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

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

ANÁLISIS DEL IMPACTO DE LAS TICS EN LOS FRAUDES INFORMÁTICOS PARA LA EMPRESA CARINEXUS S.A.

EGRESADO:

José Enrique Pérez Villena

TUTOR:

Ing. Fredy JordanCordones

AÑO:

2022

RESUMEN

El propósito del presente caso de estudio en base a un análisis del impacto de los TICS en los fraudes informáticos para la empresa Carinexus S.A. situada en la ciudad de Babahoyo. El objetivo es analizar la importancia del cambio estructural de las organizaciones empresariales, de cara a la evolución de la tecnología, especialmente la implementación y uso de las TIC'S en las empresas y evitar fraudes que ocurren en la actualidad.

La relación con las tecnologías de la información y comunicación se basa en la actualidad, es de gran importancia en el campo de los negocios, en el Ecuador existe poca inversión en sistemas tecnológicos, y por ende surge necesidad de proteger su información y así evitar anomalías. Los sistemas informáticos internos ayudan en el sector empresarial, con la necesidad de implementar procesos seguros y confiables dentro de la organización.

Los delincuentes han tomado nuevas formas de infringir la ley y los delitos más comunes encontramos: uso de redes sociales suplantando identidades, sabotaje informático, etc. Estos son medios lo cuales estas infracciones son de tipo ocupacional.

Es decir, El 90% de personas que cometen estos actos delictivos trabajan en la organización que fueron víctimas; consecuentemente, la prueba de los crímenes se encuentra en los mismos equipos de la organización.

Palabras Claves: TIC´S, Empresas, Fraude Informático, Vulnerabilidad;

ABSTRACT

The purpose of this case study based on an analysis of the impact of TICS on computer fraud for the company Carinexus S.A. located in the city of Babahoyo. The objective is to analyze the importance of the structural change of business organizations, in the face of the evolution of technology, especially the implementation and use of ICTs in companies and to avoid fraud that occurs today.

The relationship with information and communication technologies is currently based, it is of great importance in the field of business, in Ecuador there is little investment in technological systems, and therefore there is a need to protect your information and thus avoid anomalies. Internal computer systems help in the business sector, with the need to implement safe and reliable processes within the organization.

Criminals have taken new ways of breaking the law and the most common crimes are: use of social networks impersonating identities, computer sabotage, etc. These are means by which these infractions are of an occupational nature.

That is, 90% of people who commit these criminal acts work in the organization that were victims; Consequently, the proof of the crimes is found in the very teams of the organization.

Keywords: TIC´S, Companies, Computer Fraud, Vulnerability;

INTRODUCCION

Constantemente se han venido presentando vulnerabilidades en los sistemas de información, falla de procedimiento como tecnológica, dentro de las infraestructuras que se han implementado, son irrumpidas por intrusos informáticos.

Para verificar el impacto que tienen las Tecnologías de Información y la Comunicación (TICS), en el cometimiento de fraudes Informáticos se debe considerar las acciones usadas que se dan en cada caso, se hará un posicionamiento del

problema a través del análisis de las Tics, el uso de Internet y redes sociales, como lo es de vital importancia conocer la fuente digital en el proceso pericial.

Dicho problema se ha venido dando años atrás y en la actualidad se está incrementando con rapidez, razón por la cual el presente trabajo de Titulación tiene como objetivo analizar el impacto de las TICS en los posibles fraudes informáticos que se presentan en la actualidad en la Empresa Carinexus S.A. Al haber reconocido la problemática que se torna en la empresa Carinexus S.A, denotándose así de vulnerable a fraudes informáticos surge la necesidad de dar una solución óptima a la presente problemática, viéndose así obligada a implementar servicios óptimos de seguridad Para verificar el impacto que tienen las Tecnologías de Información y la Comunicación (TICS), se debe considerar las acciones usadas que se dan en cada caso, se hará un posicionamiento del problema a través del Análisis , el uso de Internet y las Redes Sociales y como es de vital importancia conocer las fuente digitales presentadas en el proceso.

En este análisis se pretende dar a conocer una posible solución a esta problemática con herramientas que están disponibles en el mercado. La metodología de investigación

utilizada en este análisis es el método inductivo ya que permitirá recopilar la información mediante la entrevista o encuesta dirigida al jefe de la Empresa, de tal lugar en la que el desarrollo está presente en proporcionar servicios eléctricos a entidades públicas como privadas.

El presente estudio de caso está bajo la línea investigativa de la Facultad de Administración Finanzas e Informática; Sistemas de información y comunicación, emprendimiento e innovación donde su sublinea se basa en Redes y tecnologías inteligentes de software y hardware. El avance tecnológico de las ciencias de la información, computación y telecomunicaciones incorpora un enfoque diferente al habitual para acceder al conocimiento, flexibilidad, interacción, economía, rapidez, independencia, comunicación y desarrollo en las organizaciones actuales.

DESARROLLO

Una empresa es una unidad productiva que se agrupa y se dedica al desarrollo de una actividad económica con ánimo de lucro. Actualmente es muy común la creación de empresas. En general, una empresa también puede definirse como ‘una unidad formada de un conjunto de personas, bienes materiales y financieros, con el fin de producir algo o prestar un servicio que satisfaga una necesidad y de la cual se obtengan beneficios. Por tanto, puedo decir que una empresa es un ente conformado por personas que buscan enriquecer su capital mediante la realización de inversiones, con las capacidades técnicas y financieras, todas las empresas tienen sus altas y bajas y en eso se detallan los fraudes. En definición un frade es un delito creativo o un engaño, abuso total de confianza de la empresa con fines propios de la persona que los ejerce. El uso de la tecnología en los sistemas informáticos va enfocado a los ataques insertando virus a los sistemas con el fin de obtener información, dinero, cuentas e incluso se puede deducir que un atacante puede proporcionar información a las empresas competentes mediante las Nuevas Tecnologías de la Información y Comunicación (TIC). (Cano, 2018)

Un sitio web, los equipos que utilizan actualmente los empleados o las herramientas ofimáticas que utilizan las empresas, llegan a gestionar toda la información y mover el trabajo más fácil gracias a la evolución que ha sufrido el mundo de las tecnologías de la información. Herramientas como un CRM Online o un ERP permiten gestionar la relación con los clientes, las interacciones entre empleados y la comunicación entre los diferentes departamentos de una empresa, a pesar de que puede estar en diferentes países o kilómetros de distancia. (Garcia, 2018)

El Talento Humano al servicio de las TIC

Desde el punto de vista empresarial, la implantación de las TIC redundará en una reducción de tiempos y costes, al introducir mejoras en la cadena de suministro, en la comercialización de mercancías, entre otros aspectos. Todo lo anterior hace que las empresas vayan a requerir los servicios de profesionales expertos en Ingeniería en Tecnologías de la Información y las Comunicaciones, capaces de gestionar soluciones necesarias para la continuidad de procesos de negocios. Las competencias digitales garantizan la sostenibilidad de los proyectos e inversiones que se están realizando para incorporar las nuevas tecnologías a los diferentes sectores públicos y privados del mercado laboral. (Colcha, 2021)

Las Tics son los recursos y herramientas que se utilizan para el proceso, administración y distribución de la información a través de dispositivos como computadores, teléfonos, televisores etc. Son un conjunto de procesos y productos derivados de nuevas herramientas (hardware y software), soporte y canales comunicaciones, relativas al almacenamiento, procesamiento y transmisión digitalizada de información. (Chavez, 2020)

ANALISIS

Las TIC son aplicaciones que se basan en un conjunto de sistemas, herramientas, técnicas y metodologías relacionadas con la digitalización de señales analógicas, de audio, texto y video, gestionables en tiempo real. En la actualidad la empresa Carinexus S.A se

basa en el manejo lógico y detallado de servicios eléctricos prestando servicios públicos y privados.

La misión es convertirse en ser el mejor proveedor de servicios eléctricos a nivel nacional e internacional. Para lograr esto, se ha establecido un arduo trabajo y apoyo a los miembros del equipo de trabajo, para que puedan brindar un servicio excepcional a los clientes. En la actualidad la visión de la empresa Carinexus S.A es ofrecer la mejor calidad y experiencia de servicio eléctrico a nivel nacional e internacional y manejar una infraestructura solvente para su distinguida clientela.

Muchas organizaciones no saben qué elegir al comprar una herramienta de gestión de metadatos. Es por ello que uno de los principales objetivos de este análisis fue conocer algunas de las herramientas de gestión que existen actualmente en el mercado. Además, desea comparar algunas de estas herramientas realizando pruebas de inserción de datos y midiendo su rendimiento para elegir la herramienta más eficaz y fácil de usar. (Figueroa, 2021)

La necesidad de realizar un análisis acerca de los fraudes informáticos que se han presentado en la empresa Carinexus S.A. La incidencia en el acceso a la información que en ella se guarda es de vital importancia, pues los procesos que se destacan en esta dependencia son de gran utilidad, es una situación que se da en la actualidad se pudo detectar que existen actividades en la empresa Carinexus S.A presenta ciertas irregularidades en la administración como contratación de personal por temporadas, falsos autónomos , falta de medidas de prevención de riesgos laborales e infra cotización al seguro social en el manejo de las mismas, por lo cual las vulnerabilidades relacionadas con amenazas estructurales , relacionadas al personal , hardware y software y con la

información existentes podrían ocasionar perdidas bastante considerables. Es una incidencia en el acceso a la información y hoy en día se considera como un proceso indispensable, debido al trabajo que resulta encontrar la manera de delimitar sus graves consecuencias, por lo cual el encargado de llevar este proceso es de gran interés el realizar la presente investigación dado el alto porcentaje de incidencia de estos delitos.

Una manera de reconocer a los fraudes informáticos son aquellas actividades que hacen uso de un sistema de computación para llevar a cabo actos ilícitos y buscar beneficios propios. Otra manera de cuestionar un fraude informático como una Actividad ilícita, donde es cometida por personas con un fin malicioso que aprovechan las debilidades de un sistema informático con la finalidad de obtener beneficios sin importarles el perjuicio ajeno, una vez detectada la vulnerabilidad esta puede ser aprovechada las veces que desee el delincuente. (Laura Mayer, 2020)

El Impacto de las Tics en la Actualidad.

En la actualidad hay una gran controversia acerca del uso que se le da a las tecnologías de información y la comunicación (Tics) ya que son utilizados en varios ámbitos ya sea económicos, educación, periodismo entre otros, dentro de los avances tecnológicos dentro de los últimos años el internet y sus derivaciones las páginas web, correos electrónicos, redes sociales, han afectado en gran parte a la comunidad en general. (Sevilla, 2019)

Los Fraudes Informáticos ocurridos en Empresas.

Todos los días podemos demostrar que vivimos en un mundo donde las personas interactúan con fines políticos, sociales, económicos, culturales y de otro tipo.

En todos los espacios del planeta hay personas que realizan actividades económicas, tales personas también sobre la base de un acuerdo de voluntad, en el que una persona se obliga a dar, a hacer o no hacer algo con otra. Esta es razón para explicar que, si estos trámites no se realizan con cautela y se toman las precauciones necesarias, pueden convertirse en víctimas de hechos delictivos, lo cual es un hecho que afecta las condiciones económicas que han vivido muchas personas y sus propiedades. (Velandia, 2017)

Las Ventajas que brindan las TIC para proteger la Información.

Una de las ventajas es que Impactan positivamente en la gestión de la organización. Ya que hoy en día, una empresa puede almacenar todos sus datos en la nube y acceder a ellos en cualquier momento. Esto le permite manejar eventos de manera eficiente y con menos tiempo y recursos. (Lemontech, 2021)

Implementación de nuevas modalidades de trabajo: Gracias a la tecnología de la información, se ha hecho posible explorar otros métodos de trabajo que no requieren la presencia de empleados o colegas. Las video llamadas, las plataformas de gestión de proyectos y otras herramientas permiten el trabajo a distancia de forma temporal o permanente. Esto reduce el potencial de gas en el imperial (ahorro en electricidad, agua, insumos de oficina) y para muchos comerciales significa un ahorro en el transporte y la posibilidad de pasar más tiempo en el hogar. (Agudelo, 2020)

Nuevas oportunidades de Negocio: Señala (Agudelo, 2020) que el desarrollo de nuevas líneas de negocio, productos o servicios en las empresas y favorece el crecimiento de la propia empresa, pero también genera nuevos empleos y oportunidades de negocio.

Desventajas

Reducción de puestos de trabajo: La automatización de procesos promovida por el uso de las TIC está haciendo que muchos perfiles laborales desaparezcan. Esto puede dejar a muchas personas en el paro, sobre todo si no tienen un perfil especial. Uno de estos casos es el de los trabajos relacionados con la atención al cliente. Esto hace que cada vez sea menos necesario que las empresas contraten personal para realizar estas tareas, generando desempleo con las nuevas tecnologías existentes. (Madrid, 2020)

Riesgo de ciberataques: (Muñoz, 2019)Los procesos automatizados de las empresas, así como su información en línea pueden ser vulnerados por terceros, bien sea para robar información importante o para pedir recompensa por la recuperación de los datos. Por ello, es importante que muchas empresas asuman la seguridad digital y actualicen constantemente los diferentes softwares que utilizan.

¿El Uso del internet es un riesgo?

El Internet permiten a las empresas cambiar la forma que se relacionan con otras empresas, clientes y proveedores. Por ejemplo, puede utilizar el comercio electrónico. Internet utilizará una utilidad roja para dedicar información sensible a investigaciones honestas, y se ha creado gradualmente para convertirse en los principales centros de intercomunicación de información en todas partes del mundo. Al mismo tiempo, se ha convertido en un refugio para sistemas y ataques comparativamente incompatibles. (Acosta, 2020)

¿Cuáles son los delitos informáticos con el uso del internet pueden causar daños en la empresa?

La evolución del manejo de la información ha traspasado las barreras del tiempo y el espacio, así como la variedad, amplitud y complejidad de los sistemas de información que se encuentran disponibles permanentemente, estos cambios han impulsado ventajas y al mismo tiempo "amenazas, riesgos y espectros de incertidumbre en los escenarios de internet, intranet, desarrollo tecnológico, gestión de la información, la comunicación y los sistemas" (Muñoz, 2019)

Tabla 1 Delitos Informáticos más comunes que se presentan en la actualidad

Elaborado por: José Pérez Villena

La Navegación inapropiada	La visita a sitios web potencialmente ofensivos o no apropiados para el sitio de trabajo fácilmente podría ser la principal causa de un lugar de trabajo.
Los Spyware o virus	Otro peligro que puede traer consigo el hecho de navegar por internet en el trabajo y visitar sitios web ilegítimos, es la posibilidad de detectar algún tipo de spyware o malware desagradable. Implica instantáneamente una pérdida de productividad, y por ende de tiempo de inactividad, mientras el departamento de informática hace todo lo necesario para erradicarlo y que el computador quede totalmente fuera de amenazas de este tipo.
La Mensajería instantánea	Para nadie es un secreto que varias organizaciones utilizan programas internos de mensajería instantánea, en un esfuerzo por facilitar la comunicación entre cada uno de los departamentos. Sin embargo, este uso de la mensajería instantánea como una forma de mantenerse al día con los amigos y la familia fuera del trabajo, fácilmente puede provocar distracciones en horas laborables.
El Phishing	Otros sitios también podrían tratar de obtener la mayor cantidad de información posible de ti, para de esta forma

	tratar de acceder a tu correo , y poner en grave peligro la seguridad de la empresa, debido a que es probable que allí se maneje bastante información privada y delicada.

Todos sabemos que Internet es una gran y maravillosa herramienta para el trabajo, el de los empleados fácilmente. Bajo este análisis los empleadores deben desarrollar una política que regule el uso de Internet en el lugar de trabajo. De esta manera, puede ayudar a proteger todos los recursos de la empresa. A cambio que se mantenga la productividad en orden.

Todas las instituciones del sector privado y público tienen la obligatoriedad de cuidar su información digital y con la ayuda de los avances tecnológicos en gran medida con la implementación de nuevas tecnologías y todos esos avances traen consigo ventajas y desventajas que fueron ya mencionadas, la mayor de ellas es que se encuentren vulnerabilidad de la información en los sistemas empresariales ocasionando los fraudes informáticos y perjuicios en contra del patrimonio de las organizaciones. (Cano, 2018) También deduce que adquisición y aplicación de las TIC´S es de gran importancia en la actualidad para el sector empresarial, relacionado a la actividad que se realiza para la innovación de nuevos productos, desarrollo de estrategias, líneas de comunicación, optimización de procesos, análisis económico-financiero en donde se presentan vulnerabilidad a la información digital apareciendo los fraudes informáticos por la poca seguridad e importancia que dan los empresarios al tema.

¿Cómo podemos evitar los fraudes informáticos en la empresa Carinexus ?

La cuarentena ha pedido a muchas empresas que elijan el Teletrabajo como método. Esto, entre otros factores, lleva a que se intensifiquen los delitos informáticos, como la suplantación de identidad e información sensible, el hackeo de cuentas o de software, y así, cómo las organizaciones se han protegido de estos ciberdelitos. (Acosta, 2020)

El presente caso de estudio, pretende dar como solución evitar fraudes y otros delitos informáticos bajo el instrumento que es la encuesta realizada al jefe de la empresa, en los cuales se detallan a continuación.

1. **Evitar dar información confidencial de la empresa por sitios de Internet.**

   Fechas de cumpleaños, fechas de vacaciones, miembros del grupo familiar, etc. Estos son los datos que los piratas informáticos suelen utilizar para iniciar un perfil que los lleva a otros datos importantes, como contraseñas de sitios, tarjetas de crédito o información de la empresa.

2. **Evitar el almacenamiento de archivos en los dispositivos con las claves de acceso.**

   Si bien es cierto que hay muchas webs que solicitan cambiar las claves de acceso cada cierto tiempo, debes evitar ingresar las claves en algunos dispositivos electrónicos.

3. **Utilizar diferentes contraseñas o claves y cambiarlas periódicamente.**

4. **Cree contraseñas difíciles de adivinar combinando números, letras mayúsculas y minúsculas y caracteres especiales.**

   Usa tu creatividad y complica tus contraseñas, no uses información personal como cumpleaños, tu nombre o apellido.

5. **Evite instalar software a menos que conozca al fabricante.**

   Si no está 100% seguro del origen de un archivo o programa, no lo instale en ninguno de los dispositivos que utiliza.

6. **Evitar conectarte a redes públicas o puntos de acceso libres.**

7. **Utilizar aplicaciones de seguridad en dispositivos como antivirus y/o firewall.**

   Estas aplicaciones lo ayudan a mantener su información a salvo de virus o intrusiones no deseadas. Mantenlos informados para su mejor desempeño.

8. **Evitar importar páginas gratuitas para descargar música, películas, videos o imágenes.**

   No importa cuán atractiva sea la oferta o promoción, el riesgo asumido puede superar la satisfacción que se puede lograr. Es más, de no hacerlo.

9. **Usar discos duros externos.**

La idea es programar una copia de seguridad diaria y guardarla. En el caso de que recibamos un ataque, nos será más fácil formatear los equipos adquiridos y utilizar los datos almacenados en estos discos.

Los delitos informáticos corporativos siempre tienen dos objetivos: robar dinero de nuestra cuenta corriente y recopilar información de los clientes para defraudarlos de la misma manera. Por lo tanto, para no poner en riesgo a las personas que confiaron en la empresa y brindan un buen seguro, que brindará información completa al respecto y también consejos básicos para que nuestra empresa sea más segura y confiable. (Canaval, 2020)

CONCLUSIONES.

El delito informático o fraude es un acto ilícito que se encuentra en las redes de información (web), atentando contra la propiedad intelectual privada de la empresas y las organizaciones y el estado en general. Los delitos informáticos van en aumento cada día, y en muchos casos algunos de ellos se deben a negligencias en cuanto a la protección de los datos de los usuarios. De esta forma, los ciberdelincuentes encuentran oportunidades para extraer información que vulnera la seguridad y estabilidad de los propietarios de la información. (Delitos tecnológicos en empresas. ¿Cómo protegerse?, 2020)

Cada día los fraudes informáticos van tomando auge en todos los niveles cibernéticos. Los infractores crean y activan diferentes modalidades que les permitan delinquir tales como, el hurto, estafas, chantajes, entre otros, perjudicando la privacidad e

identidad de cualquier persona o entidad. La necesidad de instaurar sistema de seguridad, que permita el resguardo de la información, cada día toma más relevancia, sobre toda cuando la información que se maneja es de primera línea. (Oxman, 2022)

Las empresas se enfrentan a un reto que va más allá de la simple innovación tecnológica. Este es un cambio social, económico y cultural que debe comenzar a planificar hoy en día, su gestión y una habilidad que tienen la capacidad de aquellas empresas que lo utilizan en todas sus extensiones.

BIBLIOGRAFÍAS.

Acosta, M. G. (2020). Delitos informáticos: Impunidad. *Redaldy.org*, 14-15.

Agudelo, M. (2020). Las oportunidades de la digitalización en América Latina frente al Covid-19. *Corporacion Andina de Fomento*, 18-25.

Canaval, J. D. (2020). Informática forense y auditoría forense: Nuevas. *Revista Espacios*.

Cano, G. E. (2018). Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. *Dialnet*, 4-6.

Chavez, R. (09 de 07 de 2020). ¿Que son las Tics ? *Universidad Latina de Costa Rica*, 6.

Colcha, J. (Julio de 2021). Gestión del talento humano, uso TIC´S y su relación con el desempeño laboral. *Polo del Conocimiento*, 15- 20.

Delitos tecnológicos en empresas. ¿Cómo protegerse? (2020). *Grupo Atico 34*, 2-10.

Figueroa, P. (26 de Enero de 2021). *Plan Estratégico de Tecnologías de la Información.* Obtenido de https://www.car.gov.co/uploads/files/60116c538cdaa.pdf

Garcia, A. (13 de Noviembre de 2018). *Userllcrm.net*. Obtenido de Noviembre

Laura Mayer, G. C. (2020). El delito de fraude informático: concepto y delimitación. *sCielo*, 5-15.

Lemontech. (30 de Abril de 2021). *Las TIC en el ámbito laboral: ventajas, ejemplos y tendencias*. Obtenido de Lemontech Blog: https://blog.lemontech.com/las-tic-en-el-ambito-laboral-ventajas-ejemplos-y-tendencias/

Madrid, N. (2020). Ergonomía del software y riesgos laborales.

Muñoz, H. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Realyc.org*, 5-6.

Oxman, N. (2022). Estafas informáticas a través de Internet. *Redalyc*, 1-15.

Sevilla. (15 de 01 de 2019). *El impacto de las TIC en la sociedad actual*. Obtenido de https://digitalsevilla.com/2019/01/15/el-impacto-de-las-tic-en-la-sociedad-actual/

Velandia, J. T. (2017). *Importancia de las T.I.C.s en el ambiente empresarial.* Obtenido de https://ciencia.lasalle.edu.co/administracion_de_empresas/1483

ANEXOS

Anexo 1

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

Babahoyo, febrero 16 de 2022
D-FAFI-UTB-065-UT-2022-2

Sr.
Boanerges Lenin Sánchez Rodríguez
GERENTE DE LA EMPRESA CARINEXUS 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 **PÉREZ VILLENA JOSE ENRIQUE,** con cédula de identidad No. 1207739309, 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 del impacto de las tics en los fraudes informáticos para las EMPRESA CARINEXUS S.A.**

Es por esta razón, solicito a usted si es posible se sirva autorizar el permiso respectivo para que el señor Pérez 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 ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
DECANATO

Recibido
16-02-2022

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

c.c: Archivo

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Mercedes Soto Valencia	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

Anexo 2

ENTREVISTA.

Dirigida: Boanerges Lenin Sánchez Rodríguez

GERENTE DE LA EMPRESA CARINEXUS S.A.

1. **Como influyen las Tics en la empresa Carinexus S.A.**

   Las TICS influyen de manera oportuna en el cambio organizacional en la que se maneja nuestra información, en los avances tecnológicos en el ámbito administrativo, facilitando la administración de recursos.

   Análisis: Acorde a la entrevista realizada el gerente supo manifestar que toda la información se maneja mediante la tecnología en donde se puede administrar los recursos.

2. **Cuáles son los recursos que utilizan para brindar seguridad en sus sistemas informáticos.**

   Dentro de los recursos que se utilizan en la empresa Carinexus S.A podemos destacar:

   - Firewall perimetral de red.
   - Escáner de vulnerabilidades.
   - Servidor proxy.

   Análisis: Dentro de los recursos que se pueden administrar se encuentran mencionados por parte del gerente.

3. **¿Cree usted que la empresa Carinexus S.A ha sido víctima de algún tipo de fraude informático.**

   La empresa Carinexus S.A en el 2020 enfrento uno de los fraudes informáticos con la mayor pérdida de información de una de su base de datos, la cual se comprometió información con el fin de suspender o paralizar una de sus mayores actividades laborales la cual ya estaba ejecutándose.

   Análisis: La empresa Carinexus durante su estancia ha tenido fraudes como los ya mencionados y por ende se supo acoger la problemática para el respectivo análisis.

4. **Con que finalidad se dan los fraudes informáticos.**

   En la actualidad los delitos informáticos más frecuentes se dan en el robo de información dándole un mal uso comprometiendo y dejando vulnerable.

   Análisis: Los fraudes informáticos se dan con el fin de obtener información con fines dañinos en las empresas por empleados o intrusos, empleando virus, etc.

5. **De qué manera se detectan irregularidades en el sistema.**

   Una de las herramientas en la que se detectan es mediante el escáner de vulnerabilidades, donde se realiza un reconocimiento en todo el sistema implementado para que no presente fallas y se mantenga estable.

   Análisis: la empresa Carinexus debido a su vulnerabilidad en la infraestructura de red y equipos se pretende emplear seguridad en base a los riesgos que ocurran en el futuro.

6. **¿Qué tipo de fraudes informáticos es más comunes en las empresas?**

   - ❖ Manipular datos de entrada
   - ❖ Manipular sistemas informáticos
   - ❖ Manipular datos de salida

   Análisis: El gerente supo manifestar que los fraudes más comunes son los mencionados por lo cual son perjudiciales a la integridad de la empresa.

7. **Cuál es el mayor recurso de vulnerabilidad que se encuentra en los sistemas informáticos en la empresa Carinexus S.A**

   *****Bases de datos.

   *****Sistema de información.

   *****Recursos Humanos.

   Análisis: las vulnerabilidades se pueden dar en los recursos mencionados por parte del gerente, eso se refiere que por ende se debe mantener una integridad de los datos.

8. **Que opciones se tomaría la empresa Carinexus S.A al ser víctima de fraudes informáticos.**

   Se tomarían acciones legales establecida por el COIP (Código Orgánico Integral Penal) hasta llegar con los responsables de dicho suceso.

Análisis: con un sistema que proteja la integridad de la información de la empresa se llevara a acciones legales con el intruso o estafador que se atreve a hacer daño a la empresa.