UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS

RIESGOS QUE AFECTAN LA DISPONIBILIDAD DE SERVICIO EN LOS PROVEEDORES DE INTERNET EN LOS CANTONES CAÑAR, EL TAMBO Y SUSCAL.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

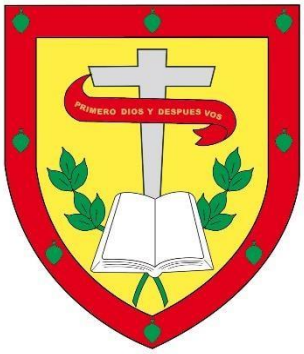
AUTOR: LIZARDO MANUEL QUIZHPI CAZHO

DIRECTOR: ING. LUIS FERNANDO PINOS CASTILLO

CAÑAR - ECUADOR

2022

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS

RIESGOS QUE AFECTAN LA DISPONIBILIDAD DE SERVICIO EN LOS PROVEEDORES DE INTERNET EN LOS CANTONES CAÑAR, EL TAMBO Y SUSCAL.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

AUTOR: LIZARDO MANUEL QUIZHPI CAZHO

DIRECTOR: ING. LUIS FERNANDO PINOS CASTILLO

CAÑAR - ECUADOR

2022

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Lizardo Manuel Quizhpi Cazho portador de la cédula de ciudadanía N°**0302913108**. Declaro ser el autor de la obra: "Riesgos que afectan la disponibilidad de servicio en los proveedores de internet en los cantones Cañar, el Tambo y Suscal", sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, 20 de abril de 2022

F: .....

Lizardo Manuel Quizhpi Cazho

C.I. 0302913108

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Est. Lizardo Manuel Quizhpi Cazho, bajo mi supervisión.

Ing. Luis Fernando Pinos Castillo

DIRECTOR DEL TRABAJO DE TITULACIÓN UNIVERSIDAD CATÓLICA DE CUENCA CAMPUS CAÑAR

RESUMEN

Este artículo presenta un estudio realizado en el Cantón Cañar, en donde participaron las empresas Proveedores de Servicio de Internet (ISP) de los Cantones Cañar, El Tambo y Suscal, con el fin de determinar cuáles son los riesgos que afectan la disponibilidad de los servicios que prestan en base a una metodología reconocida que sirva de referencia a los administradores de los ISPs. Los objetivos planteados en el presente estudio fueron: a) Realizar un estudio teórico de las metodologías para un análisis de riesgo, b) Determinar los riesgos tecnológicos que afectan la disponibilidad de los servicios de los ISPs, c) Analizar los riesgos en base a una metodología que incluya los activos informáticos de los proveedores de servicio de internet. Se realizo un análisis estadístico en base a los dominios de la norma ISO27001 enfocada a la seguridad de las Tecnologías de la Información y la Comunicación, en donde se aplicó una encuesta a los administradores de la red de cada ISP y como resultado se estableció el cumplimiento de los dominios y mediante la metodología de MARGERIT se establecen los activos críticos para los ISPs, para luego elaborar una matriz de riesgos con las amenazas, el impacto y las probabilidades propuestas por esta metodología y finalmente se determina los riesgos más críticos de los activos informáticos que pueden afectar la disponibilidad de los servicios que ofrecen las empresas proveedoras de internet lo que permitirá que dichas empresas gestionen de manera eficiente los riesgos y así asegurar la continuidad del servicio.

Palabras Clave: ISP, riesgos informáticos, amenazas.

ABSTRAC

This article presents a study carried out in the Canar Canton with the participation of the (ISP) Internet Service Providers companies of the Canar, El Tambo, and Suscal cantons, to determine the Risks that affect the availability if the services they provide, based on a recognized methodology that serves as a reference for ISP administrators. The objectives of this study were: a) To carry out a theoretical study of the methodologies for risk analysis, b) To determine the technological risks that affect the availability of ISP services, c) To analyze the risks based on a methodology that includes the IT assets of internet service providers. Statistical analysis was carried out based on the ISO27001 standard domains focused on the information and communication technologies security, surveys were applied to the network administrators of each ISP, as a result the compliance of the domains was established, and by using the MARGERIT methodology, the critical assets for the ISPs are established and then a risk matrix is elaborated with the threats, impact and chances proposed by this methodologic, finally, the most critical IT asset risks that threaten the availability of the ISP's service are determined. This will enable these companies to effectively manage the risks and guarantee the service continuity.

Keywords: IT risks, threats, ISP.

RIESGOS QUE AFECTAN LA DISPONIBILIDAD DE SERVICIO EN LOS PROVEEDORES DE INTERNET EN LOS CANTONES CAÑAR, EL TAMBO Y SUSCAL.

RISKS THAT AFFECT THE AVAILABILITY OF SERVICE IN INTERNET PROVIDERS IN THE CANTONS OF CAÑAR, EL TAMBO Y SUSCAL.

Lizardo Manuel Quizhpi Cazho

[a] Ingeniería de Sistemas, Universidad Católica de Cuenca extensión Cañar, Ecuador, lmquizhpic08@est.ucacue.edu.ec

Luis Fernando Pinos Castillo

[a] Ingeniería de Sistemas, Universidad Católica de Cuenca extensión Cañar, Ecuador, lfpinosc@ucacue.edu.ec

RESUMEN

Este artículo presenta un estudio realizado en el Cantón Cañar, en donde participaron las empresas Proveedores de Servicio de Internet (ISP) de los Cantones Cañar, El Tambo y Suscal, con el fin de determinar cuáles son los riesgos que afectan la disponibilidad de los servicios que prestan en base a una metodología reconocida que sirva de referencia a los administradores de los ISPs. Los objetivos planteados en el presente estudio fueron: a) Realizar un estudio teórico de las metodologías para un análisis de riesgo, b) Determinar los riesgos tecnológicos que afectan la disponibilidad de los servicios de los ISPs, c) Analizar los riesgos en base a una metodología que incluya los activos informáticos de los proveedores de servicio de internet. Se realizo un análisis estadístico en base a los dominios de la norma ISO27001 enfocada a la seguridad de las Tecnologías de la Información y la Comunicación, en donde se aplicó una encuesta a los administradores de la red de cada ISP y como resultado se estableció el cumplimiento de los dominios y mediante la metodología de MARGERIT se establecen los activos críticos para los ISPs, para luego elaborar una matriz de riesgos con las amenazas, el impacto y

las probabilidades propuestas por esta metodología y finalmente se determina los riesgos más críticos de los activos informáticos que pueden afectar la disponibilidad de los servicios que ofrecen las empresas proveedoras de internet lo que permitirá que dichas empresas gestionen de manera eficiente los riesgos y así asegurar la continuidad del servicio.

***Palabras Clave*:** ISP, riesgos informáticos, amenazas.

ABSTRACT

This article presents a study carried out in the Canar Canton with the participation of the (ISP) Internet Service Providers companies of the Canar, El Tambo, and Suscal cantons, to determine the Risks that affect the availability if the services they provide, based on a recognized methodology that serves as a reference for ISP administrators. The objectives of this study were: a) To carry out a theoretical study of the methodologies for risk analysis, b) To determine the technological risks that affect the availability of ISP services, c) To analyze the risks based on a methodology that includes the IT assets of internet service providers. Statistical analysis was carried out based on the ISO27001 standard domains focused on the information and communication technologies security, surveys were applied to the network administrators of each ISP, as a result the compliance of the domains was established, and by using the MARGERIT methodology, the critical assets for the ISPs are established and then a risk matrix is elaborated with the threats, impact and chances proposed by this methodologic, finally, the most critical IT asset risks that threaten the availability of the ISP's service are determined. This will enable these companies to effectively manage the risks and guarantee the service continuity.

Keywords: IT risks, threats, ISP.

INTRODUCCIÓN

Con el crecimiento y el uso de las Tecnologías de la información y la Comunicación (TIC), han generado nuevas oportunidades de crecimiento para las empresas Proveedoras de Servicios de Internet (ISP), al mismo tiempo han generado la necesidad de incorporar nuevas estrategias o mecanismos de seguridad debido a que están expuestas a los distintos ataques informáticos a sus sistemas que puedan suscitarse ya sea desde la parte exterior e interior de las empresas.

La aplicación del análisis de riesgos a los activos más críticos de las empresas ISPs ayuda a reducir los riegos, también a tomar decisiones en relación a una amenaza y que se implemente las medidas de seguridad pertinentes.

Para alcanzar una protección idónea de los activos informáticos, sistemas de información, de los datos, etc. en necesario la colaboración de todo el personal que manejan los activos y sistemas informáticos incluyendo a los gerentes que deban dar la atención adecuada en los proyectos de seguridad informática (Solarte Solarte, Enriquez Rosero, & Benavides, 2015).

Seguridad Informática

Aguilera, P. define como "La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable" (Purificación Aguilera, 2010), es decir se encarga de proporcionar seguridad a los sistemas tanto a nivel de hardware, software y de red.

Según Chuquitarco, Mario. et al (Chuquitarco & Romero, Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador, 2018), menciona que la seguridad informática surge a partir de una necesidad de dar soporte a las tecnologías que requieren las organizaciones para asegura la integridad de los datos e información.

Tipos de Seguridad Informática

Existen algunos tipos en esta categoría que los profesionales en la seguridad deberán estudiar y aplicar a un sistema de seguridad de las cuales se mencionan tres tipos:

- *Seguridad de Hardware*

Salamanca, O. (Salamanca, 2016), sostiene que la seguridad de hardware comprende de todos los factores que garantizan la seguridad de los sistemas tecnológicos de las organizaciones (Salamanca, 2016), de las cuales pueden ser aplicar restricciones a los servidores, privilegios de acceso a los de más equipos.

- *Seguridad de Software*

  Aguilera, P. (Purificación Aguilera, 2010) considera a la seguridad como "Los mecanismos y herramientas `de seguridad lógica tienen como objetivo proteger digitalmente la información de manera directa" (Purificación Aguilera, 2010).

  De acuerdo a lo expuesto la seguridad de software ha tomado gran importancia para proteger los sistemas informáticos integrados en los dispositivos de las vulnerabilidades que pueden ser aprovechados por los hackers u otros tipos de ataques.

- *Seguridad de Red*

  "Las redes informáticas, y entre ellas Internet, son uno de los mayores peligros que existen en la seguridad de un sistema informático, ya que actualmente la mayoría de las amenazas y ataques provienen desde el exterior, a través de la red" (ALEGRE RAMOS & GARCÍA-CERVIGÓN, 2011).

Vulnerabilidad, Amenaza y Riesgo

- *Vulnerabilidad*

Se conoce como vulnerabilidades la existencia de un defecto en los principales sistemas o mecanismos de seguridad de los equipos informáticos, Ortiz, J. et al (Ortiz-Lazo & Vizñay-Duran, 2019) expone que "Una vulnerabilidad común es contar con un antivirus no actualizado, lo cual permitirá al virus actuar y ocasionar daños" (Ortiz-Lazo & Vizñay-Duran, 2019).

Tipos de Vulnerabilidad

- *Vulnerabilidades Conocidas*

Quiroz, S. et al (Quiroz-Zambrano & Macías-Valencia, 2017) considera que "Son vulnerabilidades de las que ya tienen conocimiento las empresas que desarrollan el programa al que afecta y para las cuales ya existe una solución, que se publica en forma de parche" (Quiroz-Zambrano & Macías-Valencia, 2017).

- *Vulnerabilidades No Conocidas*

"Estas vulnerabilidades aún no han sido detectadas por la empresa que desarrolla el programa, por lo que, si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tiene instalado este programa" (Quiroz-Zambrano & Macías-Valencia, 2017).

- *Amenaza*

Se considera una amenaza los ataques informáticos que pueda darse y ocasionar danos a los equipos tecnológicos, sistemas de información y todo el medio que comprometen la seguridad de la información (Solarte Solarte, ENRIQUEZ ROSERO, & Benavides Ruano, 2015).

Tipos de Amenaza

- *Amenazas de Software*

"Dentro de este tipo de amenazas podemos encontrar cualquier tipo de software malintencionado, como virus, espías, troyanos, gusanos, phishing, spamming, ataques DoS" (ALEGRE RAMOS & GARCÍA-CERVIGÓN HURTADO, 2011).

- *Amenazas Físicas*

"Dentro de este tipo de amenazas se pueden encontrar todos aquellos posibles daños causados al sistema informático por razones físicas y naturales, como robos, incendios (fortuitos o provocados), catástrofes naturales" (ALEGRE RAMOS & GARCÍA-CERVIGÓN HURTADO, 2011).

- *Amenazas Humanas*

Este tipo de amenazas se consideran tanto por "Intrusos, como piratas informáticos, que pueden entrar vía web, es decir, de forma remota, o físicamente, al sistema" (ALEGRE RAMOS & GARCÍA-CERVIGÓN HURTADO, 2011).

- *Riesgo*

"Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo" (Solarte Solarte, ENRIQUEZ ROSERO, & Benavides Ruano, 2015). La existencia de un riesgo nace de las amenazas que afectan a la seguridad informática y esto produce un obstáculo al funcionamiento de los sistemas de información.

Tipos de Riesgos

- *Riesgos Lógicos*

"Son riesgos difíciles de detectar, razón de más para para considerarlos muy peligrosos. Las alteraciones que provocan en el funcionamiento normal del sistema pueden llegar a ocasionar daños imparables en el sistema. Son riesgos de este tipo los Códigos Maliciosos, el SPAM, la Piratería (Hackers), la Fuga de información o la Ingeniería Social" (Pequeño Collado, 2015) .

- *Riesgos Físicos*

"Son considerados Riesgos Físicos para los Sistemas Informáticos los fenómenos naturales como incendios, inundaciones, terremotos, etc., los actos vandálicos o los problemas eléctricos y electromagnéticos" (Pequeño Collado, 2015).

Análisis de Riesgos

"En términos generales, el riesgo se define como la posibilidad de que no se obtengan los resultados deseados (Baca Urbina, 2016)". Esto quiere decir las empresas siempre estarán expuestas a intentos de ataques informáticos (Baca Urbina, 2016) .

Metodologías y Análisis de Riesgos

Salamanca, Oscar. (Salamanca, 2016) sostiene que "Actualmente las organizaciones necesitan demostrar que realizan una gestión competente y efectiva del resguardo de los datos que gestionan, por lo tanto, es necesario seguir un conjunto estructurado de normas para garantizar la seguridad de la información" (Salamanca, 2016).

En consecuencia, existen varias metodologías para llevar a cabo con éxito un análisis de riesgo en donde se pueda evidenciar las vulnerabilidades y amenazas que puedan afectar los sistemas de seguridad.

- *Mehari*

  Esta metodología proporciona una serie de herramientas necesarias para la gestión de seguridad, que se utiliza para los procesos de análisis de riesgos de las organizaciones, a través de un análisis de seguridad de los criterios de integridad, confidencialidad y disponibilidad (Tejena-Macía, 2018).

  De acuerdo a la definición anterior se deduce que para un análisis de riesgo propone las herramientas necesarias para identificar y describir las

vulnerabilidades de sus activos y los posibles escenarios que lo pueden provocar

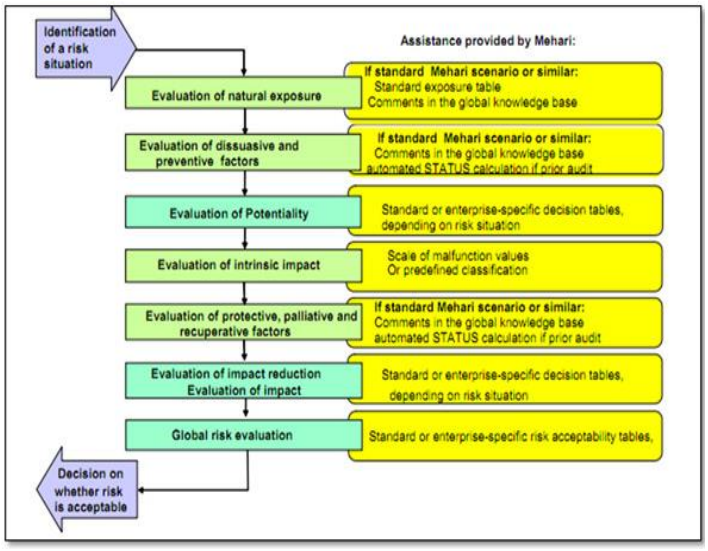


Ilustración 1 Metodología MEHARI Fuente: (Huerta, 2012)

- *Magerit*

  "Fue creada por el Concejo Superior de Administración Electrónica para minimizar los riesgos de la implementación y uso de las tecnologías de la información" (Molina-Miranda, 2017). La cual está reconocida y normalizada a nivel internacional y presenta como una de las principales características el diseño de sus catálogos a partir de riesgos ya conocidos para su posterior aplicación.

  La metodología MAGERIT presenta un mayor acierto para la toma de decisiones, por lo que realiza un análisis de riesgos completo a todos los elementos empresariales que las demás metodologías (Abril Estupiñan, Pulido, & Bohada Jaime, 2013).

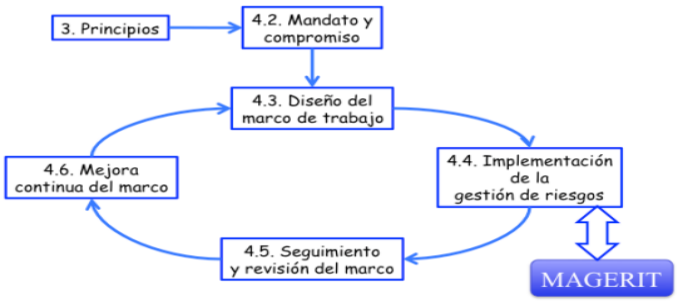


Ilustración 2 Metodología MARGERIT Fuente: (Consejo Superior de Administración Electrónica, 2012)

- *ISO270012013:*

  “Norma principal para la definición de necesidades para CMSI (sistema de gestión de la seguridad de la información). Corresponde al principio de certificación de la seguridad de las organizaciones” (CARPENTIER, 2016).

  Esta norma se encuentra entre las más conocidas y utilizadas por los expertos en seguridad informática, fue creada por la organización internacional conocida como ISOtools (ISOTools , 2013)” Esta norma supone que los riesgos en seguridad de la información son controlados por parte de la organización de una forma eficiente, tanto para la propia empresa en si, como para el resto de empresas del entorno” (ISOTools , 2013).

Ilustración 3 ISO27001:2013 Fuente: (Advisera, n.d.)

Estudios previos

Lazo, J. et al (Ortiz Lazo & Vizñay Duran, 2019) realizaron una investigación de “Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008” en España aplicada a la empresa SISTELCEL, aquí utilizaron una metodología cuantitativa y cualitativa con técnicas de encuestas, dando como resultado los diferentes tipos de riesgos a las que está expuesta. Y como conclusión de este trabajo la empresa debe implementar políticas de seguridad para minimizar los riesgos encontrados.

Murillo, N. et al (Angulo Murillo, Zambrano Vera, García Murillo, & Bolaños Burgos, 2018), titulada ”Propuesta metodológica de seguridad de información para proveedores de servicios de internet en Ecuador”, publicada por la revista Mikarimin, en la metodología utiliza un enfoque cualitativo de tipo descriptivo e interpretativo, con un análisis documentas, aplicando entrevistas y listas de verificación basada en la norma ISO27002, entre los resultados que se obtuvieron fueron listas de riesgos, amenazas y vulnerabilidades informáticas, en conclusión los lineamientos de las normas ISO 27001-

27002 mediante una reconfiguración se logró reconfigurar ciertos procesos de los ISP agregando nuevas funciones a personal para mejorar de la información sensible.

METODOLOGÍA

Enfoque de la investigación

El enfoque de la investigación será cualitativo y cuantitativo para obtener información general de los riesgos y así poder determinar los más importantes que puedan afectar a los ISPs.

Nivel de investigación

Para identificar los riesgos que afectan la disponibilidad del servicio de los ISPs se realizara una encuesta ya que es un trabajo descriptivo.

En esta investigación se hará uso de la norma ISO 27001 para un diagnóstico de los activos y posteriormente con la metodología MARGERIT para el análisis de riesgos. De acuerdo a los activos determinados se evaluarán los riesgos, para finalmente en base a los resultados del análisis de riesgo establecer recomendaciones que minimicen tales riesgos.

Población y muestra

El estudio se llevará a cabo a los IPS de los cantones Cañar, El Tambo y Suscal. La investigación o muestra se realiza a cada departamento responsable de administrar la Red como se muestra en la siguiente tabla.

Proveedores de Servicio de Internet (ISP)			
Nombre	**Cañar**	**El Tambo**	**Suscal**
Cañar Net	✓		✓
CB Visión	✓		
Austro Net	✓	✓	
Flash Net	✓		
Intelco	✓		
Fiber Media	✓	✓	
Ultra Net		✓	
Mega Net	✓		
Sistelcel		✓	✓
CNT	✓	✓	✓
Nedetel	✓	✓	
Milenium Conexion	✓		

Ilustración 4 Empresas Proveedoras de Servicio de Internet (ISP) Fuente: Autor Propio

RESULTADOS

Encuesta

Para determinar el nivel de seguridad de la información se aplicaron una encuesta en base a los dominios de la norma ISO27001 a los 12 ISPs de los cantones Cañar, El Tambo y Suscal, aplicando a cada responsable de administrar la red.

Los resultados reflejan que no cumplen con todos los objetivos de dominio, la cual refleja una debilidad y esto conlleva a que la empresa sea vulnerable ante las amenazas y riesgos.

A continuación, se detalla cada uno de los dominios y preguntas realizadas a los encargados de la administración de la red de los ISPs.

Dominio: Seguridad en las telecomunicaciones.

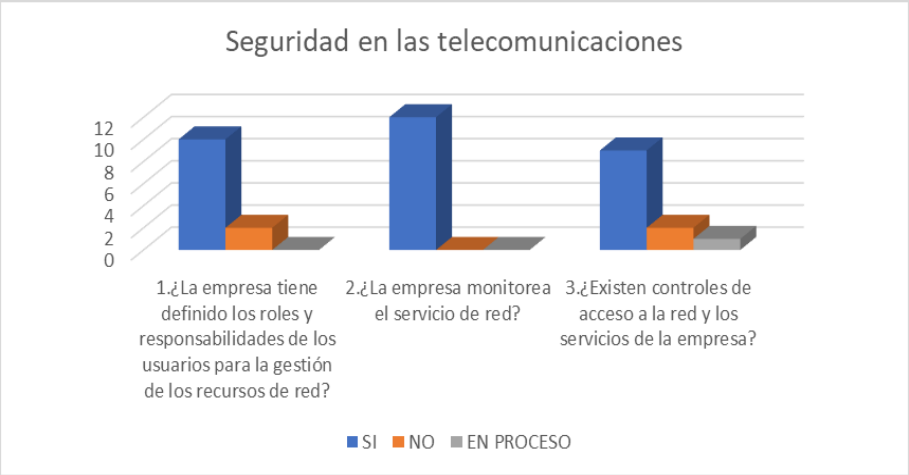


Ilustración 5 Resultados Dominio Seguridad en las Telecomunicaciones en base a la norma ISO27001 Fuente: Autor Propio

Los resultados del dominio Seguridad en la Telecomunicaciones se puede observar que la mayoría de los ISPs cumplen con los controles de este dominio. De acuerdo a esto se deduce que cuentan con roles y responsabilidades definidos para cada empleado.

Dominio: Seguridad de las Operaciones

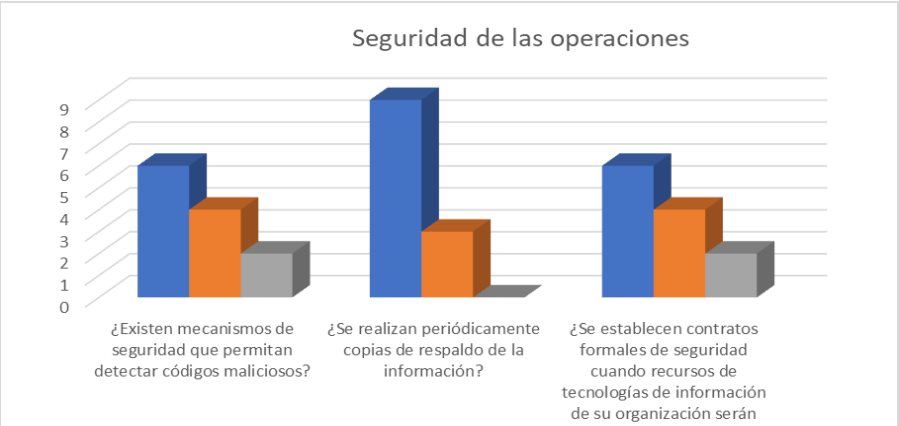


Ilustración 6 Resultados Dominio Seguridad de las Operaciones en base a la norma ISO27001 Fuente: Autor Propio

Los resultados del dominio Seguridad de las operaciones se observar que, si realizan copias de respaldo, mientras que no cuentan con mecanismos o herramientas para la detención de software códigos y también desconocen sobre contras formales de seguridad hacia terceros en cuanto vayan a manipular los equipos.

Dominio: Control de acceso.

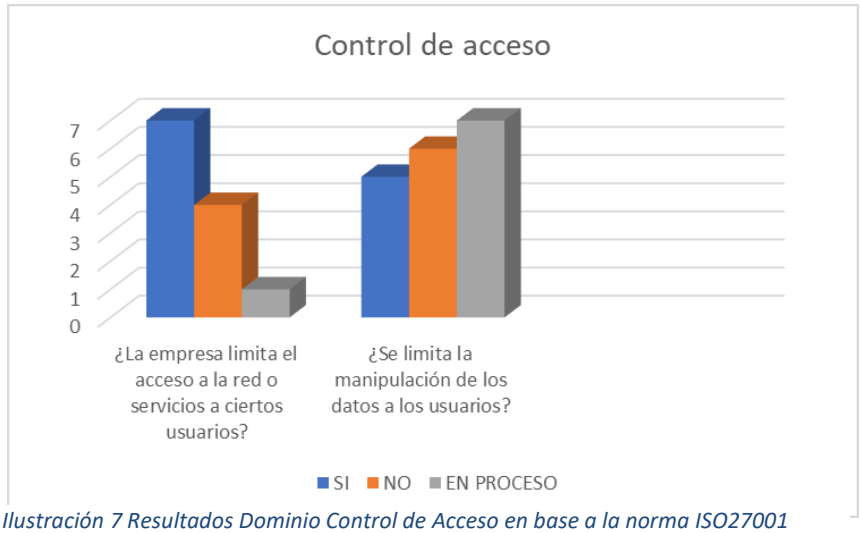


Ilustración 7 Resultados Dominio Control de Acceso en base a la norma ISO27001 Fuente: Autor Propio

De acuerdo a los resultados del dominio Control de Acceso se observar que no todos los ISPs limitan el acceso a sus servicios o red, por lo que se determina que no tiene especificado que usuarios tiene acceso a manipular información sensible.

Dominio: Seguridad Física y Ambiental.

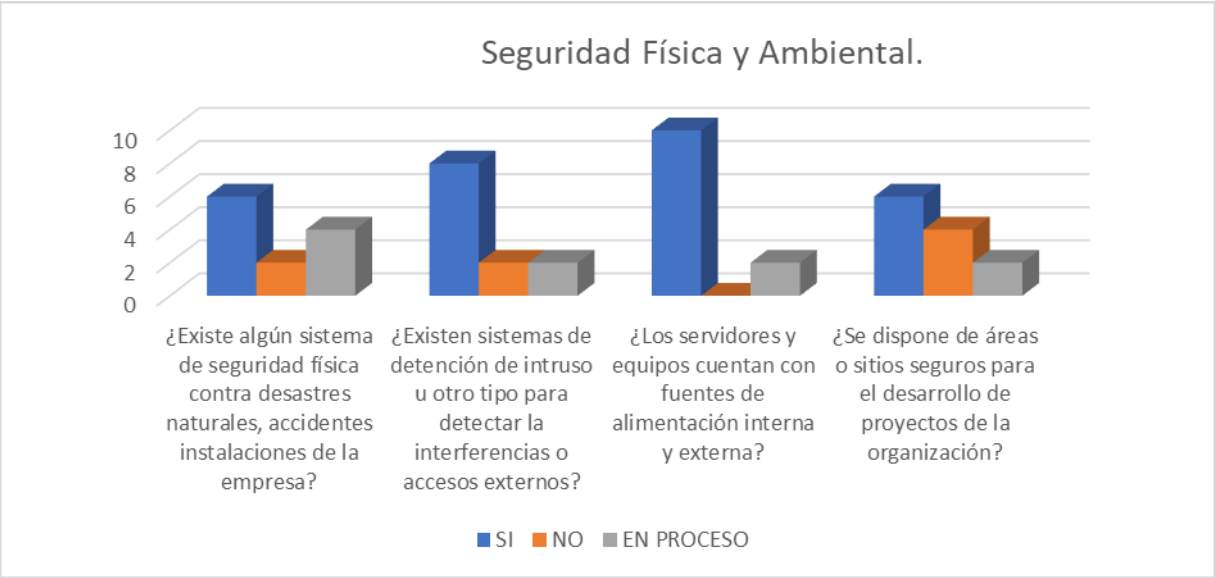


Ilustración 8 Resultados Dominio Seguridad Física y Ambiental en base a la norma ISO27001 Fuente: Autor Propio

Los resultados del dominio Seguridad Física y Ambiental se observa que la mayoría disponen de fuentes de alimentación para sus equipos informáticos, también tiene implementados sistemas detención de intrusos, sin embargo, no todos tienen sistemas para la seguridad física contra desastres naturales y accidentes en sus instalaciones, también existe una baja demanda relacionado a tener áreas específicas de desarrollo para proyectos de la empresa.

La ilustración 2

Dominio: Gestión de comunicaciones y operaciones.

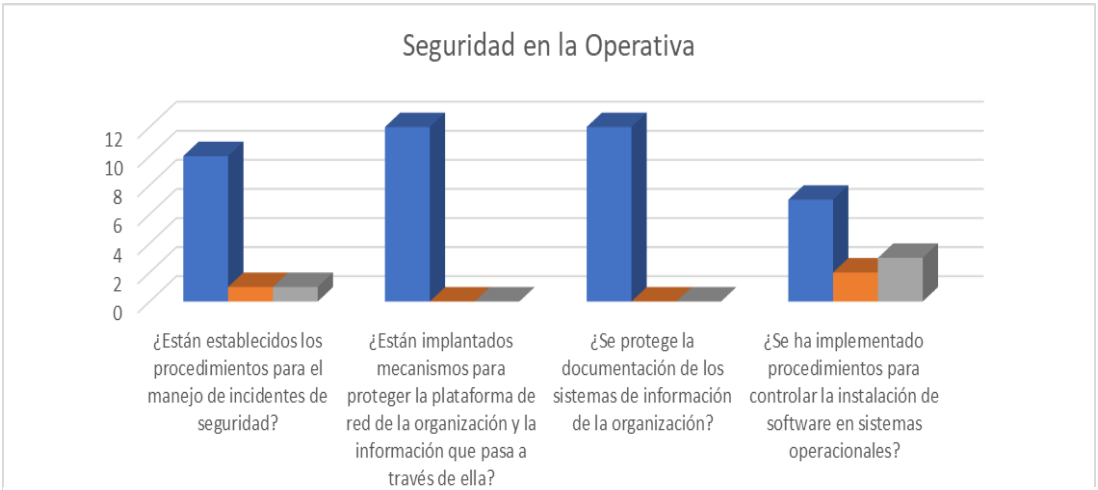


Ilustración 9 Resultados Dominio Gestión de Comunicaciones y Operaciones en base a la norma ISO27001 Fuente: Autor Propio

Los resultados del dominio Gestión de Comunicaciones y Operaciones se observa que tienen establecidos procedimientos o mecanismos para el manejo de incidentes, para proteger la plataforma de red, mientras que hay un déficit en cuanto a procedimientos para controlar la instalación de software en sus sistemas.

Dominio: Cumplimiento.

Ilustración 10 Resultados Dominio Cumplimiento en base a la norma ISO27001 Fuente: Autor Propio

Los resultados del dominio Cumplimiento se observa que todos los ISPs encuestados tienen documentación sobre las políticas de protección de datos y la privacidad de la información. Con esto se puede deducir que la información que maneja de sus clientes es confidencial.

Análisis de Riesgos

Con los resultados de las encuestas aplicadas a los ISPs se aplica el análisis de riesgos con la metodología MARGERIT a los activos más importantes de los ISPs según los principios básicos de la seguridad propuesta por MARGERIT a si mismo las amenazas el impacto, la probabilidad seleccionando los riesgos más críticos que podrían afectar la disponibilidad de sus servicios como se muestra en la siguiente imagen.

Dominios ISO 27001	ACTIVOS	Catalogo de Amenazas	Calculo del Riesgo					
			Insignificante	1	Improbable	1	R= I*P	
			Menor	2			Bajo	1--4
			Moderado	3	Probable	2	Medio	5--8
			Mayor	4			Alto	9--11
			Catastrofico	5	Casi Seguro	3	Critico	12--15
		Amenazas	Impacto		Probabilidad		RIESGO	
Seguridad en las telecomunicaciones	**Infraestructura de red**	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5		3		15	
		[E.25] Pérdida de equipos	4		3		12	
	Personal que gestiona la Red	[A.30] Ingeniería social (picaresca)	5		3		15	
		[E.7] Deficiencias en la organización	4		3		12	
		[A.5] Suplantación de la identidad del usuario	5		3		15	
Seguridad de las Operaciones	**Software(Sistemas Operativos)**	[E.8] Difusión de software dañino	5		3		15	
		[E.20] Vulnerabilidades de los programas (software)	5		3		15	
Control de acceso.	**Servidores/ Centro de Datos**	[I.6] Corte del suministro eléctrico	4		3		12	
		[E.15] Alteración accidental de la información	5		3		15	
		[A.6] Abuso de privilegios de acceso	5		3		15	
Seguridad Física y Ambiental.	**Software Antivirus**	[E.8] Difusión de software dañino	4		3		12	
		[E.20] Vulnerabilidades de los programas (software)	5		3		15	
		[E.21] Errores de mantenimiento / actualización de programas (software)	5		3		15	
		[A.5] Suplantación de la identidad del usuario	4		3		12	
		[A.11] Acceso no autorizado	4		3		12	
Gestión de comunicaciones y operaciones.	**Sistema registros usuarios**	[A.11] Acceso no autorizado	4		3		12	
		[E.18] Destrucción de información	4		3		12	
		[E.1] Errores de los usuarios	4		3		12	
	Servicio de Internet	[I.6] Corte del suministro eléctrico	5		3		15	
		[E.4] Errores de configuración	4		3		12	
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4		3		12	
		[I.5] Avería de origen físico o lógico	5		3		15	
		[I.8] Fallo de servicios de comunicaciones	5		3		15	
		[A.24] Denegación de servicio	5		3		15	

Ilustración 11 Activos que resultaron con riesgo critico en el análisis de la matriz MARGERIT Fuente: Autor Propio

DISCUSIÓN

El presente estudio ha permitido evidenciar cuales son los riesgos más críticos que amenazan la disponibilidad de los servicios que prestan los ISPs, siendo estos algunos problemas de seguridad que se relacionan con el desconocimiento de aplicar las normas de seguridad de la información, así también en la administración de la seguridad informática.

Entre los activos críticos que podrían afectar significativamente a los ISPs está la caída del servicio de internet, difusión de software dañino, personal que gestiona la red, avenía servidores las posibles amenazas son: denegación de servicios, avería de origen físico y lógico, errores de mantenimiento, etc.,

Es evidente que los activos que componen la infraestructura tecnológica como son los servidores, modem, routers, etc., deben implementar mecanismos o estrategias de seguridad para minimizar los riesgos. Ya que el funcionamiento de los ISPs depende de que los recursos informáticos estén siempre disponibles.

La toma de conciencia e importancia sobre la educación en los temas de la seguridad informática por parte del personal que gestiona la red permite estar al tanto sobre las nuevas formas de ataques informáticos por parte de hackers y a su vez tomar las medidas pertinentes que aseguren estar protegidos ante las posibles amenazas.

De igual manera la importancia de informar y otorgar sistemas que protejan la información y el uso correcto de los servicios y recursos informáticos, también difundir que nadie esta excepto de riesgos cuando se adquiere un servicio (Gantiva Henao, 2017).

Uno de los aspectos necesarios que se tiene que considerar tanto los profesionales de TI como de los proveedores de servicio y tecnología, es que resulta útil tener un modelo para diagnosticar las vulnerabilidades de las redes inalámbricas (Chuquitarco & Romero, 2018).

CONCLUSIONES

- Como resultado de este trabajo se identificaron los activos más críticos para un ISP, cuáles son las amenazas que implican, se presentó una matriz de riesgos con el nivel de riesgo, donde se puede determinar que los ISPs están en una zona vulnerable, en base a este análisis la importancia de incorporar mecanismos que minimicen los riesgos encontrados.
- Para lograr el éxito en cuanto a ofrecer los servicios de un ISP es brindar la disponibilidad, seguridad, confiabilidad de la información a sus clientes en base al cumplimiento de normas, estándares dedicados a la seguridad de las Tecnologías de Información y la comunicación.

.

REFERENCIAS BIBLIOGRÁFICAS

Referencias

Abril Estupiñan, A., Pulido, J. A., & Bohada Jaime, J. A. (2013). Análisis de riesgos en seguridad

Advisera. (s.f.). *advisera.com*. Recuperado el 06 de 07 de 2021, de https://advisera.com/27001academy/es/que-es-iso-27001/

ALEGRE RAMOS, M. D., & GARCÍA-CERVIGÓN, H. A. (2011). *Seguridad informática.* Madrid: 328124, 9788497328128.

Angulo Murillo, N. G., Zambrano Vera, M. F., García Murillo, G., & Bolaños Burgos, F. (2018). PROPUESTA METODOLÓGICA DE SEGURIDAD DE INFORMACIÓN PARA PROVEEDORES DE SERVICIOS DE INTERNET EN ECUADOR. *Mikarimin:Revista Cientifica Multidisciplinaria, 4*(165-176), 4.

Aranda, V. T. (2004). Historia y evolución de los lenguajes de programación. *Dialnet*, 11.

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* Mexico D.F: Grupo Editorial Patria.

BLANCO SOLSONA, A., HUIDOBRO MOYA, J. M., & JORDAN CALERO, JULIA. (2006). *Redes de área local: administración de sistemas informáticos.* Madrid: Editorial Paraninfo.

CARPENTIER, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Ediciones ENI.

Chuquitarco, M. (2018). Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador. *INNOVA Research Journal, 3*(2.1), 111-122.

Consejo Superior de Administración Electrónica. (2012). *www.ccn-cert.cni.es/.* Recuperado el 06 de 07 de 2021, de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Francisco Gortázar Bellas, R. M. (2016). *Lenguajes de programación y procesadores.* Madrid: Centro de Estudios Ramon Areces SA.

Gantiva Henao, L. A. (2017). GESTIÓN DE RIESGOS EN EL INTERNET DE LAS COSAS (ioT). *Universidad Piloto de Colombia*.

Huerta, A. (2 de 04 de 2012). *www.securityartwork.es*. Recuperado el 06 de 07 de 2021, de https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%e2%80%93-metodologias-ii/

ISOTools . (13 de 06 de 2013). *www.isotools.org*. Obtenido de https://www.isotools.org/2013/06/19/nueva-evaluacion-del-riesgo-segun-la-iso-270012013/

José A. Cerrada Somolinos, M. E. (2010). *Fundamentos de programación.* Madrid: Editorial Universitaria Ramon Areces.

Mangifesta, L. (03 de 12 de 2019). *canal AR.* Obtenido de https://www.canal-ar.com.ar/28339-La-importancia-de-ensenar-programacion-en-la-escuela.html

Marrero Travieso, Y. (2003). La Criptografía como elemento de la seguridad informática. *SCIELO, 11*(6).

Molina-Miranda, M. F. (2017). ANÁLISIS DE RIESGOS DE CENTRO DE DATOS BASADOS EN LA HERRAMIENTA PILAR DE MAGERIT. *Espirales revista multidisciplinaria de investigación, 1*(11).

Ortiz Lazo, J. E., & Vizñay Duran, J. K. (2019). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel. *Polo del Conocimiento, 4*(7), 174-195.

Ortiz-Lazo, J. E., & Vizñay-Duran, J. K. (2019). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel. *Polo del Conocimiento, 4*(7), 174-195.

Pequeño Collado, M. V. (2015). *MF0490_3 - Gestión de servicios en el sistema informático.* Editorial Elearning, S.L.

Purificación Aguilera, L. (2010). *Seguridad informática.* Editex.

Quiroz-Zambrano , S., & Macías-Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 03*(05), 678-688.

Salamanca, O. (2016). Sistema de gestión de seguridad para redes de área local. *Revista Venezolana de Información, Tecnología y Conocimiento, 13*(3), 114-130.

Solarte Solarte, F., ENRIQUEZ ROSERO, E. R., & Benavides Ruano, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL, 28*(5), 592-507.

Tejena-Macía, M. (2018). Análisis de riesgos en seguridad de la información. *Polo del conocimiento, 3*(18), 230-244.

Vega Abad, C. R. (2018). Análisis y estudio de políticas de seguridad informática para un ISP con usuarios residenciales. *PRO SCIENCES:REVISTA DE PRODUCCIÓN, CIENCIAS E INVESTIGACIÓN, 2*(8), 32-38.

Anexo 1: Ante Proyecto

Trabajo de Titulación

Tema:

Riesgos que afectan a disponibilidad de servicio en los proveedores de internet en los cantones Cañar, El tambo y Suscal.

Unidad Académica

Tecnologías de la Información y la Comunicación

Carrera

Ingeniera de Sistemas

Alumno

Lizardo Manuel Quizhpi Cazho

Tutor:

Ing. Luis Pinos

Abril – Agosto-2021

Cañar, 05 de marzo de 2021

Ingeniero
Leopoldo Pauta Ayabaca, Msc.
DECANO DE LA UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Ciudad.

Yo, **LIZARDO MANUEL QUIZHPI CAZHO,** con número de identificación **0302913108**, alumno de la carrera de Ingeniería de Sistemas, solicito por su intermedio a Consejo Directivo la aprobación del tema de tesis **"RIESGOS QUE AFECTAN LA DISPONIBILIDAD DE SERVICIO EN LOS PROVEEDORES DE INTERNET EN LOS CANTONES CAÑAR, EL TAMBO Y SUSCAL",** proponiendo como tutor de la misma al Ing. Luis Pinos Castillo, el tema propuesto está considerado su desarrollo en décimo ciclo, ya que estaré matriculado en la Unidad de Titulación.

Por la atención que Ud. y el Honorable Consejo Directivo le brinden a la presente, anticipo mis sentimientos de consideración y estima para cada uno de Uds.

Atentamente;

Sr. LIZARDO MANUEL QUIZHPI CAZHO
Estudiante de Ingeniería de Sistemas, extensión Cañar
CI: 0302913108

A. TÍTULO
Riesgos que afectan la disponibilidad de servicio en los proveedores de internet en los cantones Cañar, El Tambo y Suscal.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Analítica de Datos	
		Ingeniería de Software	
		Algoritmos computacionales	
		Inteligencia de negocios	
		Gobierno de TI	
		Auditoria y Seguridad Informática	X
		Simulación	

C. PLANTEAMIENTO DEL PROBLEMA

Debido al crecimiento tecnológico de los servicios que ofrecen los proveedores de internet (ISP) y la necesidad de sus usuarios de mantenerse siempre en conectividad a internet, existe la necesidad de tener una alta disponibilidad de sus servicios.

En los cantones de Cañar, el Tambo y Suscal existen algunos proveedores de servicio de internet (ISP) que se encuentran registrados por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), la cual regula y controla su funcionamiento.

La mayoría de los proveedores de servicio de internet (ISP) cuentan con una estructura de fibra óptica para mejorar la conectividad a internet de sus usuarios, sin embargo, esta conexión puede verse afectado por distintos riesgos

Por tal motivo surge la necesidad de incorporar nuevas tecnologías y estrategias que aseguren su constante operabilidad, ya que existen una gran variedad de riesgos que amenazan la disponibilidad de sus servicios.

D. OBJETIVO GENERAL

Analizar los riesgos que afectan la disponibilidad de servicio en los proveedores de internet en los cantones Cañar, el Tambo y Suscal, en base a una metodología reconocida que sirva de referencia en la cual se basaran los administradores de los Proveedores de Servicios de Internet (ISP).

E. OBJETIVOS ESPECÍFICOS

1. *Realizar un estudio teórico de las metodologías para un análisis de riesgo en la disponibilidad de servicios en los proveedores de internet.*
2. *Determinar los riesgos tecnológicos que afectan la disponibilidad de los servicios de los proveedores de Servicios de Internet (ISP) en los cantones Cañar, El Tambo y Suscal.*
3. *Analizar riesgos en base a una metodología que incluya los activos informáticos de los proveedores de servicios de internet.*

F. JUSTIFICACIÓN

Hoy en día disponemos de comunicaciones en tiempo real a través de Internet, voz sobre IP, mensajería instantánea, descarga de archivos y multitud de herramientas de ocio y entretenimiento que funcionan bajo una plataforma virtual llamada Internet a una velocidad y estabilidad inimaginable en sus comienzos. [4]

Punto importante: la organización debe poseer los recursos para comprometerse de manera adecuada a un proceso de gestión del riesgo. [5]

Por tal motivo existe una constante demanda de tener acceso a internet la cual ha provocado que muchas de las empresas proveedoras de Servicios de internet (ISP) estén en constantes

cambios tecnológicos para mejorar la cobertura de su red, razón por la que es importante contar con un plan ante posibles riesgos que afecten la continuidad de los servicios.

La presente investigación pretende determinar cuáles son los riesgos que afectan la disponibilidad del servicio de los proveedores de internet (ISP), en los cantones Cañar, El Tambo y Suscal.

G. ALCANCE

El alcance de la presente investigación tiene como objetivo evaluar y determinar los riesgos que afectan la disponibilidad del servicio de los proveedores de Servicios de internet (ISP) a los cantones de Cañar, El Tambo y Suscal. Con la finalidad que la presente investigación sirva a los encargados de administrar la red de los ISP implementar controles que minimicen los riesgos, sobre todo de disponibilidad del servicio que es factor principal que garantiza a una empresa ser un excelente proveedor de servicio de internet.

H. CONCEPTOS RELACIONADOS

El proveedor de servicios de Internet (ISP)

Un proveedor de servicios de internet (ISP, Internet Service Provider) es la empresa que facilita la conexión a internet. El ISP conecta a sus clientes o abonados a través de alguna de las tecnologías descritas en el Aparto 2.2: ADSL, fibra óptica, red móvil etc. [6]

Estructura general de los servicios de ISP

El modelo de acceso a la información en la Internet se basa en un modelo que ha llegado a ser un paradigma en otros campos de aplicación de la informática: el modelo cliente-servidor. En esencia, este modelo se basa en la interacción entre dos paradigmas diferentes, que pueden residir en ordenadores distintos, uno de los cuales se realiza peticiones (el cliente) que son

respondidas por el otro (el servidor), de acuerdo con un esquema predefinido (el protocolo). [6]

Servicios que ofrecen un ISP

Los servicios en Internet son ofrecidos por programas servidores residentes en ciertos nodos conectados a la red, que permanecen a la escucha de posibles peticiones por parte de algún cliente. El usuario de la Red interactúa con ella a través de uno o varios programas cliente, que son los que el usuario manipula directamente. [6]

Vulnerabilidad

Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. [7]

Riesgo

Se denomina riesgo a la posibilidad que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma. [7]

Amenazas

En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, maquinas o sucesos) que -de tener la oportunidad- atacarían al sistema produciéndole daños aprovechando de su nivel de vulnerabilidad. [7]

I. TRABAJOS RELACIONADOS

Para el presente proyecto se toma como referencia los siguientes trabajos y se puntualizara los temas que nos servirán.

Existen varias investigaciones realizadas sobre los riesgos que afectan a los proveedores de internet como es el caso de estudio de realizado por: Enrique Oropeza Gorocica, titulado “ESTRATEGIA DE SEGURIDAD PARA UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP) MEXICANO BASADA EN EL ESTÁNDAR”, en donde menciona el propósito del análisis de riesgo es realizar un estudio sobre los riesgos a cada tipo de

información del ISP o de sus clientes y cuáles serían los daños que se generarían si dicha información fuera comprometida. [8]

Este proyecto servirá como referencia para conocer cuáles son los pasos para realizar un análisis de riesgos adecuado a los ISP en base a una metodología y también el impacto que ocasionarían al materializarse.

Por otro lado, en la investigación realizada por los estudiantes Victor Hugo Medina Cartuche y Stalin Eduardo Yunga Rodriguez titulado "ESTUDIO DE FACTIBILIDAD Y DISEÑO DE UNA RED ISP INALÁMBRICA PARA BRINDAR EL SERVICIO DE VALOR AGREGADO A LA CIUDAD DE PALORA", mencionan
que en la selección de la tecnología idónea para ISP´s se recomienda primero realizar una evaluación sobre los principales problemas relacionados con el servicio actual de internet y después realizar una comparación entre las tecnologías implementadas a nivel de ISP´s. [9]
Esta investigación será útil para tener en cuanta cuales son los aspectos importantes que deberían incorporar un ISP para ofrecer una alta disponibilidad de sus servicios, así mismo identificar los procesos que se deben aplicar para garantizar la continuidad de los servicios.

J. METODOLOGÍA

Para realizar el presente proyecto el tipo de investigación será descriptivo, ya que se pretende describir los riesgos que afectan la disponibilidad del servicio de los proveedores de internet (ISP) en los cantones Cañar, el Tambo y Suscal. Para lo cual se lo realizara cumpliendo las siguientes fases:

1. **Identificación y delimitación del problema**

   En esta primera etapa de la investigación se identificará a los distintos proveedores de servicio de Servicios de internet (ISP) en los tres cantones ante mencionados, en las cuales se aplicará un análisis de riegos.

2. **Elaboración y construcción de los instrumentos**

   Los instrumentos a utilizar son encuestas y entrevistas al encargado de administrar el servicio de internet, para determinar los riesgos tecnológicos y elaborar un plan de análisis de riesgos mediante una metodología.

3. **Observación y registro de datos**

   Se procede al análisis e interpretación de la información obtenida a través de las encuestas y entrevistas aplicadas a los distintos proveedores del servicio de Internet, primero sobre cuáles son los principales problemas que afectan a la continuidad de los servicios, para luego determinan los riesgos tecnológicos que serán considerados para el análisis de riesgos.

4. **Análisis**

   Luego de haber aplicado el análisis de riesgos según la metodología seleccionada se analiza e interpreta cada uno de los riesgos encontrados que afectan el funcionamiento de los servicios de Internet.

K. CRONOGRAMA DE ACTIVIDADES														
N°	ACTIVIDAD	MES I				MES II				MES III				MEDIOS DE VERIFICACIÓN
		S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	
1	**Realizar un estudio teórico de las metodologías para un análisis de riesgo.**													
1.1	-Buscar y seleccionar sobre las metodologías de análisis de riesgos. .													Lista de documentos que contenga las fases de la metodología de riesgos
2	**Determinar los riesgos tecnológicos que afectan la disponibilidad de los servicios de los proveedores de Internet (ISP) en los cantones Cañar, el Tambo y Suscal.**													
2.1	Elaborar un modelo de encuesta relacionado ISP													Hojas de Excel
2.2	Permiso para admitir la aplicación de las encuestas.													Oficios de Autorización para los proveedores del servicio de internet.
2.3	Aplicación de la encuesta a los encargados de administrar la red													Hojas de Excel con sus respectivas respuestas.
2.4	Identificar los riesgos tecnológicos													Documentación de resultados
3	**Realizar un análisis de riesgos en base a una metodología que incluya los activos informáticos de los ISP.**													
3.1	Aplicación del análisis de riegos													Documentación
3.2	Identificar las amenazas que están expuestas													
3.3	Determinar si existen salvaguardas para los activos													
3.4	Estimar el impacto si una amenaza llegara a suceder													

L. DECLARACIÓN FINAL
Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES	
DIRECTOR:	Ing. Luis Pinos Castillo
ESTUDIANTE 1	Manuel Lizardo Quizhpi Cazho

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	Cañar
Fecha:	05/03/2021

Firmas:

Nombre: Ing. Luis Pinos Castillo	Nombre: Manuel Quizhpi
CC:	C.C.:0302913108
Director del Proyecto	**Estudiante / Egresado**

O. APROBACIÓN	
Firmas:	
Nombre: CC: **Primer Par Revisor**	Nombre: C.C.: **Segundo Par Revisor**

P. REFERENCIAS

Bibliografía

[1] J. P. García-Moran, Hacking y Seguridad en Internet, Madrid: RA-MA, 2014.

[2] J.-F. CARPENTIER, La seguridad informática en la PYME: Situación actual y mejores prácticas, Barcelona: Ediciones ENI, 2016.

[3] J. . F. MARTÍNEZ VALVERDE y . F. ROJAS RUIZ, Comercio digital internacional, Madrid: Ediciones Paraninfo, S.A, 2017.

[4] D. R. Lopez, Internet. la Red Con Mayusculas. E-book, Madrid: MAD-Eduforma.

[5] P. Aguilera López, Seguridad informática, Editex.

[6] E. Oropeza Gorocica, «https://repositorio.tec.mx,» Noviembre 2006. [En línea]. Available: https://repositorio.tec.mx/handle/11285/567256.

[7] V. H. Medina Cartuche y S. . E. Yunga Rodriguez, «http://dspace.espoch.edu.ec,» 2017. [En línea]. Available: http://dspace.espoch.edu.ec/bitstream/123456789/3321/1/98T00049.pdf.

[8] M. Campoverde-Molina y L. Valverde, «Accessibility analysis of the web portals of the educational institutions in Cuenca, Ecuador,» *Revista Cátedra,* vol. 2, nº 2, pp. 55-75, 2019.

[9] V. Simbaña-Gallardo y S. Luján-Mora, «Instructions about the manuscript structureof Revista Cátedra,» *Revista Cátedra,* vol. 1, nº 1, pp. 36-52, 2018.

[10] Universidad Católica de Cuenca, «Directrices para autores/as,» 2020. [En línea]. Available: https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/about/submissions.

Lizardo Manuel Quizhpi Cazho portador(a) de la cédula de ciudadanía Nº **0302913108**. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"**Riesgos que afectan la disponibilidad de servicio en los proveedores de Internet en los cantones Cañar, el Tambo y Suscal." de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, **25 de abril de 2022**

F: .....

Lizardo Manuel Quizhpi Cazho

C.I. **0302913108**