UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCION DEL TITULO DE INGENIERO(A) EN SISTEMAS

TEMA:

ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL AREA TECNICA DE REPARACION E INSTALACION DE LA CORPORACION NACIONAL DE TELECOMUNICACIONES "CNT EP" DE LA CIUDAD DE BABAHOYO.

EGRESADO:

VILLAMAR SILVA CRYSTHIAN GEOVANNY

TUTOR:

ING. IVAN RUIZ PARRALES

AÑO 2021

Introducción

La seguridad de la información es uno de los aspectos a los que se le está tomando uno de los mayores intereses en el campo informático aun cuando el mundo computacional se ha vuelto más fácil cada día le ha ido evolucionando para mejorar su accesibilidad.

Sin embargo, los peligros y las pérdidas de uno de los activos más importantes de las empresas como lo es la información Siempre son importantes de tratarlos ya que es mejor evitar y prevenir que tener que lamentar por fugas de información o pérdida total de los datos.

El cuidado de la información es responsabilidad de todos, en tal sentido, los representantes de la Corporación Nacional de Telecomunicaciones (CNT EP), han realizado diferentes estrategias encaminadas a mejorar sus contingencias en relación al manejo de la información y datos, es conocido que han realizado ya presentaciones sobre seguridad de la información a funcionarios de Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), el pasado 14 de agosto del 2021.

CNT EP es una empresa que cuenta con proyectos de inversión que permite apalancar el crecimiento tecnológico del país, esta empresa CNT EP, ofrece soluciones sostenibles al estado y al mercado ecuatoriano con soluciones corporativas y soluciones tecnológicas integrales. CNT EP trata también de apoyar con una eficiente transformación digital a todos los sectores, siendo un proveedor de servicios con un gran paquete de beneficios, donde se otorga gestión eficiente de las comunicaciones y permite la colaboración más eficiente con sus clientes, incrementando en

eficiencia y productividad, ha permitido además la evolución en la era digital a muchas instituciones del país con sus buenas gestiones de seguridad de la información.

CNT EP cuenta con servicios innovadores de Cloud Computing, que buscan cumplir con los niveles y estándares más altos de calidad y de seguridad de la información, por ello la CNT EP cuenta con certificaciones ISO 9001, ISO 27000, procesos basados en ITIL para sus soluciones tecnológicas y estándares de clase mundial Up Time Tier III.

En este estudio de caso se profundizarán temas inherentes a las normas de estandarización ISO 27001 que permiten tomar medidas de prevención antes durante y después de algún incidente con la vulneración de la información, estos estándares permiten estrategias que además están analizadas por profesionales de amplia experiencia en el campo de la informática es decir ingenieros en sistemas que laboran en la empresa CNT EP y otros profesionales de conocida trayectoria y experiencia.

DESARROLLO

Es muy conocido en el país, que se vulneró la seguridad de la información en la empresa CNT EP a nivel nacional, desplegado esto además en la ciudad de Babahoyo, al ser parte de la red global y acceso a servicios.

La norma ISO 27001 está enfocada y pensada en el aseguramiento, la integridad y la confidencialidad de los datos y la información, al igual que los sistemas que cuentan con componentes encargados de gestionar la seguridad, El estándar internacional ISO 27001, ha sido

desarrollado para ser un modelo que hace posible establecer, revisar, monitorear, implementar y mantener un sistema de seguridad de la información.

Este estándar antes mencionado, se enfoca en el proceso de gestión de la seguridad que fomenta en sus usuarios enfatizar la importancia de

Entender las necesidades de seguridad existentes en las organizaciones, para el establecimiento de políticas claras que permitan reducir el riesgo.

Operar e implementar controles para reducción de los riesgos inherentes a la seguridad de la información

Monitorear la efectividad y el desempeño de los SGSI

Mantener un mejoramiento continuo, basándose en la medición de los objetivos

En la norma ISO 27001, se tiene un anexo A, el cual es el que se implementa y dentro de este se encuentra a forma de normativa todo lo relacionado con lo más aproximado a los controles de seguridad, que son fundamentales porque al ponerlos en práctica, estos ayudan en la protección de los datos e información organizacional, haciendo que ponerlos en práctica sea un menester.

Ecuador es un país Latinoamericano que lidera en cuanto al incremento de ciberataques. Esto es del 75% en comparación a los 8 primeros meses del año anterior al 2021. Los Hackers utilizan comúnmente software malicioso para espiar, introducirse y obtener información.

La fuente primaria de esta información ha sido la empresa rusa de ciberseguridad Kaspersky, la que crea antivirus muy conocido, esta indica que, los países de América latina donde más han crecido los cyber ataques son:

Guatemala (+43%)

Panamá (+60%)

Perú (+71%)

Ecuador (+75%)

En la región se tiene registros de que se sufre en alrededor de 35 ataques por segundo; siendo los países con más infección por minuto:

1,291 Brasil

289 México

96 Perú

88 Ecuador

87 Colombia

Los internautas de Latinoamérica abren sus puertas a las cyber amenazas, a través de programas sin licencia o descarga de archivos, permitiendo de esta manera, que los cyber criminales obtengan un control totalitario sobre los equipos infectados.

La empresa informó que los cyber delincuentes están cambiando o dirigiendo su mirada a países con menor población. Por otro lado, Dmitry Bestuzhev, director en jefe del equipo técnico de Investigación y análisis de Kaspersky para latino América, mencionó:

La vulneración a los dispositivos ocurre de formas diversas, desde archivos PDF infectados, virus troyanos traídos desde la web y programas que son descargados por usuarios a través de páginas poco confiables.

JUSTIFICACIÓN

Este trabajo de caso de estudio, se justifica pues permitirá que el autor se gradué y aporte con una investigación relativa con la empresa CNT EP, que es donde inclusive labora, además de haber fortalecido esta investigación con opiniones que permiten esclarecer ciertos temas relacionados con la seguridad de la información.

La seguridad de la información en CNT EP es de vital importancia para los ecuatorianos, ya que habla bien o mal de su empresa estatal de comunicaciones y gana o pierde valor con esto; esta investigación trató de enfocarse al aspecto netamente técnico relacionado con la seguridad y la norma ISO 27001, que es una de las normas más conocidas y confiables para el tratamiento de la seguridad de la información y este estudio con su importante aporte podría lograr una referencia u opinión que permita una estrategia correctiva en CNT EP Babahoyo.

Las técnicas de que se eligió aquí, fue de un cuestionario técnico como instrumento esencial para la recolección de datos de personas con experiencia en estos aspectos técnicos de la ingeniería en sistemas, estas representan una acción metodológica seleccionada, que se podría decir que es del tipo Inductivo, porque, usted va de cada análisis puntual a una idea de un resultado generalizado y esto contrastará con las teorías aquí planteadas.

En tal sentido, reuniendo los criterios profesionales, se ha evidenciado con fundamente de hecho que, en relación a, **cómo y en que dimensión se ha visto afectada a la empresa CNT EP a nivel nacional y en el ámbito local, es decir (Babahoyo)** durante la última vulneración a sus sistemas.

Al parecer, CNT EP se vio afectada en su máxima dimensión, fue vulnerada en su información, que es el activo más importante que puede tener una organización, es una empresa que además en el listado de sus productos y servicios, contempla un datacenter TIER III, esto es un lugar donde otras empresas almacenan y aprovisionan sus servidores, haciéndole perder la imagen corporativa de confiabilidad relacionada con los datos.

CNT EP seguramente es una empresa que, durante su última afectación, perdió valor en el mercado, ya no tendrá una valoración regular o mediana como antes de la incidencia de inseguridad, tendrá una valoración de seguro que, en el rango de hacerla atractiva para la venta, por parte del gobierno de turno Ref: Ing. Saltos (anexo 1).; así mismo, el ingeniero Milton Rodríguez manifestó que a nivel nacional una vez declarada en rueda de prensa de manera oficial por las autoridades de la empresa a través del área Jurídica y el Gerente general Arq. Byron Zapata. Se dispuso el apagado inmediato de los dispositivos electrónicos y sistemas informáticos para evitar que la vulnerabilidad a la red siga avanzando.

Indicó además que: “nuestra empresa se vio afectada a nivel nacional en sus sistemas de facturación y sistemas de gestión comercial, lo cual produjo retraso en los pagos y malestar en la ciudadanía. Es así que en la ciudad de Babahoyo muchas de las empresas competidoras de Internet se aprovecharon de esta situación y elaboraron muchos planes de Instalación de Internet en la que accedieron muchos clientes nuestros desistiendo de nuestro servicio. A pesar de que la parte operativa de la red de telecomunicaciones no fue afectada.”

En el cuestionamiento de**: Si usted fuese el responsable tecnológico de manejar la seguridad de CNT EP en Babahoyo, cuáles serían las estrategias para lograr mejorar la seguridad de la información.**

Para manejar la seguridad en CNT EP Babahoyo, primero hay que pensar en que se trata de una empresa donde se manejan estándares nacionales y debe ir apegado todo a lo que la nacional aplica, lo que puede hacerse desde Babahoyo son recomendaciones para aplicarse como estándar nacional, sin embargo localmente se podría manejar cierta disciplina en cuanto a la utilización de medios de almacenamiento extraíbles, navegación por sitios confiables y aplicación de algunas secciones de normativas ISO 27001 ref: Ing. Saltos (Anexo1)

Así mismo, el Ing. Milton Rodríguez, ref: (Anexo 1) indica que, establecer protocolos de seguridad de acuerdo a las normas Internacionales según la ITu. ISO y demás, tener sistemas acordes a las nuevas tecnologías las cuales brindan soluciones integrales para protección de datos e información y capacitar y concientizar al personal encargado del manejo de información sobre el buen uso de los dispositivos electrónicos y sistemas de información.

En el cuestionamiento: **En relación a las normas ISO 27001, considera usted, que estas han sido aplicadas en CNT EP, se comentó que:** se conoce que CNT EP maneja normativas ISO 27001, sin embargo, habría que ver en qué dimensión la aplican, al no ser de la parte técnica de CNT EP, no podría dimensionar en relación a esto. Ref: Ing. Saltos (Anexo1)

La empresa es certificada en ISO 27001 pero lamentablemente el nivel de ataque a la que fue sometido sus sistemas implica reforzar mucho más a sus sistemas y servidores. Ref: Ing. Milton Rodríguez, (Anexo1)

En el cuestionamiento: **De las siguientes secciones de las que están divididos los 114 controles de la norma ISO 27001, cuales considera que están siendo aplicados o son aplicables a CNT EP Babahoyo**

Para asegurar la calidad e integridad de nuestros servicios es necesario aplicar todas las secciones de la Norma ISO sin excepción. Ing. Milton Rodríguez, (Anexo1)

Así mismo el ref: Ing. Saltos (Anexo1) indicó lo siguiente

Sección 0 – Introducción

Sección 1 – Alcance (este)

Sección 2 – Referencias normativas (este)

Sección 3 – Términos y definiciones

Sección 4 – Contexto de la organización (este)

Sección 5 – Liderazgo (este)

Sección 6 – Planificación (este)

Sección 7 – Apoyo (este)

Sección 8 – Funcionamiento (este)

Sección 9 – Evaluación del desempeño (este)

Sección 10 – Mejora (este)

Anexo A

Aquí se nota que CNT EP ya dispone de este tipo de normativas, lo que supone una seguridad total al sistema actual, sin embargo, aún no se esclarecen los agujeros de seguridad o posiblemente la aplicación de estas normas ISO 27001, son insuficientes

En el cuestionamiento: Cuál **es la estrategia recomendada por usted que podría permitir mejorar la seguridad de la información basado en la norma ISO 27001 en la empresa "CNT EP" de la ciudad de Babahoyo.**

Existen opciones básicas que podrían funcionar con la norma ISO 27001:

La implementación completa, esto es con la ayuda de empleados.

La puesta en marcha mediante la contratación de una empresa consultora.

Y la combinada, es decir, la implementación de la norma ISO 27001 con ayuda una empresa consultora y con los empleados de la CNT EP.

La implementación completa con la participación de los empleados, este caso particular se puede utilizar, cuando se decide poner a funcionar la norma ISO 27001 sin obtener de agentes externos a la organización, utilizando únicamente el conocimiento y la capacidad de sus propios empleados.

En esta opción, los empleados son los que realizan los análisis, entrevistas, y escribirán la documentación, etc., es la opción más económica, ya que no se paga ningún servicio externo.

La opción de contratar a una empresa consultora, experta, que cuente con la suficiente experiencia en aplicar la norma ISO 27001 en el sector de telecomunicaciones, esta persona necesitará la participación de personal interno de la institución, es una de las formas más rápidas y convenientes de implantar la norma ISO 27001, ya que la empresa consultora cuenta con la experiencia y el personal de la empresa cuenta con el conocimiento del funcionamiento y se adaptaría muy rápido a la disciplina alrededor a esta. Ref: Ing. Saltos (Anexo1)

El Ing. Milton Rodríguez, indica que: Se requiere realizar un pentesting para de esta manera determinar los puntos en las cuales se requiere una intervención.

Al parecer se podría profundizar un mejor estudio que permita asegurar mejor los aspectos informáticos de CNT EP y como se indicaba arriba, contratar una consultora y trabajar en conjunto con los servidores públicos de la empresa, para aprendizajes y para corroboración de funcionamientos.

En relación a este análisis, es importante fortalecer estas ideas de estudio, con fundamentación teórica como la siguiente.

¿QUÉ ES UNA CERTIFICACION ISO 27001?

Una certificación ISO 27001 prueba que se ha declarado conforme la implementación del sistema de gestión de seguridad de la información de la empresa en función a una norma internacional de buenas prácticas (Molina, 2016).

Esta norma se emplea para la certificación de los sistemas de gestión de seguridad de la información en las organizaciones empresariales; Otorga una norma internacional para sistemas de gestión de seguridad de la información.

Con la certificación del uso de la norma ISO 27001, la empresa puede demostrar a sus clientes actuales y potenciales, así como a sus proveedores y accionistas, la integridad en el manejo de la seguridad de la información. También le posibilita reforzar la seguridad de la información y disminuir los riesgos de fraude, pérdida o filtración de información.

De acuerdo a (Morán, 2020) La certificación ISO 27001 es esencial para proteger sus activos más importantes, la información de sus clientes y empleados, la imagen corporativa y otra

información privada. La norma ISO incluye un enfoque basado en procesos para lanzar, implantar, operar y mantener un SGSI.

Este tipo de norma de seguridad pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la tratan. También permite la gestión y también el control de los riesgos de la seguridad de la información en las organizaciones, promueve las mejores prácticas de seguridad de la información, para llegar a ser un auditor de esta norma se pueden adquirir a través de programas formales que incluyen el curso de formación y el examen de certificación, y que son impartidos por las entidades acreditadas para la realización de estas auditorías.

LA INFORMACION EN LA SEGURIDAD INFORMATICA

La información se considera como el oro de la seguridad informática ya que es lo que se desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo (Aguirre & Vera, 2018).

Actualmente la informática está siendo inundada por toda la información posible, pero la información por sí sola sigue siendo un universo más grande y en muchos casos más compleja de manejar, ya que los procesos en muchos casos no son tan visibles para los involucrados.

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Según (Coello, 2016) define que la seguridad informática es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o incluso la posibilidad de acceder a ellos por accidente.

Este tipo de seguridad es aquella que tiene como objetivo mantener la Integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por computadora, previniendo el robo de información importante y evitando ataques por parte de hackers o ciberdelincuentes, virus u amenazas.

SEGURIDAD DE LA INFORMACION

Por seguridad de la información se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización. (Rodriguez Arevalo & Torres Calderon, 2019)

La seguridad de la información es una pieza fundamental para que la empresa pueda llevar a cabo sus operaciones sin asumir demasiados riesgos, puesto que los datos que se manejan son esenciales para el devenir del negocio.

Además, también hay que tener en cuenta que la seguridad de la información debe hacer frente a los riesgos, analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos si se diera el caso.

CORPORACION NACIONAL DE TELECOMUNICACIONES (CNT EP)

Es una empresa estatal de telecomunicaciones ecuatoriana creada el 30 de octubre de 2008; opera servicios de telefonía fija local, regional e internacional, acceso a internet estándar y de alta velocidad (Dial-UP, DSL, Internet móvil 3g y 4G LTE), televisión satelital y telefonía móvil en el territorio nacional ecuatoriano. (CNT, 2019)

Esta empresa brinda a los ecuatorianos la mejor experiencia de servicios convergentes de telecomunicaciones y TICs, para su desarrollo e integración al mundo, impulsando el crecimiento de nuestra gente y creando valor para la sociedad. Además de tener gran amplitud de conexión a nivel nacional, para brindar la mejor conectividad alrededor del territorio ecuatoriano, que propone mejorar la capacidad de su red de datos y ampliar la cobertura nacional, incluyendo el despliegue de nuevos servicios como el video de alta definición, telepresencia, e-learning y seguridad pública.

La Corporación Nacional de Telecomunicaciones (CNT EP), entidad relacionada al Ministerio de Telecomunicaciones y de la Sociedad de la Información, logra cambios importantes en los servicios de telefonía e internet ofertados en el país. (Telecomunicaciones, 2018)

Actualmente, los avances en las redes móviles de tercera generación 3G y cuarta generación 4G LTE, están permitiendo ofrecer más y mejores servicios de telefonía móvil e internet banda ancha móvil, que brindan cobertura en las 24 provincias del país. En algunas provincias, ciudades y barrios del Ecuador como: Quito, Cumbayá, Tumbaco, Los Chillos, Ambato, Baños, Latacunga, Santo Domingo, Guayaquil, Daule, Durán, Loja e Ibarra entre otras.

ANÁLISIS Y EVALUACIÓN DE RIESGOS EN ISO 27001

El tipo de análisis de riesgos en ISO 27001 no está prescrito dentro del cuerpo de la norma. ISO 27001 requiere que la organización evalúe las consecuencias y la probabilidad de cada riesgo, pero no dice cómo hacerlo**.** Depende de los encargados del sistema decidirlo. (Bohorquéz, 2020)

Cuando se implementa el análisis de riesgos en ISO 27001, la identificación de activos, amenazas y vulnerabilidades que atañen a la seguridad de la información es tan solo la primera parte del trabajo. La segunda fase, tan importante como la primera y no menos difícil, implica evaluar las consecuencias y probabilidades de cada riesgo. En otras palabras, sin importar que modelo se elija el procedimiento debe ser documentado. La finalidad de estos enfoques es evaluar el riesgo para tener una idea sobre las posibilidades de que los objetivos no se alcancen, así como poder priorizar aquellos riesgos en los que han de centrarse los mayores esfuerzos.as, la probabilidad de que ocurra y el impacto negativo que supone su ocurrencia.

AMENAZAS EN ISO 27001

La norma ISO 27001 se fundamenta principalmente en la identificación y análisis de las principales amenazas para, a partir de este punto de partida, poder establecer una evaluación y planificación de dichos riesgos (Carrasco, 2019).

Una amenaza se puede definir como cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser: ataques informáticos externos, infecciones con malware, una inundación, un incendio o cortes de fluido eléctrico.

ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS Y SUS CONSECUENCIAS

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos se permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección. (Amutio Gómez & Candau, 2016)

Se debe analizar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información, evaluando de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades e impactos en los activos.

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento.

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades, estas están íntimamente ligadas y no puede haber ninguna consecuencia sin la presencia conjunta de estas (Tarazona, 2017)

Las amenazas contra los sistemas de información, significan un riesgo para las organizaciones y sus consecuencias pueden ser graves y deben ser evaluadas; La información ha sido uno de los elementos claves en el desarrollo y éxito de los negocios y en el desarrollo de la gran mayoría de actividades diarias de las personas. Por este motivo las organizaciones están considerando que proteger la información, ahora es una necesidad.

AMENAZAS Y VULNERABILIDADES DENTRO DE LA NORMA ISO 27001

Las amenazas son las situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información. (Martinez & Molina , 2015)

Las consecuencias de las amenazas es un incidente que modifica el estado de seguridad de los activos amenazados, por lo que se hace pasar de un estado anterior al evento a otro posterior, de cualquier forma, que se trate la amenaza o las agresiones materializadas.

La vulnerabilidad de un activo de seguridad es la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información. (Goméz Rodriguéz, 2015)

Una vulnerabilidad es un dominio entre la relación de un activo y una amenaza, aunque puede estar vinculado más al activo que a la amenaza. Existen dos tipos de vulnerabilidades: vulnerabilidad intrínseca de activo, que se refiere al tipo de amenaza que depende de todas las cantidades; Y vulnerabilidad efectiva de activo, esta tiene en cuenta todas las salvaguardas que se aplican en cada momento a los activos.

CRITICIDAD DEL RIESGO

Un SGSI basado en ISO 27001 se fundamenta principalmente en la identificación y análisis de las principales amenazas para poder evaluar dichos riesgos. Por este motivo, se deben evaluar las consecuencias potenciales para poder evaluar su criticidad: riesgo aceptable y riesgo residual. (Moncada, 2019)

El tipo de riesgo aceptable, su objetivo es reducir su posibilidad de ocurrencia y minimizar las consecuencias a unos niveles que la organización pueda asumir, sin que suponga un perjuicio demasiado grave a todos los niveles: económico, logístico, de imagen, de credibilidad, etc.

El riesgo residual, es un reflejo de las posibilidades de que ocurra un incidente, pese a verse implantado con eficacia las medidas evaluadoras y correctoras para mitigar el riesgo inherente.

CONTROLES MÁS IMPORTANTES DE LA ISO 27001

Dentro de la norma ISO 27001 se encuentra el Anexo A, el cual es indispensable implementar ya que es el normativo y dentro de este se encuentra todo lo relacionado a los controles de seguridad, que son fundamentales porque estos ayudan en la protección de la información de las empresas, además, ponerlos en práctica es de carácter obligatorio. (Arévalo, 2020)

Los controles son obligatorios según la aplicabilidad en cada organización. Los encargados de la seguridad de la información son quienes deben definir cuáles son los que se van a poner en marcha para garantizar la protección de datos. Es indispensable generar una capacitación sobre esta norma para establecer los controles adecuados en la gestión de la seguridad de la información.

Existe un total de 114 controles de seguridad; La organización debe elegir cuáles se rigen mejor a sus necesidades, es importante saber que no solo se limita al área de tecnología, sino que también comprende departamentos como el de recursos humanos, seguridad financiera, comunicaciones, entre otros.

CONCLUSIONES

Se puede concluir qué, es necesario e importante que se entienda, qué una empresa puede manejar normativas de seguridad Cómo la ISO 27001 y está puede ser vulnerada en su activo más importante que es la información, pues no solamente depende de tener certificaciones colgadas en la pared registradas en algún lugar en el internet sino que también es importante qué estas normativas tengan funcionalidad y participación con sus empleados qué utilizan recursos y sistemas de información así como los que están alrededor de quién es acceden a los sistemas.

Las normativas de seguridad de la información por los controles que estás se han diseñado para reducir los impactos como mejorar la seguridad deben venir apegadas a políticas que son normativas también pero de nivel más aterrizado la realidad de la organización, estás políticas en el caso de una empresa tan grande como CNT EP, deben también desplegarse a los territorios para ser cumplidas por todo el personal técnico hasta la persona que utiliza el sistema más mínimo o cuenta con una computadora conectada a la red local.

Este estudio también permitió concluir que podrían solucionarse ciertos aspectos de seguridad ya posterior al haber sufrido un ataque utilizando formas y técnicas básicas como las de mejorar y personalizar cada equipo para que esté se encuentre estandarizado a la institución y no permitir fugas o agujeros de inseguridad.

RESUMEN Y PALABRAS CLAVES

Este caso de estudio trata de la seguridad de la información, que es uno de los aspectos a los que han logrado tomar uno de los mayores intereses en el campo informático aun cuando el mundo computacional se ha vuelto más fácil cada día, sin embargo, la inseguridad relativa a esto es incremental.

En este documento existe referencia de los peligros y las pérdidas de uno de los activos más importantes de las empresas como lo es la información y su relación de minimizar impactos con la norma ISO 27001, ya que siempre son importantes de tratarlos para evitar y prevenir que tener que lamentar por pérdida total de los datos.

Este caso de estudio se orientó amparado en la sublínea de investigación de la carrera de ingeniería en sistemas, pues la línea de investigación es la siguiente: "Comunicación y emprendimientos empresariales y tecnológicos, desarrollo de Sistemas de la información y la sublínea es procesos de datos y telecomunicaciones".

Así mismo, con este caso de estudio, se ha necesitado fortalecer muchos temas relacionados con la seguridad de la información y las normas ISO 27001, donde se invitó también a participar a reconocidos técnicos, todos ingenieros en sistemas de la ciudad de Babahoyo, que con sus conocimientos aportaron mucho para lograr un análisis adecuado que se requería en este trabajo de fin de carrera, y con esto se entiende que mejora las debidas garantías de pensamiento técnico referenciadas por expertos en la materia; cabe indicar que, además esto ha sido muy analizado por el autor, que sumado a esto enriqueció la investigación con teorías importantes e inherentes de forma citada y referenciada, que permitieron consolidar el caso de estudio presente.

Aquí, además se incluyen anexos, donde se evidencian las varias participaciones en las entrevistas.

PALABRAS CLAVES

Norma ISO27001

Seguridad Informática

Agujeros de Seguridad

Políticas

Ramson Ware

SUMMARY AND KEYWORDS

This case study deals with information security, which is one of the aspects to which they have managed to take one of the greatest interests in the computer field even though the computational world has become easier every day, however, the Insecurity regarding this is incremental.

In this document there is a reference to the dangers and losses of one of the most important assets of companies such as information and its relationship to minimize impacts with the ISO27001 standard, since it is always important to treat them to avoid and prevent having to regret for total loss of data.

This case study was oriented under the research sub-line of the systems engineering career, since the research line is the following: "Communication and business and technological undertakings, development of information systems and the sub-line is data processes and telecommunications".

Likewise, with this case study, it has been necessary to strengthen many issues related to information security and ISO 27001 standards, where well-known technicians were also invited to

participate, all systems engineers from the city of Babahoyo, who with His knowledge contributed a lot to achieve an adequate analysis that was required in this final degree project, and with this it is understood that it improves the due guarantees of technical thinking referenced by experts in the field; It should be noted that, in addition, this has been highly analyzed by the author, who added to this enriched the research with important and inherent theories in a cited and referenced way, which allowed the consolidation of the present case study.

Here, in addition, annexes are included, where the various participations in the interviews are evidenced.

KEYWORDS

ISO27001 standard

Informatic security

Security Holes

Policies

Ramson Ware

BIBLIOGRAFIA

Aguirre, M., & Vera, S. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. *3ciencias,* 4-20.

Amutio Gómez, M. A., & Candau, J. (2016). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *Ministerio de Hacienda y Administraciones Públicas,* 47-60. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Arévalo, M. C. (13 de Octubre de 2020). *Pirani*. Obtenido de Pirani: https://www.piranirisk.com/es/blog/cuantos-controles-tiene-la-norma-iso-27001

Bohorquéz, E. (8 de Enero de 2020). *Escuela Europea de Excelencia*. Obtenido de https://www.escuelaeuropeaexcelencia.com/2020/01/analisis-de-riesgos-en-iso-27001-evaluar-consecuencias-y-probabilidades/#:~:text=An%C3%A1lisis%20de%20riesgos%20en%20ISO%2027001%3A%20evaluar%20consecuencias%20y%20probabilidades,-EEE2020%2D01&text=En%20otr

Carrasco, M. (30 de Julio de 2019). *ISOTOOLS*. Obtenido de ISOTOOLS: https://www.isotools.org/2019/07/30/analisis-y-evaluacion-de-riesgos-segun-iso-27001/

CNT. (2019). *CNT*. Obtenido de https://teayuda.cnt.com.ec/

Coello, G. (9 de Septiembre de 2016). *Universidad Tecnica de Valencia*. Obtenido de Universidad Tecnica de Valencia: https://www.universidadviu.com/ec/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

Goméz Rodriguéz, N. (27 de Mayo de 2015). *Isotools*. Obtenido de Isotools: https://www.isotools.pe/iso-27001-cuales-son-las-amenazas-y-vulnerabilidades/

Martinez, C., & Molina , S. (6 de Abril de 2015). *PMG SSI*. Obtenido de PMG SSI: https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

Molina, A. (3 de Mayo de 2016). *Conexión ESAN*. Obtenido de Conexión ESAN: https://www.esan.edu.pe/apuntes-empresariales/2016/05/que-es-y-para-que-sirve-la-norma-iso-27001/

Moncada, L. (6 de Junio de 2019). *PMG SSI*. Obtenido de PMG SSI: https://www.pmg-ssi.com/2019/06/analisis-y-evaluacion-de-riesgos-en-iso-27001-amenazas-consecuencias-y-criticidad/

Morán, P. (30 de Julio de 2020). *nqa*. Obtenido de nqa: https://www.nqa.com/es-mx/certification/standards/iso-27001

Rodriguez Arevalo, J., & Torres Calderon, W. (2019). ANALISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACION DEL AREA IT DE LA EMPRESA ROYAL SERVICES S.A. *Universidad Católica de Colombia*, 1-44. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/23389/1/ANALISIS%20DE%20RIESGOS%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION%20DEL%20AREA%20IT%20DE%20LA%20EMPRESA%20ROYAL%20SERVICES%20S.A.pdf

Tarazona, C. (2017). Amenazas informáticas y seguridad de la información. *Uniroja*, 10-34.

Telecomunicaciones. (4 de Marzo de 2018). *Telecomunicaciones*. Obtenido de Telecomunicaciones: https://www.telecomunicaciones.gob.ec/cnt-ep-conecta-con-mas-y-mejores-servicios-al-ecuador/

ANEXO 1

RELACIONADO CON: ANALISIS DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN LA EMPRESA "CNT EP" DE LA CIUDAD DE BABAHOYO.

FECHA: 13/SEPTIEMBRE/2021

NOMBRE ENTREVISTADO: ING. HARRY SALTOS VITERI

AREA DE TRABAJO: DOCENTE UTB

Como y en que dimensión se ha visto afectada a la empresa CNT EP a nivel nacional y en el ámbito local, es decir (Babahoyo) durante la última vulneración a sus sistemas.

Al parecer, CNT EP se vio afectada en su máxima dimensión, fue vulnerada en su información, que es el activo más importante que puede tener una organización, es una empresa que además en el listado de sus productos y servicios, contempla un datacenter TIER III, esto es un lugar donde otras empresas almacenan y aprovisionan sus servidores, haciéndole perder la imagen corporativa de confiabilidad relacionada con los datos.

CNT EP seguramente es una empresa que durante su última afectación, perdió valor en el mercado, ya no tendrá una valoración regular o mediana como antes de la incidencia de inseguridad, tendrá una valoración de seguro que en el rango de hacerla atractiva para la venta, por parte del gobierno de turno.

Si usted fuese el responsable tecnológico de manejar la seguridad de CNT EP en Babahoyo, cuáles serían las estrategias para lograr mejorar la seguridad de la información.

Para manejar la seguridad en CNT EP Babahoyo, primero hay que pensar en que se trata de una empresa donde se manejan estándares nacionales y debe ir apegado todo a lo que la nacional aplica, lo que puede hacerse desde Babahoyo son recomendaciones para aplicarse como estándar nacional, sin embargo localmente se podría manejar cierta disciplina en cuanto a la utilización de medios de almacenamiento extraíbles, navegación por sitios confiables y aplicación de algunas secciones de normativas ISO 27001

En relación a las normas ISO 27001, considera usted, que estas han sido aplicadas en CNT EP, comentar cuanto conoce de aquello por favor.

Se conoce que CNT EP maneja normativas ISO 27001, sin embargo habría que ver en que dimensión la aplican, al no ser de la parte técnica de CNT EP, no podría dimensionar en relación a esto.

De las siguientes secciones de las que están divididos los 114 controles de la norma ISO 27001, cuales considera que están siendo aplicados o son aplicables a CNT EP Babahoyo

Sección 0 – Introducción

Sección 1 – Alcance (este)

Sección 2 – Referencias normativas (este)

Sección 3 – Términos y definiciones

Sección 4 – Contexto de la organización (este)

Sección 5 – Liderazgo (este)

Sección 6 – Planificación (este)

Sección 7 – Apoyo (este)

Sección 8 – Funcionamiento (este)

Sección 9 – Evaluación del desempeño (este)

Sección 10 – Mejora (este)

Anexo A

Cuál es la estrategia recomendada por usted que podría permitir mejorar la seguridad de la información basada en la norma ISO 27001 en la empresa "CNT EP" de la ciudad de Babahoyo.

Existen opciones básicas que podrían funcionar con la norma ISO 27001:

La implementación completa, esto es con la ayuda de empleados.

La puesta en marcha mediante la contratación de una empresa consultora.

Y la combinada, es decir, la implementación de la norma ISO 27001 con ayuda una empresa consultora y con los empleados de la CNT EP.

La implementación completa con la participación de los empleados, este caso particular se puede utilizar, cuando se decide poner a funcionar la norma ISO 27001 sin obtener de agentes externos a la organización, utilizando únicamente el conocimiento y la capacidad de sus propios empleados.

En esta opción, los empleados son los que realizan los análisis, entrevistas, y escribirán la documentación, etc., es la opción más económica, ya que no se paga ningún servicio externo.

La opción de contratar a una empresa consultora, experta, que cuente con la suficiente experiencia en aplicar la norma ISO 27001 en el sector de telecomunicaciones, esta persona necesitará la participación de personal interno de la institución, es una de las formas más rápidas y convenientes de implantar la norma ISO 27001, ya que la empresa consultora cuenta con la experiencia y el personal de la empresa cuenta con el conocimiento del funcionamiento y se adaptaría muy rápido a la disciplina alrededor a esta.

RELACIONADO CON: ANALISIS DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN LA EMPRESA "CNT EP" DE LA CIUDAD DE BABAHOYO.

FECHA: 14-SEPTIEMBRE-2021

NOMBRE ENTREVISTADO: Ing. Milton Rodríguez

AREA DE TRABAJO: CNT – AREA TECNICA

Como y en que dimensión se ha visto afectada a la empresa CNT EP a nivel nacional y en el ámbito local, es decir (Babahoyo) durante la última vulneración a sus sistemas.

A nivel nacional una vez declarada en rueda de prensa de manera oficial por las autoridades de la empresa a través del área Jurídica y el Gerente general Arq. Byron Zapata. Se dispuso el apagado inmediato de los dispositivos electrónicos y sistemas informáticos para evitar que la vulnerabilidad a la red siga avanzando. Nuestra empresa se vio afectada a nivel nacional en sus sistemas de facturación y sistemas de gestión comercial, lo cual produjo retraso en los pagos y malestar en la ciudadanía. Es así que en la ciudad de Babahoyo muchas de las empresas competidoras de Internet se aprovecharon de esta situación y elaboraron muchos planes de Instalación de Internet en la que accedieron muchos clientes nuestros desistiendo de nuestro servicio. A pesar de que la parte operativa de la red de telecomunicaciones no fue afectada.

Si usted fuese el responsable tecnológico de manejar la seguridad de CNT EP en Babahoyo, cuáles serían las estrategias para lograr mejorar la seguridad de la información.

Establecer protocolos de seguridad de acuerdo a las normas Internacionales según la ITu. ISO y demás.

Tener sistemas acorde a las nuevas tecnologías las cuales brindan soluciones integrales para protección de datos e información.

Capacitar y concientizar al personal encargado del manejo de información sobre el buen uso de los dispositivos electrónicos y sistemas de información.

En relación a las normas ISO 27001, considera usted, que estas han sido aplicadas en CNT EP, comentar cuanto conoce de aquello por favor.

La empresa es certificada en ISO 27001 pero lamentablemente el nivel de ataque a la que fue sometido sus sistemas implica reforzar mucho más a sus sistemas y servidores.

De las siguientes secciones de las que están divididos los 114 controles de la norma ISO 27001, cuales considera que están siendo aplicados o son aplicables a CNT EP Babahoyo

Sección 0 – Introducción

Sección 1 – Alcance

Sección 2 – Referencias normativas

Sección 3 – Términos y definiciones

Sección 4 – Contexto de la organización

Sección 5 – Liderazgo

Sección 6 – Planificación

Sección 7 – Apoyo

Sección 8 – Funcionamiento

Sección 9 – Evaluación del desempeño

Sección 10 – Mejora

Anexo A

Para asegurar la calidad e integridad de nuestros servicios es necesario aplicar todas las secciones de la Norma ISO sin excepción.

Cuál es la estrategia recomendada por usted que podría permitir mejorar la seguridad de la información basada en la norma ISO 27001 en la empresa "CNT EP" de la ciudad de Babahoyo.

- **Se requiere realizar un pentesting para de esta manera determinar los puntos en las cuales se requiere una intervención.**