UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

DICIEMBRE 2021 - ABRIL 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

SISTEMAS DE INFORMACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

Análisis técnico de los riesgos de la administración remota en recursos tecnológicos en la empresa INTERDATOS S.A. de la ciudad de Babahoyo

EGRESADO:

Quinatoa Barriga Allan Alexander

TUTOR:

Ing. Nelly Karina Esparza Cruz

AÑO 2022

CONTENIDO

RESUMEN

A nivel mundial, desde los inicios de la pandemia, la seguridad de TI empresarial tuvo gran demanda, debido a que, el mundo se adaptaba a trabajar desde casa, los equipos de TI trabajaban horas extra para permitir el acceso remoto a millones de empleados. En el 2021, para hacer frente a esta problemática, la mayoría de los equipos de seguridad de TI se vieron obligados a implementar rápidamente soluciones para el acceso remoto durante un tiempo impredecible. En la actualidad, se requiere brindar a las empresas acceso a aplicaciones, datos y servicios empresariales, y también los administradores requieren equipos para acceder a esos servicios de una manera segura y confiable. Los mecanismos de seguridad para la administración de acceso remoto, necesitan tener la función de mitigar significativamente los ataques. El objetivo del presente caso de estudio es realizar un análisis técnico de los riesgos de la administración remota en recursos tecnológicos en la empresa INTERDATOS S.A. de la ciudad de Babahoyo.

Palabras clave

Análisis, riesgos, administración remota, recursos, conexiones

ABSTRACT

Globally, since the start of the pandemic, enterprise IT security has been in high demand as the world adapts to working from home, with IT teams working overtime to enable remote access for millions of employees. In 2021, to address this issue, most IT security teams were forced to quickly deploy solutions for remote access during unpredictable times. Today, businesses are required to provide access to business applications, data, and services, and administrators require equipment to access those services in a secure and reliable manner. Security mechanisms for remote access management need to have the function of significantly mitigating attacks. The objective of this case study is to carry out a technical analysis of the risks of remote administration in technological resources in the company INTERDATOS S.A. from the city of Babahoyo.

Keywords

Analysis, risks, administration, remote, resources

PLANTEAMIENTO DEL PROBLEMA

A nivel mundial, desde los inicios de la pandemia, la seguridad de TI empresarial tuvo gran demanda. Esto debido a que, el mundo se adaptaba a trabajar desde casa, los equipos de TI trabajaban horas extra para permitir el acceso remoto a millones de empleados. Esta transición se realizó sin problemas para la mayoría de las organizaciones, pero aún quedan muchas brechas de seguridad casi un año después. El riesgo constante violación de datos es un ejemplo preocupante de cuán vulnerables son las organizaciones a la actividad maliciosa en nuestro entorno de riesgo en constante evolución. Por eso el acceso a una red o a la información está totalmente ligada a las personas, por lo tanto, en cualquier acceso a la información surge un problema importante el cual es la seguridad.

En el 2021, para hacer frente a esta problemática, la mayoría de los equipos de seguridad de TI se vieron obligados a implementar rápidamente soluciones para el acceso remoto durante un tiempo impredecible y de esa manera mejorar el rendimiento de la seguridad en las empresas.

Para muchas organizaciones mexicanas, el COVID-19 cambió drásticamente el cálculo de riesgo para el trabajo remoto. En enero de 2020, muchas empresas vieron el trabajo remoto con escepticismo; en marzo, la opción para muchos era convertirse en una empresa remota o cerrar. Para muchos usuarios, adoptar tecnologías y nuevas prácticas técnicas al principio fue muy caótico, debido a la necesidad de la urgencia de continuar cona las labores empresariales. A estas alturas, la mayoría de las empresas, para sorpresa de algunos, se han adaptado con éxito al nuevo entorno.

En Ecuador, las empresas proveedoras de internet en lo referente al acceso remoto a las redes, a la administración remota de los sistemas y, por ende, de los negocios a través de la Internet, se han reconocido como las innovaciones claves de la segunda mitad del

siglo veinte atribuyendo al uso de la Internet por las empresas, un papel significativo en el sorprendente crecimiento continuo durante más de diez años de la economía estadounidense.

Este reconocimiento no hace más que ubicar al comercio y a la administración de los negocios a través de la Internet, como herramientas que afectan no solamente los medios para el intercambio de mercaderías y servicios, sino también los procedimientos internos de las organizaciones, rebajando costos en compras, controlando las relaciones con proveedores, con sistemas logísticos y de inventario más sofisticados, y mejorando la planificación de la producción.

En la empresa INTERDATOS S.A. es una empresa del Ecuador, con sede principal en Babahoyo. Opera en telefonía tradicional y telecomunicaciones alámbricas sector, la empresa fue fundada en 07 de diciembre del 2012. Tradicionalmente, solo se accedía a las redes empresariales en equipos proporcionados por la empresa. Este arreglo ha permitido a las empresas acceso sin restricciones para monitorear y configurar el dispositivo precisamente de acuerdo con sus perfiles de riesgo y estrategias de mitigación.

Con la llegada de la pandemia, la prestación servicios de internet en los hogares aumentaron su demanda, debido a que las clases se realizaron de manera virtual. Debido a esto la empresa INTERDATOS SA tuve que implementar estrategias para administrar remotamente los equipos con la finalidad solucionar las diferentes dificultades que se presentan en la prestación de servicio. Es por eso que nace la problemática de gestionar la seguridad de las conexiones remotas, cuyo objeto es garantizar la integridad de los datos que por medio estas se manejan.

JUSTIFICACIÓN

En la actualidad, se requiere brindar un mejor acceso a las aplicaciones, datos y servicios empresariales, así también los administradores requieren equipos para acceder a esos servicios de una manera segura y confiable. El uso de dispositivos electrónicos puede ahorrar una cantidad considerable de tiempo y dinero, pero presenta riesgos, especialmente vulnerabilidad a explotaciones conocidas debido a la falta de disciplina de parches, por lo cual un análisis técnico de riesgos en los recursos tecnológicos de la organización se puede realizar para mitigar ese los posibles riesgos que se puedan presentar.

Los sistemas de información de administración remota son utilizados actualmente, por sus diferentes aplicaciones. Estos deben manejar un alto nivel en seguridad en su información y sus redes, para que sus vulnerabilidades, riesgos y amenazas no sean tan factibles a un ataque se debe realizar estudios mediante matrices de análisis de riego con el fin de identificarlos y mitigarlos

Para una conexión exitosa, la empresa INTERDATOS SA con el fin de potenciar la velocidad de conexión, debe tener la posibilidad del control remoto de un mismo equipo desde ubicaciones distintas y utilizar, desde todas ellas, su gran cantidad de utilidades, como, transferencia de archivos y configuraciones de forma segura.

Los mecanismos de seguridad para la administración de acceso remoto en la empresa INTERDATOS, necesita tener la función de mitigar significativamente los ataques, como los secuestros de cuentas con contraseñas comprometidas o reutilizadas. Del mismo modo, se necesita contar herramientas virtuales que pueden mitigar algunos tipos de persistencia de atacantes. No son, ni pretenden ser, defensas sólidas contra todo tipo de ataques, especialmente cuando un cliente se ejecuta en un sistema que no es de confianza.

OBJETIVOS DEL ESTUDIO

Objetivo general

Realizar un análisis técnico de los riesgos de la administración remota en recursos tecnológicos en la empresa INTERDATOS S.A. de la ciudad de Babahoyo.

Objetivos específicos

- Comprender los elementos tecnológicos necesarios para gestionar la seguridad la administración remota.
- Examinar recursos tecnológicos de la empresa INTERDATOS S.A. de la ciudad de Babahoyo.
- Establecer las normas de seguridad del escritorio remoto para la empresa INTERDATOS S.A. de la ciudad de Babahoyo.

LÍNEA DE INVESTIGACIÓN

El presente caso de estudio titulado: “Análisis técnico de los riesgos de la administración remota en recursos tecnológicos en la empresa INTERDATOS S.A. de la ciudad de Babahoyo”, está estrechamente relacionado con la línea de investigación Sistemas de información y comunicación, emprendimiento e innovación; y a su vez está vinculado conjuntamente con la sublínea Redes y tecnologías inteligentes de software y hardware.

En consecuencia, durante la realización de mis practicas profesionales, las cuales las realicé en la empresa INTERDATOS, pude identificar esta problemática, por lo que me pareció conveniente enfocar el presente tema de titulación para evaluar esta problemática relacionándola a la línea de investigación antes mencionada.

MARCO CONCEPTUAL

Los avances tecnológicos han creado oportunidades para que las personas trabajen fuera de la oficina. Los beneficios del trabajo remoto están bien documentados en términos de costos reducidos para los empleadores, ahorro de tiempo y costos de viaje, mayor flexibilidad para los empleados y mayor productividad. Debido a la situación con el COVID-19, las empresas y los gobiernos de todo el mundo exigen que sus empleados y ciudadanos trabajen desde casa. (Bolivar, 2018)

Si bien esto puede ayudar a limitar la propagación de la enfermedad, expone a las organizaciones a ciberataques. Muchos se ven obligados a hacer el ajuste sin ninguna planificación formal. Aquí es donde entra en juego una evaluación de riesgos de ciberseguridad. Una evaluación de riesgos es el primer paso que debe tomar para comprender mejor las debilidades de seguridad de su red y qué se debe hacer para repararlas.

La administración remota del sistema permite configurar y administrar su entorno de acceso a datos desde la comodidad de su escritorio. La administración remota es una forma de controlar otro dispositivo sin estar físicamente frente a él. Esta es necesaria porque, permite a los usuarios acceder al sistema que necesitan cuando no pueden estar disponibles físicamente para conectarse. Es decir, los usuarios acceden a los sistemas de forma remota a través de telecomunicaciones o conexión a internet. Las organizaciones utilizan efectivamente los servicios de acceso remoto para conectar internamente las redes y el sistema. (Zapata, 2016)

La administración remota de servidores es un segmento de mercado que incluye productos y servicios que permiten a los profesionales de TI monitorear y controlar los centros de datos desde fuera del sitio. Sin embargo, la administración remota de

servidores no significa necesariamente que una organización instale servidores distribuidos.

Frente al servidor local, el servidor remoto se refiere a una computadora que está ubicada de forma remota y tiene un software de servidor web, una base de datos y otros recursos para manejar las solicitudes remotas enviadas por los usuarios de un sitio web. Un servidor remoto puede albergar uno o varios sitios web. Esto permite a los administradores ejecutar complementos y herramientas en una computadora remota para administrar funciones, roles y servicios de roles. El software incluye herramientas para la actualización con reconocimiento de clústeres, la gestión de directivas de grupo y la gestión de Hyper-V, así como el analizador de mejores prácticas. (Aguilar, 2017)

La práctica de administrar recursos de red desde una ubicación remota. La capacidad de administración remota es esencial en un entorno de red de área amplia (WAN) de nivel empresarial y para los administradores de red que están de viaje. Los proveedores de redes y software ofrecen muchos tipos de soluciones para la administración remota, incluidas las siguientes:

Dispositivos de acceso remoto, que permiten a los administradores marcar sus redes corporativas desde ubicaciones remotas utilizando una computadora portátil y un módem. Luego pueden usar varias herramientas de software para administrar diferentes aspectos de la red. Por ejemplo, en una red basada en Microsoft Windows 2000, los administradores pueden usar Microsoft Management Console (MMC) con complementos adecuados instalados para administrar de forma remota servidores que ejecutan Windows 2000 desde cualquier computadora que ejecute Windows 2000. También pueden usar software de control remoto como pcAnywhere para ejecutar cualquier herramienta administrativa desde una plataforma remota. (López Vargas & Vázquez Chávez, 2016)

Programas como Putty, que los administradores pueden usar a través de enlaces de acceso remoto para configurar dispositivos como enrutadores y conmutadores Ethernet desde el símbolo del sistema. Muchos de estos dispositivos admiten otra forma de administración llamada administración fuera de banda (OBM), que permite a los administradores marcar directamente el dispositivo a través de un módem conectado a un puerto serie RS-232 en el dispositivo y configurar el dispositivo mediante un programa como HyperTerminal. (Agudelo, 2020)

Administración remota segura a través de Internet. Microsoft Internet Information Server (IIS) en Windows NT - Internet Information Services en Windows 2000 - incluye una herramienta de administración remota que se implementa como una aplicación de páginas Active Server (ASP) en el servidor. Con esta herramienta, los administradores pueden usar un navegador web simple como Microsoft Internet Explorer para configurar de forma remota servidores World Wide Web (WWW) y File Transfer Protocol (FTP) que se ejecutan en Windows NT Server y Windows 2000 Server.

Conmutadores de matriz operados por código, que son útiles si es necesario reiniciar los dispositivos remotos. Un interruptor está conectado a la fuente de alimentación de un dispositivo y se puede controlar desde una ubicación remota a través de una computadora y un módem.

El acceso remoto generalmente se logra combinando hardware, software y conectividad de red. Por ejemplo, antes de la plena disponibilidad de Internet, el acceso remoto tradicional se lograba a través de un software de emulación de terminal que controlaba el acceso a través de un módem de hardware conectado a una red telefónica.

Sin embargo, hoy en día, el acceso remoto se logra comúnmente a través de soluciones de software seguras, como un software VPN que se conecta a los hosts a través

de una interfaz Wi-Fi o una interfaz de red cableada o mediante la conexión directa a través de la red de Internet.

El acceso remoto a la computadora es la capacidad de acceder a otro dispositivo o red que no está en su presencia física. El acceso remoto a la computadora le permite a un empleado acceder al escritorio de una computadora y sus archivos desde una ubicación remota. Esto ayuda a permitir que un empleado que trabaja desde casa, trabaje de manera efectiva. Con el brote del nuevo coronavirus, el acceso remoto a computadoras ha adquirido una mayor importancia. El acceso remoto a la computadora puede permitir que los empleados continúen haciendo su trabajo fuera de su lugar de trabajo físico, lo que puede ayudar a mantener las empresas en funcionamiento. (Martí, 2020)

El acceso remoto a las computadoras no es nuevo. Puede tener ventajas para las personas en el trabajo y en su vida privada. Aquí hay dos ejemplos.

- El software de acceso remoto es útil cuando está en una reunión en otra oficina con su computadora portátil, o teletrabajando, y necesita un archivo importante que está en la computadora de su oficina.
- El acceso remoto a la computadora puede ayudarlo a ayudar a alguien en su vida personal que podría estar lejos. Es posible que desee ayudar a los padres ancianos a terminar sus declaraciones de impuestos, por ejemplo. Podrá acceder a su computadora y sus documentos financieros si tiene acceso remoto configurado en sus respectivas computadoras.

Las empresas deben preocuparse por la seguridad del acceso remoto. Las soluciones de acceso remoto podrían crear vulnerabilidad. Si no se cuenta con las soluciones de seguridad adecuadas, las conexiones remotas podrían actuar como una puerta de entrada para que los ciberdelincuentes accedan a sus dispositivos y datos.

Los piratas informáticos podrían usar el protocolo de escritorio remoto para acceder de forma remota a los dispositivos encargados del proceso. Los servidores de escritorio remoto se conectan directamente a Internet cuando reenvía puertos en su enrutador. Los piratas informáticos y el malware pueden atacar una debilidad en esos enrutadores. Es por ello, que es adecuado que la empresa realice el análisis periódico de riesgos respectivo.

Una evaluación de riesgos es una forma de identificar sus datos y dispositivos más importantes, amenazas potenciales, riesgos de seguridad cibernética, cómo un pirata informático podría obtener acceso a sus sistemas, qué tan vulnerable es usted como objetivo e impacto si se explotan las vulnerabilidades. El proceso implica identificar, estimar y priorizar los riesgos para los activos, las operaciones y las personas de una organización, que resultan del uso y operación de los sistemas de información. Una evaluación de riesgos también ayuda a proteger la función, la misión, la reputación y la imagen de la empresa. (Ortiz Restrepo & Valencia Duque, 2017)

El análisis de riesgos es el proceso de identificar y analizar problemas potenciales que podrían afectar negativamente a iniciativas o proyectos comerciales clave. Este proceso se realiza para ayudar a las organizaciones a evitar o mitigar esos riesgos. Realizar un análisis de riesgo incluye considerar la posibilidad de eventos adversos causados por procesos naturales, como tormentas severas, terremotos o inundaciones, o eventos adversos causados por actividades humanas maliciosas o inadvertidas. Una parte importante del análisis de riesgos es identificar el daño potencial de estos eventos, así como la probabilidad de que ocurran. (Crespo, 2017)

Las organizaciones deben comprender los riesgos asociados con el uso de sus sistemas de información para proteger de manera eficaz y eficiente sus activos de información. El análisis de riesgos puede ayudar a una organización a mejorar su

seguridad de varias maneras. Según el tipo y el alcance del análisis de riesgos, las organizaciones pueden utilizar los resultados para ayudar a:

- identificar, calificar y comparar el impacto general de los riesgos para la organización, tanto en términos de impacto financiero como organizacional;
- identificar brechas en la seguridad y determinar los próximos pasos para eliminar las debilidades y fortalecer la seguridad;
- mejorar la comunicación y los procesos de toma de decisiones en relación con la seguridad de la información;
- mejorar las políticas y procedimientos de seguridad y desarrollar métodos rentables para implementar estas políticas y procedimientos de seguridad de la información;
- implementar controles de seguridad para mitigar los riesgos más importantes ;
- aumentar la conciencia de los empleados sobre las medidas de seguridad y los riesgos destacando las mejores prácticas durante el proceso de análisis de riesgos; y
- comprender los impactos financieros de los posibles riesgos de seguridad.

Un análisis de riesgos muy bien planificado, dirigido y ejecutado, es una herramienta importante para administrar los costos asociados con los riesgos, así como para ayudar en el proceso de toma de decisiones de una organización. Las evaluaciones de riesgos son más necesarias que nunca, ya que las organizaciones enfrentan el desafío de proteger a los trabajadores remotos e híbridos junto con los empleados en la oficina.

No se puede negar la importancia de una evaluación de riesgos. Identificar y mitigar los riesgos, amenazas y vulnerabilidades que existen dentro de las infraestructuras de TI de manera oportuna es crucial para disminuir el impacto de estos peligros y evitar que interrumpan seriamente las operaciones comerciales. (Corda, Viñas, & Coria, 2017)

Las evaluaciones de riesgos han sido durante mucho tiempo elementos esenciales en una buena planificación y gestión de TI. Ahora, a raíz de la pandemia global de COVID-19, muchas organizaciones deben realizar un nuevo tipo de evaluación de riesgos para mantener las operaciones seguras: una evaluación de riesgos de la fuerza laboral remota. En este proceso se examina los diferentes tipos de riesgos, amenazas y vulnerabilidades que la administración de TI debe abordar para minimizar las interrupciones y mantener la productividad de los empleados, y exploremos cómo una evaluación de riesgos de la fuerza laboral remota encaja en el proceso.

Desde una perspectiva de TI, los riesgos, amenazas y vulnerabilidades se definen inicialmente como internos o externos. Por ejemplo, un riesgo interno puede ser la incapacidad de proporcionar servicios de TI para mantener los sistemas y servicios existentes, mientras que los riesgos externos incluyen interrupciones en los servicios públicos, daños y destrucción de infraestructura crítica. (Altamirano, 2019)

Las amenazas internas, por otro lado, incluyen pérdida de energía, fallas en los equipos, robo de equipos y vandalismo. Las amenazas externas incluyen la pérdida de poder comercial, la pérdida de servicios de red y el acceso no autorizado a los centros de datos. Las vulnerabilidades internas incluyen sistemas que no tienen parches adecuados, planes de respaldo que no se prueban y controles de acceso de seguridad que no funcionan. Las vulnerabilidades externas incluyen no usar cámaras de seguridad o iluminación externas, pararrayos y energía de respaldo de emergencia.

Las evaluaciones periódicas de riesgos identifican problemas que deben abordarse, identifican oportunidades para minimizar la probabilidad de que ocurran riesgos y definen estrategias para mitigar la gravedad de los riesgos potenciales, en caso de que ocurra uno.

Estas mismas evaluaciones deben ser consideradas cuando se trata de trabajadores remotos e híbridos. El problema se complica porque los empleados hoy en día trabajan en muchos lugares diferentes, a diferencia de una sola oficina. Como resultado, las evaluaciones de riesgos para empleados remotos e híbridos deben realizarse como actividades individuales y deben seguir un proceso coherente. (Aguilar J. , 2021)

Al adaptar o crear una evaluación de riesgos para trabajadores remotos, los riesgos internos y externos deben identificarse y abordarse en tres áreas:

- Centro de datos;
- Recursos de red que conectan a empleados remotos; y
- Ubicación del trabajador remoto.

Las evaluaciones del centro de datos examinan los riesgos, las amenazas y las vulnerabilidades internas y externas en el centro de datos y la infraestructura de una empresa. La evaluación de riesgos, amenazas y vulnerabilidades en los centros de datos debe realizarse periódicamente en función del tamaño y la complejidad de la empresa.

Los centros de datos más grandes y más densamente poblados deben evaluarse con mayor frecuencia, tal vez trimestralmente o incluso mensualmente. Estas evaluaciones pueden verse afectadas por la cantidad de trabajadores remotos y su demanda de recursos de TI, como aplicaciones, archivos de datos y bases de datos.

Los resultados de estas evaluaciones se pueden utilizar para ajustar la administración del sistema, la respuesta a incidentes, el respaldo y la recuperación, la protección y administración de datos, la recuperación ante desastres, la seguridad del acceso físico y local y las actividades de administración ambiental.

Las evaluaciones de riesgos de la red también pueden verse afectadas por la cantidad de trabajadores remotos. La demanda de un mayor ancho de banda significa

revisiones más frecuentes del uso del ancho de banda, los tiempos de respuesta y el rendimiento general de la red.

El internet es el servicio de red utilizado con más frecuencia por los trabajadores para obtener acceso a servicios y aplicaciones, pero la gestión de los riesgos de Internet generalmente está fuera del control de una organización. Lo mismo se aplica a la gestión de riesgos asociados con los trabajadores que acceden a Internet a través de operadores de telecomunicaciones locales. (Machín & Gazapo, 2016)

Sin embargo, los usuarios pueden monitorear de manera proactiva el rendimiento de la red utilizando una variedad de herramientas especializadas. También pueden ponerse en contacto con los proveedores de red, tanto ISP como operadores de telecomunicaciones locales, en caso de que se detecten anomalías en el rendimiento.

Las evaluaciones de los trabajadores remotos son el tramo final del proceso. Los factores de riesgo que evalúa una empresa se pueden modificar para reflejar con mayor precisión una estrategia de evaluación de riesgos de la fuerza laboral remota. Los empleados que trabajan en casa o en una oficina alternativa deben ser diligentes en la administración y el mantenimiento de sus sistemas y recursos de acceso remoto.

Esto se puede hacer en asociación con el personal de TI y los equipos de la mesa de ayuda asignados para administrar las actividades de comunicaciones remotas. Los empleados que trabajan de forma remota pueden enfrentar riesgos externos que van más allá de los problemas tecnológicos, entre ellos, tratar con niños pequeños y otros miembros de la familia, así como atender problemas de salud y bienestar mental. Muchos de estos problemas han surgido a raíz de la pandemia y desafían tanto a los empleados como a las organizaciones. (Albán, 2018)

Una evaluación de riesgos de TI involucra cuatro componentes clave. Discutiremos cómo evaluar cada uno en un momento, pero aquí hay una breve definición de cada uno:

- Amenaza: una amenaza es cualquier evento que podría dañar a las personas o los activos de una organización. Los ejemplos incluyen desastres naturales, fallas en sitios web y espionaje corporativo.
- Vulnerabilidad: una vulnerabilidad es cualquier punto débil potencial que podría permitir que una amenaza cause daños. Por ejemplo, el software antivirus desactualizado es una vulnerabilidad que puede permitir que un ataque de malware tenga éxito. Tener una sala de servidores en el sótano es una vulnerabilidad que aumenta las posibilidades de que un huracán o una inundación arruine el equipo y provoque tiempo de inactividad. Otros ejemplos de vulnerabilidades incluyen empleados descontentos y hardware obsoleto. La base de datos nacional de vulnerabilidades del NIST mantiene una lista de debilidades específicas basadas en códigos.
- Impacto: el impacto es el daño total que sufriría la organización si una amenaza explotara una vulnerabilidad. Por ejemplo, un ataque exitoso de ransomware podría resultar no solo en pérdida de productividad y gastos de recuperación de datos, sino también en la divulgación de datos de clientes o secretos comerciales que resultan en pérdida de negocios, honorarios legales y multas por cumplimiento.
- Probabilidad: esta es la probabilidad de que ocurra una amenaza. Por lo general, no es un número específico sino un rango.

La evaluación de riesgos de TI es un proceso de análisis de amenazas y vulnerabilidades potenciales a sus sistemas de TI para establecer qué pérdida podría esperar incurrir si ocurren ciertos eventos. Su objetivo es ayudarlo a lograr una seguridad

óptima a un costo razonable. Hay dos metodologías predominantes para evaluar los diferentes tipos de riesgo: análisis de riesgo cuantitativo y cualitativo. (Miranda, 2016)

La evaluación cuantitativa mide el riesgo utilizando cantidades monetarias. Utiliza fórmulas matemáticas para brindarle el valor de las pérdidas esperadas asociadas con un riesgo particular, en función de:

- el valor del activo
- la frecuencia de ocurrencia del riesgo
- la probabilidad de pérdida asociada

Estos resultados monetarios podrían ayudarlo a evitar gastar demasiado tiempo y dinero en reducir riesgos insignificantes. Por ejemplo, si es poco probable que suceda una amenaza o cuesta poco o nada remediarla, probablemente presente un riesgo bajo para su negocio. Sin embargo, si es probable que suceda una amenaza a sus sistemas de TI clave, y podría ser costosa de reparar o afectar negativamente a su negocio, debe considerarla de alto riesgo.

Es posible que se desee utilizar esta información de riesgo para realizar un análisis de costo/beneficio para determinar qué nivel de inversión haría que el tratamiento de riesgo valiera la pena. Pero hay que tener en cuenta que las medidas cuantitativas de riesgo solo son significativas cuando tiene buenos datos. Es posible que no siempre tenga los datos históricos necesarios para calcular la probabilidad y las estimaciones de costos de los riesgos relacionados con TI, ya que pueden cambiar muy rápidamente.

La evaluación cualitativa del riesgo se basa en opiniones. Se basa en el juicio para categorizar los riesgos en función de la probabilidad y el impacto y utiliza una escala de calificación para describir los riesgos como:

- bajo: es poco probable que ocurra o afecte su negocio
- medio - posible que ocurra e impacte
- alto: es probable que ocurra y tenga un impacto significativo en su negocio

A menudo, puede ser mejor utilizar un enfoque mixto para las evaluaciones de riesgos de TI, combinando elementos de análisis cuantitativo y cualitativo. Puede usar los datos cuantitativos para evaluar el valor de los activos y la expectativa de pérdida, pero también involucrar a las personas en su negocio para obtener su conocimiento experto. Esto puede requerir tiempo y esfuerzo, pero también puede resultar en una mayor comprensión de los riesgos y mejores datos que los que proporcionaría cada método por sí solo.

MAGERIT versión 3, es la metodología de análisis y gestión de riesgos desarrollada por el ex Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital con la colaboración del Centro Criptológico Nacional. Esta es una metodología pública que se puede usar libremente y no requiere permiso previo. Está dirigido principalmente a las entidades en el ámbito del Esquema Nacional de Seguridad para cumplir con el principio de gestión de seguridad basada en riesgos, así como el análisis de requerimientos y gestión de riesgos, considerando la información para realizar misiones, prestar servicios y lograr los objetivos de la organización. (Chulde, 2021)

Siguiendo la terminología de las reglas ISO 31000, MAGERIT responde a lo que se denomina “proceso de gestión de riesgos”, apartado 4.4 (“Implementación de la gestión de riesgos”) dentro del “marco de gestión de riesgos”. En otras palabras, MAGERIT implementa el proceso de gestión de riesgos en el marco de las decisiones de los órganos de gobierno a la luz de los riesgos derivados del uso de las tecnologías de la información.

MAGERIT persigue los siguientes Objetivos:

1. Sensibilizar a las organizaciones de los informes de la existencia de riesgos y la necesidad de gestionar
2. Proporcionar un enfoque sistemático para analizar los riesgos derivados del uso de las tecnologías de la información y las comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento adecuado para mantener los riesgos bajo control indirecto
4. Preparar a la Organización para los procesos de evaluación, auditoría, certificación y acreditación, según corresponda en cada caso

MARCO METODOLÓGICO

El tipo de investigación utilizada es la mixta, para eso se utilizó la metodología de Análisis y Gestión de Riesgos de los sistemas de información (MARGERIT) en su versión 3,0, que dispone de cinco fases y de la cual se creyó conveniente utilizar de cuatro de ellas, las cuales son: determinar los activos relevantes para la organización, determinar a qué amenazas están expuestos los activos, estimar el impacto y estimar el riesgo.

En la fase 1 se identificaron los activos relevantes de la institución, obteniendo un inventario actualizado del hardware y el software, la nómina de talento humano, los procesos de la institución por departamentos, la dependencia que tienen los activos del área de tecnología, el levantamiento de información se llevó a cabo en matrices.

En la fase 2 se identificaron las posibles amenazas que se pueden materializar en los activos, que son eventos que pueden ocurrir causando daños en los activos y perjuicios para la institución, motivo por el cual es necesario que se identifiquen a tiempo para mitigar eventos no deseados. Para la identificación de las amenazas se tomó cuatro clasificaciones importantes de la metodología, tales como: desastres de origen natural, desastres de origen industrial, desastres de manera no intencionada e intencionada.

Luego se procedió a la estimación del impacto y la estimación del riesgo tomando en cuenta: la dimensión de seguridad en caso que se materialice, la degradación de los activos y la frecuencia de que ocurra dicho evento, para cada amenaza existe una matriz donde se detalla los tipos de activos, las dimensiones, la descripción de la amenaza, el valor del impacto y del riesgo y la causa. Las siglas significan lo siguiente: MA (Muy alta), A (Alta), M (Media), B (Baja), MB (Muy baja), MF (Muy frecuente, a diario), F (Frecuente, mensual), FN (Frecuencia normal, anual), PF (Poco frecuente, cada varios años)

RESULTADOS

Para la obtención de los resultados utilizó las siguientes matrices para el análisis de riesgo de la administración remota en recursos tecnológicos en la empresa INTERDATOS S.A. de la ciudad de Babahoyo.

Tabla 1.

Matriz para identificar las amenazas por tipos

Origen	Amenazas	Tipos de activos
Desastres naturales	[N.1] Fuego	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar
	[N.2] Daños por agua	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar
	[N.*] Desastres naturales	Equipos informáticos (hardware)
		Soporte de información
		Instalaciones
		Redes de comunicaciones
		Equipamiento auxiliar

Nota: Esta tabla muestra las amenazas por tipos (naturales, industriales, no intencionadas e intencionadas).

Tabla 2.

Matriz para estimar la valoración del impacto y el riesgo

[CÓDIGO] Descripción sucinta de lo que puede pasar									
Tipos de activos: Que se puede ver afectado por este tipo de amenazas.				Dimensiones: De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante.					
Descripción: Complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas.									
Estimación del impacto					Estimación de la frecuencia				
Impacto		Degradación			Riesgo		Frecuencia		
		1%	10%	100%			PF	FN	F	MF
Valor	MA	M	A	MA	Impacto	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: Razón detallada por la cual se considera el impacto y el riesgo de la amenaza.									

Nota: Esta tabla muestra la valoración que tiene el riesgo e impacto

Con la identificación de las posibles amenazas y los activos que se verían afectados por la misma, se pudo estimar de forma cualitativa el valor del impacto, el mismo que fue de complemento para obtener el valor del riesgo en una matriz. Estos valores fueron cuantificados de acuerdo a las siguientes magnitudes: muy alto=5, alto=4, medio=3,

bajo=2 y muy bajo=1. Posteriormente, se calculó el peso medio de riesgo que tiene cada tipo de amenaza en la institución.

Tabla 3.

Valoración cuantitativa de amenazas

Tipo de amenaza		
Código	**Amenaza**	**Valor Cuantitativo**
[N.1]	Amenaza 1	Valoración
[N.2]	Amenaza 2	Valoración
[N.*]	Amenaza n	Valoración
	Total	Sumatoria
	Media	Promedio

Nota: Esta tabla muestra la valoración cuantitativa del total de amenazas

Mediante una visita a las instalaciones de la empresa se pudo identificar los diferentes activos de la misma, para lo cual se utilizaron las matrices planteadas por la metodología MAGERIT. El inventario del hardware de la empresa INTERDATOS S.A. dio como primer resultado el valor de adquisición de los equipos de hardware y software con un valor de $188.842,59. De acuerdo con la siguiente tabla, se estimó la valoración de impacto y riesgo. En la tabla 4, se muestran un análisis de amenazas realizados.

Tabla 4.

Ataques intencionados – Difusión de software dañino

[A.8] Difusión de software dañino	
Tipos de activos: □ [SW] aplicaciones (software)	**Dimensiones:** 1. [C] Confidencialidad 2. [D] Disponibilidad 3. [I] Integridad 4. [A_S] Autenticidad del servicio 5. [A_D] Autenticidad de los datos

Descripción: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

Estimación del impacto					Estimación del riesgo					
Impacto		Degradación			Riesgo		Frecuencia			
		1%	10%	100%			PF	FN	F	MF
Valor	**MA**	M	**A**	MA	Impacto	MA	A	MA	MA	MA
	A	B	M	A		A	M	**A**	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

Causa: En la empresa INTERDATOS SA no se han registrado este tipo de incidentes, pero en caso de darse podría afectar en el buen funcionamiento tanto del hardware como del software por lo que se considera que tanto el riesgo como el impacto son altos.

MA muy alto	**A** alto	**M** medio	**B** bajo	**MB** muy bajo
PF poco frecuente	**FN** frecuencia normal	**F** frecuente	**MF** muy frecuente	

Nota: Esta tabla muestra los Ataques intencionados y la Difusión de software dañino

Con la identificación de las posibles amenazas y los activos que se verían afectados por la misma, se pudo estimar de forma cualitativa el valor del impacto, obteniendo como resultado la media de cada tipo de amenaza. Lo que indicó el riesgo medio que tiene la organización a que una amenaza se materialice en un activo tecnológico, como se detallan en las tablas: 5,6, 7 y 8.

Tabla 5.

Valoración cuantitativa amenazas naturales

Desastres Naturales		
Código	**Amenaza**	**Valor Cuantitativo**
[N.1]	Fuego	4

[N.2]	Daños por agua	2
[N.*]	Desastres naturales	3
	Total	**9**
	Media	**3**

Nota: Esta tabla muestra la Valoración cuantitativa de amenazas naturales

Tabla 6.

Valoración cuantitativa amenazas de origen industrial

Errores y fallos no intencionados		
Código	**Amenaza**	**Valor Cuantitativo**
[E.1]	Errores de los usuarios	2
[E.2]	Errores del administrador	3
[E.4]	Errores de configuración	3
[E.7]	Deficiencias en la organización	1
[E.8]	Difusión de software dañino	4
[E.9]	Errores de [re-]encaminamiento	2
[E.10]	Errores de secuencia	1
[E.14]	Escapes de información	3
[E.15]	Alteración accidental de la información	2
[E.18]	Destrucción de información	3
[E.19]	Fugas de información	3
[E.20]	Vulnerabilidades de los programas (software)	4
[E.21]	Errores de mantenimiento / actualización de programas (software)	3
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3
[E.24]	Caída del sistema por agotamiento de recursos	2

[E.28]	Indisponibilidad del personal	2
	Total	**41**
	Media	**2,56**

Nota: Esta tabla muestra la Valoración cuantitativa amenazas de origen industrial

Tabla 7.

Valoración cuantitativa amenazas por ataques

Ataques intencionados		
Código	**Amenaza**	**Valor Cuantitativo**
[A.4]	Manipulación de la configuración	3
[A.5]	Suplantación de la identidad del usuario	4
[A.6]	Abuso de privilegios de acceso	3
[A.7]	Uso no previsto	2
[A.8]	Difusión de software dañino	4
[A.11]	Acceso no autorizado	3
[A.12]	Análisis de tráfico	1
[A.13]	Repudio	2
[A.14]	Interceptación de información	2
[A.15]	Modificación deliberada de la información	2
[A.18]	Destrucción de información	4
[A.19]	Revelación de información	3
[A.22]	Manipulación de programas	3
[A.25]	Robo	4
[A.26]	Ataque destructivo	2
[E.28]	Indisponibilidad del personal	2
[A.29]	Extorsión	3
[A.30]	Ingeniería social	3
	Total	**50**
	Media	**2,78**

Nota: Esta tabla muestra la Valoración cuantitativa amenazas por ataques

Finalmente se tomó en cuenta la valoración cualitativa, se desarrolló una propuesta de salvaguardas por cada tipo de amenaza, la misma que ayudará a reducir el riesgo asegurando la continuidad de las funciones que realiza la organización, como se aprecia en la tabla 8.

Tabla 8.

Valoración económica de las salvaguardas

Código	Amenaza	Valor salvaguarda	Detalle
[I.2]	Daños por agua	300	Por mantenimiento a las instalaciones de agua se estima un pago por hora de $15, trabajando 4 horas diaria por cinco días, esta salvaguarda se hace una vez al año
[I.3]	Avería de origen físico o lógico	160	El mantenimiento preventivo de equipos se lo realiza 2 veces al año, teniendo la institución un total de 4 equipos pagando $20,00 por cada uno.
[I.4]	Condiciones inadecuadas de temperatura y/o humedad	4800	El mantenimiento de los equipos de climatización se realizará una vez al año, trabajando 4 horas diarias por tres días, pagando la institución por hora de trabajo $150
[I.5]	Fallo de servicios de comunicaciones	3000	La implementación de enlace redundante se la realiza por un monto en total de $ 3000
[I.5]	Fallo de servicios de comunicaciones	400	El mantenimiento a las redes de comunicación se las realiza una vez al año, trabajando 2 horas por 8 días, cancelando $50 la hora
[I.6]	Degradación de los soportes de almacenamiento de la información	500	El respaldo se la puede realizar en discos duros extraíbles, cd y flash memory, estimando un costo de adquisición de los mismos de $500.
[E.1]	Errores de los usuarios	500	Se capacitará a los usuarios 2 veces al año, el cual se cancelará a la persona un valor de $250 por capacitación.
[E.2]	Errores del administrador	800	Se capacitará a los administradores de la institución dos veces al año, el cual se cancelará a la persona un valor de $400 por capacitación.
[E.8]	Difusión de software dañino	160	La adquisición del antivirus para implementar a los computadores de la institución tuvo un costo de $ 160
[E.9]	Errores de [re-encaminamiento]	200	La capacitación a los usuarios se realizará una vez al año, el cual se cancelará a la persona un valor de $200.

[E.15]	Alteración accidental de la información	300	La capacitación al personal se la realizará dos veces al año, el cual se cancelará a la persona un valor de $150 por capacitación.
[E.18]	Destrucción de información	400	Se estima que el costo por adquisición de soportes de información es de $ 400
[E.19]	Fugas de información	100	La capacitación al personal se la realizará una vez al año, el cual se cancelará a la persona un valor de $100.
[E.19]	Fugas de información	600	Se estima que la adquisición de un sistema de perdida de información es de $ 600
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	400	Para evitar la pérdida de datos, se debe realizar mantenimiento preventivo a los equipos por un costo de $ 400
[A.5]	Suplantación de la identidad del usuario	50	La capacitación del personal antes de ser contratado se la realiza una hora por un valor de $ 50
[A.8]	Difusión de software dañino	700	Se estima que el costo de actualización del software de la institución es de $700
[A.18]	Destrucción de información	150	Se capacitará al 2 veces al año, pagando a la persona un valor de $150 por capacitación.
[A.22]	Manipulación de programas	500	La auditoría a las aplicaciones la realiza la misma institución, pero esta puede generar un cargo de $ 500 por el trabajo.
[A.25]	Robo	100	Las capacitaciones al personal para que no libere información confidencial de la institución tienen un costo de $ 100
[A.25]	Robo	5000	Se estima que la institución debe pagar por un seguro que ampare sus activos un valor de $3500 por año.
[A.25]	Robo	2500	La implementación de cámaras en las instalaciones de la institución tiene un costo de $550

Nota: Esta tabla muestra la Valoración económica de las salvaguardas

DISCUSIÓN DE RESULTADOS

Las instalaciones de la empresa INTERDATOS S.A. cuenta con cuatro equipos de redes (tres routers y un switch). Además, cuenta con cuatro servidores y cuatro computadoras para las oficinas. El software que manejan los servidores en la consola CMD de Windows y las computadoras trabajan con Windows 10.

El área informática de la empresa INTERDATOS S.A. tiene una infraestructura variada de equipos y se encuentra en una etapa de innovación de equipos de última tecnología: lo cual ha tolerado dificultades de compatibilidad, configuración y administración. Se pudo notar que las computadoras con cuentan con un antivirus instalado. Factor que puede ocasionar proliferación de agentes externos dañinos para los equipos de la red.

El control de acceso es controlado por el guardia en la recepción que se encarga de llevar un control del personal que ingresa y sale del edificio. También se pudo constatar que no hay cámaras de seguridad instaladas en la institución. La data Center se compone por un gabinete con puerta y dos racks abiertos donde se están alojados los equipos de comunicación.

Para tener acceso a los sistemas administrativos se lo realiza por medio de una cuenta usuario y clave, las mismas son asignadas a los usuarios, así como también la cuenta de correo electrónico de acuerdo a la petición de cada empleado. El análisis de riesgos realizado, permitió inventariar los activos, determinar las amenazas a que están expuestos, valorar los riesgos, valorar el impacto y plantear la propuesta de salvaguardas sobre los activos con amenazas más altas.

La propuesta de salvaguardas planteada, contiene medidas preventivas y servirá de apoyo a la institución ante cualquier evento que se produzca en los equipos para la

administración remota en la empresa. Ante lo mencionado se evidencia el trabajo realizado en la en la empresa INTERDATOS S.A., con el fin de identificar las amenazas y los riesgos, permitiendo a la empresa entender la situación actual en niveles de seguridad y así tomar decisiones para mitigar los riesgos.

El de los equipos para la administración remota de la empresa, demuestra la importancia de la información, la estimación del impacto, el nivel de riesgo y la propuesta de salvaguardas, pero no aporta con el cálculo del peso medio que tiene cada amenaza, este proceso fue establecido por las autoras del presente trabajo permitiendo de manera relevante, identificar el nivel de riesgos que puede tener la institución ante cualquier amenaza a los activos.

La utilización de la metodología MAGERIT permitió determinar las valoraciones para realizar las evaluaciones concernientes a los activos, amenazas y salvaguardas para posteriormente obtener los niveles de riesgo con la finalidad de ver de manera más fácil la situación actual de la organización.

Es por eso que las empresas necesitan optar por vigilar de manera más estrecha el riesgo de las conexiones que los usuarios corporativos efectúan desde el exterior, con el análisis de gestión de riesgos se busca la manera evitar la pérdida de información confidencial, y minimizar los riesgos de virus, ciberataques y suplantaciones de identidad que vulneran las redes corporativas.

CONCLUSIONES

En conclusión, se cumplieron de manera exitosa los objetivos planteados. Se comprendieron los fundamentos tecnológicos acerca de la administración remota, esto gracias a que, en la actualidad, muchas organizaciones necesitan realizar conexiones remotas para configurar, gestionar o corregir errores en los equipos informáticos que están en otra localidad, es por eso que los responsables de TI deben tomar las medidas y precauciones necesarias para garantizar la seguridad de los equipos.

Se logró examinar recursos tecnológicos de la empresa INTERDATOS S.A. de la ciudad de Babahoyo. Se detectó los activos críticos informáticos del área informática de la empresa INTERDATOS S.A., mediante levantamiento de información proporcionado por el personal del departamento con la aplicación de la metodología MAGERIT. Al realizar una identificación de las amenazas potenciales a las que están expuestos los activos, se pudo determinar la vulnerabilidad al riesgo de la institución y se tuvo una idea aproximada del impacto que tendría en ella al materializarse

RECOMENDACIONES

Se recomienda que haya una revisión periódica de las amenazas y riesgos ya que la tecnología está cambiando constantemente y deben ser controlados para evitar futuros problemas.

Se sugiere al gerente de la empresa que capacite al personal de su empresa para implementar las salvaguardas necesarias que fueron escogidas en el análisis de riesgos para la empresa INTERDATOS S.A."

Para reducir los riesgos que existen en los activos de la empresa se deberían pensar en mejorar el espacio físico del área informática para que sus equipos reciban un mejor mantenimiento. Asimismo, de capacitar al personal para que se cumplan las normas de seguridad que se emplearon en la gestión de riesgos.

Aplicar los lineamientos de seguridad propuesto en este proyecto debido a que siempre las amenazas van a estar presente a pesar de que existan las salvaguardas y estas sean implementadas. Se podrá conocer que activos informáticos están vulnerables y expuestos a estas amenazas.

Realizar cronograma de mantenimiento de equipos informáticos de administración remota, debido a que es esencial y de orden prioritario tener en buen funcionamiento estos dispositivos, los cuales que son importantes para el buen funcionamiento para la gestión, configuración y control de procesos de la empresa INTERDATOS S.A.

REFERENCIAS

Agudelo, Ó. (2020). Administración de TI en la facultad de ingeniería de la Universidad de los Llanos. *Revista Politécnica*, 68-76. Obtenido de https://www.redalyc.org/journal/6078/607863449005/html/

Aguilar, J. (2017). Aplicación Java para el control de RB Mikrotik en empresas proveedoras de servicio de Internet. *Revista Ciencia Unemi*. Obtenido de https://www.redalyc.org/articulo.oa?id=582661257015

Aguilar, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios internacionales (Santiago)*. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169

Albán, V. (2018). La teoría de redes y la gestión de riesgos. *Revista Universidad y Sociedad*. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202018000400239

Altamirano, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Avances*. Obtenido de https://www.redalyc.org/articulo.oa?id=637869113010

Bolivar, L. (2018). Diseño e implementación de una red IPv6 para transición eficiente desde IPv4. *Ingeniería y competitividad*. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-30332012000200017

Chulde, L. (2021). Diseño del Modelo de Ciberseguridad IADI para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac. *Ecuadorian Science Journal*. Obtenido de http://portal.amelica.org/ameli/jatsRepo/606/6062738023/6062738023.pdf

Corda, M. C., Viñas, M., & Coria, M. K. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave (La Plata)*, 1-18. Obtenido de https://www.redalyc.org/pdf/3505/350553375007.pdf

Crespo, E. (2017). Una metodología para la gestión de Riesgos aplicada a las MPYMEs. *Enfoque UTE*, 107-121.

López Vargas, Y., & Vázquez Chávez, A. (2016). La Gestión de Servicios de soporte técnico en el ciclo de vida del desarrollo de software. *stión de Servicios de soporte técnico en el ciclo de vida del desarrollo de software*, 46-60.

Machín, N., & Gazapo, M. (2016). LA CIBERSEGURIDAD COMO FACTOR CRÍTICO EN LA SEGURIDAD DE LA UNIÓN. *Revista UNISCI*, 47-68.

Martí, J. J. (2020). Sociedad digital: gestión organizacional tras el COVID-19. *Revista Venezolana de Gerencia,*. Obtenido de https://www.redalyc.org/journal/290/29063559021/29063559021.pdf

Miranda, M. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas*, 14-26. Obtenido de https://www.redalyc.org/pdf/3783/378345292002.pdf

Ortiz Restrepo, L., & Valencia Duque, F. J. (2017). Gestión de riesgos en eTOM. Un análisis comparativo con los estándares de riesgo corporativo. *Revista Logos, Ciencia & Tecnología*, 85-99.

Peñafiel, K. (2021). Factores que determinan la Vulneración Informática y el Desarrollo. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*. Obtenido de http://www.scielo.org.bo/scielo.php?pid=S2071-081X2021000100009&script=sci_arttext

Zapata, M. (2016). *Evaluación de parámetros de calidad de servicio (qos) para el diseño de una red vpn con MPSL*. Tesis de Mestría. Pontificia Universidad Católica Del Ecuador. Quito. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/12327/TESIS_Evaluacion%20de%20parametros%20de%20QoS%20para%20una%20VPNMPLS.pdf?sequence=1

ANEXOS

Anexo # 1. Visita a la empresa

UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
DECANATO

Babahoyo, febrero 16 de 2022
D-FAFI-UTB-019-UT-2022-2

Abg.
Parcy Riofrio
GERENTE DE INTERDATOS S.A.
Ciudad. -

De mi consideración:

La Universidad Técnica de Babahoyo y la Facultad de Administración, Finanzas e Informática (FAFI), con la finalidad de formar profesionales altamente capacitados busca prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El Señor **QUINATOA BARRIGA ALLAN ALEXANDER,** con cédula de identidad No. 125124375-2, Estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculado en el proceso de titulación en el período Noviembre 2021 – Abril 2022, trabajo de titulación modalidad estudio de caso para la obtención del grado académico profesional universitario de tercer nivel como **INGENIERO EN SISTEMAS DE INFORMACIÓN.** El Estudio de Caso: **ANÁLISIS TECNICO DE LOS RIESGOS DE LA ADMINISTRACION REMOTA EN RECURSOS TECNOLŐGICOS EN LA EMPRESA INTERDATOS S.A. DE LA CIUDAD DE BABAHOYO.**

Es por esta razón, solicito a usted si es posible se sirva autorizar el permiso respectivo para que el señor Quinatoa pueda desarrollar la investigación en la institución de su acertada dirección.

Por su gentil atención al presente, se extiende el agradecimiento institucional.

Atentamente,

UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
DECANATO

Lcdo. Eduardo Gáleas Guijarro, MAE
DECANO DE LA FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

c.c: Archivo

Anexo # 2. Oficio emitido por la Universidad a la empresa