y no brindan

garantía. Las organizaciones a menudo no reconocen la importancia de contar con soluciones de seguridad hasta que se enfrentan a un desastre grave.

Como se mencionó anteriormente, el Vicerrectorado de Investigación de la Universidad Nacional del Altiplano ha tomado medidas al respecto y cuenta con un sistema de seguridad para proteger la diversa información que se genera en ella, incluyendo finanzas, investigación, conocimiento, gestión administrativa, correo electrónico, base de datos, entre otros. Esto incluye la implementación de antivirus, un equipo de protección de correos electrónicos y firewalls para proteger la periferia de la red de área local, así como otras medidas de seguridad implementadas en servidores y computadoras en el entorno laboral. Sin embargo, estas acciones se han llevado a cabo de manera desorganizada y sin un diagnóstico previo.

Por lo tanto, podemos afirmar que no existe un sistema integral de seguridad, lo que conlleva a los siguientes problemas:

- Falta de un plan de contingencia de seguridad integral.
- Solución de posibles situaciones basada en la experiencia del supervisor.
- Falta de determinación y documentación de un plan de emergencia para solucionar problemas.
- No se han definido ni documentado las responsabilidades del personal del departamento de tecnologías de información en caso de incidente.
- Falta de comprensión por parte de los usuarios de los riesgos del mal uso de activos informáticos y del compromiso que tienen con ellos.
- Carencia de visión estratégica para desarrollar un plan de seguridad.
- Restricciones presupuestarias que limitan la implementación de proyectos de seguridad informática.
- Personal responsable no adecuadamente especializado en todos los niveles de tecnologías de información.
- Auditoría informática no realizada o poco frecuente.
- Solución de problemas de manera individual y particular.
- Falta de definición de los responsables y de los niveles de acceso requeridos para acceder a los sistemas.

El objetivo de esta investigación fue indagar y desarrollar una estrategia de análisis e implementación de condiciones de seguridad destinada a concienciar a la comunidad universitaria sobre los riesgos de almacenar su información en dispositivos digitales. Esto busca la participación de las diferentes oficinas que integran el Vicerrectorado de Investigación de la universidad para mejorar su competitividad en el mercado de la educación universitaria y mantener la disponibilidad, confiabilidad e integridad de su información. El propósito de esta investigación fue realizar un análisis de riesgos con el fin de comenzar a desarrollar un plan de seguridad de tecnologías de información para administrar y proteger la información.

2.2. Enunciados del problema

Problema general

¿Cuál es el nivel de riesgo de Seguridad informática en la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno?

Problemas específicos

a. ¿Cuáles son las amenazas que pueden ocurrir a los activos principales de la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno?

b. ¿Cuál es el nivel de impacto de daño a la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno?

2.3. Justificación

La investigación a realizarse se justifica por las siguientes razones**:**

a. Justificación teórica. La investigación permitió determinar los supuestos teóricos acerca del nivel de Seguridad informática en la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno.

b. Justificación Metodológica. Se estableció el diseño metodológico y estadístico para determinar la ocurrencia e impacto de las amenazas en los activos de vicerrectorado de investigación.

c. Justificación Práctica. El conocimiento de las variables permitió incorporar mejoras en la seguridad informática del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano.

2.4. Objetivos

2.4.1. Objetivo general

Analizar el nivel de riesgo de seguridad informática en la plataforma del vicerrectorado de investigación de la Universidad Nacional del Altiplano de Puno.

2.4.2. Objetivos específicos

a. Determinar la probabilidad ocurrencia de amenaza a los activos principales de la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno.

b. Determinar el nivel de impacto de daño a la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno.

2.5. Hipótesis

2.5.1. Hipótesis especificas

Existe probabilidad de riesgo de seguridad informática en la plataforma virtual del vicerrectorado de investigación de la Universidad Nacional del Altiplano de Puno

2.5.2. Hipótesis especificas

a. Existe probabilidad de ocurrencia de amenaza a los activos principales de la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno

b. Existe impacto de daño a la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. Lugar de estudio

El trabajo de investigación se llevó a cabo en las plataformas informáticas del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno, situado en el distrito, provincia y región de Puno. La dirección exacta es Avenida Sesquicentenario N.º 1150 en la Ciudad de Puno.

3.2. Población

Definimos como población los distintos activos de la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano Puno.

3.3. Muestra

La muestra para la presente investigación fue determinada por un muestreo no probabilístico para la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano Puno.

3.4. Método de investigación

La investigación que se realizó corresponde, al enfoque cuantitativo.

Cada etapa precede a la siguiente y no podemos “brincar o eludir” pasos, el orden es riguroso, aunque, desde luego, podemos redefinir alguna fase. Parte de una idea, que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica. De las preguntas se establecen hipótesis y determinan variables; se desarrolla un plan para probarlas (diseño); se miden las variables en un determinado contexto; se analizan las mediciones obtenidas (con frecuencia utilizando métodos estadísticos), y se establece una serie de conclusiones respecto de las hipótesis (Hernández-Sampieri *et al.*, 2014).

3.4.1. Tipo y diseño de investigación

Tipo de investigación. Según el alcance, la presente investigación es de tipo no experimental. “estamos más cerca de las variables formuladas hipotéticamente como “reales” y, en consecuencia, tenemos mayor validez externa (posibilidad de generalizar los resultados a otros individuos y situaciones comunes)” (Hernández-Sampieri *et al.*, 2014).

Diseño de la Investigación. El diseño descriptivo transeccional exploratorio pues se buscó establecer la asociación entre las variables: Ocurrencia de amenazas en la seguridad informática e impacto de daños, es decir determinar la correlación entre estas variables (Hernández-Sampieri *et al.*, 2014).

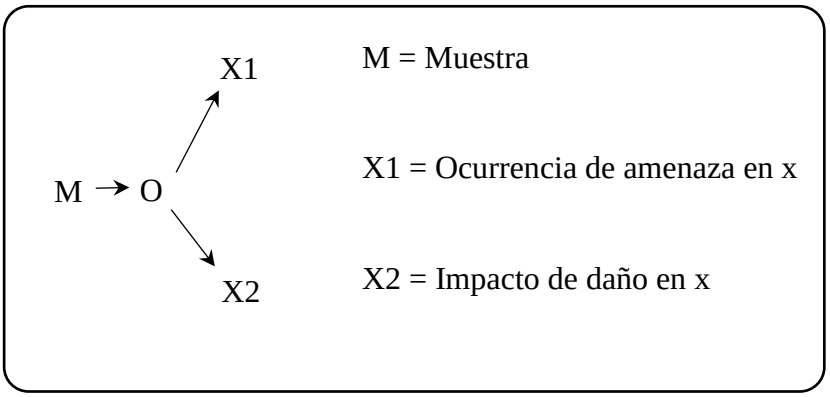


Figura 1. Diagrama de investigación descriptiva transeccional exploratorio

3.4.2. Recursos Observados

Se presentan los diferentes activos identificados por el Vicerrectorado de Investigación, a los cuales se les asigna un valor en función de su importancia para la organización, utilizando una escala de 1 a 10. Esta importancia se considera un valor subjetivo que refleja el nivel de impacto que un evento podría tener en la organización si afectara a dicho activo, independientemente de las medidas de seguridad que se hayan implementado para protegerlo.

Tabla 1

Valoración de activos y su importancia

Descripción de Activo	Importancia
Base de Datos	10
Servidores	8
Sistema de correo	5
Sistema de almacenamiento (SAN)	10
Central de Telefonía IP y teléfonos IP	5
Copias de respaldo	9
Equipos de comunicación (Routers, switches, hubs, etc)	10
Equipos de seguridad (antivirus, antispam, antipishing, detección de intrusos, cortafuego)	8
Cableado de fibra óptica y par trenzado (UTP)	10
Código fuente de las aplicaciones	9
Equipo de respaldo (backups)	9
Administrador de TI	10
Usuarios	8
Hardware	9
Insumos	7
Documentación	9
Datos del usuario	8

Fuente: Estándar ISO 17799

3.4.3. Clases de Amenazas

Clasificamos las amenazas en cinco los cuales son: develación, interrupción, modificación, destrucción y eliminación o pérdida.

Tabla 2

Definición de clases de amenazas

Clase de Amenaza	Definición
Develación	Los activos que tienen un alto requerimiento de confidencialidad son sensibles a la develación. Esta clase de amenaza compromete a los activos a la develación no autorizada de información sensible.
Interrupción	La interrupción se relaciona principalmente a los activos en servicio. La interrupción impacta en la disponibilidad del activo o servicio. Un corte de energía es un ejemplo de esta amenaza.
Modificación	El principal impacto de esta clase de amenaza es en el requerimiento de integridad. Recordar que la integridad incluye la certeza y completitud de la información. Un intento de hackeo puede caer en esta clase de amenaza si se llegan a realizar los cambios.
Destrucción	Una amenaza que destruye el activo, cae en la clase de destrucción. Un activo que tiene un requerimiento de alta disponibilidad es particularmente sensible a la destrucción. Amenazas como terremotos, inundaciones, incendios y vandalismo están dentro de esta clase.
Eliminación o Pérdida	Cuando un activo está sujeto a robo o ha sido extraviado o perdido, el impacto es principalmente en la confidencialidad y disponibilidad del activo. Las laptops son particularmente vulnerables a esta amenaza.

Fuente: Estándar ISO 17799

3.5. Descripción detallada por método por objetivo específico

3.5.1. Probabilidad de la Ocurrencia de la Amenaza

Se debe considerar el tipo de amenaza a la que suele estar sujeta el activo y la probabilidad de ocurrencia del riesgo. La probabilidad de la amenaza puede ser estimada de acuerdo a experiencias ocurridas, basándose en los sucesos acontecidos proporcionados por las principales oficinas y desde fuentes tales como otras organizaciones o servicios.

Los niveles de probabilidad de bajo, medio y alto son determinados de acuerdo a las siguientes definiciones:

Tabla 3

Definición de valores de nivel de probabilidad

Nivel de Probabilidad	Definición
Bajo	No hay antecedentes y la amenaza está considerada con poca probabilidad de ocurrencia.
Medio	Se tiene algún antecedente y una evaluación de que la amenaza pudiera suceder.
Alto	Se tiene un antecedente significativo y una evaluación de que la amenaza tiene una alta probabilidad de ocurrencia.

Fuente: Estándar ISO 17799

3.5.2. Nivel de Impacto

El impacto se define como el daño producido a la organización por un posible incidente y es el resultado de la agresión sobre el activo.

Tabla 4

Tabla de definición de niveles de impacto

Nivel de Impacto	Definición
Bajo	Indica pérdidas de información y/o recursos informáticos de nivel aceptable.
Medio	Indica pérdidas de información y/o recursos informáticos de nivel moderado.
Alto	Indica pérdidas de información y/o recursos informáticos de nivel severo hasta irrecuperable.

Fuente: Estándar ISO 17799

3.5.3. Instrumentos de recolección de datos

Para la presente investigación, se utilizó el estándar ISO 17799, que es una norma internacional que ofrece recomendaciones para llevar a cabo la gestión de la seguridad de la información, dirigidas a los responsables de iniciar, implementar o mantener la seguridad en una organización. ISO 17799 define la información como un activo que posee valor para la organización y, por lo tanto, requiere una protección adecuada. El objetivo de la seguridad de la información es proteger efectivamente este activo para garantizar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio (Rodríguez *et al.*, 2012).

Instrumento 01: Test ISO 17799, Adjunto al presente documento en el Anexo 1

3.5.4. Tratamiento de datos

Luego de recolectar los datos obtenidos mediante el uso de los instrumentos, se realizaron sus respectivas tabulaciones y representaciones gráficas de los resultados a través de tablas, cuadros estadísticos e interpretación. Se utilizaron los programas SPSS con licencia de prueba como herramienta técnica para el procesamiento de datos.

3.5.5. Operacionalización de Variables

Tabla 5

Operacionalización de variables

Variables de Estudio	Dimensiones	Indicadores	Escalas de Medición
Variable Dependiente Seguridad Informática	Disponibilidad	Interrupción	Alta
		Destrucción	Media
		Eliminación	Baja
	Confidencialidad	Develación	Alta
		Eliminación	Media
			Baja
	Integridad	Modificación	Alta
			Media
			Baja

Fuente: Estándar ISO 17799

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. Resultados

A partir de los hallazgos encontrados, aceptamos la hipótesis general que establece que, existe probabilidad de riesgo de seguridad informática en la plataforma virtual del vicerrectorado de investigación de la Universidad Nacional del Altiplano de Puno.

4.1.1. Observación de la variable: seguridad informática

Se realizó la observación de la variable (seguridad informática en el VRI de la Universidad Nacional del Altiplano) a través del instrumento 01, cuestionario estándar ISO 17790 (anexo 01) las cuales fueron valoradas a través de la siguiente escala:

Tabla 6

Observación de la variable - Definición de variable nivel de probabilidad

Nivel de Probabilidad	Definición
Bajo	No hay antecedentes y la amenaza está considerada con poca probabilidad de ocurrencia.
Medio	Se tiene algún antecedente y una evaluación de que la amenaza pudiera suceder.
Alto	Se tiene un antecedente significativo y una evaluación de que la amenaza tiene una alta probabilidad de ocurrencia.

Fuente: Estándar ISO 17799

Tabla 7

Observación de variable - definición de variable nivel de impacto

Nivel de Impacto	Definición
Bajo	Indica pérdidas de información y/o recursos informáticos de nivel aceptable.
Medio	Indica pérdidas de información y/o recursos informáticos de nivel moderado.
Alto	Indica pérdidas de información y/o recursos informáticos de nivel severo hasta irrecuperable.

Fuente: Estándar ISO 17799

Tabla 8

Tabla cruzada impacto por Probabilidad de ocurrencia

Tabla cruzada Impacto por Probabilidad de ocurrencia					
		Probabilidad. De Ocurrencia			Total
		Bajo	Medio	Alto	
Impacto	Bajo	13	2	0	15
		16,9%	3,1%	0,0%	8,5%
	Medio	47	36	11	94
		61,0%	56,3%	31,4%	53,4%
	Alto	17	26	24	67
		22,1%	40,6%	68,6%	38,1%
Total		77	64	35	176
		100,0%	100,0%	100,0%	100,0%

Interpretación: En la tabla 8. observamos que el 61,0 % de preguntas acerca del impacto son de medio impacto y también podemos observar que estos son de baja probabilidad de ocurrencia, asimismo podemos denotar que, el 56,3 % de preguntas son de medio impacto y también de probabilidad de ocurrencia media, es preciso resaltar que es de bastante riesgo, puesto que el 40,6 % son de alto impacto y la probabilidad de ocurrencia es media, en el contexto de seguridad informática esto es preocupante porque su ocurrencia podría tener alto impacto, también podemos observar que el 68,6 % de preguntas en cuanto a la probabilidad de ocurrencia alta, tienen alto impacto en la seguridad informática del vicerrectorado de investigación de la Universidad Nacional del Altiplano. Al igual que los autores Arenas-Villanueva & De-Los-Santos (2017) manifiestan que el estándar ISO 17799, proporcionan una herramienta útil con la que se pudo obtener una tabla cruzada y determinar la correlación entre ambas variables. De la misma forma Pozo-Zulueta *et al.* (2009) y el autor Cruz (2014), manifiestan que los procedimientos utilizados por testadores demuestran la correlación existente entre la probabilidad de ocurrencia de un evento y el impacto perjudicarían directamente en la integridad de la información.

Tabla 9

Correlación entre probabilidad de ocurrencia e impacto.

Pruebas de chi-cuadrado			
	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	29,424[a]	4	,000
Razón de verosimilitud	31,482	4	,000
Asociación lineal por lineal	27,049	1	,000
N de casos válidos	176		

Interpretación: En la tabla 9 podemos observar qué, de acuerdo a las pruebas de chi – cuadrado, teniendo un valor de significación de 0,000 menor a 0,05 podemos afirmar que, si existe correlación entre la variable probabilidad de ocurrencia e impacto, similar a los resultados obtenidos por Diaz-Limary (2018), quien establece que la auditoría informática se relaciona significativamente con la seguridad de la información.

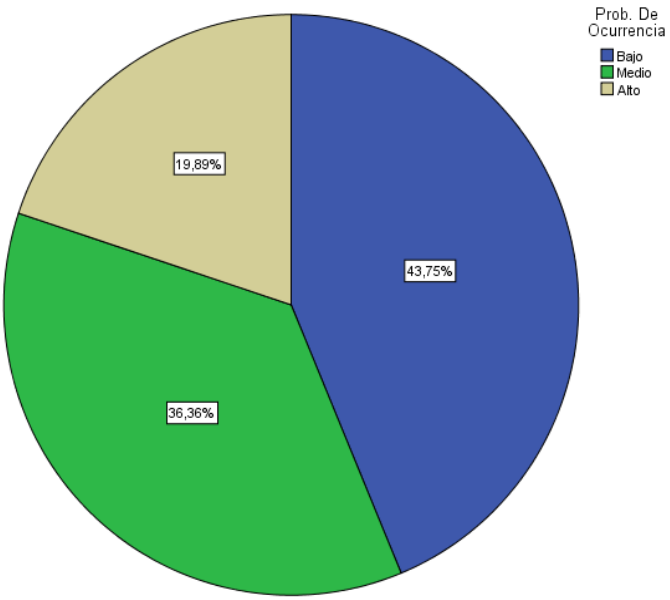


Figura 2. Gráficos circulares de porcentajes de probabilidad de ocurrencia

Interpretación: en la figura 2, podemos observar que en general la probabilidad de ocurrencia bajo es el 43,75%, es decir que menos del 50% de ítems son las que nunca ocurrieron en el ámbito de la seguridad informática en el Vicerrectorado de Investigación (VRI), esto no significa que nos encontramos con sistemas regularmente seguros, al contrario podemos considerar que es un nivel de seguridad deficiente, por otro lado podemos observar que el 36,30% de ítems son de probabilidad de ocurrencia media, lo que indica que ya ocurrió en determinadas ocasiones y estas podrían volver a repetirse, se refiere a los ataques o fallos de seguridad en los sistemas, las probabilidades de ocurrencia alto, sin duda son las más alarmantes puesto que son las que ocurrieron más de una vez pudiendo repetirse y comprometiendo la seguridad informática en los sistemas del vicerrectorado de investigación coincidiendo con los resultados de Dioppe-

Arellano (2015), que se enfocó en las amenazas a los sistemas y determinó que los usuarios y las empresas pusieron su atención en la vulnerabilidad y para contrarrestar estos fallos de seguridad.

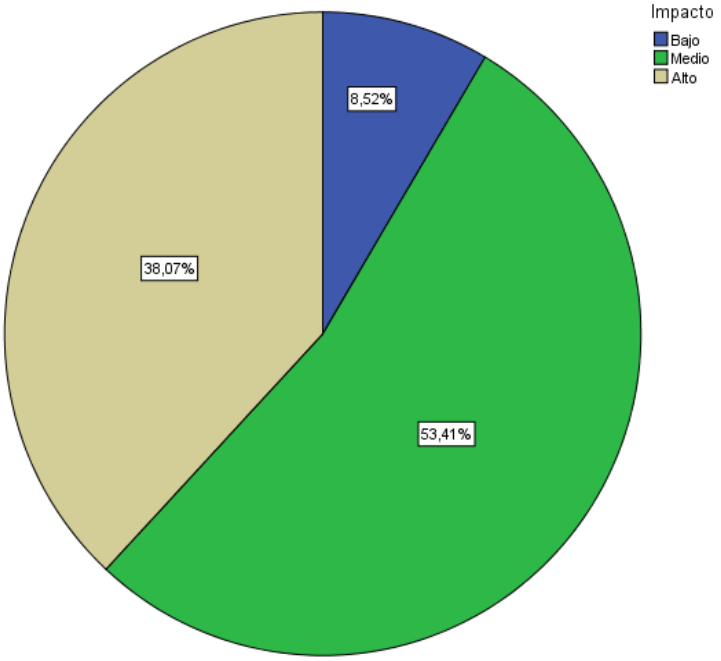


Figura 3. Gráficos circulares de porcentajes de impacto sobre activos

Interpretación: El nivel de impacto que se observa en los activos del VRI es bajo en un 8,52% los que significa que en cierta medida no podrían afectar de manera perjudicial o podrían ser recuperados. En un 53,41% el impacto que tendría en los activos del VRI serían de impacto medio, lo que significa que podría afectar, pero en cierta medida. Por otro lado, poniendo énfasis en esta parte que 38,07% de ítems observados demuestran que el impacto de darse determinados ataques a los sistemas del VRI podrían tener un alto impacto, lo que podría traducirse en la perdida, eliminación, destrucción, develación o modificación de activos, que podría traer valiosas y significativas pérdidas para el VRI.

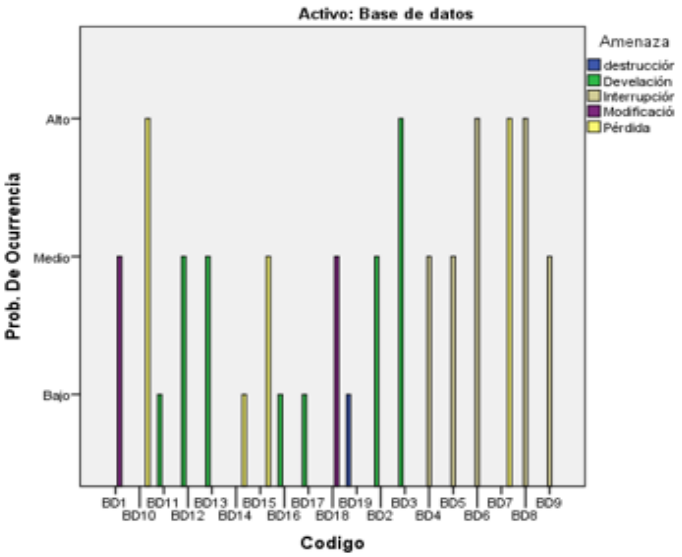


Figura 4. Probabilidad de ocurrencia en activo base de datos.

Interpretación: en el análisis de los histogramas del activo de base de datos, podemos observar que, 5 de los ítems con respecto a las bases de datos tienen una baja probabilidad de ocurrencia, 9 de los ítems tienen una probabilidad de ocurrencia media, 5 de los ítems tienen probabilidad de ocurrencia alta, en cuanto al activo base de datos en un análisis general podemos observar que tiene una alta probabilidad de ocurrencia.

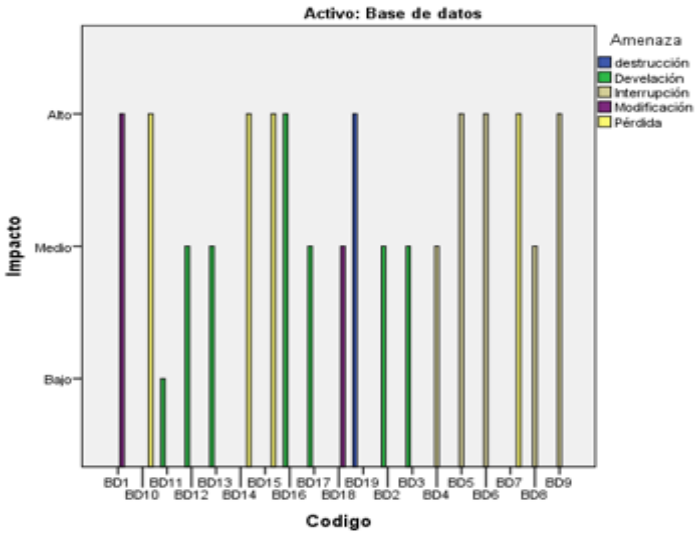


Figura 5. Impacto en activo base de datos

En la figura 5, respecto al impacto que este puede acarrear, 1 ítem tiene bajo impacto, 8 ítems tienen medio impacto, 10 ítem tienen alto impacto, esto nos

muestra que el activo de base de dato es importante y una pérdida o un fallo de seguridad podría causar alto impacto. Del mismo modo López-de-Jiménez (2017), manifiesta que, ninguna aplicación es segura y está libre de ataques, pero con el uso de test se evitan los ataques que afectan la integridad y fiabilidad de los datos.

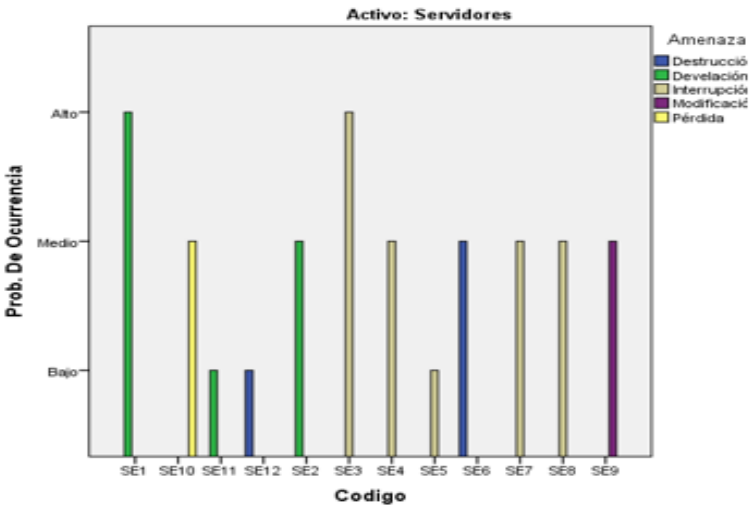


Figura 6. Probabilidad de ocurrencia en activo servidores

Interpretación: en los histogramas de la figura anterior, 3 de los ítems nos muestra una probabilidad de ocurrencia, 7 tienen una probabilidad de ocurrencia media, 2 ítems tienen una probabilidad de ocurrencia alta, en general es medianamente probable que ocurra un incidente de fallo de seguridad.

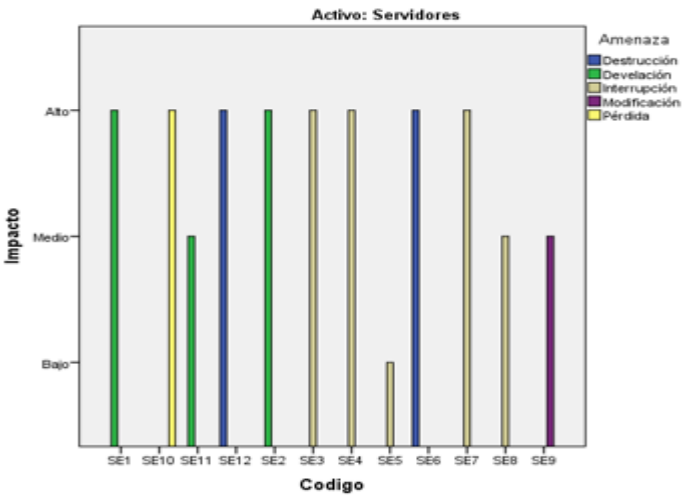


Figura 7. Nivel de impacto en activo servidores

En la figura 7, en cuanto al impacto que estos pueden presentar, 1 ítem es de bajo impacto, 3 ítems de medio, son de medio impacto, 8 ítems son de alto impacto, con esto podemos ver que el fallo de seguridad tendría un alto impacto en el activo de

servidores. Cruz-Saavedra (2014) también menciona que los servidores son los principales activos afectados por un ataque cibernético.

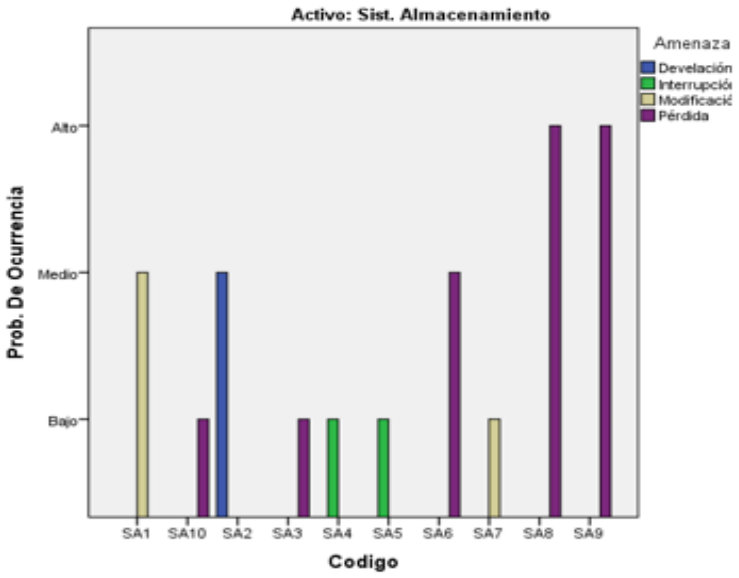


Figura 8. Probabilidad de ocurrencia en activo sistema de almacenamiento

Interpretación: en el gráfico anterior el activo con respecto al sistema de almacenamiento, 5 ítems tienen una probabilidad baja de ocurrencia, 3 una probabilidad de ocurrencia media y 2 ítems de alta probabilidad de ocurrencia.

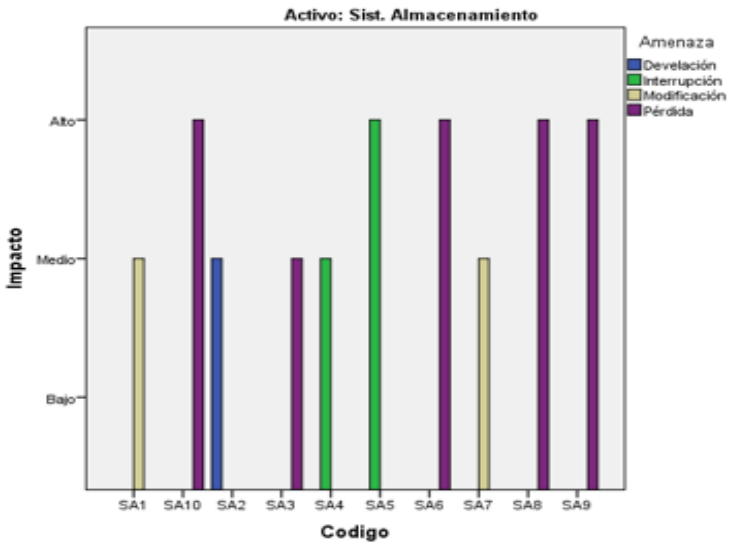


Figura 9. Nivel de impacto en activo sistemas de almacenamiento

En la figura 9, en cuanto al impacto, 5 ítems presentan un impacto medio y 5 ítems presentan un alto impacto, si bien es cierto que es poco probable que ocurra un fallo de seguridad que afecte al activo sistema de almacenamiento, el impacto que este puede causar sería de mediano hasta alto impacto. Como lo manifiesta Aro-Maquera (2021), auditar sistemas de información permitieron tener un diagnóstico sobre la situación actual tecnología.

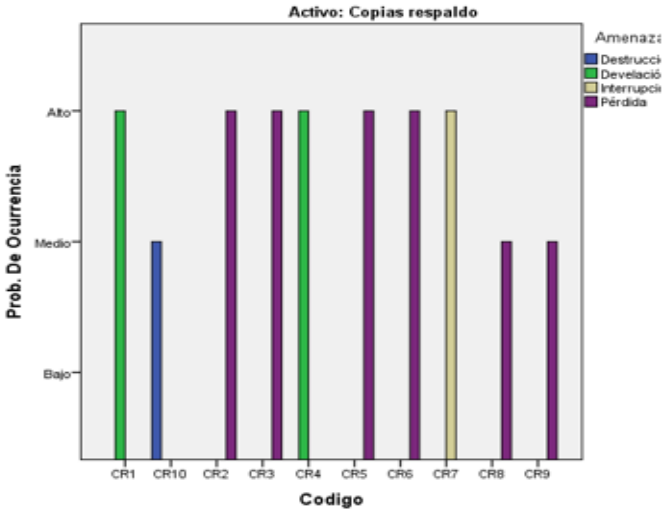


Figura 10. Probabilidad de ocurrencia en activo copias de respaldo

Interpretación: en el activo con respecto a las copias de respaldo, 3 ítems presentan probabilidad de ocurrencia medio, 7 ítems presentan probabilidad de ocurrencia alto.

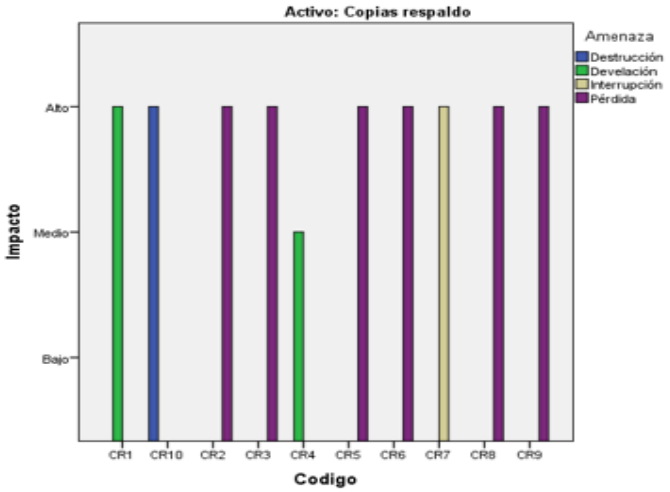


Figura 11. Nivel de impacto en activo copias de respaldo

En la figura 11, en cuanto al impacto en las copias de respaldo 1 ítem presenta un impacto medio, 9 ítems presentan un impacto alto, podemos deducir que la probabilidad de ocurrencia es alta y el impacto también de sufrir un fallo de seguridad. Al igual que Romero-Fuentes (2011) la seguridad se basa en la efectiva administración de los permisos de acceso.

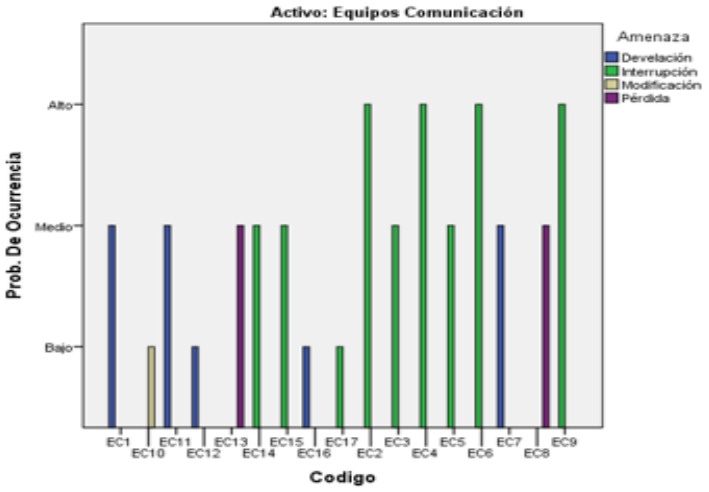


Figura 12. Probabilidad de ocurrencia de activo equipos de comunicación

Interpretación: los fallos de seguridad en activos de equipos de comunicación, 4 ítems presentan una baja probabilidad de ocurrencia, 9 ítems presentan una probabilidad de ocurrencia media, 4 ítems presentan una probabilidad de ocurrencia alta.

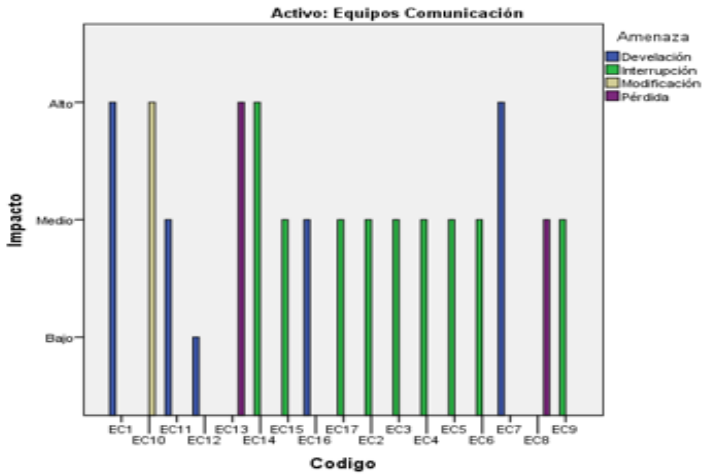


Figura 13. Nivel de impacto en activo equipos de comunicación

En la figura 13, en cuanto al nivel de impacto que puede acarrear 1 ítem es de bajo impacto, 11 ítems presentan un impacto medio, 5 ítems presentan un impacto alto, es decir es muy probable la ocurrencia de un fallo de seguridad y este puede presentar impactos en escala media lo que nos muestra que las conexiones a las redes informáticas agravan los riesgos de seguridad al igual lo manifiestan Socarrás & Santana (2019).

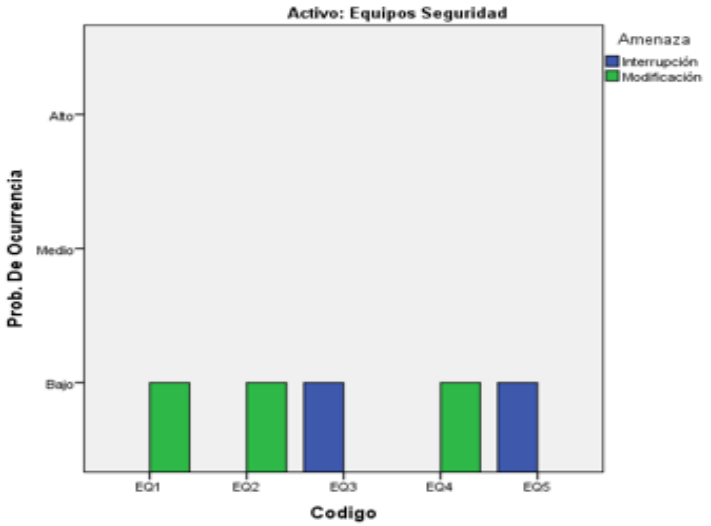


Figura 14. Probabilidad de ocurrencia en activos equipos de seguridad

Interpretación: en la figura 14, de 5 ítems tienen una baja probabilidad de ocurrencia, pero de ocurrir tendrían un alto impacto en el activo equipos de seguridad como se muestra en la figura 15.

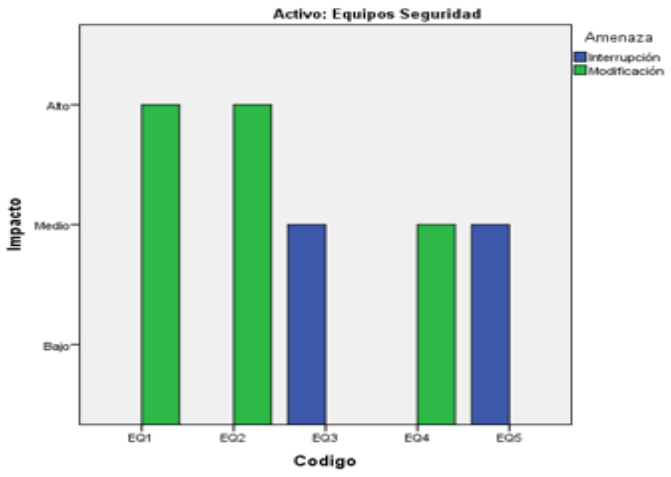


Figura 15. Nivel de impacto en activos equipos de seguridad

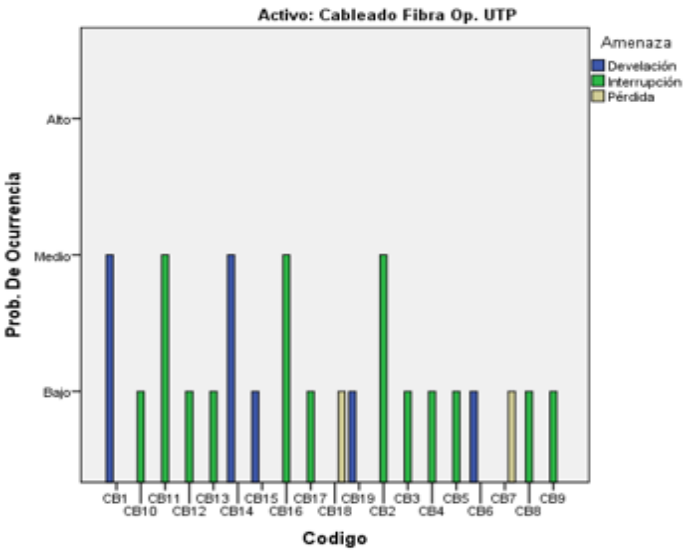


Figura 16. Probabilidad de ocurrencia en activo cableado fibra óptica y UTP

Interpretación: 14 ítems presentan una probabilidad de ocurrencia es bajo, 5 ítems presentan probabilidad de ocurrencia media como se puede observar en la figura 16.

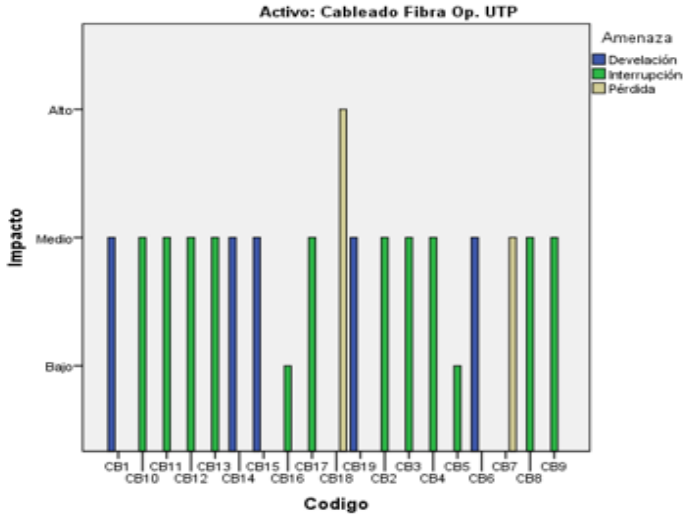


Figura 17. Nivel de impacto en activo cableado fibra óptica y UTP

En cuanto al nivel de impacto causado como se puede observar en la figura 17, se afirma que, 2 ítems presentan un bajo impacto, 16 ítems presentan un impacto medio, 1 ítem tiene un impacto alto, es decir un fallo de seguridad en el activo cableado fibra óptica y UTP es poco probable que ocurra y de ocurrir tendría un

impacto medio, lo que hace denotar que las infraestructuras físicas como el cableado estructurado de redes informáticas también deben tener especial cuidado para evitar pérdidas de información como lo sostienen Aguilar-Portilla & De-La-Cruz-Ramos (2015) en su investigación.

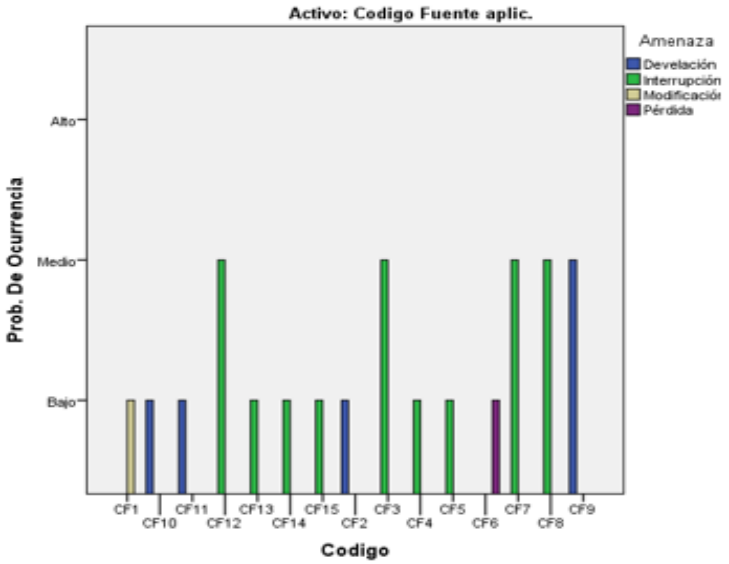


Figura 18. Probabilidad en activo código fuente de aplicación

Interpretar: con respecto al activo código, 10 ítems tienen probabilidad de ocurrencia bajo, 5 ítems tienen probabilidad de ocurrencia medio.

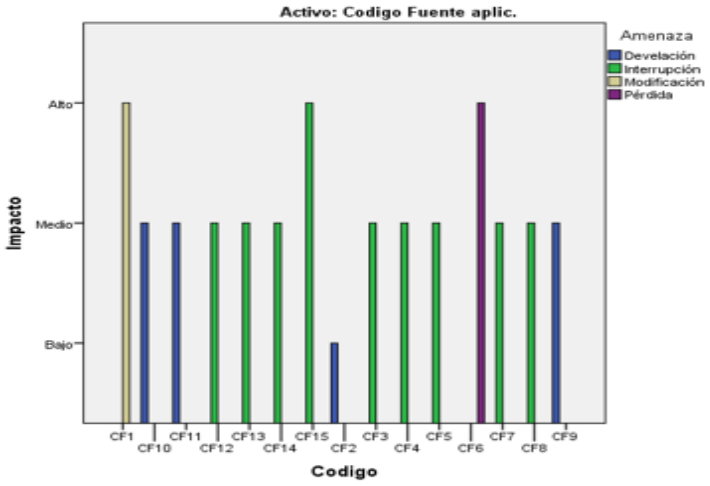


Figura 19. Nivel de impacto en activo código fuente de aplicación

En la figura 19, en cuanto al impacto que puede acarrear, 1 ítem tiene un bajo impacto, 11 ítems presentan impacto medio, 3 ítems presentan un impacto alto, es decir la probabilidad de ocurrencia de un fallo de seguridad en el activo código fuente de las aplicaciones, tendrían un impacto medio. Las aplicaciones desarrolladas dentro del VRI cuentan con las medidas de seguridad basadas en protocolos y encriptación lo que incrementa el nivel de seguridad afirmación que respalda Taco-Arias & Gamarra-Ramirez (2014).

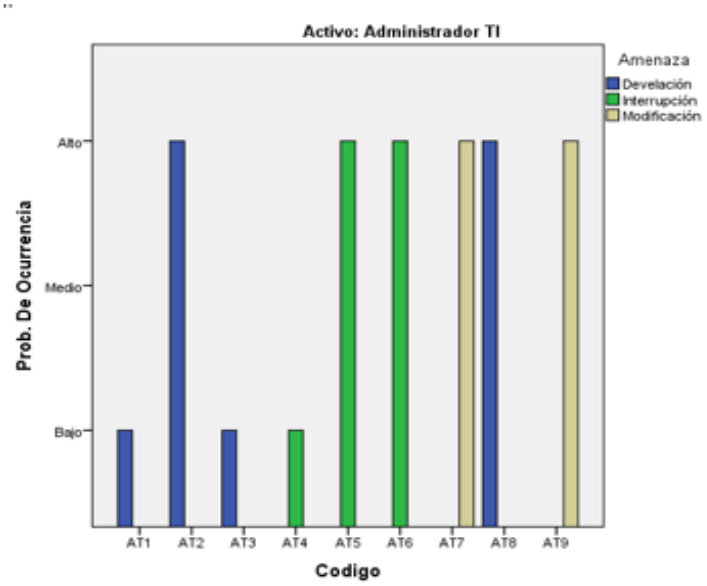


Figura 20. Probabilidad de ocurrencia en activo administrador TI

Interpretación: con respecto al activo administrador tecnología de la información, 3 ítems tienen baja probabilidad de ocurrencia, 6 ítems presentan una alta probabilidad de ocurrencia, es decir, la probabilidad de ocurrencia de un fallo de seguridad en este activo es muy alta.

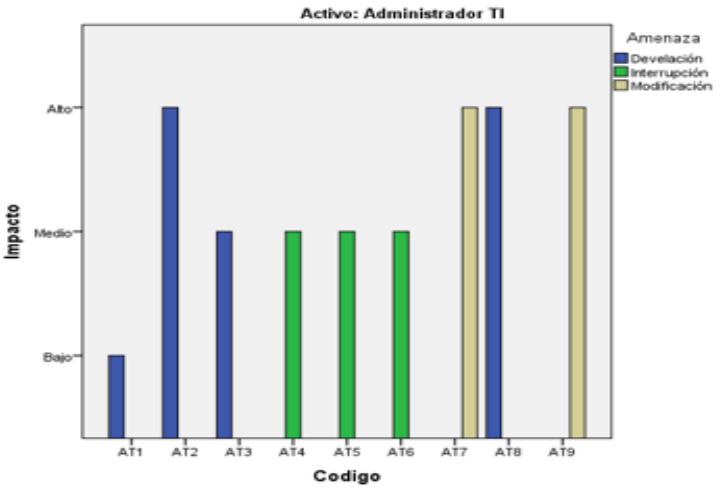


Figura 21. Nivel de impacto en activo Administrador TI

Interpretación: en la figura 21 observamos que, los impactos son de entre medio y alto. Por lo que instalar algún mecanismo de defensa y monitor que funcione como guardián ayuda prevenir transacciones no permitidas, prototipo planteado por Sanchez-Mamani & Huirse-Cruz (2017).

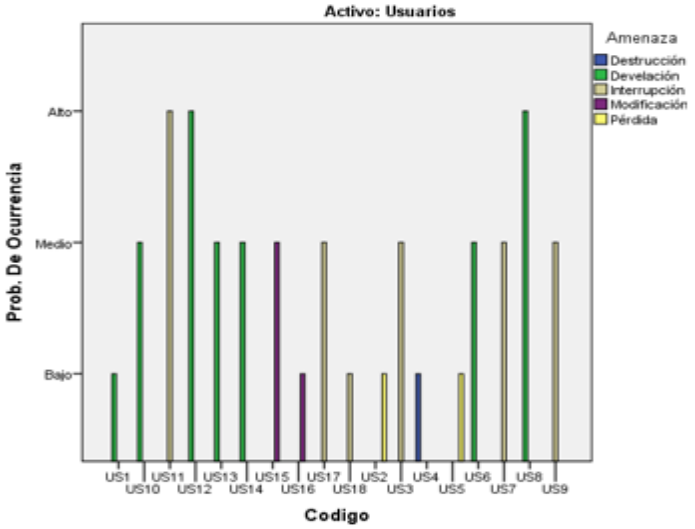


Figura 22. Probabilidad de ocurrencia en activo usuarios

Interpretar: con respecto al activo usuarios, 6 ítems tienen baja probabilidad de ocurrencia, 9 ítems tienen probabilidad de ocurrencia media, 3 ítems alta probabilidad de ocurrencia.

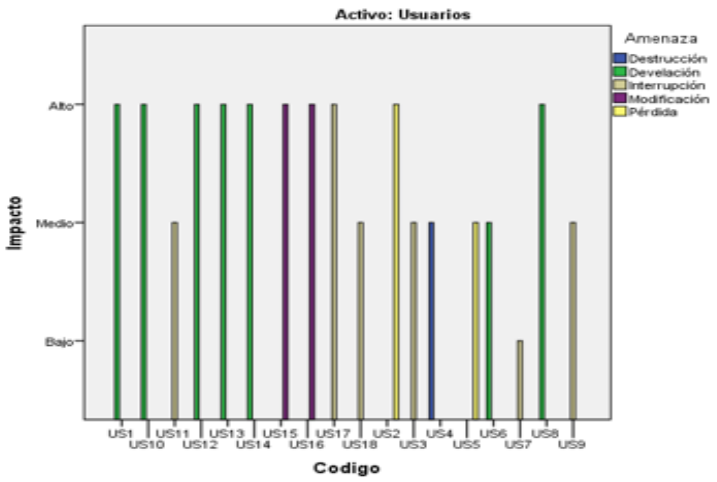


Figura 23. Nivel de impacto en activo usuarios

En la figura 23, en cuanto al impacto 1 ítem presenta bajo impacto, 7 ítems presentan impacto medio, 10 ítems presentan alto impacto. Es decir, este activo presenta una probabilidad media con un impacto alto de ocurrir un fallo de seguridad. Los usuarios son el eslabón más débil de seguridad por lo que implementar políticas de seguridad basadas en ISO 17799, ISO 27002 o COBIT 5 ayudan a determinar los protocolos de acción antes, durante y después de un ataque como también lo manifiestan los autores Aro-Maquera (2021), Puma (2017) Tarrillo-Clavo & Correa-Cubas (2013) y Carbajal-Romero (2013).

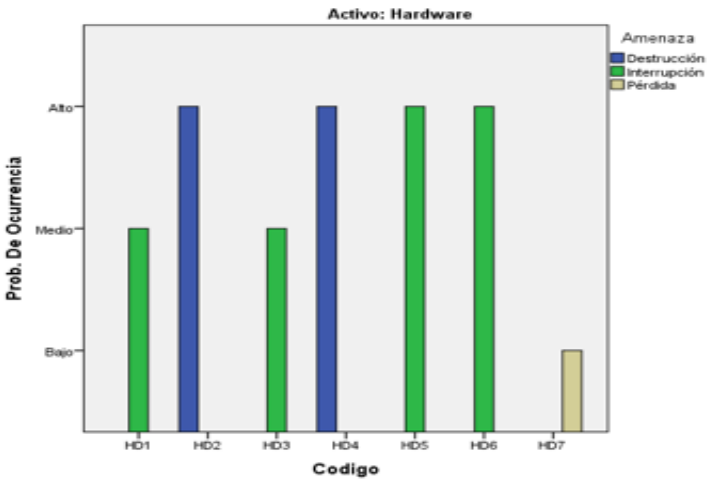


Figura 24. Probabilidad de ocurrencia en activo hardware

Interpretación: en el gráfico anterior podemos observar que, 1 ítem tiene probabilidad de ocurrencia baja, 2 ítems presentan una probabilidad de ocurrencia media, 4 ítems presentan una probabilidad de ocurrencia alta.

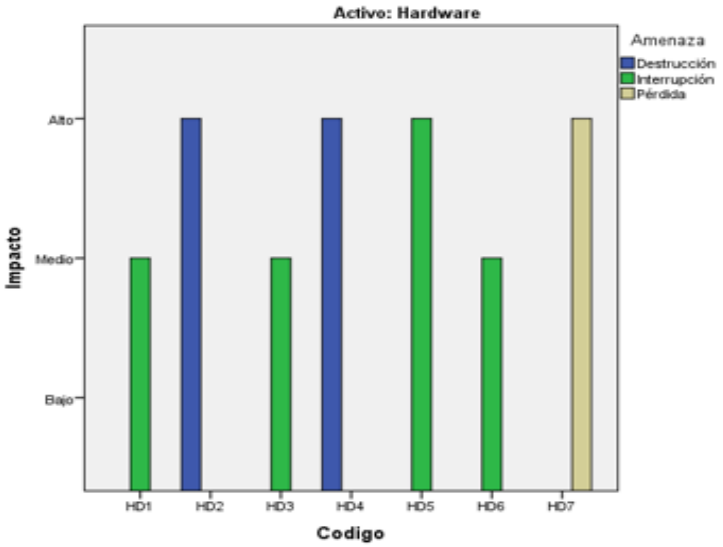


Figura 25. Nivel de impacto en activo hardware

En la figura 25, en cuanto al nivel de impacto, 3 ítems presentan impacto medio, 4 ítems presentan un impacto alto, es decir, la probabilidad de ocurrencia es alta y el impacto sobre el activo de hardware es alto. Tener los equipos e infraestructura en salvaguarda cuidando y cumpliendo los estándares establecidos bajo herramientas de gestión de riesgos proporcionados por políticas de seguridad garantiza un buen funcionamiento y previene perdidas de información afirmación que también comparte Calderón-Alvarado (2017).

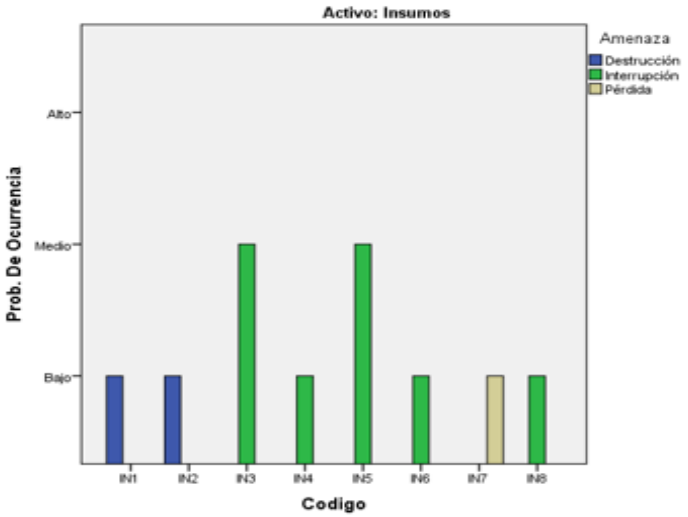


Figura 26. Probabilidad de ocurrencia en activo insumos

Interpretación: los activos de insumos, 6 ítems presentan baja probabilidad de ocurrencia, 2 ítems tienen probabilidad de ocurrencia medio.

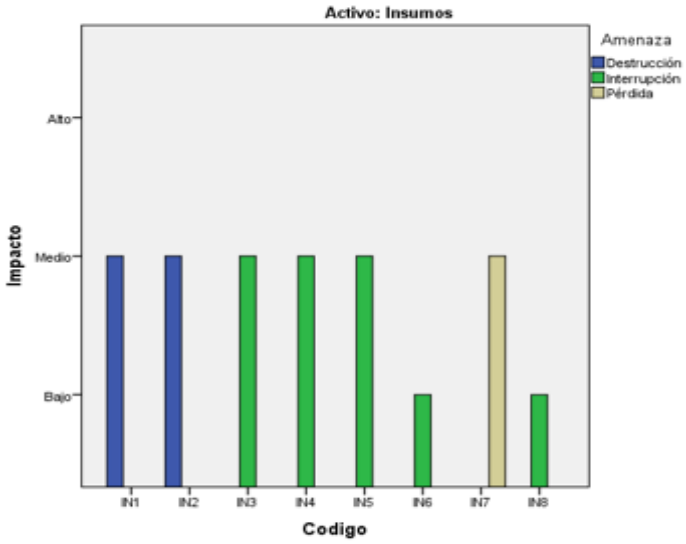


Figura 27. Nivel de impacto en activo insumos

En cuanto al impacto en la figura 27 se observa que, 2 ítems tienen bajo impacto, 6 ítems presentan impacto medio, en general podemos decir la probabilidad de ocurrencia en los activos de insumos tienen probabilidad baja, pero de ocurrir tendrían un impacto medio. Los insumos en una entidad deben tener un espacio y ser manejados adecuadamente para estos se deben apoyar de guías de implementación tales como COBIT 5 como lo recomienda Carbajal-Romero (2013).

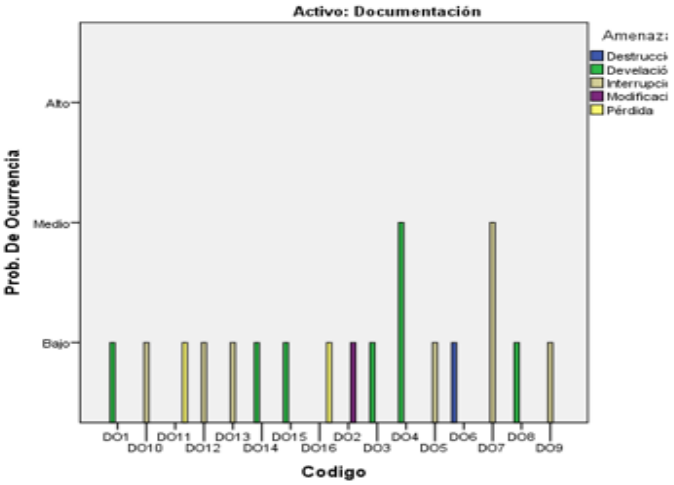


Figura 28. Probabilidad de ocurrencia en activo documentación

Interpretación: los activos de documentación presentan probabilidad de ocurrencia baja, pero de ocurrir podría acarrear un impacto medio. 14 ítems tienen baja probabilidad de ocurrencia, 2 ítems probabilidad de ocurrencia media, 5 ítems

presentan bajo impacto, 11 ítems presentan impacto medio. Documentar o registras las decisiones tomadas dentro de una organización es de vital importancia, porque ayuda al nuevo personal a poder contar con guías y antecedentes de algún determinado evento, pero estos al igual que otros activos también deben tener restricciones de acceso opinión que también comparte Romero-Fuentes (2011).

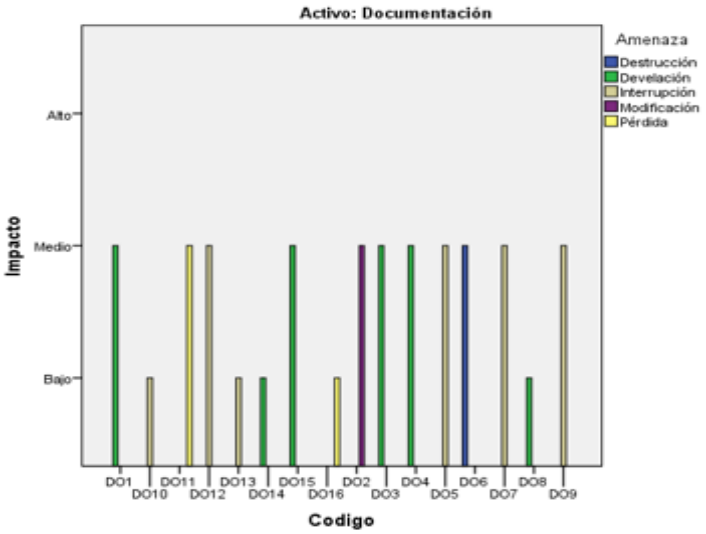


Figura 29. Nivel de impacto en activo documentación

Interpretación: en la figura 29 se observa que 11 ítems registran un nivel de impacto de medio, mientras 5 ítems registran un nivel de impacto bajo.

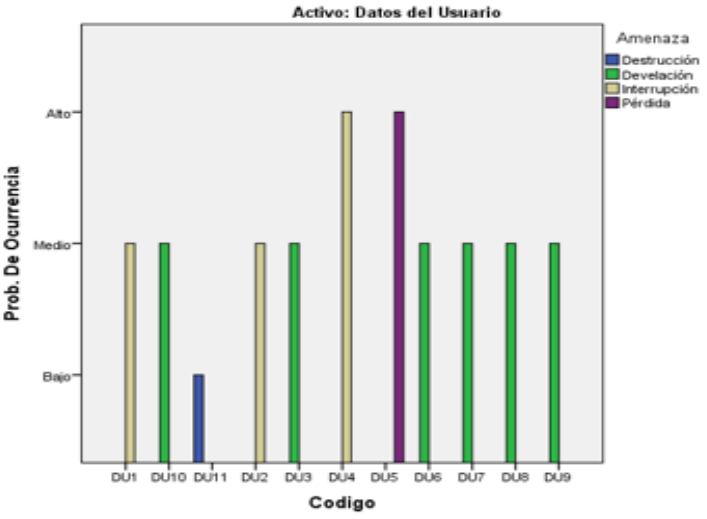


Figura 30. Probabilidad de ocurrencia activo datos de usuario

Interpretación: los activos de datos de usuarios, 1 ítem presenta baja probabilidad de ocurrencia, 8 ítems presentan probabilidad de ocurrencia media, 2 ítems alta probabilidad de ocurrencia.

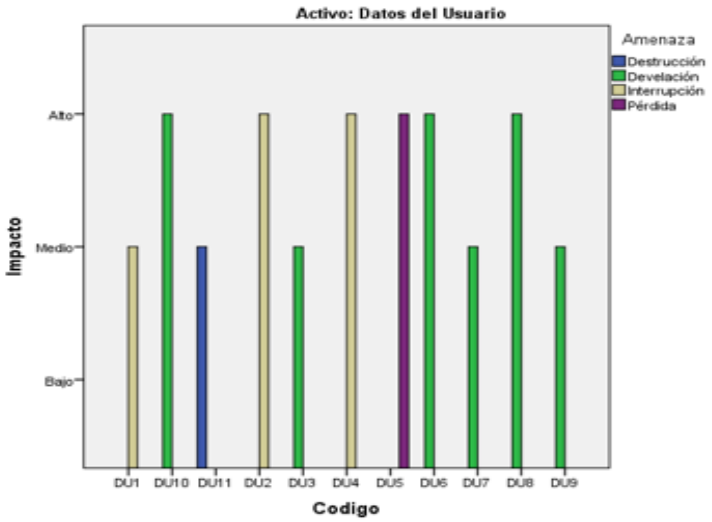


Figura 31. Nivel de impacto en activo datos de usuario

En la figura 31, en cuanto al impacto, 5 ítems tienen un impacto medio, 6 ítems tienen un alto impacto, es decir, un fallo de seguridad en los activos de datos de usuarios presenta probabilidad de ocurrencia media con medio y alto impacto en los activos de ocurrir. Los datos de los usuarios son fundamentales y hasta se podría decir que son los principales por lo que se debe tener especial cuidado, ya sea asegurando y sacando copias de seguridad periódicamente y garantizar el acceso solo a personal autorizado cuidando en todo momento la disponibilidad de esta información tal como también lo menciona Costa-Santos (2014).

CONCLUSIONES

El nivel de riesgo de Seguridad informática en la plataforma del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno, es Alto, puesto que es de alto impacto y la probabilidad de ocurrencia es media, en seguridad informática esto es preocupante porque su ocurrencia podría tener graves consecuencias, Además, se observó que los ítems con una probabilidad de ocurrencia alta también representaron un alto impacto en el nivel de riesgo de seguridad.

De acuerdo con las pruebas de chi cuadrado, se puede afirmar que existe una correlación entre la variable probabilidad de ocurrencia e impacto.

La probabilidad de ocurrencia medio y alto indican que ocurrió un suceso de amenaza a los sistemas del vicerrectorado de investigación, lo que indica un nivel de seguridad deficiente y de alto riesgo, por lo que se agruparon ambos porcentajes de ocurrencia concluyendo y determinando que el cincuenta por ciento de ítems observados representan una probabilidad de ocurrencia alta de acuerdo con el estándar ISO 17799, lo que significa que en términos de seguridad informática, los activos observados se vieron afectados y vulnerados.

Se determinó que el nivel de impacto en la plataforma del Vicerrectorado de Investigación es medio, de acuerdo con los activos que se ven comprometidos en caso de nuevos ataques a la seguridad informática hacia los activos observados.

RECOMENDACIONES

Implementar políticas de seguridad bajo algún estándar tal como podría ser el estándar ISO17799 que permitiera administrar mejor los activos del área de vicerrectorado de investigación.

Analizar toda probabilidad de ocurrencia basada en sucesos anteriores nos ayudará a identificar las posibles amenazas a los sistemas que se manejan y evitar pérdidas de información, o que la información pueda ser modificada y alterada.

Los recursos humanos suelen ser frecuentemente el eslabón más débil en la seguridad informática, por lo que se sugiere, realizar constantes capacitaciones en cuanto a políticas de seguridad y manejo de información sensible.

BIBLIOGRAFÍA

Adams, N. M., & Heard, N. (2014). *Data analysis for network cyber-security*. Imperial College London.

Aguilar-Portilla, S. S., & De-La-Cruz-Ramos, V. G. (2015). *Implementación de una solución de hacking ético para mejorar la seguridad en la infraestructura informática de la caja municipal de Sullana – Agencia Chimbote* [Universidad Nacional del Santa]. Recuperado de: http://repositorio.uns.edu.pe/bitstream/handle/UNS/2017/26316.pdf?sequence=1&isAllowed=y

Alcántara-Flores, J. C. (2015). Guía de implementación de la seguridad basado en la norma ISO/IEC27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P. en la ciudad de Chiclayo [Universidad Católica Santo Toribio de Mogrovejo]. En *Universidad Católica Santo Toribio de Mogrovejo - USAT*. Recuperado de: http://tesis.usat.edu.pe/handle/usat/539

Amasifuen-Shupingagua, J. (2015). *Seguridad en aplicaciones informáticas* [Universidad Nacional de la Amazonía Peruana]. Recuperado de: http://repositorio.unapiquitos.edu.pe/handle/UNAP/5034

Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (Second Edition). Wiley Edition. Recuperado de: https://terrorgum.com/tfox/books/security_engineering_a_guide_to_building_dependable_distributed_systems.pdf

Anthros, G. E. (2012). *Manual de Seguridad en Redes*. Subsecretaría de Tecnologías Informáticas. Recuperado de: https://centrodocumentacion.psicosocial.net/wp-content/uploads/2004/01/arcert-manual_de_seguridad_en_redes_informaticas.pdf

Arenas-Villanueva, C. A. J., & De-Los-Santos, D. (2017). *Gestión de la seguridad de la información para la toma de decisiones en la infraestructura de la red telemática de la Universidad Nacional Pedro Ruiz Gallo utilizando COBIT 5 y software open source.* [Universidad Nacional Pedro Ruiz Gallo]. Recuperado de: http://repositorio.unprg.edu.pe/handle/UNPRG/3830

Aro-Maquera, J. L. (2021). *Auditoria informática del sistema de administración Tributaria de la municipalidad distrital de Pilcuyo* [Universidad Nacional del Altiplano]. Recuperado de: https://repositorio.unap.edu.pe/handle/20.500.14082/15399

Benites-Barreiro, J. A., Chóez-Cajamarca, D. A., & Espinal-Santana, A. G. (2016). *Auditoría de seguridad en redes inalámbricas , soluciones y recomendaciones*. *1*, 1-6. Recuperado de: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/32021

Calderón-Alvarado, J. J. (2017). *Aplicación de la herramienta de gestión de riesgos para la seguridad informática del Honadomani San Bartolomé* [Universiad César Vallejo]. Recuperado de: http://repositorio.ucv.edu.pe/handle/UCV/1879

Campos-Muñoz, A. E., & Rios-Damián, C. A. (2016). *Auditoria en el uso de tecnología de información para optimizar la seguridad de la Caja Sipán S.A* [universidad Nacional Pedro Ruiz Gallo]. Recuperado de: http://repositorio.unprg.edu.pe/handle/UNPRG/1016

Carbajal-Romero, J. A. (2013). *Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano*. Universidad de Piura.

Cardwell, Kevin. (2014). *Building virtual pentesting labs for advanced penetration testing : build intricate virtual architecture to practice any penetration testing technique virtually*. Packt Publishing.

Castello, R. J. (2017). Auditoría en entornos informáticos. En *Journal of Science and Research: Revista Ciencia e Investigación* (Vol. 3). Recuperado de: https://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_download&gid=552&Itemid=19

Costa-Santos, J. (2014). *Seguridad informática* (RA-MA, Ed.). Recuperado de: https://www.ra-ma.es/libro/seguridad-informatica-grado-medio_49134/

Cruz-Saavedra, W. G. (2014). *Aplicación de auditoría penetration testing para contribuir con la seguridad de la información en los sistemas informáticos de la empresa Data Business SAC, Trujillo* [Universidad Privada del Norte]. Recuperado de: http://hdl.handle.net/11537/10239

Diaz-Limary, R. (2018). *La auditoría informática y la seguridad de la información en el área de sistemas de la Caja del Santa, Chimbote - 2018* [Universidad Privada del Norte]. Recuperado de: http://hdl.handle.net/11537/13870

Dioppe-Arellano, N. K. F. (2015). *Seguridad informática* [Universidad Nacional de la Amazonía Peruana]. Recuperado de: http://repositorio.unapiquitos.edu.pe/handle/UNAP/4898

Drake, J. J., Fora, P. O., Lanier, Z., Mulliner, C., Ridley, S. A., & Wicherski, G. (2014). *Android Hacker's Handbook*. John Wiley & Sons, Inc.

Dykstra, J. (2016). *Essential Cybersecurity Science* (Firts Edition). O'Reilly. Recuperado de: http://oreilly.com/catalog/errata.csp?isbn=0636920037231

González-Perez, P., Sánchez-Garcés, G., & Soriano-De La Cámara, J. M. (2013). *Pentesting con Kali* (0xWORD Com).

Hassan, N. A. (2019). Digital Forensics Basics. En *Digital Forensics Basics*. Apress. Recuperado de: https://doi.org/10.1007/978-1-4842-3838-7

Hernández-Hernández, E. (1993). *Auditoria de informática - Un enfoque metodológico* [Universidad Autónoma de Nuevo León]. Recuperado de: https://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_download&gid=552&Itemid=19

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2014). *Metodología de la investigación* (M. G. Hill, Ed.; 6ta edició).

Kostopoulos, G. K. (2013). *Cyberspace and Cybersecurity*. Taylor & Francis Group. Recuperado de: http://www.taylorandfrancis.com

López de Jiménez, R. E. (2017). *Pruebas de penetración en aplicaciones web usando hackeo ético*. *10*, 13-19. Recuperado de: http://hdl.handle.net/10972/3018

López-Alvarez, D. M. (2015). *Hacking ético para detección de vulnerabilidades de una empresa del sector de telecomunicaciones* [Escuela Superior Politécnica del Litoral]. Recuperado de: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/36478

Machicao-Mollocondo, S. G. (2019). Análisis de riesgo y políticas de seguridad de información de la oficina de tecnologías de información (OTI) – UNA Puno 2018 [Universidad Nacional del Altiplano]. En *Universidad Nacional del Altiplano Escuela de Posgrado*. Recuperado de: http://repositorio.unap.edu.pe/bitstream/handle/UNAP/12303/Yana_Aydee_Quispe_Patricia.pdf?sequence=1&isAllowed=y

Muniz, Joseph., & Lakhani, Aamir. (2013). *Web Penetration Testing with Kali Linux : a Practical Guide to Implementing Penetration Testing Strategies on Websites, Web Applications, and Standard Web Protocols with Kali Linux*. Packt Publishing.

Pfleeger, C. P., Lawrence-Pfleeger, S., & Margulies, J. (2015). *Security in Computing* (Pearson Education, Ed.; Fifth Edition). Prentice Hall. Recuperado de: https://eopcw.com/assets/stores/Computer%20Security/lecturenote_1704978481security-in-computing-5-e.pdf

Pinzón-Parada, I. (2017). *Gestión del riesgo en seguridad informática*. Recuperado de: http://repository.unipiloto.edu.co/handle/20.500.12277/2840

Plaza-Torres, P. J. (2014). Métodos de ataques informáticos. [universidad Nacional de la Amazonía Peruana]. En *Universidad Nacional de la Amazonía Peruana*. Recuperado de: http://repositorio.unapiquitos.edu.pe/handle/UNAP/4485?show=full

Pozo-Zulueta, D., Quinteros-Ríos, M., Hernández-Aguilar, V., Gil-Loro, L., & Lorenzo-Álvarez, M. F. (2009). *Procedimiento para pruebas de intrusión en aplicaciones web*. *5*, 70-76. Recuperado de: http://www.redalyc.org/articulo.oa?id=92217153010

Puma, M. Y. (2017). *Implantación de un proceso de auditoría de suguridad de información najo la norma ISO/IEC 27002 enuna entidad financiera de Puno - 2016* [Universidad Nacional del Altiplano]. Recuperado de: http://repositorio.unap.edu.pe/bitstream/handle/UNAP/7104/Molleapaza_Mamani_Joel_Neftali.pdf?sequence=1&isAllowed=y

Ramírez-Reyes, G. (2002). *Metodología para auditoria informática en entidades públicas*. Universidad Nacional de Ingeniería.

Rodríguez, C. I., Zapien, L., Myerson, J. M., Villal, A., & Torres, J. (2012). *Códigos de buenas prácticas UNE-ISO / IEC 17799* (Vol. 14, Número May). Recuperado de: http://pdf.usaid.gov/pdf_docs/PA00JRCT.pdf%0Ahttp://www.revista.unam.mx/vol.14/num2/art10/art10.pdf

Rodríguez, R., & Ribón Zarco, J. (2017). *Políticas de seguridad informática (PSI)*. Recuperado de: https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf

Romero, M. I., Figueroa, G. L., Vera, D. S., Álava, J. E., Parrales, G. R., Álava, C. J., Murillo, Á. L., & Castillo, M. A. (2018). *Introducción a la seguridad infromática y el análisis de vulnerabilidades* (S. L. Editorial Área de Innovación y Desarrollo, Ed.; octubre 20). Recuperado de: https://doi.org/http://dx.doi.org/10.17993/IngyTec.2018.46

Romero-Fuentes, V. G. (2011). *Plan de seguridad informática en el MTC* [Universidad Nacional de Ingeniería]. Recuperado de: http://cybertesis.uni.edu.pe/bitstream/uni/1588/1/lopez_pr.pdf

Sabillón, R., & Cano-M, J. J. (2019). *Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones*. *1*, 33-48. Recuperado de: https://doi.org/10.17013/risti.32.33

Sanchez-Mamani, J. W., & Huirse-Cruz, S. A. (2017). *Prototipo de software para el control de las vulnerabilidades esteganográficas del protocolo HTTP de la capa aplicación en la oficina de tecnología informática de la Universidad Nacional del Altiplano 2015* [Universidad Nacional del Altiplano]. Recuperado de: http://repositorio.unap.edu.pe/bitstream/handle/UNAP/9408/Rosa_Enriquez_Yuca.pdf?sequence=1&isAllowed=y

Socarrás, H. E., & Santana, I. (2019). Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação*, *32*, 83-96. Recuperado de: https://doi.org/10.17013/risti.32.83-96

Taco-Arias, L. A., & Gamarra-Ramirez, S. E. (2014). *Sistema web para el intercambio seguro de documentos electrónicos, utilizando firmas y certificados digitales x509,*

sobre un canal SSL [Universidad Católica Santa María]. Recuperado de: https://tesis.ucsm.edu.pe/repositorio/handle/UCSM/2158

Tarrillo-Clavo, E. A., & Correa-Cubas, J. C. (2013). *Metodología para un sistema de gestión de la seguridad de la información basado en la norma técnica peruana NTP - 17799 en la administración de la Municipalidad distrital de Lambayeque Setiembre 2013 - febrero 2014.* [Universidad Nacional Pedro Ruiz Gallo]. Recuperado de: http://repositorio.unprg.edu.pe/handle/UNPRG/499

Waschke, M. (2017). Personal cybersecurity: How to avoid and recover from cybercrime. En *Personal Cybersecurity: How to Avoid and Recover from Cybercrime*. Apress Media LLC. Recuperado de: https://doi.org/10.1007/978-1-4842-2430-4

ANEXOS

Anexo 1. Test ISO 17799 Factores de Riesgo

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
BASE DE DATOS	**COD**	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
	BD1	Acceso no autorizado a datos (borrado, modificación, etc.)	Pérdida, revelación o Modificación de datos; pérdida de tiempo y productividad	Un intruso accede a la base de Datos.	Modificación	M	A
	BD2	Base de datos compleja	Desarrollo complejo de sistemas	Base de datos con alta densidad de registros o tablas	Develación	M	M
	BD3	Copia no autorizada de un medio de datos	Divulgación de información	Un usuario accede a la base de datos y copia parte o toda la Información.	Develación	A	M
	BD4	Errores de software	Inconsistencia en los datos	Falla en la aplicación de usuario	Interrupción	M	M
	BD5	Falla de base de datos	Inconsistencia en los datos	Error o falla en el motor de base de datos	Interrupción	M	A
	BD6	Falta de espacio de almacenamiento	Falla en la aplicación	Discos de baja capacidad de almacenamiento	Interrupción	A	A
	BD7	Mala configuración de la programación de las copias de respaldo	Datos sin backup	Programación inadecuada en horario de producción	Pérdida	A	A
	BD8	Mala integridad de los datos	Inconsistencia y redundancia de datos	Base de datos diseñada o mantenida de forma deficiente lo cual provoca errores de integridad	Interrupción	A	M
	BD9	Medios de datos no están disponibles cuando son necesarios	Pérdida de tiempo y productividad	Base de datos diseñada o mantenida de forma deficiente lo cual provoca problemas de disponibilidad	Interrupción	M	A
	BD10	Pérdida de copias de respaldo	Incapacidad de restauración	Falla en el hardware del equipo de respaldo	Pérdida	A	A
	BD11	Perdida de confidencialidad en datos privados y de sistema	Divulgación de información	Exposición de información negligentemente	Develación	B	B
	BD12	Perdida de datos en tránsito	Inconsistencia de datos y divulgación de información	Usuario malicioso conectado Usando programas de intercepción	Develación	M	M
	BD13	Portapapeles, impresoras o directorios compartidos	Divulgación de información	Impresión de un reporte	Develación	M	M
	BD14	Robo	Pérdida de información	Sustracción del medio de almacenamiento	Pérdida	B	A
	BD15	Sabotaje	Pérdida o modificación de datos, pérdida de tiempo y productividad	Ataque a la base de datos	Pérdida	M	A
	BD16	Seguridad de base de datos deficiente	Perdida o modificación de datos	Seguridad mínima en el servidor base de datos	Develación	B	A
	BD17	Spoofing y sniffing	Divulgación y modificación de información	Usuario malicioso conectado usando programas de intercepción	Develación	B	M
	BD18	Transferencia de datos incorrectos	Inconsistencia de datos	Error de digitación	Modificación	M	M
	BD19	Virus, gusanos y caballos de Troya	Pérdida, modificación o Divulgación de datos, pérdida de tiempo, y productividad	Ingreso de virus vulnerando el sistema	destrucción	B	A

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
SERVIDORES	**COD**	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
	SE1	Acceso no autorizado a datos	Robo, modificación de información	Usuario accede a la información contenida en el servidor sin contar con los permisos necesarios	Develación	A	A
	SE2	Acceso no autorizado a equipos	Robo, modificación de información	Usuario accede al servidor sin contar con los permisos necesarios	Develación	M	A
	SE3	Corte de luz, UPS descargado o variaciones de voltaje	Falta de sistema	El suministro eléctrico sufre frecuentes interrupciones	Interrupción	A	A
	SE4	Destrucción o mal funcionamiento de un componente	Pérdida de tiempo por necesidad de reemplazo	Falla del servidor de directorio	Interrupción	M	A
	SE5	Error de configuración y operación	Aumento de Vulnerabilidades e inestabilidad en el sistema	Controladores de disco mal instalados	Interrupción	B	B
	SE6	Factores ambientales	Falta de sistema y destrucción de equipos	Equipo expuesto a un ambiente con un índice de humedad alto	Destrucción	M	A
	SE7	Límite de vida útil - Máquinas obsoletas	Deterioro en la performance del sistema	Servidores adquiridos con una antigüedad superior a 5 años	Interrupción	M	A
	SE8	Mal mantenimiento	Interrupciones en el funcionamiento del sistema	Condiciones de conservación y mantenimiento de los servidores inadecuadas	Interrupción	M	M
	SE9	Modificación no autorizada de datos	Inconsistencia de datos, mala configuración, fraude	Usuario registrando datos indebidos	Modificación	M	M
	SE10	Robo	Pérdida de equipamiento o información	Sustracción de servidores	Pérdida	M	A
	SE11	Spoofing y sniffing	Divulgación, modificación y robo de información	Usuario malicioso conectado usando programas de intercepción	Develación	B	M
	SE12	Virus, gusanos y caballos de Troya	Fallas generales del sistema y en la red	Un virus se ha introducido en el servidor	Destrucción	B	A

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
SISTEMA DE CORREO	**COD**	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
	SC1	Cuentas de correo activas de ex - usuarios	Uso indebido del servicio	No se eliminan las cuentas de alumnos egresados o personal que deja de laborar	Develación	M	B
	SC2	Errores en las funciones de encriptación	Divulgación de información (contraseñas)	Información fácil de decodificar	Develación	B	M
	SC3	Falta de autenticación	Exposición de información	Configuración automática de los clientes de correo	Develación	B	M
	SC4	Mal uso del servicio de correo	Disminución de la performance del ancho de banda	Envío de correo no deseado	No aplicable	B	B
	SC5	Mala integridad de los datos	Inconsistencia de información	Clientes de correo dañados	No aplicable	B	B
	SC6	Perdida de confidencialidad en datos privados y de sistema	Divulgación de información	Dejar abierta la sesión al momento de ausentarse	No aplicable	B	B
	SC7	Perdida de datos en tránsito	Pérdida de información	Falla de equipos intermedios	No aplicable	B	B
	SC8	Sabotaje	Pérdida del servicio	Conflicto IP al servidor de correo	No aplicable	B	B
	SC9	Spoofing y sniffing	Divulgación, modificación y robo de información	Usuario malicioso conectado Usando programas de intercepción	No aplicable	B	B

	SC10	Virus, gusanos y caballos de Troya	Pérdida, modificación o Divulgación de datos, pérdida de tiempo, y productividad	Un virus se ha introducido en los buzones de los usuarios	No aplicable	B	B

ACTIVO					**CLASE DE AMENAZA**	**PROBAB. DE OCURRENCIA**	**IMPACTO**
SISTEMA DE ALMACENAMIENTO (SAN)	**COD**	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
	SA1	Acceso no autorizado a equipos	Robo, modificación de información	Usuario accede a la SAN sin Contar con los permisos necesarios	Modificación	M	M
	SA2	Administración impropia del sistema	Modificación de datos, perdida de la configuración	Acción negligente del sistema de administración de la SAN	Develación	M	M
	SA3	Condiciones de trabajo adversas	Pérdida de datos, deterioro del equipo	Falta de un ambiente Refrigerado y con voltaje regulado	Pérdida	B	M
	SA4	Daño de cables inadvertido	Pérdida e interrupción de datos	Tendido de fibra entre los servidores y la SAN sin seguridad y de fácil acceso	Interrupción	B	M
	SA5	Falla en la SAN	Pérdida de información, paralización del servicio	Mal funcionamiento de los discos de canal de fibra	Interrupción	B	A
	SA6	Falla en medios externos	Pérdida de datos en medios externos	Deterioro del medio de almacenamiento	Pérdida	M	A
	SA7	Mala integridad de los datos	Inconsistencia de información	Falla en el sistema de Redundancia	Modificación	B	M
	SA8	Mantenimiento inadecuado o ausente	Perdida o deterioro de datos	Reducción de la vida útil del equipo sin un debido mantenimiento	Pérdida	A	A
	SA9	Medios de datos no están disponibles cuando son necesarios	Pérdida de tiempo y productividad por falta de datos	Caída de medios de almacenamiento	Pérdida	A	A
	SA10	Sabotaje	Pérdida o robo de información	Acceso indebido al sistema de administración	Pérdida	B	A

ACTIVO					**CLASE DE AMENAZA**	**PROBAB. DE OCURRENCIA**	**IMPACTO**
CENTRAL DE TELEFONÍA IP Y TELÉFONOS IP	**COD**	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
	CT1	Acceso no autorizado a equipos	Robo, modificación de información	usuario accede a la central sin contar con los permisos necesarios	Modificación	B	M
	CT2	Administración impropia del sistema	Modificación de datos, perdida de la configuración	Acción negligente sobre la central telefónica	Modificación	B	B
	CT3	Ancho de banda insuficiente	Interrupción del servicio	Medios de transmisión Saturados por aplicaciones multimedia	Interrupción	B	M
	CT4	Conexiones de cables inadmisible	Interrupción del servicio	Uso de cables deteriorados u obsoletos	Interrupción	B	M
	CT5	Conservación deficiente	Interrupción del servicio	Uso de equipo sin un mínimo cuidado de conservación	Destrucción	B	M
	CT6	Factores ambientales	Interrupción del servicio	Exceso de humedad, exposición directa al sol	Destrucción	B	M
	CT7	Interferencia	Perdida del servicio	Interferencia electromagnética	Interrupción	B	M
	CT8	Mantenimiento inadecuado o ausente	Perdida o deterioro de Equipos	Reducción de la vida útil del Equipo sin un debido mantenimiento	Destrucción	B	M
	CT9	Sabotaje	Interrupción del servicio	Daño físico a los equipos	Destrucción	B	M

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
COPIAS DE RESPALDO	COD	FACTORES DE RIESGO	CONSECUENCIA	DESCRIPCIÓN			
	CR1	Accesos no autorizados al medio de almacenamiento	Perdida, alteración o revelación de información	Usuario accede a las copias de respaldo sin contar con los permisos necesarios para ello	Develación	A	A
	CR2	Clasificación deficiente de medios	Pérdida de medios de almacenamiento o retrasos en su restauración	Mala gestión del mantenimiento de las copias de respaldo	Pérdida	A	A
	CR3	Conservación deficiente	Problemas en la restauración de la información	Medidas deficientes para el almacenamiento y conservación de medios	Pérdida	A	A
	CR4	Copia no autorizada de un medio de datos	Robo de información	Copias desde CDs, DVDs y/o cintas	Develación	A	M
	CR5	Errores de respaldo	Problemas en la restauración de información	El proceso de realización de Copias de respaldo sufre errores frecuentes	Pérdida	A	A
	CR6	Falla en medios externos	Pérdida de datos en medios externos	Cartuchos para respaldo defectuosos	Pérdida	A	A
	CR7	Fallos en la disponibilidad de medios	Pérdida de medios de almacenamiento o retrasos en su restauración	Problemas para la obtención de copias de respaldo cuando son necesarias	Interrupción	A	A
	CR8	Pérdida de medios	Imposibilidad de restauración de información	Imposibilidad de encontrar un medio de almacenamiento	Pérdida	M	A
	CR9	Robo	Pérdida de información, Imposibilidad de restauración	Sustracción de copias de respaldo	Pérdida	M	A
	CR10	Sabotaje	Pérdida o robo de información	Daño físico a los cartuchos de respaldo	Destrucción	M	A

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
EQUIPOS DE COMUNICACIÓN (ROUTERS, WITCHES, BS, ETC)	COD	FACTORES DE RIESGO	CONSECUENCIA	DESCRIPCIÓN			
	EC1	Abuso de puertos para el mantenimiento remoto	Posibles intrusiones y robo o divulgación de información	Puerto de administración vulnerable	Develación	M	A
	EC2	Ancho de banda insuficiente	Ralentización de la transmisión de información	El ancho de banda empleado para las transmisiones es inferior al adecuado	Interrupción	A	M
	EC3	Configuración inadecuada de componentes de red	Errores de transmisión, interrupción del servicio de red	Utilización de configuraciones básicas	Interrupción	M	M
	EC4	Corte de luz, UPS descargado o variaciones de voltaje	Interrupción de las transmisiones	El suministro eléctrico sufre frecuentes interrupciones	Interrupción	A	M
	EC5	Denegación de servicio	Interrupción de todos o algunos de los servicios de red	Saturación de acceso a un servicio	Interrupción	M	M
	EC6	Errores de operación	Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades	Falta de experiencia en la operación del equipo	Interrupción	A	M
	EC7	Falta de autenticación	Posibles intrusiones y robo o divulgación de información	Inapropiado nivel de seguridad	Develación	M	A
	EC8	Límite de vida útil – Máquinas obsoletas	Uso deficiente del sistema	Los componentes de transmisión no son los idóneos para una transmisión óptima	Pérdida	M	M

	EC9	Mantenimiento deficiente	Errores de transmisión, mal funcionamiento de la red	Mantenimiento inadecuado de Los componentes de transmisión	Interrupción	A	M
	EC10	Modificación de paquetes	Alteración de la información	Hacker en la red	Modificación	B	A
	EC11	Penetración, intercepción o manipulación del medio de transporte	Robo de información	Acceso indebido al cableado estructurado o a los equipos de comunicación	Develación	M	M
	EC12	Perdida de datos en tránsito	Divulgación de información	Intercepción de señales microondas	Develación	B	B
	EC13	Robo	Interrupción de la transmisión, gastos de reposición	Sustracción de equipos de transmisión	Pérdida	M	A
	EC14	Sabotaje	Red inaccesible	Interrupción del medio de transmisión	Interrupción	M	A
	EC15	Sincronización de tiempo inadecuada	Inconsistencia en datos	Utilización de configuración por defecto	Interrupción	M	M
	EC16	Spoofing y sniffing	Divulgación, modificación y robo de información	Usuario malicioso conectado Usando programas de intercepción	Develación	B	M
	EC17	Velocidad de transmisión insuficiente	Ralentización de la transmisión de información	La velocidad empleada para las transmisiones es inferior a la adecuada, exceso de usuarios	Interrupción	B	M

ACTIVO					**CLASE DE AMENAZA**	**PROBAB. DE OCURRENCIA**	**IMPACTO**
EQUIPOS DE SEGURIDAD	**COD**	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
	EQ1	Acceso no autorizado a equipos	Robo, modificación de información	Usuario accede al equipo de seguridad sin contar con los permisos necesarios	Modificación	B	A
	EQ2	Administración impropia del sistema	Modificación de datos, perdida de la configuración	Acción negligente sobre el equipo de seguridad	Modificación	B	A
	EQ3	Complejidad de las configuraciones	Administración más laboriosa	Configuraciones largas que causan lentitud en el equipo de seguridad	Interrupción	B	M
	EQ4	Modificación de paquetes	Alteración de la información	Equipo en deterioro o falto de mantenimiento	Modificación	B	M
	EQ5	Sabotaje	Pérdida o robo de información	Modificación de la configuración de seguridad	Interrupción	B	M

ACTIVO					**CLASE DE AMENAZA**	**PROBAB. DE OCURRENCIA**	**IMPACTO**
CABLEADO DE FIBRA ÓPTICA Y PAR TRENZADO (UTP)	**COD**	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
	CB1	Abuso de puertos para el mantenimiento remoto	Posibles intrusiones y robo o divulgación de información	Falta de protección a los medios de transmisión	Develación	M	M
	CB2	Ancho de banda insuficiente	Transmisión pesada en la Red o imposibilidad de utilizar el sistema en línea	Incremento del uso de servicios multimedia	Interrupción	M	M
	CB3	Ausencia o falta de segmentación	Tramos de red extensos y Dificultades en la comunicación	Falta el tendido de red en ubicaciones de difícil acceso	Interrupción	B	M
	CB4	Complejidad en el diseño de las redes de sistemas de TI	Dificultad en la Administración y en el mantenimiento	Tamaño de la red y variedad de topología	Interrupción	B	M
	CB5	Conexión de cables inadmisible	Robo de datos, spoofing y sniffing	Cableado que no va de acuerdo con el estándar	Interrupción	B	B
	CB6	Conexiones todavía activas	Intrusión de usuarios no autorizados al sistema	Puntos de red activos en ubicaciones de poca actividad	Develación	B	M

	CB7	Daño o destrucción de cables o equipamiento inadvertido	Pinchaduras de cables, robo de datos, spoofing y sniffing	Descuido en obras civiles	Pérdida	B	M
	CB8	Factores ambientales	Interferencias o daños de equipamiento	Medio de transmisión expuesto a un ambiente sin protección	Interrupción	B	M
	CB9	Falla en la SAN	Una o más servidores incomunicados	Deterioro de la fibra óptica	Interrupción	B	M
	CB10	Interferencias	Errores en los datos de transmisión o imposibilidad de utilizar los servicios en línea	Fuentes electromagnéticas en La ruta del cableado estructurado	Interrupción	B	M
	CB11	Límite de vida útil del cableado estructurado	Cableado obsoleto y deterioro de la comunicación	Cableado estructurado con una antigüedad superior a 5 años	Interrupción	M	M
	CB12	Longitud de los cables de red excedida	Transmisión lenta o con interferencias, o imposibilidad de utilizar los servicios de red	Cableado que no va de acuerdo con el estándar	Interrupción	B	M
	CB13	Mal mantenimiento	Errores de transmisión o interrupción del servicio de red	Mantenimiento realizado por un personal principiante	Interrupción	B	M
	CB14	Penetración, intercepción o manipulación del medio de transporte	Robo de información	Realización de conexiones clandestinas	Develación	M	M
	CB15	Perdida de datos en tránsito	Divulgación de información	Intercepción de señales en la red	Develación	B	M
	CB16	Reducción de velocidad de transmisión	Pérdida de tiempo de los usuarios, o imposibilidad de utilizar los servicios de red	Incremento de usuarios conectados a la red	Interrupción	M	B
	CB17	Riesgo por el personal de limpieza o personal externo	Daño en cables o equipos, interrupción del servicio	Ignorancia sobre sistemas de información por el personal de limpieza	Interrupción	B	M
	CB18	Sabotaje	Pérdida o robo de información	Destrucción del cableado estructurado	Pérdida	B	A
	CB19	Transporte inseguro de archivos	Divulgación de información	Falta de encriptación de la información	Develación	B	M

ACTIVO					**CLASE DE AMENAZA**	**PROBAB. DE OCURRENCIA**	**IMPACTO**
CÓDIGO FUENTE DE LAS APLICACIONES	**COD**	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
	CF1	Acceso no autorizado a datos (borrado, modificación, etc.)	Modificación del software en desarrollo	Acceso no autorizado al área de desarrollo	Modificación	B	A
	CF2	Aplicaciones obsoletas	Disminución de productividad, mayor sensibilidad a vulnerabilidades	Las aplicaciones empleadas no Están actualizadas para aprovechar todo su potencial	Develación	B	B
	CF3	Aplicaciones sin licencia	Multas y problemas con Software Legal	No contar con software debidamente licenciado para el desarrollo de aplicaciones	Interrupción	M	M
	CF4	Conocimiento insuficiente de Los documentos de requerimientos en el desarrollo	Sistema inestable y excesivo pedido de cambios	Mala definición de requerimientos	Interrupción	B	M
	CF5	Error de configuración y operación	Mal funcionamiento de los sistemas	Mala definición de variables en las aplicaciones	Interrupción	B	M
	CF6	Errores en las funciones de encriptación	Problemas en la recuperación de archivos encriptados o divulgación de información	No se toma en cuenta las medidas de seguridad en el desarrollo de aplicaciones	Pérdida	B	A
	CF7	Falla del sistema	Falta de sistema y posibles demoras	Falta de documentación completa de toda la	Interrupción	M	M
	CF8	Falta de compatibilidad	Datos erróneos e inestabilidad del sistema	Uso de diferentes versiones de software de desarrollo	Interrupción	M	M

	CF9	Falta de confidencialidad	Divulgación de información	Divulgación de información fuera del área de desarrollo	Develación	M	M
	CF10	Mala administración de control de acceso (salteo del login, etc.)	Divulgación y modificación de información	Toma de privilegios indebidos de acceso a la aplicación	Develación	B	M
	CF11	Pérdida de código fuente	Divulgación de información	Deterioro del medio de almacenamiento	Develación	B	M
	CF12	Poca adaptación a cambios del sistema	Sistema inestable y de difícil modificación	Cambio en los requerimientos de la aplicación	Interrupción	M	M
	CF13	Prueba de software deficiente	Sistema poco confiable	No se cuenta con un entorno de pruebas previas a la puesta en producción	Interrupción	B	M
	CF14	Software desactualizado	Probabilidad incremental de vulnerabilidades y virus	Software defectuoso explotado	Interrupción	B	M
	CF15	Virus, gusanos y caballos de Troya	Inestabilidad y mal funcionamiento de sistemas	Modificación de los archivos en desarrollo por código malicioso	Interrupción	B	A

ACTIVO					**CLASE DE AMENAZA**	**PROBAB. DE OCURRENCIA**	**IMPACTO**
EQUIPO DE RESPALDO (BACKUPS)	**COD**	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
	ER1	Conservación deficiente	Pérdida de información, Imposibilidad de restauración	Medidas inadecuadas para la conservación de medios de almacenamiento			
	ER2	Copia no autorizada a un medio de datos	Robo de información	Copias desde CDs, DVDs y/o cintas			
	ER3	Errores de software	Error en la generación o en la copia de respaldo a medios externos	El proceso de realización de Copias de respaldo sufre errores frecuentes			
	ER4	Falla en medios externos	Pérdida de copias de respaldo	Mala gestión del mantenimiento de las copias de respaldo			
	ER5	Falta de espacio de almacenamiento	Falla en la generación de copias de respaldo	Saturación de los cartuchos de respaldo			
	ER6	Mala configuración de la programación de las copias de respaldo	Falta de copias de respaldo de datos	Proceso de backup en horas de producción			
	ER7	Mala integridad de los datos resguardados	Errores durante la restauración de datos	Falla en el hardware del equipo de respaldo			
	ER8	Medios de datos no están disponibles cuando son necesarios	Pérdida de copias de Respaldo y retraso del sistema	Problemas para la obtención de copias de respaldo cuando son necesarias			
	ER9	Pérdida de copias de respaldo	Falta de datos, incapacidad de restaurarlos y divulgación de información	Imposibilidad de encontrar un medio de almacenamiento			
	ER10	Robo	Incapacidad de restaurarlos y divulgación de información	Sustracción del equipo de respaldo			
	ER11	Rótulos inadecuados en los medios de datos	Errores durante la restauración de datos	Descripción de los cartuchos ineficientemente			
	ER12	Sabotaje	Pérdida o robo de información	Destrucción del equipo de respaldo			
	ER13	Spoofing y sniffing	Divulgación, modificación y robo de información	Usuario malicioso conectado usando programas de intercepción			
	ER14	Virus, gusanos y caballos de Troya	Pérdida de datos de copias de respaldo	Un virus se ha almacenado en el medio de respaldo junto con los datos			

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
ADMINISTRADOR DE TI	COD	FACTORES DE RIESGO	CONSECUENCIA	DESCRIPCIÓN			
	AT1	Administración impropia del Sistema de IT (responsabilidades y roles del personal de sistemas)	Asignación de responsabilidades impropia	No contar con el Cuadro de Asignación de Personal - CAP ni el Manual de Operaciones y Funciones - MOF	Develación	B	B
	AT2	Almacenamiento de contraseñas negligente	Divulgación de contraseñas y uso indebido de derechos de usuarios	Guardar las contraseñas en post-it	Develación	A	A
	AT3	Configuración impropia del Postfix	Divulgación de mensajes, uso del servidor para enviar SPAM, fallas en la administración de cuotas de discos	Personal no capacitado	Develación	B	M
	AT4	Errores de configuración y operación del sistema	Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades	Personal no capacitado	Interrupción	B	M
	AT5	Falta de auditorías en sistemas informáticos	Imposibilidad del seguimiento de usuarios y de la generación de reportes	Limitación de tiempo y falta de aplicaciones para auditar	Interrupción	A	M
	AT6	Mala evaluación de datos de auditoría	No se analizan los logs y por lo tanto no hay evaluación de los resultados	Limitación de tiempo y falta de aplicaciones para auditar	Interrupción	A	M
	AT7	Mal uso de derechos de administrador	Mala distribución de los permisos y de las cuentas de administrador	Delegación de funciones de forma indebida	Modificación	A	A
	AT8	Uso de derechos sin autorización	Robo de información	Acceso al sistema fuera del horario de trabajo	Develación	A	A
	AT9	Uso impropio del sistema de IT	Administración deficiente	Abuso de privilegios por el personal de TI	Modificación	A	A

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
USUARIOS	COD	FACTORES DE RIESGO	CONSECUENCIA	DESCRIPCIÓN			
	US1	Acceso no autorizado a datos	Divulgación o robo de información	Un usuario accede a datos a los cuales no está autorizado	Develación	B	A
	US2	Borrado, modificación o revelación desautorizada o inadvertida de información	Inconsistencia de datos o datos faltantes	Un usuario provoca una pérdida o alteración de los datos existentes	Pérdida	B	A
	US3	Condiciones de trabajo adversas	Predisposición a distracción, bajo rendimiento de usuarios	El espacio de trabajo no reúne las debidas condiciones para un desarrollo óptimo de las actividades	Interrupción	M	M
	US4	Destrucción de un componente de hardware	Pérdida de tiempo por necesidad de reemplazo	Uso inapropiado de un equipo	Destrucción	B	M

	US5	Destrucción negligente de datos	Pérdida de información	Alteración de datos por desconocimiento o negligencia	Pérdida	B	M
	US6	Desvinculación del personal	Robo o modificación de información, sabotaje interno	Los procedimientos asociados a la baja de un empleado no son los adecuados	Develación	M	M
	US7	Documentación deficiente	Mayor probabilidad de Errores por falta de instrucciones	Los procedimientos de trabajo no se encuentran debidamente detallados	Interrupción	M	B
	US8	Entrada sin autorización a los ambientes	Robo de equipos o insumos, divulgación de datos	Falta de control en el acceso de personas externas	Develación	A	A
	US9	Entrenamiento de usuarios inadecuado	Predisposición a errores y bajo rendimiento de usuarios	La formación y entrenamiento del personal no es el adecuado	Interrupción	M	M
	US10	Errores en el control de permisos y privilegios	Robo de información	El control de permisos y privilegios no es llevado con el debido rigor	Develación	M	A
	US11	Falta de auditorías	Predisposición a un rendimiento deficiente y falta de concienciación sobre responsabilidades y seguridad	No se cuenta con una medida del rendimiento del uso del sistema	Interrupción	A	M
	US12	Falta de cuidado en el manejo de la información (Ej. Contraseña)	Divulgación de datos	Contraseñas en post-it	Develación	A	A
	US13	Ingeniería social – Ingeniería social inversa	Robo o modificación de información	Un usuario divulga datos confidenciales a personas no autorizadas	Develación	M	A
	US14	Mal uso de derechos de Administrador (sesiones abiertas)	Divulgación o robo de información, sabotaje interno	Violación a la privacidad de los usuarios y alteración de	Develación	M	A
	US15	No-cumplimiento con las medidas de seguridad del sistema	Medidas correctivas tomadas por la gerencia, según la gravedad del incidente	Fácil acceso a hacker's a la violación del sistema	Modificación	M	A
	US16	Pérdida de confidencialidad o integridad de datos como resultado de un error humano	Error en la información	Trabajar más de las horas debidas, problemas ajenos a la institución	Modificación	B	A
	US17	Problemas en el acceso físico a equipos	Respuesta tardía a evento	Un usuario tiene dificultades para acceder a su puesto de trabajo	Interrupción	M	A
	US18	Uso descontrolado de recursos	Retraso en las actividades o falta de sistema	Malversación de recursos informáticos	Interrupción	B	M

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
HARDWARE	COD	FACTORES DE RIESGO	CONSECUENCIA	DESCRIPCIÓN			
	HD1	Corte de luz, UPS descargado o variaciones de voltaje	Interrupción del funcionamiento de equipos	El suministro eléctrico sufre frecuentes interrupciones	Interrupción	M	M
	HD2	Destrucción o mal Funcionamiento de un componente	Interrupción de la tarea del usuario	Frecuentes errores en el desempeño de un equipo	Destrucción	A	A
	HD3	Errores de funcionamiento	Interrupción/problemas en el funcionamiento del sistema	Frecuentes errores en el desempeño de un equipo	Interrupción	M	M
	HD4	Factores ambientales	Destrucción o avería de equipos	Hardware expuesto al medio ambiente sin protección	Destrucción	A	A
	HD5	Límite de vida útil	Avería de equipos	Equipos existentes demasiado Anticuados para un funcionamiento óptimo	Interrupción	A	A
	HD6	Mal mantenimiento	Avería de equipos e incremento en el costo de equipamiento de respaldo	El mantenimiento llevado a cabo sobre los elementos hardware no es el adecuado	Interrupción	A	M
	HD7	Robo	Pérdida de equipamiento e interrupción de la tarea del usuario	Sustracción de equipos de hardware	Pérdida	B	A

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
INSUMOS	COD	FACTORES DE RIESGO	CONSECUENCIA	DESCRIPCIÓN			
	IN1	Factores ambientales	Destrucción de insumos	Insumos expuestos al medio ambiente sin protección	Destrucción	B	M
	IN2	Límite de vida útil	Destrucción o avería de los insumos	La caducidad o periodo de uso correcto de insumos no está debidamente controlado	Destrucción	B	M
	IN3	Mala disponibilidad	Ralentización de las actividades	Los insumos no se encuentran disponibles cuando son necesarios	Interrupción	M	M
	IN4	Malas condiciones de conservación	Destrucción o avería de los insumos	Las medidas de conservación de los insumos no son las adecuadas	Interrupción	B	M
	IN5	Recursos escasos (recorte presupuestal)	Interrupción en el funcionamiento normal del sistema	Falta de presupuesto para la compra de insumos	Interrupción	M	M
	IN6	Uso descontrolado de recursos	Incremento no justificado del gasto de insumos	El uso que se hace de los insumos no es el idóneo	Interrupción	B	B
	IN7	Robo	Pérdida de insumos e incremento en el gasto	Sustracción de insumos	Pérdida	B	M
	IN8	Transporte inseguro de insumos	Pérdida de insumos, e incremento en el gasto	Perdida o sustracción de insumos durante el transporte	Interrupción	B	B

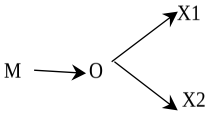
ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
	COD	**FACTORES DE RIESGO**	**CONSECUENCIA**	**DESCRIPCIÓN**			
DOCUMENTACIÓN	**DO1**	Acceso no autorizado a datos de documentación	Divulgación, robo o modificación de información	Un usuario accede a la Documentación sin estar autorizado para ello	Develación	B	M
	DO2	Borrado o modificación desautorizada de información	Documentación incorrecta	Información sensible a un nivel bajo de seguridad	Modificación	B	M
	DO3	Rebuscar información	Divulgación de información	Datos compartidos con bajo nivel de seguridad	Develación	B	M
	DO4	Copia no autorizada de un medio de datos	Divulgación de información	Usuario que realiza una copia de información confidencial	Develación	M	M
	DO5	Descripción de archivos Inadecuada	Documentación incorrecta	La clasificación empleada para el almacenamiento de documentación no es la idónea	Interrupción	B	M
	DO6	Destrucción negligente de datos	Documentación incorrecta	Ignorancia o negligencia del usuario	Destrucción	B	M
	DO7	Documentación insuficiente o faltante, funciones no documentadas	Entorpecimiento de la administración y uso del sistema	La documentación existente es escasa en relación a las aplicaciones y equipos existentes	Interrupción	M	M
	DO8	Factores ambientales	Destrucción de datos	Documentos expuestos al medio ambiente sin protección	Develación	B	B
	DO9	Fallos de disponibilidad (Falta De organización de la documentación)	Ralentización y problemas en el mantenimiento del sistema	Problemas para encontrar la documentación que es precisa en un momento dado	Interrupción	B	M
	DO10	Mala interpretación	Entorpecimiento de la administración y uso del sistema	Falta de claridad en la redacción de los documentos	Interrupción	B	B
	DO11	Malas condiciones de conservación	Pérdida de información	Las medidas de conservación y Preservación de la documentación no son las adecuadas	Pérdida	B	M
	DO12	Mantenimiento inadecuado o ausente (falta de actualización)	Documentación incorrecta, redundante y compleja	No se tiene actualizada la documentación	Interrupción	B	M
	DO13	Medios de datos no están Disponibles cuando son necesarios	Entorpecimiento de la administración y uso del sistema	Documentación no está de fácil acceso al personal encargado	Interrupción	B	B
	DO14	Robo	Divulgación de información	La documentación ha sido sustraída	Develación	B	B
	DO15	Uso sin autorización	Divulgación, robo o modificación de Información	Exposición de documentación confidencial	Develación	B	M
	DO16	Virus, gusanos y caballos de Troya	Pérdida, modificación o Divulgación de datos, pérdida de tiempo, y productividad	Documentación almacenada en formato digital en un medio con alta probabilidad de acción de códigos maliciosos	Pérdida	B	B

ACTIVO					CLASE DE AMENAZA	PROBAB. DE OCURRENCIA	IMPACTO
DATOS DEL USUARIO	COD	FACTORES DE RIESGO	CONSECUENCIA	DESCRIPCIÓN			
	DU1	Falta de espacio de almacenamiento	Retraso de las actividades	El espacio de que disponen los usuarios para su trabajo cotidiano es insuficiente	Interrupción	M	M
	DU2	Mala configuración de la programación de las copias de respaldo	Pérdida de datos del usuario	Realizar copias durante las horas en producción	Interrupción	M	A
	DU3	Mala gestión de recursos compartidos	Revelación, pérdida o modificación de información	La gestión de la compartición de datos por parte de los usuarios no es la adecuada	Develación	M	M
	DU4	Medios de datos no están Disponibles cuando son necesarios	Retraso en las actividades	Medios de almacenamiento caros o de difícil adquisición	Interrupción	A	A
	DU5	Pérdida de copias de respaldo	Pérdida de datos del usuario y retraso de la tarea	Pérdida del medio de almacenamiento o deterioro de ella	Pérdida	A	A
	DU6	Perdida de confidencialidad en datos privados y de sistema	Divulgación de información	Un usuario accede a datos a los que no está autorizado	Develación	M	A
	DU7	Portapapeles, impresoras o directorios compartidos	Divulgación de información	Bajo nivel de seguridad en los recursos compartidos	Develación	M	M
	DU8	Robo	Divulgación de información.	Sustracción de los datos de un usuario	Develación	M	A
	DU9	Sabotaje	Pérdida, modificación o divulgación de datos	Acción maliciosa sobre la información de los usuarios	Develación	M	M
	DU10	Spoofing y sniffing	Divulgación, modificación y robo de información	Un intruso accede a los datos de un usuario	Develación	M	A
	DU11	Virus	Pérdida, modificación o Divulgación de datos, pérdida de tiempo y productividad	Un virus se introduce en el equipo del usuario, afectando a los datos que contiene	Destrucción	B	M

Anexo 2. Matriz de consistencia de la investigación

MATRIZ DE CONSISTENCIA

TITULO: **Seguridad informática en la plataforma virtual del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno - 2019**

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIÓN	INDICADORES	TIPO Y DISEÑO DE INVESTIGACIÓN	POBLACIÓN Y MUESTRA	TÉCNICAS	INSTRUMENTOS
Definición General ¿Cuál es el nivel de Seguridad informática en la plataforma virtual del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno? **Definición Específica** ¿Cuáles son las amenazas que pueden ocurrir a los activos principales de la plataforma virtual del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno? ¿Cuál es el nivel de impacto de daño a la plataforma virtual del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno?	**Objetivo General** Analizar el nivel riesgo de seguridad informática en la plataforma virtual del vicerrectorado de investigación de la Universidad Nacional del Altiplano de Puno **Objetivos Específicos** Determinar la ocurrencia de amenaza a los activos principales de la plataforma virtual del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno. Determinar el nivel de impacto de daño a la plataforma virtual del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno.	**Hipótesis General** Existe probabilidad de riesgo de seguridad informática en la plataforma virtual del vicerrectorado de investigación de la Universidad Nacional del Altiplano de Puno es alta **Hipótesis Específicos** Existe probabilidad de ocurrencia de amenaza a los activos principales de la plataforma virtual del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno Existe impacto de daño a la plataforma virtual del Vicerrectorado de Investigación de la Universidad Nacional del Altiplano de Puno.	Variable 1 (Seguridad informática)	Disponibilidad Confidencialidad Integridad	Interrupción Destrucción Eliminación Develación Eliminación Modificación	**ENFOQUE** Cuantitativo **TIPO DE INVESTIGACIÓN** No Experimental (descriptivo) **DISEÑO DE INVESTIGACIÓN** Transeccional exploratorio **DIAGRAMA DEL DISEÑO DE INVESTIGACIÓN**  **M** = muestra **X1** = ocurrencia de amenaza en **x** X1 = el impacto de daño en **x** **O** = observación de la variable	MUESTRA Procesamiento de información de la plataforma VRI Pilar de la una puno	Observación sistemática	Test

Universidad Nacional del Altiplano Puno | Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo Edson Denis Zanabria Ticona,
identificado con DNI 45899134 en mi condición de egresado de:

☐ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☒ **Programa de Maestría o Doctorado**

Maestría en informática con mención en gerencia de tecnologías de información y comunicaciones,
informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
"SEGURIDAD INFORMÁTICA EN LA PLATAFORMA VIRTUAL DEL VICERRECTORADO DE INVESTIGACIÓN DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO DE PUNO - 2019"

Es un tema original.

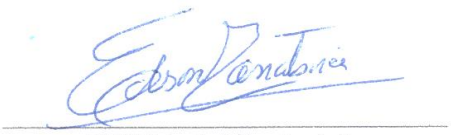
Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 18 de diciembre del 20 23



FIRMA (obligatoria)

Huella

Universidad Nacional del Altiplano Puno | Vicerrectorado de Investigación | Repositorio Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo Edson Denis Zanabria Ticona,
identificado con DNI 45899134 en mi condición de egresado de:

☐ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☒ **Programa de Maestría o Doctorado**

Maestría en informática con mención en gerencia de tecnologías de información y comunicaciones,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:

"SEGURIDAD INFORMÁTICA EN LA PLATAFORMA VIRTUAL DEL VICERRECTORADO DE INVESTIGACIÓN DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO DE PUNO - 2019"

para la obtención de ☒**Grado,** ☐ **Título Profesional** o ☐ **Segunda Especialidad.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno 18 de diciembre del 2023

FIRMA (obligatoria)

Huella