ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Newman
Escuela de Posgrado

Propuesta de mejora de la seguridad de la red LAN del Gobierno Regional de Apurímac mediante Hacking Ético

Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autor:
Bach. Hurtado Rayme, Anthony Stalin

Docente Guía:
Mtro. Espinoza Villalobos, Luis Enrique

TACNA – PERÚ

2022

Propuesta de mejora de la seguridad de la red LAN del Gobierno Regional de Apurímac mediante Hacking Ético

INFORME DE ORIGINALIDAD

17%	16%	2%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

DEDICATORIA

Me gustaría dedicar este proyecto de maestría a toda mi familia. Para mis padres Clotilde Rayme y Gregorio Hurtado, por su comprensión y ayuda en momentos malos y menos malos, Me han enseñado a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento. Me han dado todo lo que soy como persona, mis valores, mis principios, mi perseverancia y mi empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio.

Para mi hermano, por su comprensión, por sus consejos, por su apoyo incondicional en los malos momentos es sin duda mi referencia para el presente y para el futuro. A todos ellos, muchas gracias de todo corazón.

Anthony Stalin Hurtado Rayme

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Las instituciones públicas cada vez son más dependientes de las redes informáticas y el gobierno de Apurímac no es la excepción, pues posee una red de área local donde se ha comprobado que no se la ha sometido a ninguna técnica de “hacking ético” para detectar vulnerabilidades y esto presenta un alto nivel de riesgo para la información pues puede ser alterada y en el caso extremo robada. Evidenciada la problemática de las variables de investigación se plasmó el objetivo general, el mismo que fue plasmado en desarrollar una propuesta de mejora de la seguridad de la red LAN del Gobierno Regional de Apurímac mediante Hacking Ético.

Para el cumplimiento de los objetivos se realizó el diagnóstico respecto a parámetros de seguridad de la red, para ello se utilizó el cuestionario y con la información obtenida se plasmó estrategias de mejora mediante la matriz de mejora, luego se determinó mecanismos de control por medio de indicadores KPI que permitan para verificar el seguimiento y cumplimiento de las estrategias de mejora. Finamente se determinó cuales es el costo de implementar el plan de mejora al área de seguridad.

Con el diseño y desarrollo de la propuesta de mejora hacia la seguridad de la red LAN del Gobierno Regional de Apurímac haciendo uso de la herramienta Hacking Ético, como resultado se definió realizar una serie de pruebas que identifiquen las vulnerabilidades que presenta la red de la institución y posterior a ello se identificó cuáles son los riesgos a los que se enfrenta con el análisis correspondiente de la recopilación de información.

Palabras clave: Hacking Ético, red LAN, Gobierno Regional de Apurímac, instituciones públicas, redes informáticas, área local, vulnerabilidades.

ABSTRACT

Public institutions are increasingly dependent on computer networks and the government of Apurímac is no exception, since it has a local area network where it has been verified that it has not been subjected to any "ethical hacking" technique to detect vulnerabilities. and this presents a high level of risk for the information as it can be altered and in the extreme case stolen. Once the problem of the research variables was evidenced, the general objective was reflected, the same one that was embodied in developing a proposal to improve the security of the LAN network of the Regional Government of Apurímac through Ethical Hacking.

For the fulfillment of the objectives, the diagnosis was made regarding network security parameters, for this the questionnaire was used and with the information obtained, improvement strategies were shaped, then control mechanisms were determined by means of indicators that allow to verify monitoring and compliance with improvement strategies. Finally, the cost of implementing the improvement plan in the security area was determined.

With the design and development of the proposal for improvement towards the security of the LAN network of the regional government of Apurímac using the Ethical Hacking tool, as a result it was defined to carry out a series of tests that identify the vulnerabilities presented by the institution's network. and after that, the risks faced with the corresponding analysis of the information gathering were identified.

Keywords: Ethical Hacking, LAN network, Apurímac Regional Government, public institutions, computer networks, local area, vulnerabilities.

INTRODUCCIÓN

En la actualidad con el constante desarrollo de las tecnologías de la información estás se han convertido en aliados para las instituciones privadas y públicas ya que permite procesar datos de manera digital enfocada en los usuarios. Las instituciones en ciertas ocasiones no le dan la importancia a la seguridad informática sabiendo, que existe la probabilidad de sufrir ataques a datos privados por parte de la ciberdelincuencia por ello surge la importancia de mejorar la seguridad en la red LAN en el Gobierno Regional de Apurímac mediante Hacking Ético.

En la actualidad la información pública se preserva y protege no solo a daños en los sistemas también en contra de vulnerabilidades por su importancia para los usuarios y para el personal que maneja la información, en este sentido los primeros deben tener la seguridad y confianza que sus datos se encuentran seguros, por medio de la utilización del hacking ético se busca investigar las vulnerabilidades en los sistemas informáticos y con ello plasmar soluciones y correctivos necesarios que sean aplicados a tiempo.

El desarrollo del plan de mejora se divide en los siguientes capítulos: Capítulo I: se plantea los antecedentes donde se identifica la problemática, se plantea los objetivos, luego tenemos la justificación, unas pequeñas definiciones, técnicas de recopilación de datos, así como la Población como muestra finalizando con las limitaciones y alcances.

Capítulo II: se lo conoce como Marco Teórico donde se señala la variable y tópicos clave de la investigación que va a permitir un mayor entendimiento, luego se presenta la importancia de la variable, se realiza el análisis comparativo y crítico sobre las variables de análisis.

Capítulo III: descrito como el Marco Referencial donde exclusivamente se va a expresar sobre la institución objeto de análisis entre ellas están: una pequeña historia, cual va ser su filosofía y organigrama institucional, cuáles son los productos y servicios que ofrece la institución y el diagnostico por medio del instrumento FODA.

Capítulo IV: es el capítulo más importante denominado Resultados donde va a realizar el diagnostico, luego tenemos las estrategias para el diseño de la mejora, estableciendo mecanismos de control que permiten el buen desarrollo de la variable objeto de estudio.

Capítulo V: es el que cierra la investigación con la Sugerencias y recomendaciones en base a los resultados que se obtuvieron de acuerdo con el levantamiento de información por las encuestas realizadas al personal encargado del departamento de sistemas.

Anexos: en este apartado es donde contiene el formato de los cuestionarios realizados, tablas, libros.

CAPÍTULO I: ANTECEDENTES DE ESTUDIO

1.1 Título del tema

Propuesta de mejora de la seguridad de la red LAN del Gobierno Regional de Apurímac mediante Hacking Ético.

1.2 Planteamiento del problema

Las instituciones públicas y privadas a nivel mundial cuentan redes de área local que permiten enviar información, ya sea en grandes o pequeñas cantidades. Con la mejora continua de las Tecnologías de la Información “TIC” ha permitido a las instituciones ser parte de este progreso, pero durante los últimos años cada vez se registra un incremento de arremetidas por parte de los hackers. (Huaylla & Vargas)

En un inicio los ataques de los hackers eran benignas, en el peor de las circunstancias estos solo conseguían ralentizar los equipos, con el paso del tiempo ya podían dañar completamente los sistemas, borrar, modificar y extraer información confidencial. En intentos por proteger estos datos los administradores utilizaron medidas restringidas para el acceso a los computadores, pero esto no impidió que los Hackers realicen ataques más estructurado y destructivos. (Macías, 2021)

Las instituciones públicas cada vez son más dependientes de las redes informáticas y de existir un problema que le afecte este puede llegar a comprometer rigurosamente la continuidad en las operaciones. El gobierno de Apurímac posee una red de área local con sus servicios pertinentes a la cual no se la ha sometido a ninguna técnica de “hacking ético” para detectar vulnerabilidades.

Se ha podido evidenciar que el principal problema que presenta el Gobierno Regional de Apurímac es un sistema vulnerable con bajo nivel de identificación de vulnerabilidades que no permiten identificar los riesgos a los que están expuestos los servidores de internet con el cual trabaja la institución y esto presenta un alto nivel de riesgo para la información pues puede ser alterada y en el caso extremo robada.

Al no utilizar ningún tipo de sistema que permita identificar los riesgos o vulnerabilidades existentes en la red LAN conlleva a presentar deficiencias en la seguridad de los servidores, esto genera riesgo e inseguridad de la información que maneja la institución ya que pueden ser víctimas de ataques cibernéticos por no contar con las medidas de seguridad y políticas necesarias que prevengan la pérdida o alteraciones de la información manejada por la institución.

Por tal motivo se requiere llevar a cabo la mejora de la seguridad de la red de área local LAN mediante la aplicación del hacking ético que permita detectar vulnerabilidades en la red, esto con el objetivo de mejorar los servicios en la red de información y datos.

1.3 Objetivos

1.3.1 Objetivo general

Desarrollar una propuesta de mejora de la seguridad de la red LAN del Gobierno Regional de Apurímac mediante Hacking Ético.

1.3.2 Objetivos específicos

- Realizar el diagnóstico de la seguridad de la red LAN del Gobierno Regional de Apurímac mediante Hacking Ético.

- Diseñar estrategias de mejora de la seguridad de la red LAN del Gobierno Regional de Apurímac mediante Hacking Ético.
- Establecer mecanismos de control y seguimiento a las estrategias diseñadas de la red LAN del Gobierno Regional de Apurímac mediante Hacking Ético.
- Estimar la inversión necesaria para la aplicación de las estrategias de mejora propuestas para la red LAN del Gobierno Regional de Apurímac mediante Hacking Ético.

1.4 Metodología de la investigación

Para desarrollar efectivamente los objetivos planteados en la presente investigación se utilizara diversas técnicas e instrumentos, como por ejemplo para el desarrollo del diagnóstico se utilizará el instrumento denominado como cuestionario para la recolección de información, mismo que servirá para identificar las causas y posibles soluciones a la problemática presentada, el cuestionario se desarrollará con la elaboración de preguntas específicas y cerradas que determinen las respuestas otorgadas por los colaboradores del Gobierno Regional de Apurímac, el cuestionario será aplicado a los colaboradores del área de TIC, ya que es el personal encargado de las actividades que involucran el análisis y verificación de la red LAN.

Para el cumplimiento del segundo objetivo específico denominado como el diseño de la mejora se utilizará una matriz de oportunidades de mejora esta herramienta facilita la toma de decisiones en la elaboración de la propuesta de mejora donde se priorizará objetivos propios y las oportunidades de mejora una vez realizado el diagnostico con sus causas y efectos. Al realizar dichas actividades se podrá contar con los mejores niveles de seguridad en su red LAN.

Una vez realizada la matriz del diseño de la mejora se desarrollará el tercer objetivo específico en donde se determinan los mecanismos de control, por medio de indicadores KPI de calidad o también llamados indicadores de control que permitan comprobar los procesos de intrusión, estos se los determinará por medio de una matriz. Finalmente se resolverá el ultimo objetivo específico mismo que trata sobre el cálculo del presupuesto referencial de la implementación de las estrategias de mejora con el cual se obtendrá su costo y beneficio de la propuesta de mejora propuesta.

Brevemente se describirá la metodología de la investigación que se usará para el trabajo actual. El tipo de investigación según el autor Sampieri et al. (2006) La investigación se enmarco en el uso de conocimientos y teorías relacionados al fenómeno de estudio. Desde el enfoque se hace uso del tipo cuantitativo por la obtención de información de datos numéricos porque la problemática requiere investigación interna pues es importante mejorar la seguridad de la red LAN. Pero al mismo tiempo se usará el enfoque cualitativo por el uso de técnicas de recolección de datos como el cuestionario.

Donde el nivel de investigación será de tipo descriptiva para Sampieri et al. (2006) “busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis” (p. 92). Se la considero porque permitirá analizar la problemática planteada para el desarrollo en el presente trabajo e ir construyendo el análisis y la textualización de la investigación.

Dentro de las técnicas para recopilar información se utilizará la encuesta que para los autores Casa, Repullo, & Donado (2003) “La técnica de encuesta es ampliamente utilizada como procedimiento de investigación, ya que permite obtener y elaborar datos de modo rápido y eficaz” (p. 143), la misma se aplicará a las personas encargadas del área de TIC donde se espera recopilar información sobre los procedimientos acerca de la seguridad de la red LAN.

El instrumento será el cuestionario por su parte Bernal (2010) “Se trata de un plan formal para recabar información de la unidad de análisis objeto de estudio y centro del problema de investigación” (p. 250). El cuestionario va constar de diez preguntas cuya estructura es cerrada y se la va realizar mediante Microsoft forms.

La población a la cual se aplicará el cuestionario va a estar estructurada por la Dirección Regional de Transporte y Comunicaciones de Apurímac “DRTCA” teniendo un valor de 20 personas. La muestra va a estar determinada por las personas a cargo de la TIC el cual son 12 personas.

1.5 Justificaciones

1.5.1 Justificación teórica

Teóricamente se considerarán principios teóricos a partir de los fenómenos de la investigación, esto permitirá conocer de manera imparcial la situación real y los procesos operativos de la gestión tecnológica y los procesos de seguridad informática. Entre las bases teóricas nos apoyaremos del libro “Seguridad informática: Hacking Ético” de la asociación ACISSI, así como “Gestión de la Seguridad de la Información” de la Escuela Superior de Redes (ESR).

1.5.2 Justificación metodológica

Metodológicamente la investigación permitirá proponer información que presenta en su entorno real y los procesos de seguridad información. Esto va a permitir construir un modelo de análisis descriptivo para concientizar sobre políticas de seguridad informática. Dentro de ello nos basaremos en el ciclo Deming planificar, hacer, comprobar y actuar como metodología para la mejora continua, de acuerdo con García, Quispe, Páez (2003) en sus artículos “Mejora Continua de la calidad de los procesos” este permite realizar un estudio objetivo utilizando la estadística y gráficos que permiten tomar las decisiones adecuadas para la que el Gobierno Regional de Apurímac consiga cumplir sus objetivos y éxito.

1.5.3 Justificación práctica

La investigación se basa en la necesidad de mejorar los requerimientos de la TIC y los procesos de seguridad informática en la red LAN en el Gobierno Regional de Apurímac, por lo tanto, el tema de estudio permitirá elabora estrategias concretas para mejorar los servicios y lograr un servicio adecuado para la comunidad.

1.6 Definiciones

1.6.1 Hacking ético

Según la Universidad de la Rioja (2020) “El hacking ético es la práctica que consiste en utilizar las habilidades en sistemas informáticos y de red para ayudar a las organizaciones a probar sus mecanismos y procedimientos de seguridad con tal de identificar debilidades y/o vulnerabilidades”.

1.6.2 Seguridad en red LAN

La seguridad red es un pilar fundamental en los sistemas informáticos pues en estas se debe procurar seguir normas de seguridad al instalarlas con la finalidad de crear políticas de seguridad en las redes para evitar ataques de intrusos. Por ello es importantes considerar la seguridad física: actualizaciones de software, contraseñas, autenticación, accesos seguros. (Molinetti, 2020)

1.6.3 Red LAN

Para el autor Molinetti (2020) “es un sistema de interconexión entre ordenadores, situados a una distancia relativamente próxima, que permite compartir recursos e información. Para crearla es necesario contar con ordenadores, tarjetas de red, cables de conexión, dispositivos periféricos y el software correspondiente”.

1.6.4 Seguridad operativa

“Decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría” (Kaspersky Lab, 2022).

1.6.5 Delito informático

Según el autor García, (2017) son todas las acciones que antentan contra la integridad, confidencialidad de los datos, redes y sistemas informaticos asi como el ingreso sin autorizacion a los mencionados sistemas para dañar o robar inforamcion que se maneja cada organización, empresa o institucion.

1.7 Alcances y limitaciones

1.7.1 Alcances

El alcance se centra en definir las estrategias de mejora para el departamento de Apurímac específicamente al área de las TIC.

1.7.2 Limitaciones

- Una de las limitantes es la participación negativa de las personas del área para la aplicación de los cuestionarios.
- La disponibilidad de tiempo por pare de las personas que se encuentran a cargo del área de la seguridad informática.
- Otra limitante que se considera para el desarrollo de la presente investigación es el escaso material bibliográfico relacionado a la variable de la localidad.

CAPÍTULO II: MARCO TEÓRICO

2.1 Conceptualización de las variables de estudio

2.1.1 Redes LAN

Hoy en día permiten la interconexión entre puntos de forma segura y fácil al mismo tiempo son aquellas que permiten a los usuarios la facilidad de conectarse a una red local. De acuerdo con los autores Álvarez & Pérez (2004) las “redes Wireless Local Área Network (WLAN) permite comunicarse entre varios dispositivos sin la incidencia de cables” (p. 173), entregando de esta manera mayor libertad a los usuarios impidiendo el uso de la red por personas exteriores al sistema.

En los últimos tiempos estas se utilizan en las instituciones para que se realicen las actividades. Esta red permite la conexión entre dispositivos para el manejo y procesamiento de datos en una institución u organización, donde se puede compartir recursos entre dispositivos. Estas se encuentran conectadas a internet con todas las ventajas y desventajas una de ella es que su ubicación se la realiza en sitios específicos de poco alcance que se pueden presentar, entre las cuales se encuentra el posible ataque vulnerando la seguridad. (Rodríguez E. , 2021)

La red al permitir conectarse entre sí y ya que de ellas depende trabajar activamente con él envió de información. Al ser víctima de ataques pueden llegar a interrumpir los servicios que dependen de la red. De acuerdo con Álvarez & Pérez (2004) las amenazas periódicas en estos sistemas son:

- Robo de información.
- Interrupción de servicios.
- Manipulación de datos. (p. 174)

Dentro de la importancia que conlleva el uso de esta red permite a los trabajadores de una institución colaborar entre sí, permite compartir información entre las distintas áreas, archivos, colaborar en múltiples proyectos y enviar mensajes instantáneos por medio de correo electrónico simultáneamente. En las instituciones pequeñas existe el gran interés por usar este tipo de red pues no se necesita muchos recursos de hardware para su funcionamiento y al estar conectadas entre sí permite compartir los recursos. Estos recursos se los controla por medio de una ubicación central donde resulta fácil archivar la información y realizar copias de seguridad.

Se debe considerar que estas redes pueden estar expuestas a los ataques informáticos maliciosos si en la red existiera vulnerabilidades por lo tanto es importante tomar las respectivas medidas y estrategias adecuadas que permitan garantizar la seguridad y confiabilidad de la información.

2.1.1.1 Seguridad en redes LAN

La seguridad en redes combina varias capas de defensa en el perímetro y la red en donde cada capa de seguridad implementa controles y políticas en el cual los usuarios autorizados tienen acceso a los recursos de red mientras que a los usuarios maliciosos se bloquea con la finalidad de evitar que ataquen vulnerabilidades y amenacen la seguridad. La digitalización ha transformado el mundo, cambiando la manera de trabajar, aprender, vivir y entretenernos. Todas las instituciones que prestan servicios de acuerdo con las necesidades y exigencias de los clientes tienen la responsabilidad y necesidad de proteger su red pues permite cuidar la información personal de posibles ataques al mismo tiempo que protege la reputación de la institución. (Aranda, 2022)

Dentro de los tipos de seguridad de red, para CISCO (2022) tenemos:

Segmentación de red: Clasifica el tráfico de red y permite la aplicación de políticas de seguridad.

Firewalls: Estas son barreras de entre la red interna de confianza y la externa que no es de confianza

Seguridad del correo electrónico: Son el vector principal de amenaza para infracciones de seguridad por medio del “phishing”.

Software antivirus y antimalware: Evita que los “malware o software malicioso” ataquen la red y la infecten causando latencias en el sistema.

Control de acceso: Los usuarios no tienen acceso a la red y se debe reconocer todos los dispositivos y usuarios.

Seguridad de las aplicaciones: Cualquier software que permita operar el negocio debe contar con seguridades ya sea construida o por medio de compra.

Dentro de las amenazas más recurrentes que se presentan en las redes son el robo de información e identidad, paralización de servicios y la manipulación de datos este tipo de amenazas son la constante en las instituciones pues genera una serie de inconvenientes en las instituciones.

Las amenazas al mismo tiempo generan un alto impacto como consecuencia de los múltiples ataques que se puedan presentar, al mismo tiempo estas amenazas para las instituciones se traducen en pérdidas económicas, información perdida a corto o largo plazo ante un posible ataque. (Ortiz, 2015)

En la siguiente tabla se determina un método cualitativo que permite identificar el nivel de impacto según ciertos parámetros como: control y modificación de la información, tiempo para emplear los correctivos necesarios, acciones a realizar ante un potencial ataque cibernético.

Tabla 1

Asignación de niveles de impacto

NIVEL DE IMPACTO	DESCRIPCIÓN DEL IMPACTO
Bajo	Impacto mínimo al sistema y su corrección es fácil
Medio	El impacto es medio al sistema, pero su corrección se realiza mediante auditorias o herramientas
Alto	Pérdida del control del sistema total Pérdida de la confidencialidad e integridad de los datos, el sistema sufre ataques con mayor prisa mediante la red.

Nota: Adaptado de Open Information System Security Group, pág. 249, 2008

Dentro de las vulnerabilidades en sistemas de información son aquellas debilidades que son aprovechadas para materializar las amenazas consideradas anteriormente, estas pueden aparecer durante la configuración de la red, actualizaciones inactivas, debilidades tecnológicas y parches de seguridad en la siguiente se muestra las amenazas recurrentes:

Tabla 2

Vulnerabilidades, amenazas y riesgos de las redes inalámbricas

AMENAZA	VULNERABILIDAD	RIESGO
Recopilación de información	Contiene información de la versión y tipo del servidor.	"Adquirir información de hardware y software identificando la topología de red, equipos y servicio"
Tráfico en la red	Seguridad y autentificación física débil.	"Suplantar la identidad donde el objetivo es conseguir clave" [a]
Ataques de acceso	Des autenticar y elaborar un falso punto de acceso	"Clonar una página web autentica para lograr credenciales por medio de la captura SSID ocultos"
Secuestro de sesión	Escasez de comunicaciones cifradas	"Visualizar información confidencial de la institución mediante el spoofing" [a]
Rechazo de servicios	Configuración débil en ruteadores y switch	"Afectar la operación de internet e intranet de la institución a partir de la explotación de vulnerabilidades en servidores"

Nota: Adaptado de *Seguridad Informática,* (pág. 177), por Álvarez & Pérez (2004).

2.1.2 Hacking ético

Al hablar de hacking ético se hace referencia a las herramientas que permiten proteger y prevenir los datos de ataques. En realidad, lo que se pretende es ir un paso delante de quienes de alguna u otra forma intentan hacer ataques a una institución privada o pública por medio del uso de varias técnicas de ataque digital. (Florez, 2017)

En tal razón permite la utilización en conocimientos de seguridad informática que permita el acceso a pruebas en redes, sistemas, dispositivos electrónicos en busca de vulnerabilidades y con ellos reportarlas al personal encargado con el fin de reportarlas para que se puedan tomar las medidas correctivas sin que exista el riesgo para el sistema y demás dispositivos. (Florez, 2017)

Otra definición nos entrega el autor Rodríguez (2020) el hacking ético es el uso de habilidades para detectar en los sistemas informáticos y redes posibles vulnerabilidades y ayudar a las organizaciones a probar estos sistemas o mecanismos ante debilidades que se presenten.

El avance de la tecnología ha permitido que el mundo se mueva digitalmente prueba de ello es el internet y los hackers. Es así como el autor Medina (2020) define “Un hacker ético es la persona que usa habilidades como conocimientos en programación, redes de computadoras, instalación y mantenimiento de infraestructura basada en los sistemas operativos más conocidos y usados como lo son Unix1 y Windows NT2” (p. 3).

El denominado “hacking ético” con el paso del tiempo este tiene sus adeptos y contrincantes estos no ingresan a los sistemas informáticos con la finalidad de alterar o dañar información de las empresas al contrario su objetivo se centra en comprobar las vulnerabilidades y fallos que existan para más adelante por medio de un informe dar a conocerlos y mitigarlos a la brevedad posible. (Rodriguez, 2020)

Las ventajas de la aplicación del hacking ético son:

- Saber las diferentes vulnerabilidades de los sistemas informáticos.
- Proteger incremento de costos, inversión y tiempo por la pérdida de información.
- Mantener la confianza y ventaja empresarial de los interesados cuando este comprometida la seguridad.

Para el autor Huilca (2012) los objetivos que presenta el hacking ético son:

- Evaluar a la empresa para detectar un ataque externo o interno encaminado en fortalecer la seguridad de los sistemas de información.
- Detectar las debilidades en la infraestructura TIC.
- Proporcionar fiabilidad y protección a sistemas de información. (p. 17)

Con la finalidad de asegurar el funcionamiento y la seguridad es indispensable describir con amplios conocimientos donde estos se enfocan bajo las estrategias ante los ataques de piratas cibernéticos. Existen modos del hacking ético que en la institución la infraestructura tecnológica puede ser auditada de varios modos, para el autor Guevara (2018) son:

> Con equipo robado. – se da cuando una laptop es robada por delincuentes, considerando que estas almacenan información de correos, contraseñas o conexiones remotas esta es una vulnerabilidad clara para la empresa donde se debe considerar como esa información está protegida contra atacantes que desea acceder a la información.

> Ataque local. – se refiere a la simulación de un posible ataque de la red por parte de un empleado o hacker con privilegios para acceder al sistema y equipos de la red.
>
> Por medio de quipos sin autentificación. – es la búsqueda de accesos inalámbricos por parte del atacante para comprobar el nivel de control y seguridad al cual tienen acceso. (p. 14)

Dentro de las destrezas de un hacker ético estos deben presentar la combinación de habilidades técnicas y personales, para probar la seguridad de ahí que se debe reclutar un hacker ético confiable a pesar de que en el camino es probable que se rompan leyes que muchas de las veces generan controversia:

- **Técnicas**
  - Conocimiento de los sistemas operativos
  - Elevado conocimiento sobre seguridad
  - Excelente conocimiento sobre ataques cibernéticos
  - Experiencia en red de hardware, software, etc.

- **Personales**
  - Continuo aprendizaje
  - Comunicación adecuada
  - Alta capacidad para resolver problemas
  - Concienciación sobre cumplimientos estándares

Solo existe una tipología de actividad ética y el resto presentan intensiones que no pueden ser muy buenas intenciones o ambiguas. Entre estas están: 1) los Hacktivistas que no es más cuando un hacker puede dejar de un mensaje en la ventana principal de un sitio web. Así lo menciona el autor Sánchez (2019) “esta es la técnica mediante la cual un hacker informático está ingresando ilegalmente a cualquier sistema informático por cualquier motivo, ya sea social o político” (p. 3).

Figura 1

Grupo hacktivista

Nota: Adaptado *Hacking Ético: Impacto en la Sociedad,* (pág. 2) por Sánchez (2019)

Estos pueden mostrar algún tipo de mensaje social con la finalidad de atraer a los usuarios que se realiza mediante un ataque cibernético donde se utiliza estrategias que directamente afectan a los sitios web y demás servicios de accesibilidad como medio de protesta. (UNIR, 2021)

Tenemos los Cyber – Warrior este término tiene diferentes significados de acuerdo con el contexto que se usa, primero puede referirse a personas “el atacante” con intenciones maléficas en la información o por el contrario referirse a un profesional que desarrolla mecanismos para defenderse contra los ataques. (Sánchez, 2019)

Figura 2

Grupo Cyber-Warrior

Nota: Adaptado *Hacking Ético: Impacto en la Sociedad,* (pág. 2) por Sánchez (2019)

Hace referencia a un soldado cibernético el cual participa en una guerra cibernética, ya sea por los motivos que le induzcan a ello pudiendo ser religiosas, patrióticas o personales. Este tipo de guerra cibernética se lleva a cabo con la finalidad de defender y proteger los sistemas de información e informáticos y en el caso más extremo atacarlos para adquirir una ventaja. (Huilca, 2012)

Luego de haber considerado los tipos de pentesting sus aplicaciones, restricciones y hacking existen pruebas de penetración que las realizan personas contratadas por la empresa para ingresar a su red y sistemas informáticos, de cierto modo irrumpen legalmente en la red de computadores con el objetivo de ayudar a la empresa a explicarles sobre las debilidades y vulnerabilidades que tiene el sistema actualmente. De ahí que este tipo de pruebas se deben realizar de manera periódica según el estilo y enfoque que se aplicará (Sánchez, 2019)

De acuerdo con el autor Sánchez (2019) Estas pruebas van más allá y realiza lo siguiente:

- Considera múltiples vectores de ataque
- Busca información de la efectividad del sistema de seguridad
- Descubre vulnerabilidades y las explota. (p. 5)

Este tipo de hacker ético certificado para el autor Sánchez (2019), son todos los profesionales que se encuentran con licencia o certificados en el área de seguridad para desempeñar las funciones de hacker ético de acuerdo con pentesting de caja negra o blanca en donde su responsabilidad recae en descubrir las debilidades y vulnerabilidades.

Figura 3

Certificación CEH

Nota: Adaptado *Hacking Ético: Impacto en la Sociedad,* (pág. 2) por Sánchez (2019)

Las certificaciones son otorgadas por el "Consejo Internacional de Consultores de Comercio Electrónico", esta acredita que los profesionales proyectan de conocimientos mínimos en seguridad informática y hacker ético haciendo uso de herramientas de los atacantes, pero de forma legal. (UNIR, 2020)

2.1.2.1. Fases del hacking ético

Dentro del hacking ético existen distintas fases que se desarrollan para garantizar las pruebas en la prueba de vulnerabilidades:

Fase 1, Footprinting: Dentro de esta fase se establece la principal regla a seguir y esta consiste en definir y conocer el objetivo es decir se debe tener clara cuál es la huella identificada o Footprinting esto es comúnmente conocido como el arte de extraer la mayor información de la red que presenta vulnerabilidades y corre riesgos de ataques cibernéticos, de aquí parte la importancia de planificar y analizar adecuadamente los posibles ataques que pueda sufrir el sistema. (Veloz et al., 2017)

Objetivos del Footprinting

- Conocer de manera clara la topología de la red, así como el sistema de cableado y las direcciones IP de todos los servidores que se encuentren enlazados dentro de la institución.
- Detectar la dirección IP host donde se localiza el dominio
- Conocer cuáles son los servidores que han sido asignados de manera dinámica por medio del DHCP.
- Verificar la conectividad entre el servidor proxy y el servidor de la base de datos.

Fase 2, Scanning: El segundo paso por desarrollar es el cráneo general del sistema éste se lo realiza después de definir el objetivo que se desea alcanzar considerando que el escaneo es el análisis de las características de la red o el sistema que se desea analizar en este proceso se determinan los equipos disponibles en la organización y con los servidores que dispone se realiza el escaneo de la red y con ello se determinan los hosts activos que se encuentran en la red. (Rodríguez A. , 2020)

Objetivos del scanning:

- Identificar los hosts que se encuentren activo en la red LAN de la institución.
- Escanear y determinar puertos abiertos en: servidores proxy, base de datos, routers.
- Una vez determinado los puertos abiertos se debe pensar las posibilidades de ataques utilizando estas debilidades.
- Nivelar la versión del sistema.
- Identificar e ingresar archivos confidenciales.
- Ingresar al servidor por medio de comandos NetBIOS.

Fase 3, búsqueda de vulnerabilidades: en esta fase se realiza el análisis de las vulnerabilidades existentes en la red LAN y se consideran los resultados obtenidos en él escaneo con la verificación de puertos abiertos además se buscarán las vulnerabilidades existentes en los servidores de la base de datos de la empresa. (Rodríguez A. , 2020)

Objetivos de la búsqueda de vulnerabilidades

- Realizar el escaneo a todos los servidores y detectar vulnerabilidades.

Fase 4 penetración y acceso al sistema: posterior a la identificación de vulnerabilidades de los servidores se realiza el proceso de acceso desautorizado es decir que se aprovechan las vulnerabilidades existentes y se busca la manera de acceder a la información y servidores de la empresa vulnerando todo el sistema de seguridad. (Veloz et al., 2017)

Objetivos de la penetración y acceso al sistema

- Atacar los servidores de la empresa.
- Robo de información.
- Ataque y daño a los servidores.
- Eliminación de información confidencial.

Fase 5, borrado de huellas: esta fase consiste en eliminar todo rastro del acceso no autorizado y vulnerabilidad de los servidores, esto con la finalidad de no dejar rastros que puedan guiar al responsable del acceso a los servidores sin autorización, es importante destacar que en la presente investigación no se hará uso del borrado de las huellas ya que el ataque es planificado con el fin de identificar sus vulnerabilidades y los posibles riesgos. (Rodríguez A. , 2020)

2.1.3 Seguridad informática

Para el autor Gómez (2017), considera “medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos” (p. 25).

Por su parte el autor García (2017) define “La seguridad informática se ocupa de generar buenas prácticas, destinadas a garantizar sistemas de información seguros y confiables antes posibles riesgos. La seguridad informática busca reducir la posibilidad de que se materialicen los riesgos” (p. 2).

Sin embargo el autor Aguilera (2011) considera sobre la seguridad informática es una disciplina que tiene la responsabilidad y compromiso de realizar procedimientos, métodos y técnicas que permitan conseguir un sistema de información de manera confiable y segura garantizando que los equipos conectados por medio de la red LAN tenga confiabilidad y respaldo en la información. Finalmente, el autor Costas (2011) define sobre la seguridad informática consiste: en asegurar que los recursos del Sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación sólo sea posible a las personas que se encuentren acreditadas.

Para el autor Costas (2011) plantea los siguientes objetivos:

- Limitar las pérdidas de información al ocurrir un incidente de seguridad.
- Garantizar el uso adecuado de las aplicaciones y recursos de los sistemas.
- Cumplir normativas legales impuestas a nivel organizativo.
- Detectar problemas y amenazas a la seguridad.

Existen varios tipos que forman parte de la seguridad informática, estas son una parte elemental y se convierte en la mejor aliada de las empresas u organizaciones entre las cuales tenemos las que son de tipo físico: estas no son más que medidas de prevención y detección que tiene la finalidad de impedir daños físicos a los sistemas de información por lo tanto salvaguardar los datos almacenados en ellos. En este punto se debe considerar el entorno físico es decir posibles desastres naturales como terremotos, inundaciones entre otros y el entorno humano en robos, sabotajes. (Escriva et al., 2013)

Existe también las que son de tipo lógico que de acuerdo con Escriva et al. (2013) “Conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, así como a garantizar el acceso a la información únicamente por las personas autorizadas”. Complementado a esta definición el autor Molinetti (2019) referente con la seguridad lógica menciona las siguientes:

- De la red. – corresponde a la seguridad de información como datos personales, contraseñas, bancarios para evitar la suplantación de identidad, virus, etc. Los mecanismos de seguridad más usados en la red son:
    - Antispyware: impide que un tercero robe información del ordenador
    - Antivirus: protege la información de virus
    - Redes privadas VPN red que permite la extensión de la red interna LAN
- Del software. – seguridad de las aplicaciones de ataques maliciosos
    - Los firewalls
    - Software de filtración de contenido.

La necesidad que los datos sean íntegros, confiables y estén disponibles en cualquier momento para obtener el rendimiento máximo con riesgos mínimos. El enfoque de la seguridad no se centra solo en proteger el software y hardware, adicional a ellos se tiene tres puntos conocidos como la disponibilidad, integridad y confiabilidad. (Macías, 2021)

Figura 4

Pilares de la seguridad

Nota: Tomado de *Seguridad Informática* (pág. 6), por Samaniego & Ponce, 2021, Grupo Compás

Por su parte el autor Costas (2014) indica la confiabilidad no permite la revelación de datos a usuarios no autorizados. Para el autor Gómez (2017) cita que la integridad consiste en garantizar y certificar que los datos informáticos no hayan sido maniobrados. Finalmente, para los autores Samaniego & Ponce (2021) asegura que la disponibilidad “permite que la información esté disponible para quien la necesita, para ello hay que implementar las medidas necesarias para que tanto la información como los permisos estén disponibles” (p. 7).

2.1.3.1 Vulnerabilidad en sistemas informáticos

En los sistemas informáticos la vulnerabilidad puede aparecer en los elementos básicos del computador tales como programas, cables de red, almacenamiento, etc. Una primera definición de vulnerabilidad describe que es la impotencia de un recurso pueda implicar de alguna u otra manera en el trabajo correcto y confiable del sistema informático. (Escriva et al., 2013)

Para la Escuela Superior de Redes RED CEDIA (2018) define respecto a las vulnerabilidades que están son fallas que pueden permitir la manifestación de inconvenientes en la seguridad general de la red o los equipos que se encuentren conectados por medio de configuraciones mal realizadas tanto en los equipos como en la red permite crear estas vulnerabilidades.

Así mismo los autores Yeison & Orozco (2020) “una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas”. Es por lo tanto una debilidad o falla que pueden ser aprovechadas por amenazas y pueden ser utilizadas por atacantes causando a corto plazo daños a los sistemas informativos de la empresa u organización, así como los datos personales que son mucho más importantes y se debe tener mayor cuidado que no caiga en manos equivocadas la información.

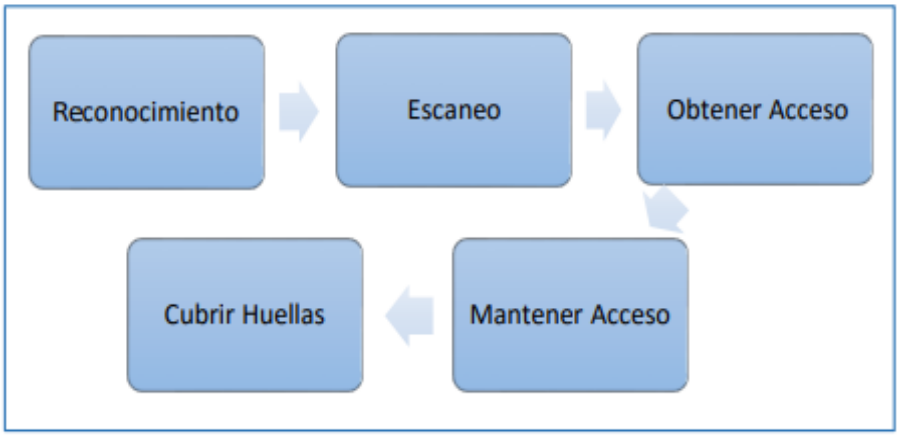
Dentro de las vulnerabilidades tenemos los ataques y los conocidos agujeros de seguridad los primeros para el autor Baca (2016) describe dos tipos que pueden hacer a la empresa más vulnerable ante posibles ataques los cuales se describen a continuación:

- Intencionados. – son accesos no autorizados donde el atacante logra acceder a los recursos del sistema sin autorización con el objetivo de robar o alterar registros.
- No intencionados. – son acciones no intencionales por alguien que perjudica a la empresa como fallas de energía, incendios, etc. (p. 157)

El ataque a la seguridad informática daña o desequilibra los sistemas de ahí que existe la necesidad de comprender cuales son las debilidades que comprometa la seguridad y aplicar procedimientos, prácticas para reducir o minimizar este porcentaje. Por ello se ha identificado cinco fases que permitan de manera eficiente aplicar estrategias que sean efectivas, el autor (Mamami, 2013)

Figura 5

Fases de un ataque informático



Nota: Adaptado de *Diseño de un Modelo de Seguridad de Información en Redes LAN* (pag.30), por Tufiño, 2018.

- Reconocimiento: cuando el atacante realiza un estudio a su víctima.
- Escaneo: una vez con la información del reconocimiento realiza un estudio a profundidad para identificar las vulnerabilidades.
- Obtener acceso: aquí el atacador utiliza todas sus habilidades para realizar cualquier ataque.
- Mantener acceso: radica en mantener el acceso logrado en la fase anterior por medio de herramientas Sniffer.

Mientras que los agujeros de seguridad es el fallo que se presenta en un programa permitiendo violar la seguridad informática de un sistema generalmente se da al utilizar los servicios de correo, web. Los autores Escriva, Romero, & Ramada (2013) definen que estos son falos que se relacionan por el mal funcionamiento de un sistema por ello es sumamente importante y necesario reprender estas vulnerabilidades en el momento que se las manifieste ya que en varios casos esta puede generar inestabilidad de seguridad dentro de los sistemas de información.

Existen diversos tipos de atacantes de acuerdo con el autor Macías (2021) se diferencian por su motivación y especialidad describiéndose a continuación:

Hacker

Se destacan por su habilidad y excelencia en las ramas de la programación el cual poseen conocimientos valiosos en redes y ordenadores informáticos, donde su principal propósito es detectar y buscar vulnerabilidades en las redes o dispositivos hardware informático.

Cracker

Son de características parecidas a los hackers. Donde las acciones de romper vulnerabilidades a los sistemas la realizan por el coste económico que pueden obtener al tomar información confidencial.

Carders

Se los denomina así ya que tiene como propósito realizar transacciones con tarjetas adulteradas por medio del cracking. El cracking no es más que uso ilegal de las tarjetas de crédito de manera fraudulenta y se vinculan a prácticas de pirateo para obtener números de tarjeta.

Warez

Son personas que se dedican a distribuir software de manera ilegal “piratas”. Estos grupos son los que perjudican a las empresas dedicadas a la creación de software generalmente de pago para varias disciplinas y usos, este tipo de “piratas” se dedican a la creación de los famosos keygen.

Grey Hats

Este tipo de personas busca encontrar vulnerabilidades para más adelante venderlas al público que esté dispuesto a pagar por la información adquirida, estos se pueden exteriorizar como expertos en seguridad por lo tanto su enfoque va hacia las ganancias económicas que pueden recibir antes que perjudicar a la empresa. entre su público están los gobiernos, instituciones militares y hackers. (Tufiño, 2018)

Cuando los colaboradores se colocan la piel CEO de una empresa cuando esta acaba de sufrir un ciberataque muchas de las veces se genera confusión respecto a las medidas que se debe tomar como invertir en seguridad para proteger toda la información de la empresa.

El análisis de vulnerabilidad realizado por medio del hacking ético cuenta con varias fases de penetración mediante el cual se accede al sistema de la red LAN de la institución, por lo que se analizará las fases que intervienen y los objetivos de cada una de ellas además de presentar los pasos que implica realizar para las pruebas correspondientes del hacking ético. A continuación, se realiza la conceptualización del pentesting enfocado en realizar pruebas de vulnerabilidad.

En pentesting es una abreviatura en inglés “penetration” y “test”. La definición completa es que es una práctica o metodología realizada para descubrir vulnerabilidades en los sistemas de seguridad, página web u otro entorno (Guillén, 2017). Por parte del autor Romero (2019) menciona que para las empresas es de gran utilidad pues pueden comprobar hasta qué punto su red interna o algún sistema informático es seguro ante algún ataque informático.

Al ser un tipo de prueba que se realiza a la misma empresa tiene la finalidad de concientizar a los colaboradores de vulnerabilidades que afecten el entorno y bases para prevenir futuros ataques. Existen varios tipos de pentesting los cuales se los diferencia por el alcance que cubren, pero a pesar de ser diferentes, estos tienen el objetivo asociado a la mejora de las vulnerabilidades en las organizaciones.

La caja blanca o “White Box” este tipo consiste en una prueba competa realizando un análisis a la estructura. Una vez con toda la información recopilada es mucho más fácil conocer que se puede modificar o mejorar. “Lo agridulce de esta metodología es que aseguramos internamente toda nuestra infraestructura frente a un ataque desde dentro” (Esaú, 2015).

Por su parte la caja negra o “Black Box” se le proporciona información confidencial, esta prueba se asemeja a un ataque real, realizado por personal externo a la empresa con amplia experiencia en seguridad. “Las pruebas más comunes realizadas son, pruebas de penetración de infraestructura o de red, pruebas de penetración a aplicaciones y un ataque simulado completo” (Vanegas, 2019, p. 3).

Finalmente, la caja gris “Grey Box”, es la combinación de las otras anteriores. De acuerdo con la Universidad En Internet (2020) “se realiza con conocimiento parcial de la red del cliente, emulando el ataque de un empleado no-autorizado o de un contratista externo que se conecta desde Internet, o bien, tiene acceso físico a la red interna del cliente”. A esta se la proporciona información como contraseñas de acceso y arquitectura para atacar partes específicas de la aplicación.

2.2 Importancia de la variable de estudio

Los sistemas informáticos se encuentran vulnerables ante amenazas ya sea por persona extrañas o programas astutos donde su objetivo principal es perjudicar de la institución. por este motivo la protección de la información es de importancia para evitar las amenazas por el contrario la seguridad no es un juego y debe darse la importancia del caso para prevenir perdidas o daño en la información por parte de ciber delincuentes, hacker, virus, entre otros. La inversión en seguridad informática muchas de la vez llegan a ser grande, aunque está en función de que se quiere

resguardar y proteger considerando que los datos o información para las empresas es el mayor activo por conservar y cuidar. Por lo tanto, el costo - beneficio en seguridad es inigualable por todos los detalles antes mencionados.

La red al estar vulnerable a diversos ataques informáticos provoca inestabilidad en los servicios que ofrece la institución debido a no existir la comunicación entre dispositivos y al ser estos vulnerables los servicios que facilitan no van a tener la confiabilidad o seguridad obteniendo como resultado daños irreversibles a la información dificultando su acceso o conexión entre si ya que de ellas depende trabajar activamente con él envió de información.

Como ya se ha mencionado el defectuoso control de acceso a personas no autorizadas trae el riego de perder información sumamente confidencial donde esta pérdida o robo de información trae consecuencias negativas para el Gobierno Regional de Apurímac manteniendo que la información es el corazón de cualquier institución y si esta es alterada o robada afecta a la organización.

Con la finalidad de equilibrar esto existen los “Ethical” Hacking quienes son personas especializadas en descubrir vulnerabilidades de los sistemas informáticos y realizar mejoras a los sistemas informáticos cuidando el mínimo detalle. Bajo ese escenario, los hackers éticos realizan escenarios de pruebas denominados pentesting el cual ayudan a garantizar la protección de los datos. La seguridad informática garantiza y determina que el uso de esta herramienta “Ethical Hacking” es de gran utilidad en el cuidado y protección de la información, sin embargo, las empresas deben ser conscientes de la gran importancia de la seguridad en los sistemas financieros en la actualidad, de ahí que la mejora de la seguridad de la red LAN es de gran importancia para el Gobierno Regional de Apurímac.

2.3 Análisis comparativo

Tabla 3

Análisis comparativo de la variable de estudio

VARIABLE / TOPICO	PRIMER AUTOR	SEGUNDO AUTOR	TERCER AUTOR	COMENTARIO
HACKING ÉTICO	"El hacking ético es la práctica que consiste en utilizar las habilidades en sistemas informáticos y de red para ayudar a las organizaciones a probar sus mecanismos y procedimientos de seguridad con tal de identificar debilidades y/o vulnerabilidades" (Rodriguez, 2020, p. 117).	"Un hacker ético es la persona que usa habilidades como conocimientos en programación, redes de computadoras, instalación y mantenimiento de infraestructura basada en los sistemas operativos más conocidos y usados como lo son Unix1 y Windows NT2" (Medina, 2020, p. 3).	"El hacking ético es la práctica que consiste en utilizar las habilidades en sistemas informáticos y de red para ayudar a las organizaciones a probar sus mecanismos y procedimientos de seguridad con tal de identificar debilidades y/o vulnerabilidades" (UNIR, 2020)	El Hacking Ético es unos de los métodos más utilizados para realizar de forma correcta pruebas de vulnerabilidad y que es necesario implantarlo como políticas en diversas instituciones públicas, privadas.

Tabla 4

Análisis comparativo del tópico clave

VARIABLE / TOPICO	PRIMER AUTOR	SEGUNDO AUTOR	TERCER AUTOR	COMENTARIO
VULNERABILIDAD INFORMÁTICA	"La vulnerabilidad puede aparecer en los elementos básicos del computador tales como programas, cables de red, almacenamiento, etc. Vulnerabilidad es la Debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento de un sistema informático" (Escriva et al., 2013).	"Una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas"	"Las vulnerabilidades son fallas que permiten la aparición de deficiencias en la seguridad general del equipo o de la red. Configuraciones incorrectas en el equipo o en la seguridad también permiten la creación de vulnerabilidades" (RED CEDIA, 2018, p. 24).	Los autores tienen una similitud sobre los procesos e implementación de las pruebas vulnerabilidad y que para salvaguardar en necesario tener como políticas la implementación de este tipo de diagnóstico de forma más seguidas y permanentes.

2.4 Análisis crítico

La aplicación del hacking ético en las instituciones públicas o privadas para revelar vulnerabilidades en la red LAN es uno de los problemas principales que estas presentan y no es la excepción para el Gobierno Regional de Apurímac pues esto lleva a no descubrir cuales son las deficiencias en la seguridad de los servicios de la red LAN, estimulando vulnerabilidad a los sistemas informáticos.

La red al estar vulnerable a diversos ataques informáticos provoca inestabilidad en los servicios que ofrece la institución debido a no existir la comunicación entre dispositivos y al ser estos vulnerables los servicios que facilitan no van a tener la confiabilidad o seguridad obteniendo como resultado daños irreversibles a la información dificultando su acceso o conexión entre si ya que de ellas depende trabajar activamente con él envió de información. Por tal razón la red debe mantener la configuración adecuada con medidas de seguridad para minimizar la interrupción de los servicios lo que conlleva a u aumento en la inseguridad informática.

Como ya se ha mencionado el defectuoso control de acceso a personas no autorizadas trae el riego de perder información sumamente confidencial donde esta pérdida o robo de información trae consecuencias negativas para el Gobierno Regional de Apurímac manteniendo que la información es el corazón de cualquier institución y si esta es alterada o robada afecta a la organización.

CAPITULO III: MARCO REFERENCIAL

3.1. Reseña histórica

El Gobierno Regional de Apurímac es una institución pública encargada de la administración superior de cada departamento, este consta de personalidad jurídica con patrimonio propio, autonomía política, administrativa, económica y derecho público que tiene la responsabilidad de administrar el departamento de Apurímac, Perú. Este gobierno forma parte del Mancomunidad Regional Macro Región Sur y Mancomunidad de los Andes. Estos gobiernos se componen de dos órganos uno determinado por el Consejo Regional y el Gobernador Regional no es antes del 2015 que se usaba el termino de presidente regional.

El gobernador regional es el órgano ejecutivo quien es el representante del departamento, luego el teniente gobernador y los consejeros regionales de cada departamento siendo siete el mínimo y 25 como máximo. Su elección es cada cuatro años y como dato adicional el mismo no puede ser reelegido inmediatamente. Desde el 1 de enero de 2015 este órgano ejecutivo está conformado miembro. (Gobierno Regional de Apurimac, 2022)

De acuerdo con el ordenamiento jurídico peruano la gestión que deben cumplir estos corresponde al gobierno a nivel regional el cual se introdujo por medio de la legislación peruana que fue puesta en la constitución del 79. Según la Ley Orgánica de Gobiernos Regionales, los compromisos de los gobiernos incluyen el desarrollo de la planificación, promover actividades económicas, ejecutar proyectos de inversión pública junto con la administración pública de la propiedad. (Gobierno Regional de Apurimac, 2022)

3.1.1. ¿Qué hacemos?

Para el Gobierno Regional Apurímac (2022) las actividades que realiza son:

Fomentamos el desarrollo integral y sostenible de la región, promoviendo el empleo, así como la inversión pública y privada.

Garantizamos el ejercicio pleno de los derechos y la igualdad de oportunidades de nuestros habitantes, de acuerdo con los planes nacionales, regionales y locales de desarrollo.

3.2. Filosofía organizacional

3.2.1. Misión

“Promovemos el desarrollo integral sostenible en la región Apurímac de forma participativa, transparente, inclusiva y eficiente” (Gobierno Regional Apurímac, 2022).

3.2.2. Visión

“Ser una región agroecológica y minera que previene de conflictos, y promueve la producción diversificada, ambientalmente sostenible, que mejora la calidad de vida de sus habitantes a través de la erradicación la desnutrición crónica infantil y la violencia de género” (Gobierno Regional Apurímac, 2022).

3.2.3. Objetivos

De acuerdo con el Gobierno Regional de Apurímac (2022) presenta los siguientes:

Construir una comunidad integrada, unida y con identidad cultural, donde se garantice el acceso a la educación, la atención de salud, el empleo digno y la calidad de vida para todas y todos, la población ejerce sin restricciones sus derechos a la igualdad de oportunidades, la inclusión y equidad social.

Construir una economía regional andina, moderna competitiva y solidaria, armónica con el desarrollo humano y sostenible, que se sustenta en su producción agroecológica y pecuaria, la integración de la actividad turística y una minería sujeta al uso ambiental y socialmente responsable de sus recursos naturales.

Convertir Apurímac en una región saludable y ambientalmente sostenible, ordena territorialmente, donde sus habitantes conocen y hacen uso adecuado del ambiente y sus recursos naturales en sus diversos pisos ecológicos y han desarrollado sus capacidades y mecanismos eficientes para el planeamiento y la gestión territorial con un adecuado manejo de riesgos y adaptada a los cambios climáticos.

Forjar una sociedad andina y democrática donde su población ejerce sus derechos y ha fortalecido sus capacidades para autogobernarse desde la participación social y ciudadana de sus hombres y mujeres, quiénes concretan desde sus organizaciones e instituciones de la sociedad civil, con las autoridades regionales y locales para alcanzar un clima de paz, libertad y justicia social.

3.2.4. Fines

"La finalidad esencial del Gobierno Regional, es fomentar el desarrollo regional integral sostenible, promoviendo la inversión pública, privada y el empleo y garantizar el ejercicio pleno de los derechos y la igualdad de oportunidades de sus habitantes" (Gobierno Regional de Apurímac, 2017).

3.2.5. Objetivos estratégicos

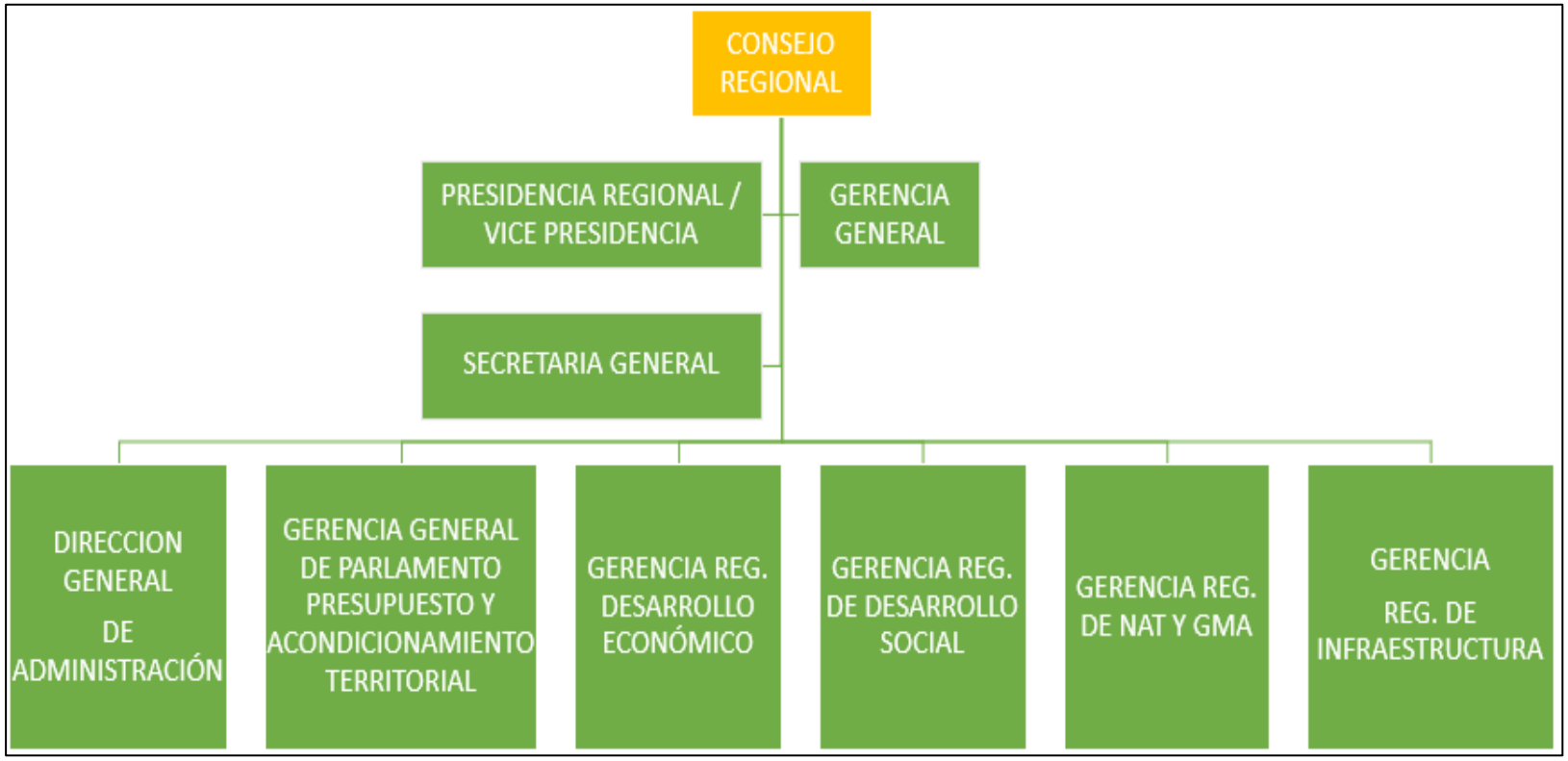
El Gobierno Regional de Apurímac (2020) describe:

- Salud,
- Educación,
- Agropecuario,
- Transporte,
- Industria,
- Saneamiento,
- Turismo,
- Cultura y deporte,
- Protección social,
- Trabajo,
- Orden público y seguridad,
- Planeamiento, gestión y reserva de contingencia.

3.3. Diseño organizacional

Figura 6

Organigrama del Gobierno Regional de Apurímac



Nota: Tomado de Estructura Orgánica del Gobierno de Apurímac, (pág. 1), por Gobierno Regional de Apurimac, 2022.

3.3.1. Presentación y explicación del organigrama de la Institución

- **La presidencia regional:**

  Quien es la máxima autoridad de su jurisdicción

- **La gerencia general:**

  Es quien coordina a las gerencias y direcciones regionales en la gestión pública y se rige a lineamientos de políticas regionales

- **Secretaria general:**

  Tiene la responsabilidad de dar apoyo al gobierno regional la parte administrativa de su competencia.

- **Gerencia Regional de Planeamiento Presupuesto y Acondicionamiento Territorial:** su función es entregar los servicios referentes a planificación, inversiones, administración

- **Gerencia Regional de Desarrollo Económico:**

  Coordina, dirige, controla, supervisa y evalúa el desarrollo equilibrado de la región de tal forma se transforme en oportunidades para la sociedad.

- **Gerencia Regional de Desarrollo Social:**

  Tiene la responsabilidad de ejecutar funciones específicas referentes a educación, salud, deportes, empleo, vivienda, desarrollo social entre otros.

- **Gerencia Regional de Recursos Naturales y Gestión del Medio Ambiente:**

  Sus funciones específicas es la gestión ambiental y recursos naturales

- **Gerencia Regional de Infraestructura:**

  Su responsabilidad se centra en la ejecución, supervisión de proyectos públicos fomentando la participación de la sociedad civil

3.4. Servicios

El Gobierno Regional de Apurímac (2022) ofrece los siguientes servicios:

- Licencia con goce de remuneraciones,
- Bonificaciones,
- Expedición de constancias y crédito de trabajo,
- Realización de prácticas profesionales,
- Consultas y observaciones,
- Recurso de apelación en procedimiento de selección,
- Traslado de capital de distrito y/o provincia,
- Reconocimientos de comunidades campesinas,
- Calificación de documentos,
- Anotación de inscripción de registros públicos,
- Exhibición de documento,
- Evaluación de estudios de impacto ambiental,
- Certificación de obras viales,
- Certificación de kilometraje de carreteras y puentes,
- Liquidación de obra,
- Elaboración de formatos,
- Renuncia a la concesión
- Duplicado de la tarjeta única de circulación,
- Habilitación de agencia o estaciones de ruta,

- Base legal,
- Expedición de la licencia de clase a categoría 1,
- Examen de conocimiento,
- Examen de habilidades de manejo,
- Reporte de estado de licencia de conducir,
- Constancia de atención,
- Certificado de discapacidad.

3.5. Diagnóstico organizacional

3.5.1 Diagnostico FODA

Tabla 5

Diagnóstico FODA

FACTORES INTERNOS	
FORTALEZAS	**DEBILIDADES**
- Promover una cultura de planeamiento. - El gobierno cuenta con personal calificado. - Equipos de trabajo organizados en varias gerencias regionales. - Potencia a los trabajadores mediante capacitaciones. - Coordinación constante con las autoridades distritales de la región. - Desarrollo de proyectos de instalación de banda ancha para conectividad regional.	- Limitada capacitación en gestión pública. - Deficiente prestación de servicios. - Niveles de ejecución de inversión deficientes - Sistemas de seguridad no actualizados. - Escaso control y conocimiento en seguridad informática. - Ausencia de evaluación periódica a los planes operativos institucionales (POI). - Mala planificación de la ejecución presupuestal.

OPORTUNIDADES	AMENAZAS
- Adecuada flota de transporte de pasajeros en la región. - Asignación presupuestal anual. - Elaboración del plan de desarrollo regional concertado Apurímac al 2030.	- Violaciones a la seguridad informática. - Geografía accidentada y de difícil acceso. - Desconocimiento o falta de apoyo de autoridades estatales con los intereses de la región.

FACTORES EXTERNOS

3.5.2 Análisis de la matriz FODA

3.5.2.1 Fortalezas

Las fortalezas que destaca es la potenciación de las capacidades de los empleados mediante capacitación constante el cual entrega la institución a sus trabajadores esto va de la mano para cumplir con los objetivos propuestos de ahí que la promoción de una cultura de planeamiento en la organización genera que se mejore los equipos de trabajo organizados en varias gerencias regionales. Otra fortaleza es el desarrollo de instalación de banda ancha para lograr conectividad regional acompañada de la coordinación de las autoridades de la región.

3.5.2.2 Debilidades

Las debilidades que presenta el gobierno son la deficiente prestación de servicios que brinda la entidad por dificultades en la red al transmitir la información, esto con los sistemas de seguridad al no estar actualizados conlleva el riego de perder datos de información personal de los usuarios. El área de las TIC por el escaso control y conocimiento en seguridad acompañado de la ausencia de evaluación a los planes operativos institucionales incrementa el riesgo de sufrir algún ataque que ocasionen

perdida de información valiosa para la entidad pública. La mala planificación y gestión pública de los datos incrementa esta problemática en la información.

3.5.2.3 Oportunidades

Para las oportunidades que presenta la entidad se encuentra la asignación presupuestal anual esta se convierte en un instrumento de suma importancia para construir adecuadamente las estrategias que le permitan minimizar las debilidades y aprovechar las oportunidades del avance de la tecnología que día a día se presentan y mediante la elaboración del plan de desarrollo regional se pueden construir los objetivos que se plantea la institución para mejorar la protección y seguridad de la red.

3.5.2.4 Amenazas

Como ya se ha mencionado las violaciones a la seguridad de la información conlleva un gran riego para la institución además la falta de apoyo por parte del gobierno siempre se convierte en una amenaza para las instituciones públicas ya que al no contar con la asignación del presupuesto necesario no se podría implementar las estrategias de mejora en las áreas que presenten dificultades pero mucho más importante es mejorar la seguridad ante ataques maliciosos con fines de robo de información de usuarios.

CAPITULO IV: RESULTADOS

4.1. Diagnóstico a la seguridad LAN del Gobierno Regional de Apurímac

4.1.1. Diagnostico general del Gobierno Regional de Apurímac

El Gobierno Regional de Apurímac es cada vez más dependiente de las redes informáticas y en caso de existir un problema se estaría comprometiendo la continuidad de sus operaciones. La falta de mejoras en la seguridad de la red LAN presenta un riesgo de nivel elevado vulnerando la información pudiendo ser esta modificada, alterada y en casos graves robada lo cual ocasionaría un impacto más grande para la institución, esta problemática pone en evidencia la necesidad de realizar acciones de mejoras que contribuyan al uso de un sistema de identificación vulnerables efectivo que permita disminuir los niveles de riesgo para la institución.

El Gobierno Regional de Apurímac cuenta con una red LAN para el desarrollo de sus actividades diarias, de esto se ha podido evidenciar que actualmente la red LAN con la que opera la institución no cumple con las necesidades y efectivo control de vulnerabilidades es decir presente un sistema vulnerable lo que genera varias causas problemáticas entre las más importantes se menciona la ausencia del respectivo sistema de identificación, por consiguiente se ha podido determinar que existe un sistema de red LAN vulnerable y con ello se incrementa potencialmente los niveles de riesgos de intrusión o ciberataques, creando grande desventajas e inestabilidad en la organización de la Institución Gubernamental.

La Institución en cuestión maneja gran información y de tipo confidencial de todo un sector o población, considerando este factor se ha podido determinar que dicha información se encuentra en alto riesgo debido al alto nivel de vulnerabilidad

existente y la falta de control por parte de las autoridades pertinente quienes no han tomado acciones correctivas que permitan mejorar el sistema respectivo.

4.1.1.1. Problema central

Como se explicó con anterioridad el problema central objeto de esta investigación es la presencia de un sistema vulnerable lo que genera varias causas problemáticas entre las más importantes se menciona la ausencia del respectivo sistema de identificación, entonces se ha podido evidenciar que el principal problema que presenta el Gobierno Regional de Apurímac es un sistema vulnerable generado por el uso de un sistema de red LAN con bajo nivel de identificación de vulnerabilidades que no permite identificar los riesgos a los que están expuestos los servidores de internet con el cual trabaja el Gobierno Regional de Apurímac.

Al no utilizar ningún tipo de sistema que permita identificar los riesgos o vulnerabilidades existentes en la red LAN conlleva a presentar deficiencias en la seguridad de los servidores, esto genera riesgo e inseguridad de la información que maneja la institución ya que pueden ser víctimas de ataques cibernéticos por no contar con las medidas de seguridad y políticas necesarias que prevengan la pérdida o alteraciones de la información manejada por el Gobierno Regional de Apurímac.

4.1.1.2. Causas del problema

La presencia de un sistema vulnerable es el problema central que se pretende resolver en la presente investigación, pero de ahí se derivan varias causas a este problema en mención, entre las más importantes se menciona la ausencia del respectivo sistema de identificación. De igual manera se ha podido evidenciar que el Gobierno Regional de Apurímac tiene servidores vulnerables ante el ataque

cibernético por lo cual presenta un alto grado de inestabilidad en dichos servidores donde se almacena la información la cual no cuentan con la seguridad necesaria y esto indica que podrían acceder a ella y ocasionar daños irreversibles, uno de los principales daños a los que está expuesto es la pérdida total de la información.

Como causa del problema también se ha identificado la ausencia del respectivos sistema que permita identificar las vulnerabilidades a las que está expuesto lo que genera un alto nivel de riesgo en cuanto a la pérdida de la información confidencial que maneja la institución y su alto grado de alteración también genera vulnerabilidad en su sistema informático en general.

4.1.1.3. Efectos del problema

Es importante destacar que al existir una aplicación que no permite identificar las vulnerabilidades de la red LAN del Gobierno Regional de Apurímac incrementa los niveles de inseguridad de los servidores, es decir que al afrontar un ataque cibernético es más alta las probabilidades de perder toda la información que resguarda en los servidores y como consecuencia visualizando el peor de los escenarios puede suceder la pérdida total de la información almacenada.

Se ha podido evidenciar que el principal problema que presenta el Gobierno Regional de Apurímac es el uso de un sistema de identificación de vulnerabilidades deficiente que no permita identificar los riesgos a los que están expuestos los servidores de internet con el cual trabaja la institución y esto presenta un alto nivel de riesgo para la información pues puede ser alterada y en el caso extremo robada.

Al no utilizar ningún tipo de sistema que permita identificar los riesgos o vulnerabilidades existentes en la red LAN conlleva a presentar deficiencias en la seguridad de los servidores, esto genera riesgo e inseguridad de la información que maneja la institución ya que pueden ser víctimas de ataques cibernéticos por no contar con las medidas de seguridad y políticas necesarias que prevengan la pérdida o alteraciones de la información manejada por la institución.

Un sistema vulnerable de la red LAN de esta institución, evidencia la inefectiva gestión y falta de protocolos de seguridad implementados por las autoridades correspondientes del Gobierno, pues al tratarse de manejo de información confidencial de una región se deberían implementar las normas y reglas necesarias que resguarden y brinden total seguridad a la información y los servidores actuales.

4.1.2. Presentación de resultados del levantamiento de información

4.1.2.1. Aplicación del cuestionario

El instrumento de recolección de información para identificar las causas y posibles soluciones a la problemática presentada es el cuestionario el cual se desarrollará con la elaboración de preguntas específicas y cerradas que determinen las respuestas otorgadas por los colaboradores del Gobierno Regional de Apurímac, se debe considerar que el cuestionario será aplicado a los colaboradores del área correspondiente de TIC, ya que es el personal encargado de las actividades que involucran el análisis y verificación de la red LAN de esta institución.

Al ser considerado para la aplicación del instrumento únicamente al área antes mencionada la población de esta es específica y pequeña ya que el total de colaboradores de esta área son 12 y por ello se determina que dicha población es finita y no se considera necesario el uso de fórmulas que determinen la muestra a

utilizar, pues se tomará el total de la población como muestra y en este caso el instrumento será aplicado a 12 colaboradores de la institución del área de TIC.

La finalidad con la que se usa el instrumento antes mencionado es poder conocer de los colaboradores involucrados cuáles son los problemas que genera la el bajo nivel de identificación de vulnerabilidades de la red LAN y los riesgos que esto genera para la información que se alberga en los servidores así como también se pretende identificar las acciones de mejora que se puedan realizar con la finalidad de disminuir el riesgo de pérdida de información o cualquier ataque cibernético al que se puede enfrentar el Gobierno Regional de Apurímac.

4.1.2.2. Resultados estadísticos del cuestionario

1. ¿Opina usted que las instalaciones del Gobierno Regional de Apurímac poseen una conexión segura y estable de internet?

Tabla 6

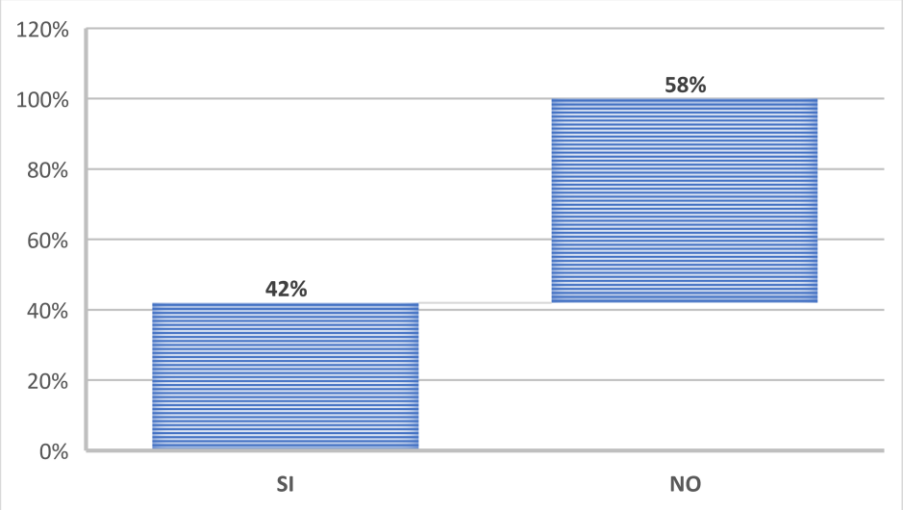
Conexión segura de internet

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	42%	58%	100%
Casos	5	7	12

Los resultados del cuestionario ante la pregunta realizada con respecto a la seguridad y estabilidad de la red de internet que utiliza esta institución muestran que el 58% de los funcionarios de la institución concuerdan en que la conexión de internet no es segura ni estable para el desarrollo de las actividades sin embargo el restante 42% de ellos manifiestan que desde su punto de vista la conexión de internet si es segura y estable.

Figura 7

Conexión segura de internet



2. ¿Considera usted que los funcionarios del gobierno tienen acceso limitado a los navegadores e información?

Tabla 7

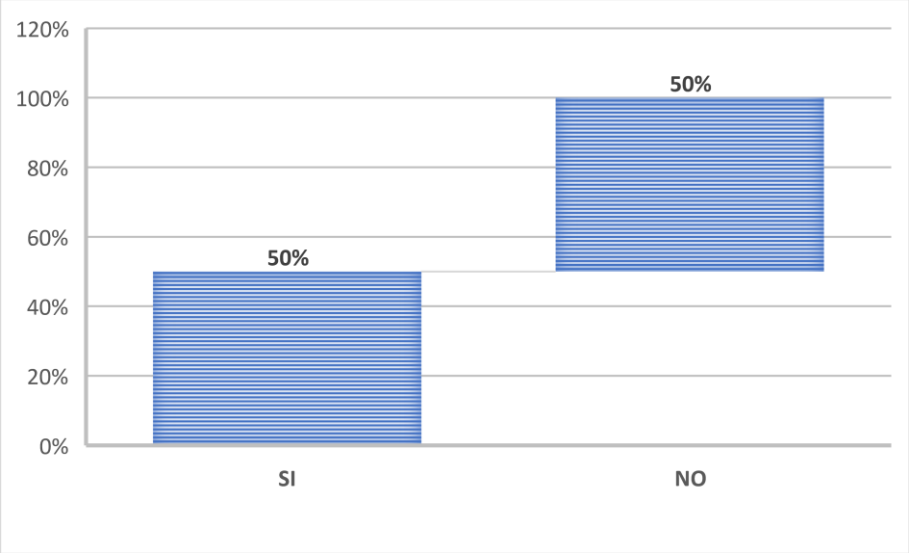
Acceso limitado a navegadores e información

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	50%	50%	100%
Casos	6	6	12

El resultado de la pregunta número dos realizado en el cuestionario referente al acceso limitado en los navegadores de los equipos de esta institución demuestran que el 50% de los colaboradores indican que no existe acceso limitado para los navegadores en los equipos, por otra parte el otro 50% restante menciona que si existen los accesos limitados en los navegadores e información de la Institución.

Figura 8

Acceso limitado a navegadores e información



3. ¿Considera que la red LAN cumple con las normas de seguridad para evitar el acceso por parte de usuarios externos?

Tabla 8

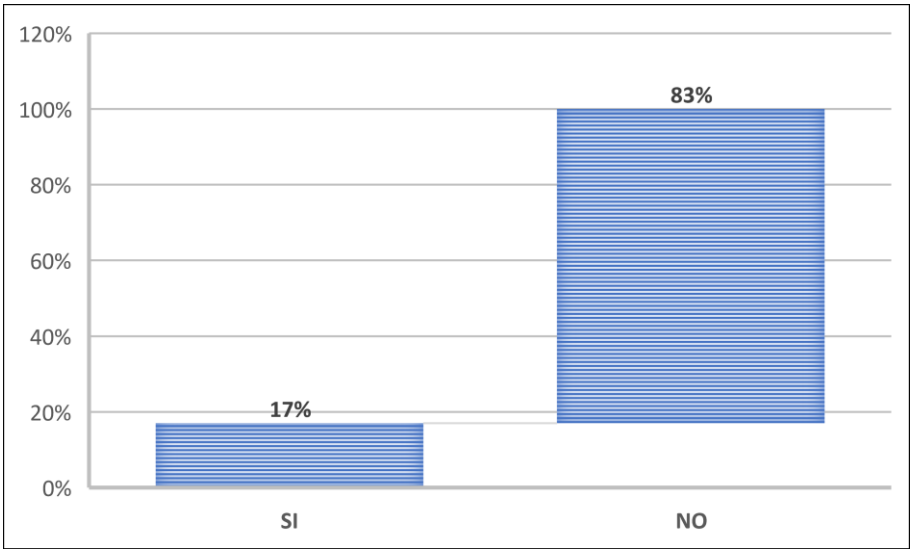
Normas de seguridad contra usuarios externos

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	17%	83%	100%
Casos	2	10	12

Los resultados de la pregunta número 3 del cuestionario donde se requiere conocer y analizar qué opinan los colaboradores acerca de la existencia de normas de seguridad que eviten el acceso por parte de usuarios externos a la red la de la institución y se tiene como resultado que el 83% de los colaboradores mencionan que no existe ningún tipo de norma o seguridad que evite el acceso de usuarios externos Por otra parte el 17% menciona que sí tienen normas de seguridad para este tipo de acceso realizado por usuarios externos.

Figura 9

Normas de seguridad contra usuarios externos



4. ¿Cree que en los últimos años la red LAN del Gobierno Regional de Apurímac ha sufrido ataques de tipo cibernéticos?

Tabla 9

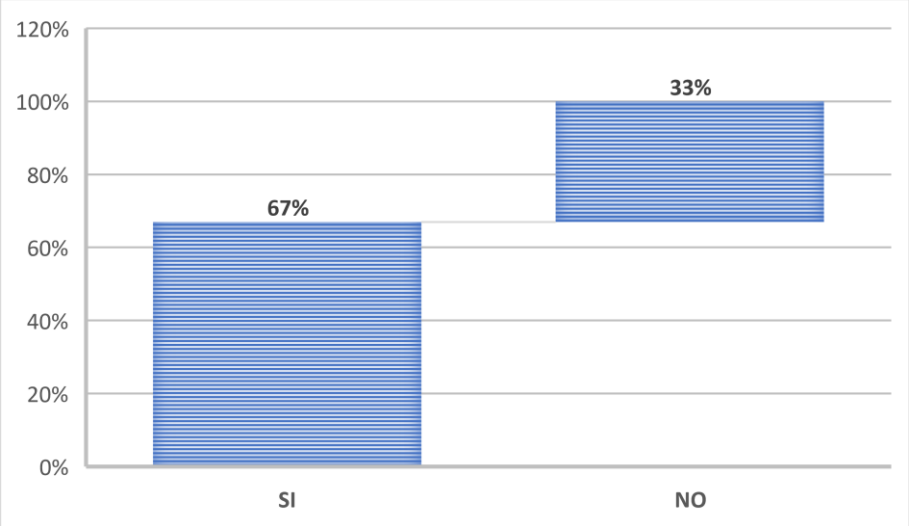
Ataques cibernéticos

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	67%	33%	100%
Casos	8	4	12

Como respuesta a la pregunta número cuatro referente a los ataques cibernéticos que haya podido afrontar la institución en el último año se tiene que el 33% de los colaboradores mencionan que no ha existido ataques cibernéticos en el último año sin embargo y siendo el porcentaje mayoritario con un 67% se indica que en el último año sí ha existido ataques cibernéticos en la red LAN del Gobierno Regional de Apurímac.

Figura 10

Ataques cibernéticos



5. ¿Conoce usted si el Gobierno Regional de Apurímac hace uso de firewall o controles de acceso que proteja la información de la red LAN?

Tabla 10

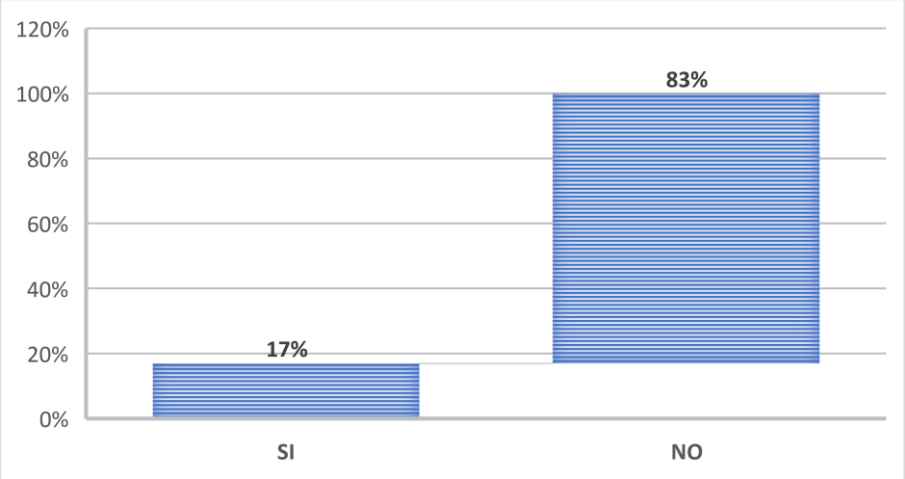
Firewall

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	17%	83%	100%
Casos	2	10	12

Como necesitado de la pregunta número 5 donde se considera necesario conocer si la institución hace uso de los controles de acceso que permita proteger la información de la red LAN se tiene como resultado que el 83% de los colaboradores han concordado en que no existe ningún tipo de uso de este tipo de controles que genere y proteja la información de la red LAN y el 17% restante menciona que si existe este tipo de control por parte del Gobierno Regional de Apurímac.

Figura 11

Firewall



6. ¿Considera usted que el Gobierno Regional de Apurímac da a conocer a los funcionarios las políticas de seguridad de las cuentas?

Tabla 11

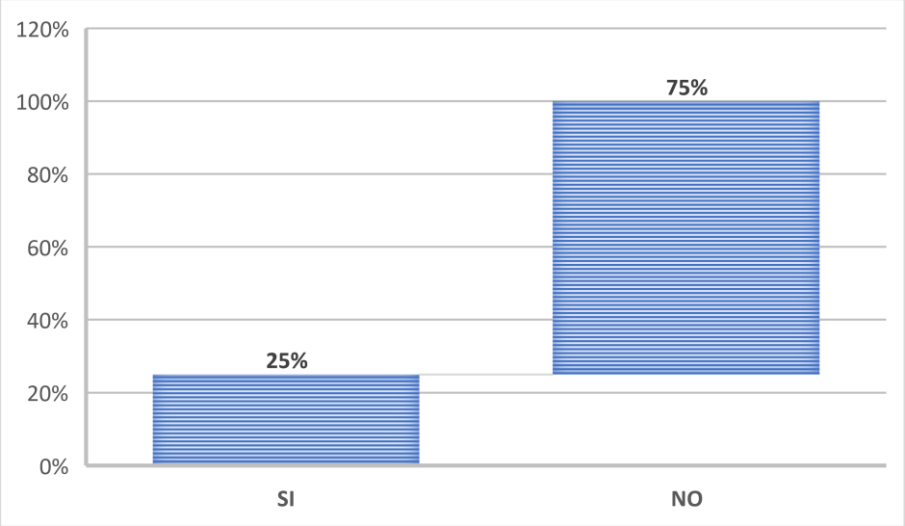
Políticas de seguridad

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	25%	75%	100%
Casos	3	9	12

Como resultado de la pregunta número 6 del cuestionario referente a las políticas de seguridad en la institución se tiene que el 75% de los colaboradores encuestados mencionan que el Gobierno Regional de Apurímac no tiene implementado o da a conocer a los funcionarios las políticas de seguridad de las cuentas que se deben realizar sin embargo por su parte el 25% restante menciona que el gobierno sí cuenta y da a conocer a sus funcionarios dichas políticas de seguridad informática.

Figura 12

Políticas de seguridad



7. ¿Opina usted que en el último año se ha realizada una prueba de vulnerabilidad de la infraestructura de la red?

Tabla 12

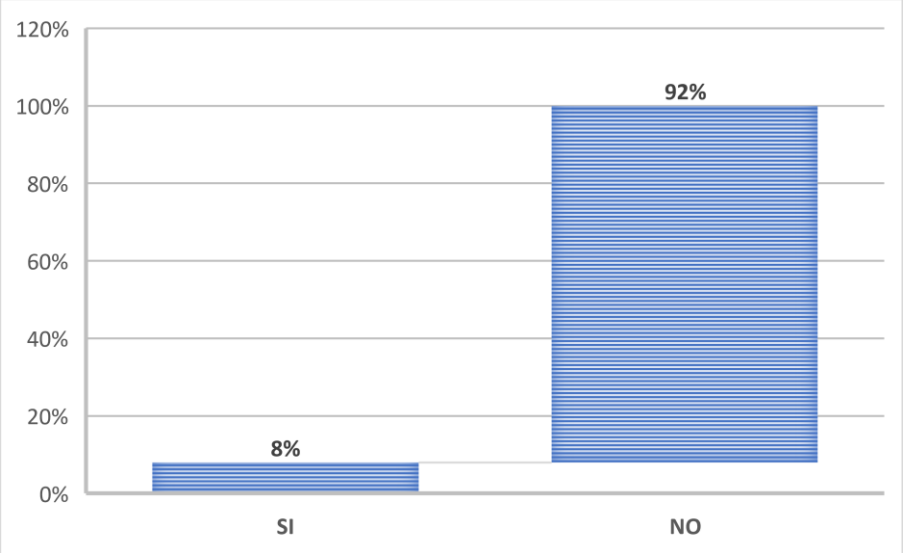
Pruebas de vulnerabilidad de la infraestructura

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	8%	92%	100%
Casos	1	11	12

Como resultado de la pregunta número 7 realizada en el cuestionario referente a las pruebas de vulnerabilidad realizadas a la infraestructura de la red se tiene que el 92% de los colaboradores menciona que en el último año el Gobierno Regional de Apurímac no ha realizado ningún tipo de prueba de vulnerabilidad y el 8% restante menciono que si se ha realizado este tipo de pruebas.

Figura 13

Pruebas de vulnerabilidad de la infraestructura



8. ¿Cree usted que el Gobierno Regional de Apurímac cuenta con herramientas que detecten y detengan las vulnerabilidades de la red LAN como el hacking ético?

Tabla 13

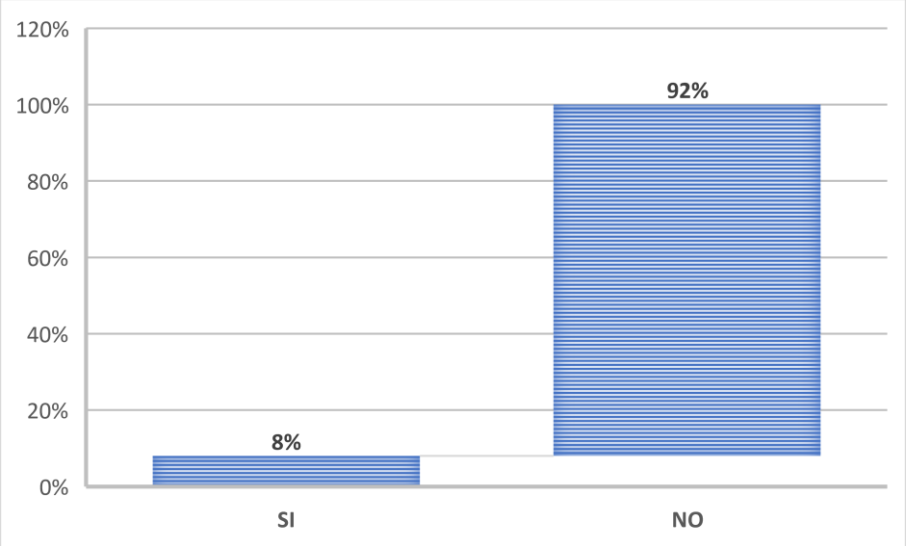
Herramientas de detección de vulnerabilidad

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	8%	92%	100%
Casos	1	11	12

El resultado de la pregunta número 8 del cuestionario con relación a sí el Gobierno Regional de Apurímac cuenta con las herramientas que detecten las vulnerabilidades de la red LAN se puede indicar como resultado que 92% de los colaboradores mencionan que el Gobierno regional actualmente no cuenta con ningún tipo de herramienta que le permita realizar estas actividades y el 8% restante indican que sí cuentan con dichas herramientas.

Figura 14

Herramientas de detección de vulnerabilidad



9. ¿Opina que en el Gobierno Regional de Apurímac trabaja de manera interna con la encriptación de la información?

Tabla 14

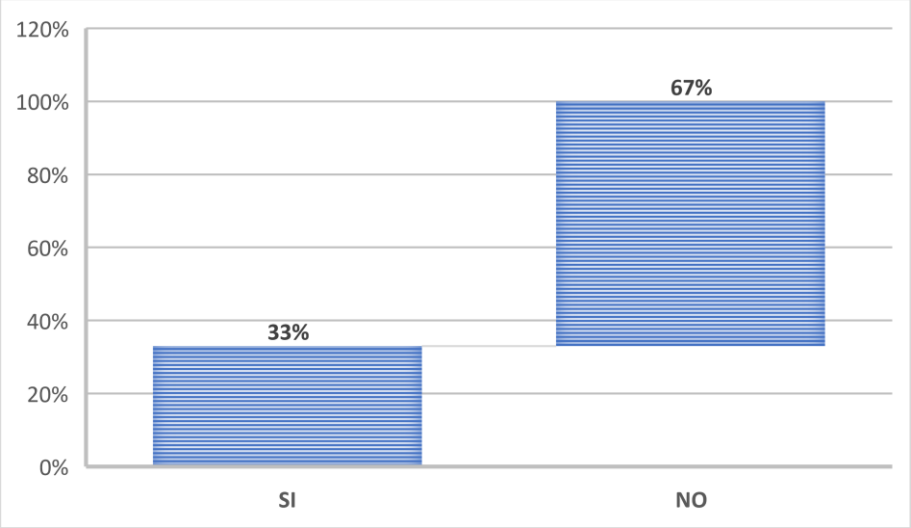
Encriptación de información

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	33%	67%	100%
Casos	4	8	12

Como resultado de la pregunta número 9 ante la verificación de inscripción de la información se ha podido verificar que el 67% de los colaboradores indican que el Gobierno Regional de Apurímac actualmente no cuenta con ninguna manera o acción que le permita incrementar la información manejada internamente por otra parte 33% de los colaboradores restantes ha mencionado que sí existe esta manera de inscripción de información dentro del Gobierno regional.

Figura 15

Herramientas de detección de vulnerabilidad



10. ¿Considera necesario que el Gobierno Regional de Apurímac implemente una mejora en la seguridad de la red LAN?

Tabla 15

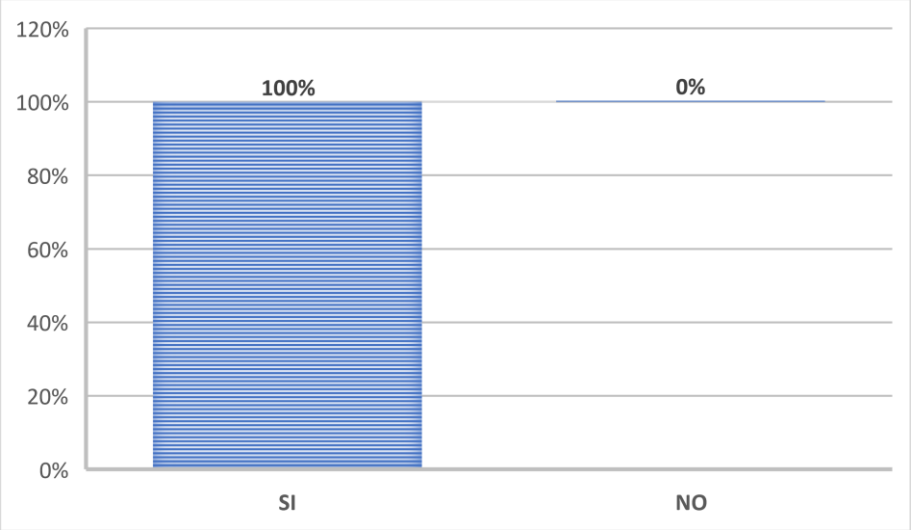
Mejora en la seguridad de la red LAN

RESULTADOS DEL CUESTIONARIO			
PARÁMETROS	**SI**	**NO**	**TOTAL**
Porcentaje	100%	0%	100%
Casos	12	0	12

Como resultado la pregunta número 10 del cuestionario se consultó a los colaboradores del área de TIC sí consideran necesario que el Gobierno Regional de Apurímac implemente medidas de mejora ante la seguridad de la red LAN donde se obtuvo como resultado que el 100% de los colaboradores concuerdan en que si es necesario realizar medidas de mejora que garanticen la seguridad de la red LAN y de la información que se maneja dentro de la institución.

Figura 16

Mejora en la seguridad de la red LAN



4.1.2.3. Principales resultados de la aplicación del cuestionario

Con la información recopilada mediante el uso del cuestionario el cual fue aplicado y contestado por los colaboradores del área de TIC quienes conocen y saben de la problemática existente en cuanto a la red LAN del Gobierno Regional de Apurímac se ha podido evidenciar y analizar los siguientes resultados:

- Como resultado de la información obtenida se ha podido verificar que actualmente el Gobierno Regional de Apurímac no cuenta con una conexión de internet segura ni estable es decir que a más de presentar problemas de conexión esto genera dificultades en la realización de actividades a los colaboradores de manera interna la inestable e insegura conexión a internet genera de riesgo ante la posibilidad de ser atacados de manera cibernético y pone en riesgo la información que se resguarda en los servidores y bases de datos de la Institución.

- También se ha podido evidenciar como resultado de la recopilación de información que la institución no tiene delimitado el acceso a los navegadores e información de la institución es decir que todos los colaboradores de esta institución tienen acceso a la información y además pueden navegar de manera libre en todos los navegadores de la institución esto quiere decir que se incrementa el riesgo de vulnerabilidad existente en la red LAN.

- La ausencia de normas y políticas de seguridad también se evidenciaron los resultados obtenidos de la recopilación de información ya que los colaboradores manifiestan en un alto porcentaje que la institución no cuenta ni informa a sus colaboradores acerca de las normas o políticas existentes que se deben seguir para el manejo adecuado de la red LAN así como también del acceso a la información que se tienen los servidores y bases de datos de la institución por ende éste es otro de los factores que incrementa el nivel de riesgo y vulnerabilidad de la red del Gobierno Regional de Apurímac.

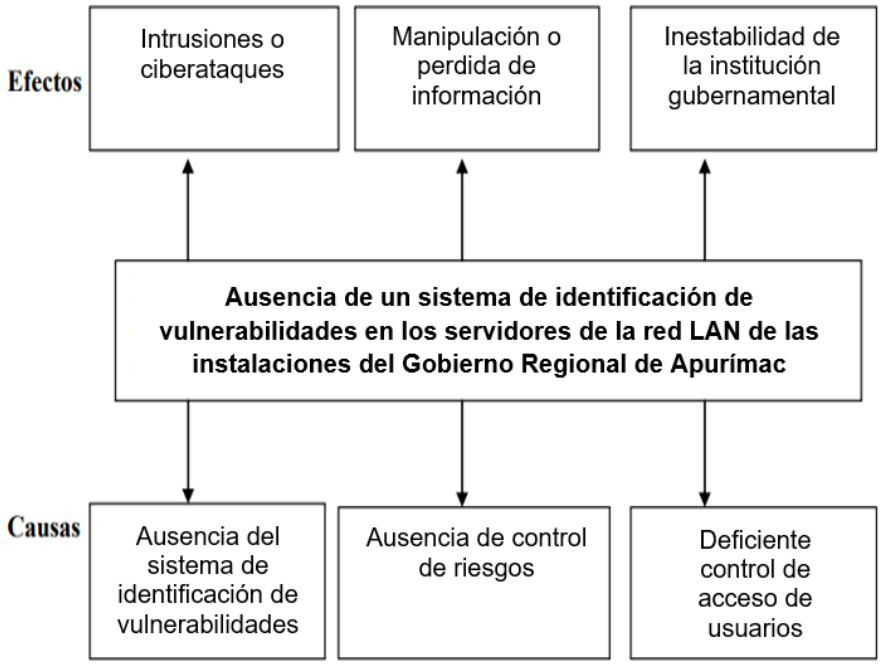
- En los resultados obtenidos con la recopilación de información se pudo evidenciar que la institución no realiza pruebas de ningún tipo que permitan identificar las vulnerabilidades que existen en la red LAN de la institución al indicar que no existe ningún tipo de pruebas también se pudo evidenciar que la institución no hace uso del hacking ético que es una herramienta que permite identificar dichas vulnerabilidades y riesgos que pueda presentar la red LAN de la institución como tal al no tener estas medidas de prevención la institución desconoce cuáles son los riesgos a los que está expuesto y los problemas que esto puede ocasionar.

- Una de las preguntas que generó el 100% de concordancia en los colaboradores del área de TIC del Gobierno Regional de Apurímac fue el consultar si consideran necesario la realización de mejoras que garanticen la seguridad en la red LAN de la institución donde todos los colaboradores encuestados mencionaron que si es necesario la implementación de dichas mejoras que permitan resguardar y asegurar la información que se tiene en los servidores y el manejo de la red LAN.

4.1.2.4. Árbol de problemas (causa/efecto)

Figura 17

Árbol causa efecto



- **Interpretación del árbol de problemas**

A nivel general las instituciones de tipo públicas y privadas hacen uso de los servicios de internet estos le permiten transmitir su información de manera rápida y eficiente, es evidente que la transformación e incremento de la tecnología actualmente facilita y genera grandes posibilidades para las empresas, ya que mediante la tecnología se puede llevar a cabo en menor tiempo posible las acciones y desarrollo de la gestión empresarial.

Sin embargo, pese a que la tecnología ha avanzado a grandes pasos, hoy en día es muy común su uso y hasta cierto punto indispensable para la sociedad, a nivel empresarial existe una preocupación por parte de los directivos de las empresas ya que actualmente ha crecido el número de ataques cibernéticos que ponen en riesgo la información y operación de las empresas.

Al inicio de los ataques cibernéticos estos serán realizados mediante benignas lo que quiere decir que este tipo de acciones en el peor de los casos lo que generaba en las instituciones empresariales eran ralentizar sus equipos tecnológicos conforme avanzó el tiempo y la mejora de tecnología los ataques fueron evolucionando junto con ellos y estos podrían llegar a dañar y colapsar sistemas o servidores completos, acceder a la información, eliminar archivos entre otros es decir que los ataques cibernéticos empezaron a ser destructivos y afectar en gran magnitud a la gestión empresarial de cualquier institución sea pública o privada.

En la actualidad el sistema empresarial depende cada vez más de las redes informáticas esto hace que las instituciones busquen las maneras necesarias para proteger y asegurar la información que manejan dentro de sus servidores y más aún las empresas gubernamentales que manejan información confidencial busca en la manera más óptima para asegurar sus sistemas informáticos y servidores.

Al identificar las causas y efectos que genera la problemática dentro de la Institución Gubernamental sujeta de estudio, se ha podido identificar como principal causa la ausencia del respectivo sistema de identificación de vulnerabilidades lo que inciden en incrementar los riesgos para la red con la que trabaja la institución y su principal efecto seria la incidencia potencial a la que se enfrenta ante las interrupciones

o ciberataques externos que puede afrontar la red de la institución, dejando totalmente vulnerable la información y todo lo que se encuentre dentro del sistema.

4.1.3. Pasos para aplicar la prueba de hacking ético

Tabla 16

Pasos pruebas hacking ético

PASOS	DESCRIPCION
Autorización firmada mediante un contrato	El contrato debe ser firmado por las autoridades principales de la Institución Gubernamental, este es un paso obligatorio para proceder con las pruebas.
Definir las reglas del procesos	- Pruebas 100% para el sistemas de la Institución Gubernamental - No se instalarán software secundarios en los equipos que se encuentran conectados a la red LAN. - Al ejecutar accesos no autorizados no se cubrirán las huellas - No se guardarán copias de la información obtenida en las pruebas en ningún equipo que se encuentre conectado a la red LAN del Gobierno Regional de Apurímac.
Planear el ataque	La duración de las pruebas y ataque se realizarán durante un aproximado de 30 días estas incluyen el análisis y pruebas en la red LAN cableada e inalámbrica.
Recopilación de información	Se procede a realizar la recopilación de la información más relevante de la institución esto se lo realiza mediante la herramienta Footprinting.
Reporte	Se presenta el reporte de los análisis y pruebas realizadas.
Presentación y planeación de mejoras.	Se presenta y explica los resultados del reporte final y se determinan los pasos a seguir para implementar mejoras en la red LAN.

La tabla muestra cuáles son los pasos que a seguir para llevar a cabo las pruebas correspondientes con la herramienta hacking ético, se debe considerar que en los pasos mencionados se han omitido factores como la eliminación de huellas ya que al ser una prueba autorizada no es necesario la eliminación de estas, los pasos a realizar permiten identificar las vulnerabilidades existentes en la red LAN de la

Institución Gubernamental regional de Apurímac con esto se pretende establecer cuáles son las falencias y los riesgos que se presentan para posteriormente dar solución y control de la disminución de riesgo.

4.1.3.1. Pruebas de hacking ético realizadas en el Gobierno Regional de Apurímac en busca de fallas y vulnerabilidad del sistema de la red LAN

Para llevar a cabo las pruebas de hacking ético se requirió el uso de un computador con el sistema operativo de la Institución Gubernamental en el cual se procedió a realizar la instalación de las herramientas que permitieron validar las pruebas cabe destacar que dichas pruebas fueron realizadas tanto en la red cableada y en la red inalámbrica de la institución, en dichas pruebas se tuvo como resultado varias vulnerabilidades en más del 80% de los equipos analizados que se encuentran conectado a la red LAN de la Institución Gubernamental, las vulnerabilidades y riesgos encontrados son los siguientes:

- Seguridad del sistema desactualizado.
- Existencia de varios puertos que son innecesarios.
- Carpetas compartidas inutilizadas.
- Impresoras compartidas que no cumplen el sistema y protocolo de seguridad.
- Red inalámbrica con bajas medidas de seguridad.
- Inexistencia de restricción de usuarios en el servicio web.
- Alto nivel de puntos de acceso a internet.
- Usuarios y contraseñas débiles con fácil acceso.
- Servidores de correos con inexistente protección.
- Servidores de bases de datos utilizados sin seguridad ni contraseñas de acceso.

- Activación de cuentas de invitados en más del 50% de equipos.
- Servidores http ejecutados en varios equipos y sin ser utilizados.

4.1.3.2. Resultado de las pruebas de hacking ético

Tabla 17

Resultados pruebas hacking ético

DIRECCIÓN IP	PUERTOS ABIERTOS	ADVERTENCIAS	AGUJEROS DE SEGURIDAD
209.45.107.211	5	1	3
209.45.107.212	8	0	1
209.45.107.217	6	1	1
209.45.107.218	3	1	2
209.45.107.219	3	1	2
209.45.107.220	3	1	2
209.45.107.225	3	2	2
209.45.107.240	3	1	2
209.45.107.246	7	2	1
209.45.107.248	4	1	2
209.45.107.249	3	2	2
209.45.107.250	4	1	2

Las pruebas realizadas mediante la herramienta hacking ético muestra la existencia de varias falencias y riesgos a las cuales están expuestas la red LAN y servidores del Gobierno Regional de Apurímac entre ella se ha seleccionado las principales direcciones IP con mayor número de puertos abiertos e incidencias que se pudieron localizar al realizar las pruebas correspondientes se puede apreciar que la mayor debilidad e inconsistencia que presenta el puerto LAN de la institución es la apertura de puertos mediante el cual puede acceder cualquier persona interna o externa ya que al encontrarse abierto no requiere de ningún tipo de usuario y contraseña por ende su acceso es inmediato y fácil para cualquier colaborador o usuario externo que quisiera acceder.

Tabla 18

Resultados pruebas hacking ético por equipo

DIRECCIÓN IP	ADVERTENCIA
209.45.107.211	Es posible enumerar recursos de red compartidos.
209.45.107.212	Es posible enumerar recursos de red compartidos.
209.45.107.217	El nombre de la comunidad SNMP puede ser consultado.
209.45.107.218	Es posible obtener acceso remoto al equipo.
209.45.107.219	Es posible enumerar recursos de red compartidos.
209.45.107.220	Es posible enumerar recursos de red compartidos.
209.45.107.225	Es posible obtener acceso remoto el equipo.
209.45.107.240	Es posible enumerar recursos de red compartidos.
209.45.107.246	Es posible en depender la impresión desde la red.
209.45.107.248	Si se trata de un router puede ser colgado por medio de una vulnerabilidad publicada.
209.45.107.249	El puerto acepta conexiones.
209.45.107.250	Es posible enumerar recursos de red compartidos.

Los resultados presentados muestran las inconsistencias que se dan en la red LAN de la institución y estos son factores que generan riesgo total y posibilitan los ataques cibernéticos hacia los servidores y bases de datos de la institución por lo tanto se ha procedido a realizar el análisis correspondiente de dichos factores y frente a este se han analizado las posibles mejoras es decir que con los resultados obtenidos tanto en el diagnóstico como el levantamiento de información y los resultados obtenidos con la aplicación de las pruebas de hacking éticos se procederá a analizar las principales mejoras que aportarán a reducir el riesgo y las vulnerabilidades que presenta el Gobierno Regional de Apurímac.

4.2. Diseño de la propuesta de mejora

4.2.1. Presentación y diseño de las acciones de las acciones de mejora

Tabla 19

Acciones de mejora

JERARQUÍA DE LAS MEJORAS	ACCIONES DE MEJORA	DESCRIPCION DE LAS ACCIONES DE MEJORA	IMPLEMENTACIÓN DE LA MEJORA
Primera estrategia de mejora	*Instalar software antivirus en todos los equipos.*	Para esta actividad se debe implementar y establecer actualizaciones diarias para brindar mayor seguridad y protección a los servidores y software.	Implementación permanente Actualización diaria
Segunda estrategia de mejora	*Instalar actualizaciones de seguridad en el sistema.*	Es de vital importancia instalar parches y actualización que incrementen la seguridad en los sistemas operativos de la institución, este proceso deberá ser ejecutado en los horarios donde exista menor tráfico en el uso de los servidores.	Horarios de descanso de los funcionarios Horarios nocturnos hoy en la madrugada.
Tercera estrategia de mejora	*Utilizar firewall que bloqueen los accesos en puertos abiertos.*	Esto consiste en instalar un programa que identifique los puertos abiertos que se encuentran sin utilizar y automáticamente lo bloquee denegando el acceso total ya sea por la red cableada o inalámbrica.	Implementación permanente Activación continua 24/7

Cuarta estrategia de mejora	*Crear cuentas de usuarios y contraseñas seguras y restringidas*	Implementar un sistema de selección de usuarios y contraseñas seguras estos deberán ser realizadas con al menos 8 caracteres mínimos que contengan números letras mayúsculas y minúsculas y deberán solicitar su cambio por lo menos cada 3 meses.	Actualización trimestral
Quinta estrategia de mejora	*Evitar la compartición de recursos en la intranet.*	Limitar y prohibir el uso de las cuentas administrativas para tareas personales o diarias para ello se requerirá restringir los permisos necesarios.	Limitación permanente
Sexta estrategia de mejora	*Implementar un sistema que permita encriptar la información para la red inalámbrica*	Esta actividad consistirá en hacer uso de los comandos de interpretación cuando se realice el uso de información de manera inalámbrica.	Implementación permanente Uso únicamente con el acceso de red inalámbrica
Séptima estrategia de mejora.	*Capacitar al personal acerca del adecuado uso y medidas de seguridad de la red LAN.*	Esta consiste en programar capacitaciones de manera trimestral para todo el personal de la institución donde se para la manipulación y acceso a la red.	Periodos trimestrales

Octava estrategia de mejora.	*Realizar análisis de vulnerabilidad media hacking ético en periodos programados.*	Esto consiste en realizar por lo menos dos veces al año ataques programados mediante el hacking ético para identificar posibles riesgos y vulnerabilidades en la red LAN.	Periodos semestrales
Novena estrategia de mejora.	*Restringir el acceso y permisos al personal según sus roles.*	Analizar y determinar los permisos y acceso a la información que tiene cada funcionario y delimitar dichos accesos según sus funciones laborales.	Actualizaciones mensuales
Decima estrategia de mejora	*Implementar políticas de seguridad.*	Definir las políticas de seguridad donde se identifique las reglas que debe seguir el personal que tiene acceso a los servidores e información delicada de la institución.	Implementación permanente

4.2.1.1. Principales resultados y análisis de las mejoras planteadas

Como se mencionó anteriormente las mejoras planteadas se establecieron a raíz de los análisis correspondiente al diagnóstico y levantamiento de información y principalmente con los resultados obtenidos en las pruebas realizadas con el hacking ético y es importante analizar cada una de las mejoras que se plantearon para entender con mayor facilidad en qué consiste y el aporte que brindarán ante la reducción de las vulnerabilidades y riesgos de la red LAN del Gobierno Regional de Apurímac y así también determinar la implementación de cada una de las acciones.

- **Instalar software antivirus en todos los equipos**

Esta actividad de mejora consiste en implementar y establecer actualizaciones diarias en el software de los equipos con los que cuenta el Gobierno Regional de Apurímac y de esta manera podré generar mayor seguridad y protección a los servidores y la red LAN de la institución, es decir que al contar con actualizaciones automáticas y permanente de los antivirus se reducen las posibilidades de cualquier ataque cibernético que pueda recibir la institución ya que los principales ataques son mediante virus que se esparcen en los servidores por esta razón es importante que el software de antivirus está implementado permanentemente en todos los equipos de la institución y además se los actualice de manera automática y diaria.

- **Instalar actualizaciones de seguridad en el sistema**

La actividad de mejora en cuanto a las actualización de seguridad en el sistema es considerada importante y vital por lo cual se requiere instalar parches y actualizaciones que mejoren la seguridad de los sistemas operativos con los que cuenta la institución dentro de este proceso se deberán determinar y ejecutar los horarios para dichas actualizaciones los cuales deben ser horarios donde exista menor tráfico de uso de los servidores o de preferencia un uso nulo de ellos, y además de esta manera no se interfiere en la gestión diaria realizada por los colaboradores de la Institución Gubernamental Regional.

Tomando en consideración las observaciones antes mencionadas y para mayor seguridad de las actualizaciones realizadas al sistema es necesario realizar la implementación de dichas actualizaciones en horarios nocturnos o de preferencia en la madrugada, es decir que el técnico responsable deberá programar de manera automática las actualizaciones en todos los equipos y servidores de la institución.

- **Utilizar firewall que bloqueen los accesos en puertos abiertos**

Para la mejora presentada es importante que el Gobierno Regional de Apurímac de programas automatizados que bloqueen los accesos a los puertos abiertos es decir que dicho programa identifique automáticamente cuando exista un puerto habilitado y sin uso permitido de tal manera que el proceso sea bloquear y denegar el acceso total a dicho puerto este programa deberá identificar puertos abiertos tanto en la red cableada como inalámbrica de manera que se reducirá el riesgo de acceso a la información y a los servidores por estos canales.

La implementación de esta actividad de mejora se deberá realizar de manera permanente es decir que se establecerá en los servidores y equipos tecnológicos de la institución el programa correspondiente que detecte los puertos abiertos y los bloquea automáticamente y el mismo debe funcionar de manera automática 24 horas 7 días así se garantizará la fiabilidad y seguridad de proteger los puertos abiertos en la red LAN de la Institución Gubernamental.

- **Crear cuentas de usuarios, contraseñas seguras y restringidas**

En esta actividad de mejora es necesario implementar un sistema de selección de usuarios el cual de manera segura identifique los usuarios que menor riesgo generen al momento de presentar cualquier tipo de jaqueo, de la misma manera se procederá a informar a los colaboradores que la creación de las contraseñas deberán tener un alto grado de dificultad para ser jaqueadas por lo tanto las contraseñas deberán contar con mínimo ocho caracteres y dentro de ellos se deberá tener números y letras mayúsculas y minúsculas que garanticen la fiabilidad y seguridad de los usuarios y contraseñas teniendo un alto nivel de dificultad de acceso para usuarios

externos la implementación o actualización de las claves deberán ser trimestrales es decir que los colaboradores deberán cambiar cada tres meses la contraseña.

- **Evitar la compartición de recursos en la intranet**

Una actividad de mejoras que se ha planteado para evitar la compartición de recursos en la intranet es limitar y prohibir el uso de las cuentas administrativas para realizar las tareas personales y diarias de los colaboradores es decir que las cuentas administrativas únicamente tengan acceso e interacción con la gestión interna del Gobierno Regional de Apurímac por ello se establece la restricción de permisos entre los usuarios y colaboradores, la limitación y restricción de los permisos debe ser implementado de manera permanente y para todos los colaboradores de la institución según los permisos que concedan en base a sus funciones.

- **Implementar un sistema que permiten encriptar la información para la red inalámbrica**

La encriptación de información que se genere y transfiera de manera inalámbrica permitirá reducir el nivel de vulnerabilidad existente en este canal por ello esta actividad consiste en hacer uso de los comandos de interpretación cuando se realice el uso transferencia de información en modo inalámbrico, los comandos de interpretación son los encargados de incrementar toda la información que se maneje y se establezca dentro de dicho comando de esta manera únicamente los usuarios que tengan los permisos necesarios podrán visualizar y acceder a la información mediante el comando correspondiente.

El periodo o la implementación a llevar a cabo será de manera permanente y el uso de estos comandos se lo realizará únicamente con el acceso y transferencia de información mediante la red inalámbrica la actualización y verificación de dichos comandos se lo realizará de manera mensual para validar la seguridad y validez de la información encriptada.

- **Capacitar al personal acerca del adecuado uso y medidas de seguridad de la red LAN**

La capacitación a todo el personal del Gobierno Regional de Apurímac es indispensable para garantizar la seguridad de la red LAN y servidores de la institución debido a que es necesario que todo el personal conozca cuáles son las normas establecidas a las que se debe regir su uso y manipulación de los equipos e información a la cual tiene acceso la institución, esta actividad consiste en implementar programas de capacitación de manera trimestral para todo el personal donde se enfoque el correcto uso y manipulación de la información así como también el acceso a la red de la institución.

- **Realizar análisis de vulnerabilidad mediante hacking ético en periodos programados**

La actividad de realizar y llevar a cabo los análisis y verificación de vulnerabilidad de la red LAN mediante el hacking ético consiste en realizar por lo menos 2 veces al año las pruebas correspondientes a los ataques programados mediante esta herramienta de tal manera que se pueda conocer los riesgos y vulnerabilidades de la red para tomar medidas y acciones correctivas, el periodo de implementación se recomienda realizarlo de manera semestral ya que esto permite

controlar cualquier eventualidad que se enfrente ante los ataques cibernéticos o cualquier tipo de pérdida de información que se pueda dar en el sistema.

- **Restringir el acceso y permisos al personal según sus roles**

La actividad de restringir el acceso y permisos al personal dependiendo sus funciones y roles laborales consiste como primer paso analizar y determinar cuáles son las funciones de cada uno de los colaboradores y de aquí verificar los accesos correspondientes y necesarios para el desarrollo de sus actividades de esta manera al existir accesos información o servidores que no competen a sus funciones se debe delimitar dichos accesos, el periodo de implementación de estas actividades es necesario realizarlo de manera mensual es decir que mensualmente será una actualización para verificar si la limitación de acceso genera conflicto o retrasos en las actividades laborales de los funcionarios.

- **Implementar políticas de seguridad**

Es fundamental dentro de todo este proceso realizar la implementación de políticas de seguridad cuya actividad consiste en que las autoridades y directivos correspondientes de la institución juntamente con el área de TIC analicen y definan las políticas de seguridad que ayuden a resguardar y reducir los riesgos de pérdidas de información al igual que la reducción de vulnerabilidad de la red LAN, para ello es importante dar a conocer e identificar claramente las reglas que deben ser seguidas por todo el personal en especial aquellos que tengan acceso a los servidores de información del Gobierno Regional de Apurímac, la implementación de las políticas deberá ser de manera permanente y obligatoria para todo el personal.

Las actividades antes mencionadas deben ser llevadas a cabo según lo especifica la matriz de la propuesta de mejora, y es importante considerar que al realizar dichas actividades el Gobierno Regional de Apurímac podrá contar tus mejores niveles de seguridad en su red LAN, es decir que al ser consciente de las vulnerabilidades que presenta su sistema y tomar medidas correctivas logrará garantizar la seguridad correspondiente de la información y servidores de la institución además que esto garantizará que el Gobierno Regional de Apurímac tenga las medidas correspondientes para afrontar cualquier ataque cibernético que se pudiera presentar, por lo que la pérdida de información o alteración de la misma ya no representaría un riesgo importante para su gestión.

4.3. Establecimiento de los mecanismos de control

Tabla 20

Mecanismos de control para la propuesta de mejora

ACCIONES DE MEJORA	MECANISMOS DE CONTROL	RESPONSABLES DEL CONTROL	FORMA DE IMPLEMENTACIÓN
Instalar software antivirus en todos los equipos	Tiempo promedio para porcentaje de eficiencia en el mantenimiento de equipos.		Implementación permanente Actualización diaria
Instalar actualizaciones de seguridad en el sistema	Número de incidentes presentados en periodos trimestrales.		Horarios de descanso de los funcionarios Horarios nocturnos hoy en la madrugada
Utilizar firewall que bloqueen los accesos en puertos abiertos	Porcentaje de efectividad de control de acceso.	Departamento técnico	Implementación permanente Activación continua 24/7

Crear cuentas de usuarios y contraseñas seguras y restringidas	Porcentaje de eficiencia de administración de usuarios		Actualización trimestral
Evitar la compartición de recursos en la intranet	Número de dispositivos conectados a la red no autorizados	Jefes de áreas	Limitación permanente
Implementar un sistema que permita encriptar la información para la red inalámbrica.	Promedio del nivel de riesgo		Implementación permanente Uso únicamente con el acceso de red inalámbrica
Capacitar al personal acerca del adecuado uso y medidas de seguridad de la red LAN.	Porcentaje de productividad y eficiencia	Recursos humanos	Periodos trimestrales
Realizar análisis de vulnerabilidad media hacking ético en periodos programados.	Número de vulnerabilidades existentes	Departamento técnico	Periodos semestrales
Restringir el acceso y permisos al personal según sus roles.	Promedio de nivel de riesgos		Actualizaciones mensuales
Implementar políticas de seguridad.	Tasas de fallas mensuales	Directivos	Implementación permanente

4.3.1.1. Análisis e interpretación de los mecanismos de control

Los mecanismos de seguimiento y control son indicadores que sirven como herramienta para poder verificar el cumplimiento de las acciones o actividades propuestas y verificar los resultados que estos generan a partir de su desarrollo, es decir que mediante estos indicadores se puede determinar si las acciones realizadas representan un factor positivo ante la mitigación de la problemática presentada, o caso contrario se requiere tomar mayores medidas correctivas que incidan en la reducción de la problemática o acontecimientos que se han presentado, por consiguiente en la presente investigación y posterior al desarrollo de las actividades a realizar para la mejora correspondiente se establecen los siguientes mecanismos de control.

En la mejora realizar con la instalación del software antivirus en todos los equipos del Gobierno regional Apurímac sea considerado como la mejor medida de control la identificación del tiempo promedio para porcentaje de eficiencia en el mantenimiento de equipos, es decir que mediante este mecanismo de control se deberá identificar en caso de existir cualquier falencia de inconveniente en los equipos debido a los virus el tiempo que toma el realizar el mantenimiento del equipo, ya que al tener instalado un software antivirus el daño que éstos puedan provocar deberá ser menor y por ende su tiempo de reparación o mantenimiento del equipo también deberá reducir al punto de ser una solución inmediata, el responsable de llevar esta actividad a cabo será el departamento de TIC.

Una vez puesta a cabo la acción de mejora en cuanto a la instalación de actualizaciones en la seguridad del sistema de la institución la medida de control establecida para dicha actividad es determinar el número de incidentes presentados en periodos trimestrales, es decir que el responsable a cargo deberá analizar y emitir

un informe identificando si el número de incidentes que representen inseguridad en el sistema se han incrementado o disminuido a partir de la actualización de seguridad de este es decir que esta medida de control deberá de identificar que existe una disminución en dichos incidentes y esta actividad será llevado a cabo por un colaborador del departamento de TIC.

En cuanto a la mejora presentada qué es el uso de firewall con los cuales se establezca un programa que permita bloquear el acceso a los puertos abiertos de manera automática e inmediata al ser detectado se establece como medida de control el porcentaje de efectividad de control de acceso es decir que el responsable a cargo deberá analizar a manera general mensualmente los accesos bloqueados por los firewall implementados analizando y determinando el tiempo que le toma al programa identificar la apertura del puerto así como también el tiempo que tarda en realizar el bloqueo de este, de la misma manera que las actividades anteriores esta estará a cargo de un colaborador del área de TIC.

En cuanto a la mejora de crear cuentas de usuarios y contraseñas seguras y sobre todo restringidas para usuarios externos que se dificulte su jaqueo o acceso se ha implementado como medida de control el porcentaje de eficiencia de administración por parte de los usuarios es decir que mediante este indicador se deberá analizar la eficiencia y responsabilidad con la que los colaboradores realizan la selección de sus contraseñas y resguardan su información.

Esta actividad de la misma manera deberá ser controlada por un colaborador del área de TIC sin embargo los colaboradores deberán tener conocimiento del requerimiento de la actualización y cambio de sus contraseñas de manera trimestral, por medio de estos acciones se logrará reducir los posibles saqueos de usuarios y contraseñas de los colaboradores ya que al tener un cambio constante y no repetitivo de sus contraseñas genera mayor seguridad.

Para evitar la compartición de recursos en la intranet se ha presentado el indicador de seguimiento y control el número de dispositivos conectados a la red no autorizados es decir que esta actividad se complementa con el uso de firewall ya que mediante el mismo programa se podrá analizar cuáles han sido los dispositivos que se han conectado a los servidores o red LAN de la Institución Gubernamental sin tener autorización y poder tomar las medidas correctivas de manera inmediata, para llevar a cabo la responsabilidad de esta actividad sea considerado el jefe de cada área correspondiente en el Gobierno Regional de Apurímac.

Es decir que en cada área el jefe inmediato de manera permanente y según lo considere necesario debe analizar la compartición de recursos en la intranet que han sido efectuadas por los colaboradores que se encuentren a su cargo, posterior a ellos deberá levantar las limitaciones pertinentes y de manera permanente para que no se pueda realizar dicha compartición que exponga la información de la institución.

En la implementación de un sistema que permiten captar la información de la red inalámbrica se ha establecido como medida de seguimiento y control el promedio del nivel de riesgo de igual manera esta actividad deberá ser analizada y controlada por los jefes inmediatos de cada área de la institución, quienes presentarán un informe indicando la eficiencia de los comandos utilizados para la encriptación de información

que se usa y transfiere por medio de equipos conectados a la red inalámbrica, dentro del informe pertinente deberá identificar el nivel de riesgo que genera esta actividad para la información que se transfiere.

Para la actividad de capacitación al personal referente a los temas de uso y medidas de seguridad en cuanto a la red LAN sea seleccionado como seguimiento y control de esta actividad la verificación de porcentajes de productividad y eficiencia en el desarrollo de las actividades laborales que intervienen con el uso de la red LAN y servidores de la institución es decir que al contar con el personal debidamente capacitado con las medidas de seguridad el manejo de la información y de la red deberá ser óptimo por lo cual la gestión realizada por los colaboradores deberá notar mayor productividad y eficiencia en los resultados obtenidos.

Dentro de la propuesta de mejora también se planteó realizar un análisis de vulnerabilidad mediante la herramienta hacking éticos la cual debe ser realizada en periodos programados es por ello que para esta actividad se estableció como métrica de control el número de vulnerabilidades existentes, es decir que cómo será una actividad que permita identificar los riesgos a los cuales se encuentra expuesto la red LAN de la institución y al ser realizados en periodos semestrales los resultados obtenidos deberán mostrar reducción constante de las vulnerabilidades ya que cada vez que sean realizadas las pruebas correspondientes con esta herramienta la institución deberá tomar en consideración los riesgos e implementar medidas de mejoras y seguridad para su sistema y la red LAN.

Por lo que como personal responsable a cargo de la actividad se ha definido al departamento de TIC quien deberá realizar un análisis comparativo con los informes semestrales de las vulnerabilidades presentadas y definir si existe una reducción continua frente a los riesgos que pueda tener la red, además de analizar si las medidas correctivas que se toman posterior a cada prueba generan los resultados que se espera para mitigar o mejorar los riesgos y vulnerabilidades.

La restricción de acceso y permisos al personal según sus funciones laborales tiene como medida de control el promedio de nivel de riesgos es decir que al limitar el acceso y permiso a los colaboradores según lo requieran sus funciones automáticamente debe disminuir el riesgo de pérdida de información, adulteración de información entre otras, es decir que al existir un correcto y adecuado uso de la información por parte del personal y no exponer toda la información a libre acceso de los colaboradores disminuye los riesgos que se puedan presentar y como tal el responsable a cargo de llevar esta actividad de control deberá realizar un informe de manera mensual y hacer un análisis comparativo de estos identificando el porcentaje de reducción de estos riesgos.

Con la actividad de mejora de implementación de políticas de seguridad al ser presentadas está para todo el personal dentro de la institución de Gobierno regional Apurímac la métrica de control será la tasa de fallas mensuales es decir que como los colaboradores tienen pleno conocimiento de las normas y políticas de seguridad establecidas por la institución éstas deben ser llevadas a cabo y por ende la tasa de fallas deberá disminuir de manera importante y para esto el responsable deberá identificar la reducción de dichas fallas y la aplicación de las políticas de seguridad.

4.4. Estimación de la inversión para la propuesta de mejora

Tabla 21

Costo económico de la propuesta de mejora

PROCESO DE MEJORA	DESCRIPCIÓN	COSTO POR EQUIPO	CANTIDAD	COSTO TOTAL
Hacking ético	- Sistema operativo	S/ 350,00	38	S/13.300,00
	- Instalación del sistema operativo	S/150,00	38	S/5.700,00
	- Configuración	S/150,00	38	S/5.700,00
Capacitación	- Todo el personal	S/3.500,00	--	S/3.500,00
	VALOR TOTAL			**S/28.200,00**

4.4.1. Análisis e interpretación del costo económico de la propuesta de mejora

La propuesta de mejora realizada para el Gobierno Regional de Apurímac se enfoca en mejorar la seguridad de la red LAN, la misma que carece de medidas de seguridad teniendo un alto riesgo de pérdida de información al igual que la modificación de esta e inseguridad frente a los robos informáticos, considerando que estas actividades involucran el uso de una herramienta llamada hacking ético mediante el cual se puede llevar a cabo pruebas de ataques a la red, la propuesta de mejora y por ende el costo que implica su implementación consta del uso e implementación de la herramienta la cual permiten llevar a cabo las actividades de mejora que se desarrollaron en la propuesta y adicional a ella se establece también el costo que representa las capacitaciones al todo el personal de la institución.

A razón de lo expuesto se determinó que te entró de la utilización e implementación de la herramienta hacking ético intervienen tres factores que determinan el costo de esta herramienta el principal es el sistema operativo el cual debe ser instalado en todos los equipos que se encuentren en esta institución para poder llevar a cabo las mejoras correspondientes que se presentaron en la propuesta dentro de este factor también interviene canción del sistema operativo y adicional su configuración cada uno de estos ítems mencionados corresponde a un valor que ha sido detallado en la tabla correspondiente al costo de la propuesta al igual que el valor económico que representa la realización de las capacitaciones a impartir.

Tomando en consideración todos los gastos que involucra el desarrollo de la propuesta de mejora y su implementación se determina que el total del costo de la propuesta es de 28.200 soles, al considerar que las instituciones públicas tienen un presupuesto designado de manera anual, se puede indicar que el valor económico de la propuesta es accesible para su implementación.

4.4.2. Beneficios económicos de la propuesta de mejora

Tabla 22

Monetización de los beneficios de la propuesta de mejora

	AHORRO ECONOMICO APLICANDO LA MEJORA	
-	Incremento en la seguridad de la red LAN.	S/3.500,00
-	Reducción en la modificación y pérdida de información.	S/4.000,00
-	Mejora de la gestión interna.	S/4.800,00
-	Personal capacitado en cuanto a las políticas de seguridad.	S/4.000,00
-	Optimización de tiempo y recursos.	S/5.000,00
-	Eficiencia y productividad.	S/5.000,00
	TOTAL	**S/26.300.00**

- **Interpretación**

Se presenta la monetización de beneficios considerando que al realizar una inversión económica con la implementación de la propuesta de mejora a más de garantizar la seguridad de la red LAN, todas las acciones tomadas también representan un incremento en la gestión interna de la institución, es decir qué se tendrá beneficios económicos puesto que mediante las acciones realizadas se optimizará el tiempo y recursos e incrementará la eficiencia y productividad de los colaboradores gracias al nivel de capacitación que se implementará para ellos y con esto todas las gestiones realizadas por el personal al igual que el rendimiento y productividad del sistema o la red LAN del mineral los gastos económicos por errores cometidos de tipo humano y fallas técnicas.

La monetización de beneficios muestra claramente que al contar con una herramienta efectiva que determine la vulnerabilidad y riesgos de la red LAN se podrá optimizar los recursos económicos que se empleaban en solventar y subsanar las fallas existentes por ende cada una de las acciones y beneficios aportan también un grado de recuperación y optimización económica para el Gobierno Regional.

CONCLUSIONES

Mediante el diagnóstico realizado se concluye que actualmente el Gobierno regional Apurímac no cuenta con normas ni herramientas de verificación de riesgos y vulnerabilidad de la red LAN que ocupa para el desarrollo y gestión de las actividades internas de la institución, razón por la cual se han presentado una serie de problemas que afectan directamente su gestión y seguridad de la red LAN, ya que se ha evidenciado que existe un alto índice de riesgo en cuanto a la pérdida y modificación de información, como también existe una deficiente mejora de la seguridad de la red, lo que provoca que esté expuesta a ataques cibernéticos en los cuales pueda perder absolutamente toda la información que resguardan sus servidores y base de datos que se encuentran enlazada a la red LAN.

Con el diseño y desarrollo de la propuesta de mejora hacia la seguridad de la red LAN del Gobierno Regional de Apurímac haciendo uso de la herramienta Hacking Ético, se concluye que fue necesario realizar una serie de pruebas que identifiquen las vulnerabilidades que presenta la red de la institución y posterior a ello se identificaron cuáles son los riesgos a los que se enfrenta con el análisis correspondiente de la recopilación de información y los resultados obtenidos mediante esta herramienta se planteó una serie de acciones de mejora que conllevan a resguardar e implementar la seguridad de la red LAN protegiendo los datos y toda la información que se encuentran en los servidores y bases de datos de la institución que están enlazado a esta red.

Por medio de los mecanismos de seguimiento y control que se establecieron para las actividades de mejoras designadas a mejorar la seguridad de la red LAN del Gobierno Regional de Apurímac, se concluye qué estos mecanismos son de vital importancia en la implementación de la propuesta ya que con ello se podrá verificar el cumplimiento indicado de las acciones a realizar y además se puede identificar y analizar los resultados obtenidos a partir de la implementación de la propuesta lo que garantiza un mayor éxito para alcanzar el objetivo planteado que es mejorar la seguridad de la red la de esta Institución Gubernamental.

Como conclusión final se establece que la propuesta de mejora diseñada representa un valor económico que es accesible para el presupuesto de la Institución Gubernamental, por lo que al realizar su implementación la institución obtendrá varios beneficios que mejorarán sin lugar a dudas las normas y medidas de seguridad en la red de uso y además generarán un mayor rendimiento en el desarrollo de las actividades internas de la institución, esto gracias al aporte que dará las acciones de mejora a la red y a los equipos que se encuentran conectados a está generando mayor eficiencia y efectividad en las acciones y actividades laborales realizadas.

RECOMENDACIONES

Se sugiere a las autoridades correspondientes Del Gobierno regional Apurímac realizar el respectivo reconocimiento de la estructura de la red designando al personal correspondiente del área de TIC para poder determinar el estado de la infraestructura de su red cableada e inalámbrica de tal manera que pueda identificar cuáles son las falencias en cuanto a la estructura física que requieran mejoras o cambios correspondientes y que incidan en los riesgos o vulnerabilidad que presente la red LAN del Gobierno Regional de Apurímac.

Se sugiere al área técnica de TIC establecer un cronograma y definir las fechas periódicamente en la cual deban realizar escaneos que identifiquen las características internas de la red LAN de la institución esto va a permitir que los técnicos correspondientes al área conozcan cuál es el estado interno de la red y si requiere actualizaciones o verificación de cualquier falencia que se presente y afecte la vulnerabilidad del acceso a la red e información.

Se sugiere a los analistas de TIC verificar cuáles son las necesidades presentadas por los colaboradores en cuanto a la red LAN de la institución esto con la finalidad de seleccionar, instalar y configurar las aplicaciones que solventen dichas necesidades o requerimientos y además mejoren las posibilidades de reducir los riesgos y vulnerabilidades de la red y los servidores de uso diario por parte de los colaboradores de la Institución Gubernamental Regional de Apurímac.

Se sugiere a los directivos y representantes de la institución implementar de manera continua las pruebas de riesgo y vulnerabilidad de la red LAN de la institución, ya que esto va a permitir que los colaboradores correspondientes al área de TIC tengan en conocimiento absoluto cuáles serán las principales actividades a realizar para mitigar los riesgos definidos con las pruebas y además estén preparados para solventar de la mejor manera un ataque cibernético que le permita resguardar la información que se mantiene en las bases de datos y servidores sin riesgos de pérdida o alteraciones de información en el Gobierno Regional de Apurímac.

Se sugiere además llevar a cabo los métodos planteados con la finalidad de verificar que se cumpla cada una de las actividades propuestas a beneficio y resguardo de la red LAN de la institución, por lo que es importante que cada departamento o área correspondiente seleccione a los responsables de llevar a cabo el seguimiento y control así como también la presentación de los análisis y resultados obtenidos a partir de la implementación de la propuesta de mejora que se realizó posterior a las pruebas mediante la herramienta hacking ético. Es analizar los periodos o fechas de implementación de cada una de las estrategias tomando en consideración que debe existir actualizaciones constantes y verificación de los resultados por ello es importante que dichas acciones sean llevadas e implementadas según se lo estipula en la propuesta de mejora.

Se sugiere examinar y controlar los dispositivos y equipos electrónicos que se encuentren conectado a la red LAN de la institución con la finalidad de identificar que estos se encuentran funcionando de manera adecuada que no interfiera ni afecte a la red convirtiéndose en un punto vulnerable o acceso de riesgo que permita ingresar a usuarios externos a los servidores o bases de datos de la institución por ello es importante analizar y dar mantenimiento continuo a todos los equipos instalados y que se encuentren conectados mediante cable o con la red inalámbrica, esto generará mayor seguridad para el Gobierno Regional de Apurímac.

Como última sugerencia se la realiza a los directivos y responsables de la Institución Gubernamental Regional de Apurímac indicando la consideración del valor económico de la propuesta dentro del presupuesto correspondiente al vigente año para proceder con su implementación y mejoras correspondientes las cuales traerá consigo grandes beneficios que aportarán a mejorar la gestión interna de la institución así como también garantizar una red LAN segura y confiable para el manejo y almacenamiento de información.

BIBLIOGRAFÍA

Aguilera, P. (2011). *Seguridad Informática.* Edietx. https://books.google.com.ec/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=seguridad+informatica+articulos&ots=PrpmRzDGZ5&sig=AqwTMfIFbF0BFGVjhhPjyn3lzro#v=onepage&q=seguridad%20informatica%20articulos&f=true

Álvarez, M., & Pérez, G. (2004). *Seguridad informática para empresas y particulares.* McGraw-Hill. https://fliphtml5.com/oazu/cgdk/basic

Aranda, M. (2022). *Metodología de Hacking Ético.* AIEP de la Universidad Andrés Bello: https://1library.co/document/q5n33gjq-metodologias-de-hacking-etico.html

Baca, G. (2016). *Introducción a la Seguridad informática.* Grupo Editorial Patria. https://books.google.com.ec/books?id=IhUhDgAAQBAJ&printsec=copyright#v=onepage&q&f=true

Bernal, C. (2010). *Metodología de la Investigación* (3a ed.). Bogotá: Pearson. https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf

Casa, J., Repullo, J., & Donado, J. (2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos. *ELSEVIER, 31*(8), 527-538. https://www.elsevier.es/es-revista-atencion-primaria-27-articulo-la-encuesta-como-tecnica-investigacion--13047738

Costas, J. (2011). *Seguridad y Alta Disponibilidad.* Ra-Ma. https://www.academia.edu/8334995/Seguridad_y_Alta_Disponibilidad_RAMA

Esaú, A. (30 de septiembre de 2015). *Tutorial hacking: Razones para hacer un Pentesting a nuestra empresa*. OpenWebinars:

https://openwebinars.net/blog/Tutorial-hacking-razones-para-realizar-un-pentesting-a-nuestra-empresa/

Escriva, G., Romero, S., & Ramada, D. (2013). *Seguridad Informática.* Madrid: Grupo Macmillan.

Florez, J. (2017). *Metodología para realizar hacking ético en bases de datos para Positiva Compañía de Seguros S.A en la ciudad de Bogotá.* Tesis de Grado. Universidad Nacional Abierta y a Distancia . https://repository.unad.edu.co/bitstream/handle/10596/17375/19418118.pdf?sequence=1&isAllowed=y

García, M. (2017). *Seguridad Informatica y el malware.* Universidad Piloto de Colombia: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2641/00004128.pdf?sequence=1&isAllowed=y

Gobierno Regional de Apurimac. (2022). *DATOS GENERALES*. Gobierno Regional de Apurimac GR-Apurimac: https://www.transparencia.gob.pe/enlaces/pte_transparencia_enlaces.aspx?id_entidad=10130&id_tema=1&ver=D#.Y37k73bMLIU

Gomez, A. (2017). *Enciclopedia de la Seguridad Informática* (2a ed.). Madrid: RA-MA. https://books.google.com.ec/books?id=Bq8-DwAAQBAJ&printsec=frontcover&dq=Enciclopedia+de+la+Seguridad+Inform%C3%A1tica+Gomez&hl=es-419&sa=X&ved=2ahUKEwib6P6694P6AhXnQzABHQ8BCB4Q6AF6BAgLEAI#v=onepage&q=Enciclopedia%20de%20la%20Seguridad%20Inform%C3%A1tica%

Guillén, J. (20 de julio de 2017). *Introducción al pentesting.* Universitat de Barcelona: http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf

Huaylla, A., & Vargas, M. (s.f.). *Gestión de tecnologías de información y comunicación y los procesos de seguridad informática en el Gobierno Regional de Apurimac, 2021.*

Huilca, G. (2012). *Hacking ético para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.* Tesis de Grado. Universidad Técnica de Ambato. https://repositorio.uta.edu.ec/bitstream/123456789/2900/1/Tesis_t764si.pdf

Kaspersky Lab. (2022). *¿Qué es la ciberseguridad?* kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Macías, B. (2021). *Aplicación de Hacking Ético para la determinación de amenazas riesgos y vulnerabilidades en la red wifi de la Universidad Estatal del sur de Manabí.* Universidad Estatal del Sur de Manabí. http://repositorio.unesum.edu.ec/bitstream/53000/3062/1/TESIS%20DE%20-%20MACIAS%20PICO%20BRYAN.pdf

Mamami, D. (2013). Fases de un Ataque Hacker. *Revistas Bolivianas*. http://www.revistasbolivianas.ciencia.bo/pdf/rits/n8/n8a29.pdf

Medina, E. (2020). *Hacking Ético: Una herramienta para la seguridad informática.* Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00002050.pdf

Molinetti, S. (23 de septiembre de 2020). *Descubre las principales medidas de seguridad en una red LAN*. Telefonica: https://empresas.blogthinkbig.com/medidas-de-seguridad-en-una-red-lan/

Ortiz, B. (2015). *Hacking ético para detectar fallas en la seguridad informática de la intranet del Gobierno Provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGSI), basado en la Norma ISO/IEC 27001:2005.* Tesis de Grado. Universidad Técnica del Norte. http://repositorio.utn.edu.ec/bitstream/123456789/4332/1/04%20RED%20045%20TESIS.pdf

RED CEDIA. (2018). *Gestión de la seguridad de la información.* Escuela Superior de Redes RED CEDIA: https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI8.pdf

Rodriguez, A. (2020). Herramientas fundamentales para el hacking ético. *RCIM, 12*(1), 116-131. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592020000100116#:~:text=El%20hacking%20%C3%A9tico%20es%20una,que%20m%C3%A1s%20adelante%20se%20presentar%C3%A1n.

Rodríguez, A. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica, 12*(1), 116-131. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592020000100116

Rodríguez, E. (2021). Diseño de una red de área local (LAN). *Revista Científica Multidisciplinaria , 5*(4), 143-150. https://doi.org/https://doi.org/10.47230/unesum-ciencias.v5.n4.2021.583

Samaniego, E., & Ponce, J. (2021). *Fundamentos de seguridad informática.* Grupo Compás. https://www.researchgate.net/publication/354054517_Libro_Fundamentos_de_seguridad_informatica

Sampieri, R., Fernandez, C., & Baptista, P. (2006). *Método de la investigación* (Cuarta edición ed.). México: McGrawHill.

Sánchez, M. (2019). *Hacking Ético: Impacto en la Sociedad.* Universidad Piloto de Colombia: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4919/00005096.pdf?sequence=1&isAllowed=y

Tufiño, A. (2018). *Diseño de un Modelo de Seguridad de Informacion en Redes LAN.* Tesis de Grado. Pontificia Universidad Católica Del Ecuador. http://repositorio.puce.edu.ec/bitstream/handle/22000/15420/Tesis%20Ana%20Cristina%20Tufi%c3%b1o%20Galan%20Version%20Final.pdf?sequence=1&isAllowed=y

UNIR. (11 de febrero de 2020). *¿Qué es el hacking ético y cómo se realiza?* Ingeniería y Tecnología: https://www.unir.net/ingenieria/revista/hacking-etico/

UNIR. (5 de marzo de 2020). *CEH (Certified Ethical Hacker): ¿en qué consiste esta certificación?* INGENIERÍA Y TECNOLOGÍA: https://www.unir.net/ingenieria/revista/ceh-certified-ethical-hacker/

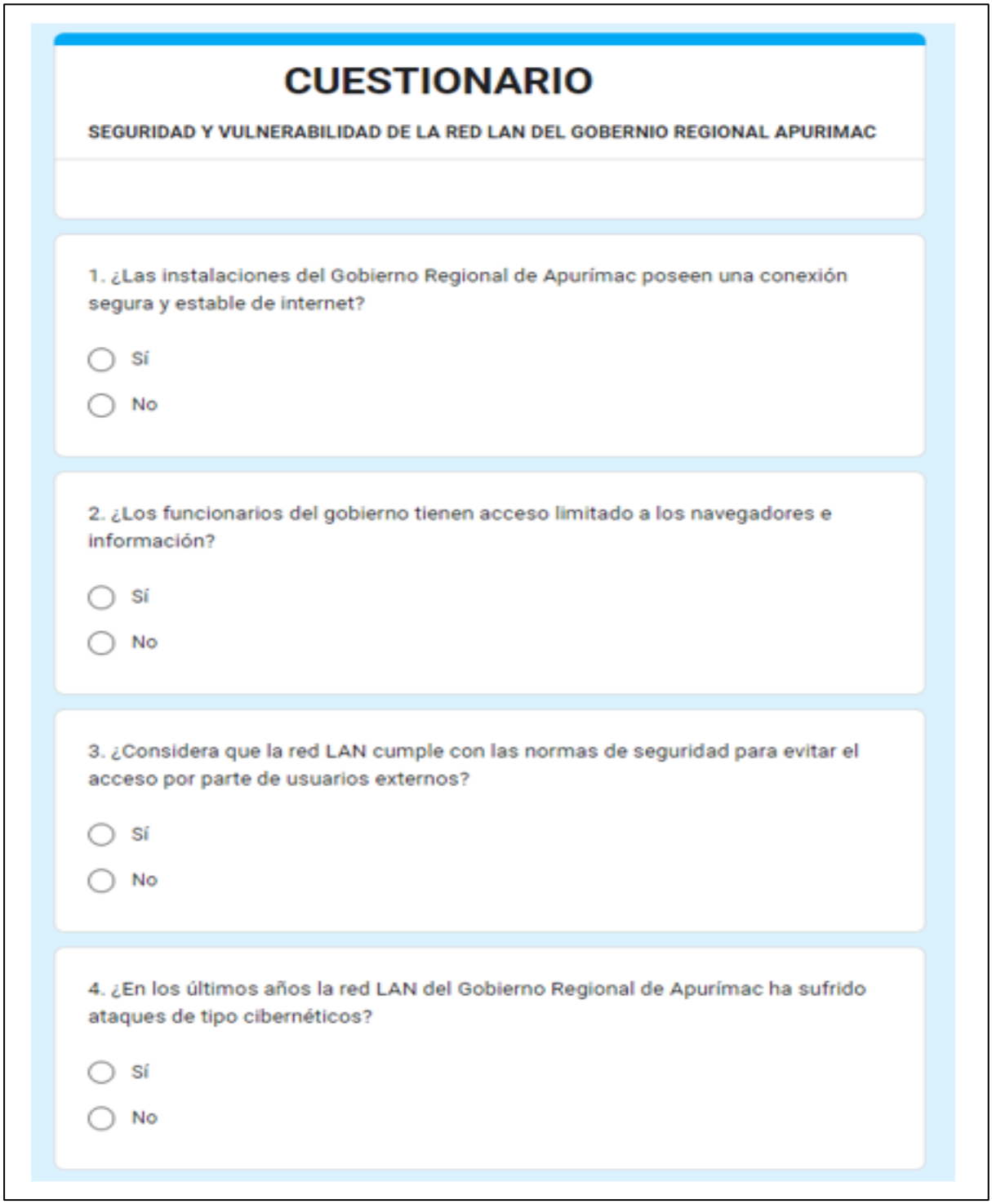
UNIR. (13 de diciembre de 2021). *¿Qué es el hacktivismo y qué delitos implica?* https://www.unir.net/derecho/revista/hacktivismo/#:~:text=El%20hacktivismo%20es%20un%20tipo,acciones%20relacionadas%20buscan%20simplemente%20notoriedad.

Vanegas, A. (2019). *Pentesting, ¿Porque es importante para las empresas?* Universidad Piloto de Colombia: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1

Veloz, J., Alcivar, A., Salvatierra, g., & Silva, C. (2017). Ethical hacking, una metodologia para descubrir fallas de seguridad en sistemas informaticos mediante la herramienta KALI-LINUX. *Revista de tecnologías de la informática y las comunicaciones, 1*(1), 1-12. https://revistas.utm.edu.ec/index.php/Informaticaysistemas/article/download/194/156/

ANEXOS

- Formato del cuestionario aplico en el Gobierno Regional de Apurímac



CUESTIONARIO

SEGURIDAD Y VULNERABILIDAD DE LA RED LAN DEL GOBERNIO REGIONAL APURIMAC

1. ¿Las instalaciones del Gobierno Regional de Apurímac poseen una conexión segura y estable de internet?

- ◯ Sí
- ◯ No

2. ¿Los funcionarios del gobierno tienen acceso limitado a los navegadores e información?

- ◯ Sí
- ◯ No

3. ¿Considera que la red LAN cumple con las normas de seguridad para evitar el acceso por parte de usuarios externos?

- ◯ Sí
- ◯ No

4. ¿En los últimos años la red LAN del Gobierno Regional de Apurímac ha sufrido ataques de tipo cibernéticos?

- ◯ Sí
- ◯ No

5. ¿Conoce usted si el Gobierno Regional de Apurímac hace uso de firewall o controles de acceso que proteja la información de la red LAN?

- ◯ Sí
- ◯ No

6. ¿EL Gobierno Regional de Apurímac da a conocer a los funcionarios las políticas de seguridad de las cuentas?

- ◯ Sí
- ◯ No

7. ¿El último año se ha realizada una prueba de vulnerabilidad de la infraestructura de la red?

- ◯ Si
- ◯ No

8.¿El Gobierno Regional de Apurímac cuenta con herramientas que detecten y detengan las vulnerabilidades de a red LAN?

- ◯ Si
- ◯ No

9. ¿El Gobierno Regional de Apurímac trabaja de manera interna con la encriptación de la información?

- ◯ Si
- ◯ No

10. ¿Considera necesario que el Gobierno Regional de Apurímac implemente una mejora en la seguridad de la red LAN?

- ◯ Sí
- ◯ No