UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
PROCESO DE TITULACIÓN

NOVIEMBRE 2020 – MAYO 2021

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA
PRUEBA PRÁCTICA

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

TEMA:

ANALISIS DE LOS SISTEMAS INFORMATICOS APLICANDO LA NORMA ISO 27005 EN LA UNIDAD DE TRANSITO MUNICIPAL DEL CANTON PUEBLOVIEJO

EGRESADA(O):

YANEZ FAJARDO ROMARIO ALDAIR

TUTOR:
ING. LEON ACURIO JOFFRE VICENTE

AÑO 2021

INTRODUCCION

Los sistemas informáticos surgen de la necesidad de transmitir y procesar información su propósito original es ayudar a las personas a participar en esas tareas diarias, repetitivo, generalmente una repetición del cálculo y la gestión, para la elaboración del caso de estudio cuyo tema es, "**ANALISIS DE LOS SISTEMAS INFORMATICOS APLICANDO LA NORMA ISO 27005 EN LA UNIDAD DE TRANSITO MUNICIPAL DEL CANTON PUEBLOVIEJO**",

La UNIDAD DE TRANSITO MUNICIPAL DEL CANTON PUEBLOVIEJO se dedica a la revisión y matriculación de vehículos. Hoy en día, a menudo se escucha que los piratas informáticos infiltran la información de los clientes de la empresa y exigen grandes cantidades de fondos. Para ello, es necesario establecer una infraestructura que cumpla con los más altos estándares en términos de seguridad, integridad y confidencialidad.

En la actualidad, la Agencia Nacional de Transporte de Ecuador está utilizando el sistema AXIS versión 4.0, debido a diferentes factores, el sistema ha ocasionado algunos problemas en el proceso de entrada y salida de información

Deben adoptarse normativas que apoyen la implementación de medidas de control para abordar la importancia que las empresas deben considerar al implementar medidas de seguridad relacionadas con el acceso y robo de información. El activo más valioso de la empresa es la información, por lo que enfatiza la implementación de la normativa ISO 27005 que aporta en detalle con múltiples formatos y escalas de evaluación para **facilitar la identificación de los activos, sus vulnerabilidades, amenazas y controles.**

Según (Acissi, 2015), la seguridad Informática en los sistemas de información, representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información, entendiendo como tal al conjunto de datos y de recursos (físicos, lógicos y humanos) que permiten almacenar y que circule la información que contiene. También representa la red de actores que intervienen sobre él, que intervienen datos, acceden a ellos y los usan.

A medida que los negocios iban evolucionando, el volumen de información y de las transacciones se incrementaban, por lo que las organizaciones tuvieron la necesidad de

recurrir a la automatización de sus sistemas de información, por ejemplo, tuvieron que automatizar los registros contables y varios procesos operativos, los cuales tenían que ser soportados por activos de tecnología como servidores, redes, software y hardware especializado (Espinoza, 2016)

Al desempeñar su trabajo, el auditor se encuentra con diferentes sistemas de administración de la información implementados las organizaciones, sobre todo automatizados, como los registros contables, sistemas de personal, gestión de inventarios, transferencias bancarias electrónicas, registros biométricos, y la aparición de activos de tecnología que soportan estos sistemas como ser los servidores, redes, centrales de comunicación, son solo algunos ejemplos (Espinoza, 2016)

El número de amenazas se incrementa y obliga a que garantizar la disponibilidad, confidencialidad e integridad de la información signifique un aspecto de primer orden sobre el cual invertir para evitar la pérdida, modificación o robo de los activos informáticos. (Miranda Cairo, M., Valdés Puga, O., Pérez Mallea, I., Portelles Cobas, R., & Sánchez Zequeira, R., 2016)

DESARROLLO

Considerando que el gobierno municipal descentralizado es autónomo se puede implementar un mecanismo de control mediante la norma ISO 27005 para tener un enfoque diferente, unos de los requisitos a tener en cuenta en las normas ISO es de tener una información documentada sobre los objetivos de seguridad en la cual se adoptan diferentes maneras de llevar a cabo dichas formas. El departamento técnico, legal y los colaboradores de la unidad se encuentran en Según todas las resoluciones de la ANT, la "Ley de Transporte Terrestre, Tráfico y Seguridad Vial" Y normativa municipal, es necesario utilizar un manual como Una herramienta que puede transferir la práctica y el conocimiento del proceso a realizar e instrucciones. Lo que se necesita paso a paso.

Además, un punto importante a considerar son los recursos que posee la organización para comprometerse de manera adecuada a un proceso de gestión del riesgo y otro es el motivo por el cual la organización decide implementar una metodología. Según el contexto, puede ser por un gran número de incidentes relacionados con la seguridad de la información, para la preparación de un plan de continuidad de las actividades, por aspectos legales o requisito para la creación de un Sistema de Gestión de Seguridad de Información (Carpentier, 2016)

En las entidades públicas existe la necesidad de implementar nuevos sistemas de seguridad de la información, con el objeto de fortalecer las políticas y procedimientos de uso, estando supeditadas incluso a políticas a nivel de entes de control, encargadas de verificar que se administren y gestionen eficientemente. (Gonzalez, 2018)

Teniendo en cuenta el artículo 264 de la Constitución Política de la República del Ecuador, en 2014 se creó la Agencia Nacional de Transporte para otorgar al gobierno municipal la facultad exclusiva de planificar, controlar y fiscalizar el transporte público y el tránsito dentro de su territorio estatal. El gobierno autónomo descentralizado del estado de San Francisco de Puebloviejo requiere capacidades activas dentro de su jurisdicción para planificar, organizar y administrar el tránsito y el transporte terrestre.

Actualmente en la Agencia Nacional de Transporte del Estado de Puebloviejo, hay muchas incidencias en el sistema de registro, cuando se ingresa la renovación del registro al

mismo propietario, el proceso duraba unos 5 minutos y en ocasiones el sistema fallaba. Y cada persona tarda entre 15 y 30 minutos en responder, y el resultado es que los recursos no se utilizan de forma eficaz.

Análisis de los Sistemas dentro de la Empresa

Tabla 1: Análisis del Sistema AXIS 4.0 utilizado en la UNIDAD MUNICIPAL DE PUEBLOVIEJO

AXIS 4.0	
Metodología	XP
Herramientas	Oracle Exalogic y Oracle Linux.
Sistemas de ingeniería	Oracle SuperCluster. Oracle Exadata
Bases de datos	OLTP, Data Warehouses
Sistema	AXIS (CRM + BSS + OSS),
IP	Fija conectada a la red de datos.
Sistema operativo	Android, Windows o Linux

Tabla 1. Elaborado por Yanez Romario.

Análisis:

Es una aplicación web que es utilizada por parte de la Unidad Municipal de transito de Puebloviejo, para la matriculación y revisión vehicular, debido a nuestro análisis con la norma ISO 27005 se puede establecer pautas para gestionar los riesgos de seguridad. Sobre posibles amenazas potenciales para aprovechar la posibilidad de vulnerabilidades en activos o grupos. Activos que causan daños a la organización. La cual se mide de acuerdo con la combinación de la probabilidad de un evento y su tasa de ocurrencia.

A través de la observación directa de la tecnología, se descubrió que hubo una violación del sistema en la Unidad de tránsito municipal de Puebloviejo, utilizar la norma ISO 27005 nos permitirá comprender las actividades y la gestión que se llevan a cabo, así como algunas técnicas y para probar posibles soluciones a los problemas ocasionados por la falta de actualizaciones. También comprende la información en el sistema mediante la realización de entrevistas con personas involucradas en la gestión del sistema AXIS.

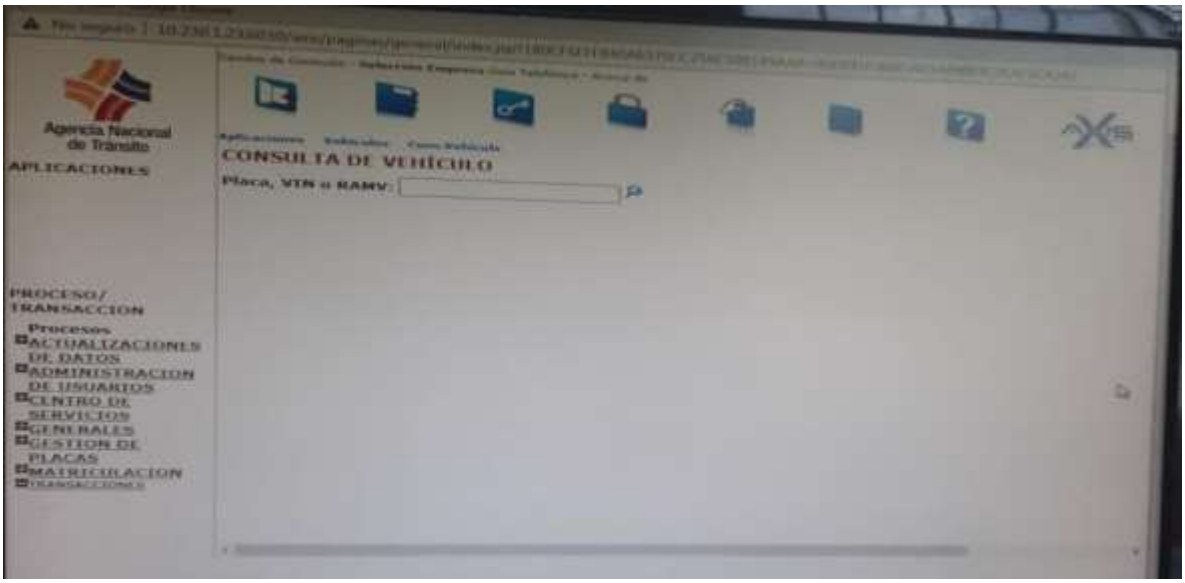

Figura 1. Funcionamiento del Sistema AXIS4.0

La visión de desarrollo es controlar el movimiento del transporte terrestre, el tráfico y las capacidades de seguridad vial, con base en la calidad y transparencia del servicio, para asegurar que la sociedad ecuatoriana controle efectivamente el transporte terrestre a través de la planificación.

INFORMACIÓN GENERAL

Se necesita un método sistemático de gestión de riesgos de seguridad de la información para identificar las necesidades de la organización en cuanto a los requisitos de seguridad de la información y crear un sistema de gestión de seguridad de la información (SGSI) eficaz. Este método debe ser adecuado para el entorno de la organización y, en particular, debe cumplir con todas las pautas de gestión de riesgos de la empresa. El trabajo seguro debe realizarse en el momento y lugar necesarios para hacer frente a los riesgos de manera eficaz y oportuna. La gestión de riesgos de seguridad de la información debe convertirse en una parte integral de todas las actividades de gestión de seguridad de la información y debe aplicarse a la implementación y operación continua del SGSI al mismo tiempo.

El sistema de gestión de la seguridad de la información debe basarse en un enfoque sistemático, no solo para comprender los procesos comerciales, sino también para comprender el flujo de información entre estos procesos.

La gestión de riesgos de seguridad de la información debe ser un proceso continuo. Dicho proceso debe configurar el entorno, evaluar el riesgo y utilizar el plan de tratamiento para implementar recomendaciones y decisiones para tratar el riesgo. Antes de decidir qué se debe hacer y cuándo, la gestión de riesgos analiza las posibles situaciones y posibles consecuencias para reducir el riesgo a un nivel aceptable.

La seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de ordenadores a concentrarse en políticas, procedimientos y controles basados en las personas. (Cárdenas Solano , L. J., Martínez Ardila, H., & Becerra Ardila, L. E., 2016)

La siguiente tabla resume las actividades de gestión de riesgos de seguridad de la información relacionadas con las cuatro etapas del proceso del SGSI:

Proceso de SGSI	Proceso de gestión del riesgo en la seguridad de la información
Planificar	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continuos de los riesgos
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

SISTEMA DE INFORMACIÓN

Un sistema de información (SI) es un conjunto de elementos interrelacionados con el propósito de prestar atención a las demandas de información de una organización, para elevar el nivel de conocimientos que permitan un mejor apoyo a la toma de decisiones y desarrollo de acciones

(Peña, 2006)

Además, (Gomez, 2013) determina al proceso de análisis de riesgos como "una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y objetividad para que cumpla su función con garantías". Las entidades públicas están obligadas a realizar un proceso de gestión de riesgos, que es un análisis en profundidad de los eventos que pueden tener un impacto negativo en la continuidad de las actividades organizacionales.

En particular en el apartado 410-10 Seguridad de tecnología de información, recomienda el establecimiento de mecanismos que protejan y salvaguarden contra las pérdidas y fugas de los medios físicos y la información que se procesa mediante sistemas informáticos. Igualmente, indica que se debe implementar acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados. (Ecuatoriana, 2009)

La seguridad de la información tiene por objeto proteger a los sistemas informáticos de las amenazas a los que están expuestos. Debido a lo anterior, la aplicación de medidas de seguridad debe realizarse de manera planificada y racional, para evitar dirigir esfuerzos e invertir recursos en áreas que no lo requieren. Para que las medidas y mecanismos de protección resulten eficaces, deben integrarse dentro de un sistema más amplio de gestión de la seguridad de la información

IMPORTANCIA DE LA INFORMACIÓN.

La información es una herramienta para la difusión del conocimiento y se ha convertido en un factor importante en el progreso social. “Entre otros factores, el desarrollo de todas las disciplinas se caracteriza por agilizar la recolección, almacenamiento, procesamiento y transmisión de información. Ha producido diversas influencias a través de los elementos estratégicos que constituyen el desarrollo integral de la sociedad ". (Alfonso, 2013)

Para lograr este objetivo se requiere de personal capacitado y comprometido con el desarrollo de la importancia de la información diversa generada por diversas instituciones (públicas o privadas), y la información que puede aportar al país ya la comunidad internacional.

La tecnología de la información (TI) se ha convertido en un elemento esencial para apoyar el crecimiento y la sostenibilidad de todo tipo de organizaciones; para controlar este conjunto heterogéneo de tecnologías, es necesaria su gestión eficaz utilizando estructuras, procesos y mecanismos relacionales; cada uno de estos mecanismos tiene una función y cuando se implementa, debe impactar positivamente a la organización (Scalabrin, I. & Dinis, R., 2016)

La importancia de la información para el destinatario será la medida en que ha cambiado la actitud o el comportamiento de un individuo. Los resultados se obtienen de los medios de comunicación que generan información, gran parte del cual no es importante Para ellos, porque apenas cambia significativamente Ellos mismos. Esto significa Expectativas de futuro. A veces la gente sabe que los hechos lo hacen imposible Algunas cosas y más otras

cosas, la importancia está relacionada con la reducción. Las opciones posibles son relativas a otras opciones.

La auditoría de seguridad informática es un concepto relacionado con la seguridad de la información., el cual según el autor (Chicano Tejada, 2015): "La auditoría de seguridad informática analiza todos los procesos referentes a la seguridad informática, tanto física como lógica"

Las normas internacionales de auditoría establecen que el auditor debe contar con conocimientos suficientes, dentro lo que comprende el enfoque moderno de auditoría basada en riesgos, estos conocimientos se refieren a habilidades y competencias para el examen de los controles de aplicación que están directamente relacionados a los procesos del negocio, pero también llegar a comprender los controles generales de las tecnologías de la información, ya que a través de la comprensión e identificación de los probables riesgos y de los controles clave, puede planificar, dirigir, supervisar y revisar el proceso (Espinoza, 2016)

Lo importante en este contexto es que la gestión de la informática empresarial está muy influenciada no sólo por los estándares antes mencionados directamente creados para, o al menos remotamente conectados con la tecnología de la información, sino también por muchas otras normas que aparentemente no tienen nada en común. (Haufe, K.; Colomo, R.; Dzombeta, S.; Brandis, K. & Stantchev, W., 2016)

DEFINICIÓN DE UN SGSI

Toda la información almacenada y procesada por la organización está amenazada por ataques (por intereses comerciales, intelectuales y / o en blanco y negro y extorsión), errores (intencionales o negligentes), medio ambiente (como inundaciones o incendios), sistemas (storage de datos). , informática, remota Cuando falla la red de procesamiento de información, todavía existen algunas vulnerabilidades, que representan las debilidades inherentes de su propio uso en el ciclo de vida que se muestra a continuación.

Proporcionar información precisa y completa al personal autorizado de manera oportuna es un catalizador para mejorar la eficiencia empresarial.

Después de establecer los objetivos de seguridad de la información, necesitamos asegurar la forma efectiva de lograr estos objetivos, en resumen, la forma abreviada del sistema de gestión de seguridad de la información o SGSI.

Por lo tanto, el SGSI consiste en un conjunto de estrategias, procedimientos y lineamientos, así como recursos y actividades relacionadas administrados conjuntamente por la organización, con el fin de buscar proteger sus activos básicos de información.

SGSI desde la perspectiva de la norma internacional ISO / IEC 27001 es una empresa de métodos de sistemas que establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información de una organización y logra sus objetivos comerciales y / o de servicio (por ejemplo, en lugares públicos), Organizaciones sin ánimo de lucro, ...).

El alcance del SGSI puede incluir, dependiendo de la ubicación de los activos de información básica que se identifican y ubican, una parte de la organización total, funciones específicas y definidas de la organización, partes específicas y definidas de la organización, o una o más funciones en la organización.

El término "seguridad de la información" generalmente se basa en el hecho de que la información se considera un activo y su valor debe protegerse adecuadamente, como evitar la pérdida de disponibilidad, confidencialidad e integridad.

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. (Urbina, 2016)

Toda organización puede ampliar e integrar las tres características básicas iniciales en el SGSI para definir la seguridad como características adicionales, tales como autenticidad, trazabilidad, no repudio, auditabilidad, ... se consideran aptas para satisfacer requisitos internos y / o requisitos externos aplicables a cada actividad.

Independientemente del tipo y escala de la actividad, cualquier organización recopila, procesa, almacena y transmite información mediante el uso y la aplicación de procesos, sistemas, redes y personales internos y / o externos. Todos estos son activos de información necesarios para lograr los objetivos de la organización. Según el contexto (tipo de industria, entorno operativo, etc.) y cada momento concreto de la actividad, la organización se enfrentará inevitablemente a riesgos en función de diversos factores que pueden afectarla. Pueden tener un impacto negativo en los activos de información más necesarios. La supervivencia de una organización dependiente en gran medida de la identificación correcta de los factores más relevantes y de una evaluación adecuada del grado de incertidumbre

Confidencialidad: las personas, entidades o procesos no autorizados ni deben proporcionar ni divulgar información a otros.

Integridad: mantener la precisión y la integridad de la información y sus métodos de procesamiento.

Disponibilidad: Autorizar a las personas, entidades o procesos a acceder y utilizar la información y sus sistemas de procesamiento cuando sea necesario.

ISO/IEC 27000

Publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012, una tercera edición de 14 de Enero de 2014 y una cuarta en Febrero de

2016. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua). Existen versiones traducidas al español, aunque hay que prestar atención a la versión descargada. El original en inglés y su traducción al francés en su versión de 2018 puede descargarse gratuitamente.

La serie ISO 27000 es una de las normas que enumera los siguientes temas: Seguridad de la información y otra seguridad de la información relacionada con los estándares Ayúdelo a desarrollarse para ser totalmente compatible, por ejemplo, Norma ISO 9000 y norma ISO 14000.

ISO/IEC 27001

Publicada el 15 de octubre de 2005, revisada el 25 de Septiembre de 2013 segunda edición). Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Es una norma que proporciona los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información. El sistema de gestión de la seguridad de la información se basa en salvaguardar la integridad, disponibilidad y confiabilidad de la información en una organización (ISO/IEC, 2017)

Desde el 12 de Noviembre de 2014, esta norma está publicada en España como UNE-ISO/IEC 27001:2014 y puede adquirirse online en UNE. En 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015) y en diciembre de 2015 una segunda modificación (ISO/IEC 27001:2013/Cor.2:2015) esta última matizando especificaciones en la declaración de aplicabilidad. Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27001), Chile (NCh-ISO27001) o Uruguay (UNIT-ISO/IEC 27001). El original en inglés y la traducción al francés pueden adquirirse en iso.org.

Existe una reciente edición puesta a libre disposición pública por "Industria Conectada 4.0" de la versión UNE-ISO/IEC 27001:2017 que es una edición consolidada de la traducción del 2013 y que incorpora las correcciones de 2015.

ISO/IEC 27002

Publicada desde el 1 de Julio de 2007, renombra la norma ya publicada ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 también está publicada en español por, entre otros, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondo norma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002) o Uruguay (UNIT-ISO/IEC 27002).

La última edición de 2013 este estándar fue actualizada reestructurando el contenido en un total de 14 Dominios, 35 Objetivos de Control y 114 Controles.

Puede descargarse una lista actualizada para la versión 2013 de todos los controles de esta norma en una práctica única página como mejor referencia.

Existe una reciente edición puesta a libre disposición pública por "Industria Conectada 4.0" de la versión UNE-ISO/IEC 27002:2017 que es una edición consolidada de la traducción del 2013 y que incorpora las correcciones de 2015.

ISO/IEC 27003

Publicada el 01 de febrero de 2010 y actualizada el 12 de Abril de 2017. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO/IEC 27004

Publicada el 15 de Diciembre de 2009 y revisada en Diciembre de 2016. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

ISO/IEC 27005

Publicada la tercera edición en Julio de 2018 con actualizaciones respecto a requisitos de norma ISO/IEC 27001:2013. La segunda edición es de 1 de Junio de 2011 y la primera edición del 15 de Junio de 2008. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000.

ANALISIS DE RIESGOS

La NORMA ISO 27005 puede proporcionar orientación para realizar análisis. Los riesgos de seguridad de la información contienen diferentes recomendaciones Y pautas, que especifican que debe estar en Diferentes etapas del proceso (identificación de activos, Requisitos legales y comerciales, tasación de activos, once Amenazas, vulnerabilidades y probabilidad de ocurrencia y análisis de riesgos y Tu valoración)

El término Amenaza puede entenderse como algún hecho que puede producir algún daño provocado por algún evento natural o antrópico, es decir originado por alguna actividad humana. Viéndolo desde un entorno informático, se puede considerar como cualquier elemento que comprometa al sistema. (Espinoza Zallas, E. A., & Rodríguez Pérez, R., 2017)

La posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza" (Instituto Nacional de Cibeseguridad de España, 2017)

EVALUACION DE RIESGOS

Cada organización debe determinar el proceso más adecuado y contar con una asistencia más directa en las directrices ISO / IEC 27005 e ISO 31000. Los auditores esperan un proceso estructurado y repetible, es decir, un procedimiento de evaluación de riesgos documentado que explique cómo identificar, analizar (por ejemplo, en función de las posibles consecuencias y la probabilidad de que ocurra) y evaluar (por ejemplo, mediante Aplicar criterios específicos al riesgo aceptado) y priorizar los riesgos asociados a los activos de información más relevantes del alcance (por ejemplo, considerando los niveles de riesgo definidos).

Se requiere que la organización lleve a cabo inspecciones y actualizaciones periódicas, y / o refleje los cambios sustanciales que enfrenta la organización, para reflejar los riesgos antes de que cambien, para mantener la atención preventiva y predictiva a las medidas de mitigación o control.

CONCLUSIONES

El personal del departamento técnico de la entidad pública debería de capacitarse sobre la gestión de riesgos para brindar mayor conocimiento sobre posibles amenazas y conciencia de las posibles consecuencias si no se tratan con su debido cuidado. Además, ayudará a mejorar el control interno de los servicios técnicos, aumentará la eficiencia de las actividades realizadas por los funcionarios públicos y hará que las personas tengan más confianza en la ciudadanía de los servicios que reciben. Garantizar la seguridad de la información se ha convertido en la máxima prioridad de empresas, organizaciones e instituciones.

Dentro de la empresa se puede ver falencias de vulnerabilidad dentro de dicho sistema, lo podemos mejorar con la implementación de seguridad y riesgo con la norma ISO/27005, para verificar dentro de la Unidad de tránsito, Se deben implementar buenas prácticas que permitan el establecimiento de medidas de gestión. Existen varias herramientas para proteger las funciones de seguridad de la información. Empresas privadas que apoyan los sistemas de gestión de seguridad de la información y optimizan los procesos.

Se tiene que tener en cuenta al responsable en base en la información obtenida de la investigación. El desarrollo de la empresa, podemos determinar si tienen conocimientos y están aplicando los estándares mencionados dentro de la investigación, la empresa aprobará los siguientes temas seguridad y aplicación de sistemas de gestión e información de clientes.

BIBLIOGRAFIA

1. Acissi. (2015). Seguridad Informática Hacking ÉTICO. Barcelona: ENI.
2. Cárdenas Solano , L. J., Martínez Ardila, H., & Becerra Ardila, L. E. (noviembre de 2016). Gestión de seguridad de la información. El profesional de la información, 25(6).
3. Carpentier, J.-F. (2016). La seguridad informática en la PYME - Situación actual y mejores prácticas. ENI. Recuperado el 10 de diciembre de 2016
4. Chicano Tejada, E. (2015). Auditoría de seguridad informática. IC Editorial.
5. Espinoza Zallas, E. A., & Rodríguez Pérez, R. (junio de 2017). Seguridad informática una problemática de las organizaciones en el sur de sonora. Revista de InvestigaciónAcadémica sin Frontera, 10(25). Obtenido de http://revistainvestigacionacademicasinfrontera.com
6. Espinoza, W. (2016). La tecnología de la información como herramienta construccionista para el auditor financiero hibrido. Fides Et Ratio, 11, 17-35.
7. Gil Vera, V. D., & Gil Vera, J. C. (02 de Junio de 2017). Seguridad informática organizacional. Scientia Et Technica, 22, 193-197. Obtenido de http://www.redalyc.org/pdf/849/84953103011.pdf
8. Gonzalez, D. (Febrero de 2018). Diseño de un plan estratégico de seguridad de la información, mediante la aplicación de análisis de riesgos con la norma ISO/IEC 27005. Caso de estudio INAMHI. INNOVA Research Journal, Vol. 3(No.2.1), 84-91. doi:https://doi.org/10.33890/innova.v3.n2.1.2018.672
9. Haufe, K.; Colomo, R.; Dzombeta, S.; Brandis, K. & Stantchev, W. (2016). Security Management Standards: A Mapping. Procedia Computer Science, 100, 755-761. DOI: http://dx.doi.org/10.1016/j.procs.2016.09.221
10. INEN ISO/IEC 27001. (2017). Tecnología de la Información-Técnicas de seguridad - Sistemas de gestión de la seguridad de la información- Requisitos.

11. Instituto Nacional de Cibeseguridad de España. (14 de febrero de 2017). INCIBE. Obtenido dehttps://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestio n_riesgos_0.pdf
12. Miranda Cairo, M., Valdés Puga, O., Pérez Mallea, I., Portelles Cobas, R., & Sánchez Zequeira, R. (abril de 2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. SciELO, vol.10(2). Obtenido de http://scielo.sld.cu/scielo.php?pid=S2227-18992016000200002&script=sci_arttext&tlng=en
13. Negrín, E., López, L., Rodriguez, K., & Martínez, D. (Diciembre de 2017). Propuesta de un programa de Auditoría a los Sistemas de Información. ECA Sinergia, 8(2), 13.
14. Urbina, G. B. (2016). Introducción a la seguridad informática. México: Grupo Editorial Patria.
15. Scalabrin, I. & Dinis, R. (2016). IT Governance mechanisms in higher education. Procedia Computer Science, 100, 941-946. DOI: https://doi.org/10.1016/j.procs.2016.09.253

RESUMEN

El actual documento presenta una metodología basada en la gestión de riesgos basada en analizar datos con respecto a la norma ISO/27005, Considere estas instrucciones “qué" se requiere En cuanto a la gestión de riesgos, no indicaron “cómo” se podría implementar la gestión. Ante el incremento de los riesgos tecnológicos, se ha desarrollado un método para riesgos tecnológicos

El uso de la tecnología de la información puede alcanzar puntos de ruptura o Por esta razón, tiene lagunas de seguridad en su uso. Una garantía y control de la infraestructura (nivel físico), Sistema de información (nivel lógico) y medidas organizativas (factor tecnología). la segunda parte, Métodos para integrar la metodología en la gestión de la continuidad del negocio. Como soporte para el análisis de impacto empresarial y la formulación de estrategias. Sobre procesos basados en tecnología.

Palabras Claves: ISO 27005, volumen de información, gestión de riesgos de seguridad, disponibilidad, Industria Conectada 4.0.

ABSTRACT

The current document presents a methodology based on risk management based on analyzing data with respect to ISO / 27005, Consider these instructions “what” is required Regarding risk management, they did not indicate “how” could be implemented Given the increase in technological risks, a method for technological risks has been developed

The use of information technology can reach breakpoints o for this reason, it has security loopholes in its use. A guarantee and control of the infrastructure (physical level), Information system (logical level) and organizational measures (technology factor). the second part, Methods to integrate the methodology in the management of business continuity. As support for business impact analysis and strategy formulation. On technology-based processes.

Keywords: ISO 27005, volume of information, security risk management, availability, Connected Industry 4.0.

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

Babahoyo, febrero 22 de 2021
D-FAFI-UTB-054-UT-2021

Abg.
Jorge Quinto Gutiérrez
DIRECTOR DE LA UNIDAD DE TRÁNSITO MUNICIPAL DEL CANTÓN PUEBLOVIEJO.
Pueblo viejo. -

De mis consideraciones:

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

El Señor **YÁNEZ FAJARDO ROMARIO ALDAIR**, con cédula de identidad No. 120650141-1, Estudiante de la Carrera de Ingeniería en Sistemas, matriculado en el proceso de titulación en el periodo Noviembre 2020 – Mayo 2021, trabajo de titulación modalidad Estudio de Caso para la obtención del grado académico profesional universitario de tercer nivel como **INGENIERO EN SISTEMAS.** El Estudio de Caso: **ANALISIS DE LOS SISTEMAS INFORMATICOS, APLICANDO LA NORMA ISO 27005 EN LA UNIDAD DE TRÁNSITO MUNICIPAL DEL CANTÓN PUEBLOVIEJO.**

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

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

Atentamente.

U.T.M. GAD. PUEBLOVIEJO

Lcdo. Eduardo Gabas Guijarro MAE
DECANO

c.c. Archivo

G.A.D. MUNICIPAL DE PUEBLOVIEJO
UNIDAD TECNICA MUNICIPAL DE CONTROL TRANSPORTE TERRESTRE TRANSITO Y SEGURIDAD VIAL - UTM. CSFP
FECHA 8-MARZO-2021
HORA 15:38
RECIBIDO