UNIVERSIDAD TECNICA 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 OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

NORMAS ISO DE SEGURIDAD DE LA INFORMACIÓN Y SUS UTILIDADES EN EL AREA DE TI

EGRESADO:

FAVIO EFREN CHISPON DAVILA

TUTOR:

ING. JOSE TEODORO MEJIA VITERI

AÑO 2022

Contenido

INTRODUCCION

El objetivo principal de este trabajo fue estudiar las normas ISO para la seguridad de la información y su utilidad en el área de TI, esto fue posible gracias a la aplicación de la norma ISO 27001 la cual permite la cobertura, seguridad de cálculo e integridad de los datos, así como los sistemas que la procesan dentro de las organizaciones; la información es un activo, como cualquier otro activo, esencial para las operaciones y los negocios de una organización y, por lo tanto, debe protegerse adecuadamente. El riesgo es una medida de la probabilidad de que una parte amenazada aproveche una vulnerabilidad y afecte con éxito un activo de información. La seguridad informática se ocupa de la protección de las infraestructuras TIC (Tecnologías de la Información y la Comunicación) tales como: redes, impresoras, computadoras, servidores, estaciones de trabajo; mientras que la seguridad de la información se enfoca en proteger los activos de información que son importantes para la organización, tales como: bases de datos, correos electrónicos, contratos, sitios web, documentos. La información puede considerarse segura cuando reúne las siguientes características: confidencialidad (la información no será conocida por personas, entidades o procesos no autorizados), integridad (la información será confiable), completa, inmutable), disponibilidad (la información será tomada cuando sea solicitado por una entidad autorizada), no repudio (garantiza que quien genera un evento no puede ser retirado válidamente, ya que se puede probar la ocurrencia de un evento y su origen).

Como se puede apreciar, la gestión de la seguridad de la información requiere una gestión integral de los procesos de recursos humanos, recursos tecnológicos, leyes y reglamentos en concordancia con los objetivos de la organización. El sistema que hace esto se conoce como Sistema de Gestión de Seguridad de la Información, conocido de forma abreviada como SGSI.

La norma ISO 27001 es una norma desarrollada como modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI para cualquier tipo de organización. Permite el diseño y la implementación de un SGSI, en función de las necesidades, los objetivos, los requisitos de seguridad, los procesos, el personal, el tamaño, los sistemas de soporte y la estructura de una organización.

DESARROLLO

El uso de tecnologías de procesamiento de información dentro de una organización, como computadoras poderosas junto con conexiones a Internet de alta velocidad, les permite convertirse en objetivos fáciles para entidades maliciosas que tienen como objetivo causar daños tales como: robar o destruir información, provocar caídas del sistema, denegación de servicio, entre otros. Ante esto y en la medida en que la tecnología actual puede vulnerar cualquier sistema sofisticado, es fundamental que la información esté protegida con el mayor nivel de seguridad posible. Para satisfacer esta necesidad, las empresas u organizaciones confían en el uso de herramientas, metodologías o estándares que soporten la gestión de la seguridad de TI. Estos mecanismos brindan mecanismos de seguridad, los cuales son esenciales para el correcto manejo de la información.

En el Ecuador existen organizaciones que procesan datos a través de sistemas de información y comunicación, muchas veces estas organizaciones no cuentan con un buen funcionamiento, ni la seguridad necesaria, ni su correcto uso, por lo que es necesario implementar una serie de mecanismos para mejorar su uso y disponibilidad. Con el objetivo de aprovechar estas falencias, se desarrollan nuevos métodos cada vez que existe un impacto en la seguridad de la información, es por ello que es necesario realizar el análisis de las amenazas antes mencionadas e identificar una amenaza adecuada. Un sistema de gestión de seguridad de la información ayuda para reducir los riesgos asociados con el acceso y uso de un determinado sistema de forma no autorizada y, a menudo, maliciosa, reduciendo así el porcentaje de riesgo.

El área de la tecnología de la información (TI) es de vital importancia para todo lo que hacemos hoy. Estas empresas deben cuidar la seguridad de sus sistemas y datos, y garantizar la eficiencia en la prestación del servicio y la satisfacción del cliente para protegerse frente a la competencia en un entorno competitivo de mercado en crecimiento. La seguridad es importante no solo a nivel tecnológico, sino en todos los niveles de la organización, desde el director general hasta el personal de limpieza. La implementación y certificación de estándares internacionales de sistemas de gestión de calidad es una excelente herramienta para que las organizaciones de TI manejen estos desafíos y aseguren a sus clientes que su información está a la mano.

La información es un recurso de vital importancia en las TI, por tal motivo se debe gestionar de manera eficiente la seguridad de la misma, sobre todo por las graves amenazas contra el sistema informático que ha aparecido en nuestro entorno. Que corre el riesgo de que esa información sea robada o que se use de manera inapropiada. Por ello, la investigación en seguridad basada en estas normas ISO contribuirá en gran medida al adecuado manejo y gestión de la información en TI, en el que algunas instituciones aún no cuentan con una metodología de gestión de la información. Cuando se trata de seguridad de la información, existen diferentes estándares aplicados en TI, ya que son los más apropiados para cumplir con el objetivo de crear una estructura de seguridad de la información en TI. En futuros proyectos, se podrá optar por el uso de Normas a efectos de implementar controles o realizar evaluación y tratamiento de riesgos. Los beneficios más importantes que obtendrán serán la integridad, confidencialidad y disponibilidad de la información. Además de su buena gestión, esto supondrá un sinfín de ventajas para las instalaciones ya que una adecuada y eficiente administración se traduce en una mayor eficiencia de los procesos que tienen lugar en la organización. Por lo expuesto anteriormente se justifica el desarrollo del presente proyecto, el mismo que de ser aplicado brindará un aporte de suma importancia en las TI.

Seguridad de la información

Definición: La seguridad de la información es el conjunto de precauciones y respuestas por parte de las organizaciones y los sistemas tecnológicos para proteger la información buscando la confidencialidad, disponibilidad e integridad de la información. Así, los tres pilares básicos de la seguridad de la información son:

Confidencialidad: La información no debe ser proporcionada o divulgada a personas, entidades o procesos no autorizados.

Integridad: mantener la exactitud e integridad de la información y la forma en que se procesa.

Disponibilidad: El derecho a acceder y utilizar información y sistemas de procesamiento de información por parte de personas, organizaciones o procesos autorizados según sea necesario.

La seguridad es un concepto que trata de la certeza, la ausencia de riesgo o la redundancia. Se entiende por confidencialidad el estado de cualquier sistema o tipo de información (informatizada o no) que indique que dicho sistema o información está libre de peligro, daño o riesgo. Peligro o daño significa cualquier cosa que pueda afectar su funcionamiento directo o los resultados obtenidos. (ISOTools, 2018)

Riesgos

En la gestión de riesgos, existe un elemento de incertidumbre con respecto a la probabilidad de amenazas. En otras palabras, la amenaza solo se puede predecir dentro de ciertos límites. Un evento adverso tiene tres componentes: amenaza, vulnerabilidad e impacto. Las vulnerabilidades indican la debilidad de los activos que pueden ser explotados por una amenaza. Estos riesgos se contrarrestan con la implantación de políticas, es decir medidas que se deben llevar a cabo para cumplir con dicho objetivo. (Guevara, 2017)

Tipos de seguridad.

Activa: Este es un conjunto de medidas tomadas para minimizar el impacto de un incidente de seguridad y permitir que el sistema se recupere. Estas medidas también se conocen como "correcciones".

Pasiva: Son los mecanismos y procedimientos que ayudan a prevenir y detectar amenazas a la seguridad de los sistemas de información.

La seguridad activa y la seguridad pasiva se aplican a los elementos físicos y lógicos que integran los sistemas de información. (Prosegur, (s.f))

NORMAS ISO DE LA SEGURIDAD DE INFORMACION

Definición

ISO (Organización Internacional para la Estandarización) es una red global que define los estándares internacionales requeridos por las empresas, el gobierno y la sociedad; desarrollarlos junto con los campos que los utilizarán; aplicarlos a través de procedimientos transparentes basados en aportes nacionales de múltiples partes interesadas; y hacerlos disponibles para su uso en todo el mundo. Las normas ISO se basan en un consenso internacional extraído de la base más amplia de grupos de partes interesadas. Los aportes de expertos provienen de quienes están más cerca de las necesidades estándar y los resultados de su implementación. (Que son las normas Iso, 2020)

NORMAS ISO 27000

La serie de normas ISO/IEC 27000 se titula "Requisitos para la especificación de sistemas de gestión de seguridad de la información (SGSI)". Proporciona un marco de estándares para la seguridad de la información aplicable dentro de una organización o negocio e incluye un conjunto de estándares sobre los siguientes temas. (Guevara, 2017)

- ✓ Sistema de gestión de seguridad de la información.

- ✓ Valoración de riesgos.
- ✓ Controles.

ISO 27001

El estándar 27001 incluye un conjunto de estándares relacionados con la seguridad informática. Según esta norma, norma principal de esta serie de normas, la seguridad de la información es el mantenimiento de la confidencialidad, integridad y disponibilidad, así como de los sistemas que intervienen en su tratamiento. El modelo de sistema de gestión de seguridad de la información ISO 27001 sigue una estructura PHVA (planificar - hacer - verificar). El proceso comienza con la planificación del alcance del SGSI, definiendo las áreas o procesos organizacionales a los que se aplicará el sistema. En general, se seleccionan las áreas más importantes o vulnerables en términos de gestión de la información. Una vez definido el alcance, se debe desarrollar y publicar una política de gestión de la seguridad de la información, que establezca los lineamientos generales que la organización debe tener en cuenta al momento de enfrentar el riesgo de la información, teniendo en cuenta aspectos legales, contractuales y específicos de la empresa. El eje central de la planificación del SGSI es la identificación de los riesgos de la información, relacionados con las posibles amenazas y vulnerabilidades de la organización en términos de seguridad, confiabilidad y disponibilidad de la información. Con base en la identificación de estos riesgos, se determinará un análisis y planes para evaluar, controlar o tratar los riesgos. También incluye la documentación y aplicación de los procedimientos necesarios para aplicar estos controles, así como la capacitación y concientización de los empleados sobre la seguridad de la información y los controles que deben tener en su uso. La verificación incluye medir el desempeño del SGSI, evaluar los riesgos y la eficacia de los controles establecidos, realizar una revisión interna del sistema y abordarla por parte de la gerencia. (ISOTools, 2017)

ISO 27002

La Norma ISO/IEC 27002 hace mejores prácticas de gestión de seguridad de la información y proporciona recomendaciones para cualquier persona interesada y responsable de iniciar, implementar o mantener sistemas de seguridad de la información y gestión de seguridad de la información. La seguridad de la información se define en la norma como "mantener la confidencialidad (garantiza que solo las personas autorizadas puedan acceder a la información), la integridad (garantiza que la información y su justificación sean correctas y completas) y la disponibilidad (garantiza que los usuarios autorizados tengan acceso a la información y sus activos asociados cuando sea necesario)". La versión 2013 del estándar describe las siguientes catorce áreas clave y métricas que se deben cumplir para una implementación adecuada:

Políticas de seguridad: Sobre principios y políticas de seguridad de la información. Revisa la política de privacidad de la información. (Google, 2021)

Organización de seguridad de la información: Se ocupa de problemas organizativos internos: asignación de responsabilidades relacionadas con la seguridad de la información, división de funciones, contacto con autoridades, contacto con grupos de interés especial segregación y confidencialidad de la información en la gestión del proyecto. (ISO 27001, (s.f))

Seguridad de los recursos humanos: Incluye aspectos a considerar antes, durante y al parar o cambiar de trabajo. Antes de contratar, es recomendable investigar los antecedentes del candidato y revisar los términos y condiciones del contrato. En la licitación, es necesario abordar los temas de responsabilidad de gestión, conciencia de seguridad de la información, educación y capacitación. En caso de despidos o cambios de trabajo, también se deben tomar medidas de seguridad, como deshabilitar o actualizar privilegios o derechos de acceso. (ISOTools, 2017)

Gestión de los activos: Responsabilidad patrimonial (inventario, uso aceptable, propiedad y devolución de bienes), clasificación de la información (instrucción, etiquetado y manipulación, disposición) y gestión de medios de almacenamiento (gestión de manipulación de vehículos muebles, desechados y en tránsito). (Cuevara, 2017)

Control de accesos: Aborda los requisitos de la organización para el control de acceso, la gestión de acceso de usuarios, la responsabilidad de los usuarios y el control de acceso a sistemas y aplicaciones. (Escuela Europea, 2019)

Cifrado: Describe controles como la política de uso de cifrado y los controles de administración de claves. (Kaspersky, (s.f))

Seguridad física y ambiental: Incluye el establecimiento de Zonas Seguras (Perímetro de Seguridad Física , Control de Entrada Física, Oficina, Coordinación de Seguridad y Recursos, Protección contra Amenazas Externas y ambientales), Trabajo en Zonas Seguras y área de acceso público) y seguridad de equipos (ubicación y protección de equipos, instalaciones de aprovisionamiento, seguridad de cableado, mantenimiento de equipos, eliminación de activos periféricos, dispositivos seguros y activos periféricos, reutilización o eliminación de dispositivos de almacenamiento, dispositivos y estaciones de trabajo de usuarios desatendidos y pantallas de bloqueo). (ISO 27001, (s.f))

Seguridad en las operaciones: Procedimientos y responsabilidades; Protección de malware; sostener; registros y seguimiento de actividades; control de software operativo; gestión de vulnerabilidades técnicas; coordinar las auditorías de los sistemas de información.

Seguridad de las telecomunicaciones: Gestión de la seguridad de la red; gestión de transferencia de información.

Adquisición de Sistemas, Desarrollo y Mantenimiento: Requisitos de seguridad del sistema de información; seguridad en los procesos de desarrollo y soporte; datos de prueba.

Relaciones con los proveedores: Confidencialidad de la información en las relaciones con los proveedores; gestionar la prestación de servicios de los proveedores de servicios.

Gestión de sucesos que afectan a la seguridad de la información: Gestión de incidentes que afectan a la seguridad de la información; mejoras

Aspectos de seguridad de la información para la administración de la continuidad del negocio: Continuidad de la seguridad de la información.

Cumplimiento: Cumplimiento de requisitos legales y contractuales; evaluación de la seguridad de la información.

A quien va dirigida la norma: La norma ISO 27002 puede ser utilizada por cualquier tipo de organización o empresa, privada o pública. Si la organización utiliza sistemas internos o externos que contienen información confidencial, depende de esos sistemas para el funcionamiento normal de las operaciones o simplemente desea verificar el nivel de seguridad de sus operaciones. Proteja su información siguiendo el estándar reconocido, ISO Standard 27002 es un marco de metodología de confianza. (Consuelo de la Torre, (s.f))

ISO 27003

La norma internacional ISO 27003 establece lineamientos para la implementación de un Sistema de Gestión de Seguridad de la Información. Este estándar puede ser aceptado por aquellos que deseen establecer un SGSI y por consultores en su trabajo de rutina, porque proporciona una solución o una respuesta a algunos de los aspectos faltantes del SGSI. La norma ISO 27003 demuestra su preocupación por los elementos necesarios para un buen diseño e implementación del SGSI, que la ISO 27001 incluye la definición del procedimiento de dimensionamiento del SGSI, así como su implementación Mostrar y diseñar diferentes layouts. Establece un proceso para obtener el consentimiento para la implementación de un SGSI, describe un cronograma para su implementación, definido en la norma ISO27003, y

proporciona una serie de instrucciones para hacer todo esto. (ISO/IEC 27003 – Guía para la implementación de un Sistema de Gestión de Seguridad de la Información., 2014)

El contenido del estándar es el siguiente:

- ✓ Impacto
- ✓ Reseñas normativas
- ✓ Definiciones y términos
- ✓ Parametrización del estándar
- ✓ Acuerdo de la alta dirección alcanzado para iniciar el SGSI.
- ✓ Describa el alcance, la política y las limitaciones del SGSI.
- ✓ Evaluar los requisitos de seguridad de la información.
- ✓ Diseño de la SGSI.

ISO 27004

El estándar ISO27004 permite muchas de las mejores prácticas para medir los resultados de los Sistemas de Gestión de Seguridad de la Información (SGSI) en ISO 27001. Este estándar especifica cómo se debe estructurar el sistema de medición, la información, qué números medir, cuándo y cómo medir ellos. Además, ayuda a las empresas a establecer objetivos relacionados con el desempeño y criterios de éxito. El tipo de métodos requeridos por la norma ISO 27004 dependerá de la complejidad, el tamaño de la organización, la relación costo-beneficio y el grado de integración de la seguridad de la información implementada en los procedimientos llevados a cabo por la organización. Esta norma internacional especifica cómo deben constituirse estos métodos y cómo deben integrarse y documentarse los datos obtenidos en el SGSI. Para medir o evaluar la efectividad de la seguridad de la información, los pasos sugeridos por ISO27004 son:

Selección de objetivos y procesos de medición: La organización necesita medir la gama de métodos. En la medición, solo se tienen en cuenta los procesos documentados sistemáticamente. La realización de procedimientos o controles y las acciones de los empleados es uno de los objetos de medición.

Descripción de líneas clave: Los valores clave que exponen puntos de referencia deben definirse para cada objeto medido.

Selección de datos: Los datos deben ser precisos, oportunos y dimensionales. Las técnicas de recopilación de datos programados se pueden aplicar para la recopilación y la presentación de informes estandarizados.

Desarrollo de un sistema de medición: Una secuencia lógica de actividades según ISO2700 aplicada a varias propiedades del objeto seleccionado para la medición. Los indicadores se utilizan como fuente de datos para mejorar el desempeño de los programas relacionados con la seguridad de la información.

Interpretación de los valores medidos: La desviación entre el valor original y el valor real medido se determinará utilizando tecnología y procedimientos apropiados para la interpretación y análisis de los valores antes mencionados.

Aviso de valores medidos: Los datos obtenidos de la medición deben ser comunicados a los interesados. Esto se puede hacer con los paneles de operación, informes, boletines o formularios gráficos. (Evaluación de la Seguridad de la Información, (s.f))

ISO 27005

ISO 27005 es el estándar internacional para la gestión de riesgos de seguridad de la información. Esta norma internacional brinda orientación sobre la gestión de riesgos, con base en los requisitos relevantes definidos en ISO 27001. Esta norma es aplicable a todo tipo de

organizaciones. Las decisiones de gestión de riesgos pueden complicar la seguridad de la información de su organización y reemplazar las normas ISO/IEC TR 13335-3: 1998 e ISO/IEC TR 13335-4: 2000 sobre gestión de la información y seguridad de la tecnología de las comunicaciones. ISO 27005 no recomienda una metodología específica, ya que dependerá de una variedad de factores relevantes para cada empresa que planee implementarla, tales como: el alcance práctico del sistema de gestión, la seguridad de la información (SGSI) o su área comercial de la propia industria. Sin embargo, al igual que otras normas ISO y sistemas basados en procesos, un método que se considera válido y por lo tanto recomendado es utilizar el modelo PHVA como base para establecer procesos de gestión enfocados a la mejora continua de acuerdo al siguiente esquema:

Planificar: Los objetivos, procesos y procedimientos del proceso de gestión de riesgos tecnológicos se establecen para lograr resultados que sean consistentes con las políticas y objetivos generales de la organización.

Hacer: Corresponde a la implementación y operación de controles, procesos y procedimientos e incluye la operación e implementación de las políticas definidas.

Verificar: Evaluar y medir el rendimiento del proceso frente a la política y los objetivos de seguridad, e informar los resultados.

Actuar: Incluye establecer una política de gestión de riesgos tecnológicos e implementar los cambios necesarios para mejorar los procesos. (La gestión de la seguridad de la información, 2015)

ISO 27006

ISO 27006 se titula oficialmente “Tecnología de la información. Requisitos de Ingeniería de Seguridad para Organismos de Auditoría y Certificación de Sistemas de Información de Gestión de Seguridad”, consta de 10 capítulos y anexos. La norma ISO 27006 brinda

orientación a los organismos de certificación sobre los procesos formales que deben seguirse durante las auditorías del SGSI. Los procedimientos descritos en esta norma aseguran la validez de los certificados emitidos de acuerdo con la norma ISO 27001. ISO 27006 está destinado a respaldar la acreditación de organismos de certificación que brindan certificación de sistemas de gestión de seguridad de la información. Es responsable de definir los requisitos y proporcionar orientación para la evaluación y certificación del sistema. Cualquier organización que tenga la certificación ISO27001 también debe cumplir con los requisitos de la norma ISO 27006. El proceso de certificación implica auditar el SGSI para el cumplimiento de la norma ISO 27001. El evaluador de la certificación solo tiene una preocupación pasajera con los controles reales de seguridad de la información administrados por el sistema de gestión. Cualquier empresa con una queja de SGSI debe gestionar sus riesgos de seguridad de la información con cuidado. (ISO/IEC 27006 guía para la certificación del SGSI, 2014)

Los requisitos generales que trata son:

- ✓ Directrices específicas de la SGSI sobre la equidad.
- ✓ Lista de trabajos potencialmente conflictivos.
- ✓ Incluye un listado de todas las actividades que se pueden realizar al aire libre.

ISO 27007

Este estándar proporciona orientación para los organismos de certificación acreditados, auditores internos, SGSI externos/auditores de terceros y otros involucrados en las auditorías ISO/IEC 27001 (es decir, auditorías) calificación del sistema de gestión para el cumplimiento del estándar). ISO/IEC 27007 y gran parte de la reflexión se refiere a la norma ISO 19011, sistema de evaluación de la calidad y gestión ambiental ISO "sistema de gestión", que es, por supuesto, el elemento común que unifica las normas ISO27k. Proporcionar orientación adicional específica para la CMSI. ISO / IEC 27007 también se basa en los requisitos de

evaluación de conformidad de ISO 17021 para organizaciones que brindan servicios de auditoría y certificación de sistemas de gestión y, de acuerdo con ISO / IEC 27006, la acreditación de organismos de certificación de SGSI. (ISO 27007, 2017)

Estructura: El estándar cubre aspectos específicos del SGSI de la auditoría de cumplimiento:

Administrar el programa de auditoría del SGSI (determinar qué necesita ser auditado, cuándo y cómo; designar a los auditores apropiados; evaluación, mantenimiento de registros de evaluación, mejora continua del proceso);

Llevar a cabo una auditoría ISMS SMS (planificar el proceso de auditoría, realizar actividades clave de auditoría, incluida la investigación de campo, el análisis, la presentación de informes y el control);

Gestión del auditor del SGSI (habilidades, competencias, atributos, evaluaciones).

METODOLOGIA

En este proyecto se usó la metodología cualitativa ya que esta nos da un criterio y razonamiento que puede ser capaz de determinar o definir el proceso del trabajo utilizado en la empresa, también se aplicó la metodología cuantitativa porque es la que se basa en modelos matemáticos estadísticos lo cual permite la optimización de la investigación.

Técnica e instrumento de recolección de información a usarse en el estudio de caso es la siguiente:

- La técnica de encuesta es la que permitió recoger información involucrada en la investigación de este caso de estudio. La encuesta fue realizada a los ingenieros y directores del área de Tecnologías de información.

- Método de trabajo de campo con esta técnica se analizan los resultados y la expectativa de la empresa, para de esta forma definir a los entandares ISO como una herramienta necesaria dentro del área de TI.

Propuesta de Solución

Este proyecto plantea la utilidad de las normas ISO, que, a través de una planificación estructurada, servirán como un plan de acción para mejorar la seguridad, con el fin de alcanzar un alto nivel de eficiencia en las operaciones para preservar y proteger la información. Existen varias metodologías y estándares para gestionar la seguridad de la información entre ellos podemos mencionar los principales ISO, ITIL y COBIT entre otros. Estás normas y estándares hay que adaptarlos al contexto particular de las empresas. Las Normas ISO 27001-2013 especifican los requisitos para la implantación del SGSI (Sistemas de Gestión de la Seguridad de la Información). Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos, existen otras normas complementarias como ISO 27002-2013 que especifica los Dominios, Objetivos de Control y Controles que se deben implementar para mejora del SGSI y la Norma ISO 27005 que surgió en el 2009, proporciona directrices para la gestión del riesgo en la seguridad de la información, dando soporte a los SGSI. (Mejía et al, 2016, pág. 225)

Acontinuación se propone realizar los siguientes procesos:

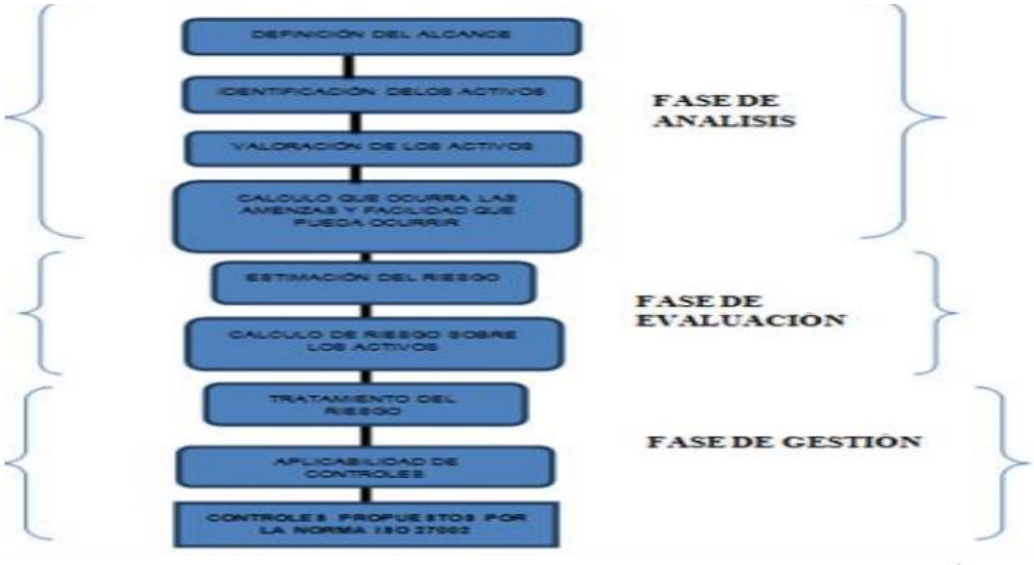


Figura 1-Metodologia de análisis de riesgo

CONCLUSIONES

La norma ISO 27001 es una poderosa herramienta para gestionar un sistema de gestión de seguridad de la información en cualquier organización, por medio de su uso se puede mejorar continuamente la confidencialidad, integridad y disponibilidad.

Las normas ISO son el estándar de calidad a nivel mundial que permiten a las organizaciones estandarizar y mejorar sus procesos, operaciones y acreditación, hoy en día es de vital importancia para la supervivencia de un negocio en un mundo globalizado.

Las Normas ISO buscan mejorar la integridad, confidencialidad y la disponibilidad de los recursos de la infraestructura tecnológica por lo que esto se puede traducir en un aumento en el presupuesto para la implementación de soluciones que ayuden a mejorar estos indicadores pero son compensados con la mejora en la seguridad integral de la infraestructura.

Bibliografía

Consuelo de la Torre, M. d. ((s.f)). Planteamientos Básicos para la implementacion de las normas Iso 27001 e Iso 27002. *ciberseguridad*, 18-21.

Cuevara, A. (11 de 2017). Gestion de activos. *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*, 54. Obtenido de Gestion de activos: https://repositorio.uta.edu.ec/jspui/bitstream/123456789/26932/1/Tesis_t1339si.pdf

Escuela Europea. (5 de 09 de 2019). Obtenido de Gestionar controles de acceso: https://www.escuelaeuropeaexcelencia.com/2019/09/como-gestionar-los-controles-de-acceso-segun-iso-27001/

Evaluación de la Seguridad de la Información. ((s.f)). Obtenido de ISO TOOLS EXCELLENCE: https://www.isotools.cl/isoiec-27004/

Google. (14 de 04 de 2021). Obtenido de La política de seguridad: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

Guevara, A. (2017). Seguridad de la informacion. *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*, 7.

ISO 27001. ((s.f)). Obtenido de ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: https://normaiso27001.es/a6-organizacion-de-la-seguridad-de-la-informacion/

ISO 27001. ((s.f)). Obtenido de Seguridad fisica y del entorno: https://normaiso27001.es/a11-seguridad-fisica-y-del-entorno/

ISO 27007. (11 de 2017). Obtenido de Seguridad de la informacion: https://www.pmg-ssi.com/2017/11/iso-27007-auditores-seguridad-informacion/

ISO/IEC 27003 – Guía para la implementación de un Sistema de Gestión de Seguridad de la Información. (17 de 01 de 2014). Obtenido de Seguridad de la informacion blog especializado en seguridad de la informacion y ciberseguridad: https://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

ISO/IEC 27006 guía para la certificación del SGSI. (7 de 02 de 2014). Obtenido de Seguridad de informacion: https://www.pmg-ssi.com/2014/02/isoiec-27006-guia-para-la-certificacion-del-sgsi/

ISOTools. (17 de 07 de 2017). Obtenido de Seguridad de la informacion: https://www.pmg-ssi.com/2017/08/seguridad-de-la-informacion-recursos-humanos/

ISOTools. (20 de 04 de 2017). Obtenido de Seguridad de la informacion Blog especializado en seguridad de informacion y ciberseguridad: https://www.pmg-ssi.com/2017/04/dominios-iso-27001-2013/

ISOTools. (1 de 02 de 2018). Obtenido de Seguridad de la informacion, blog especializado en seguridad de la informacion y ciberseguridad: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Kaspersky. ((s.f)). Obtenido de Cifrado: https://latam.kaspersky.com/resource-center/definitions/encryption

La gestión de la seguridad de la información. (10 de 2015). Obtenido de Cómo implantar eficazmente la norma ISO 27005: https://www.isotools.org/2015/10/05/como-implantar-eficazmente-la-norma-iso-27005/#:%7E:text=La%20norma%20ISO%2027005%20es,definidos%20en%20la%20ISO%2027001

Mejía Viteri, J. T., Campi Mayorga, J. A., Campi Mayorga, I. I., España León, A. R., & Gonzáles Valero, M. I. (2016). Análisis y Evaluación del Riesgo de la Información. *UNIANDES EPISTEME*, 225.

Prosegur. ((s.f)). Obtenido de Seguridad pasiva y activa: https://blog.prosegur.es/diferencia-entre-seguridad-pasiva-y-activa/

Que son las normas Iso. (5 de 03 de 2020). Obtenido de GlobalSuite Solutions: https://www.globalsuitesolutions.com/es/que-son-normas-iso/

ANEXOS

Diseño de formulario de la encuesta realizada

Relacionado con: NORMAS ISO DE SEGURIDAD DE LA INFORMACIÓN Y SUS UTILIDADES EN EL AREA DE TI

Responda las siguientes preguntas según su experiencia y conocimientos.

¿Tiene conocimiento de los estándares ISO?

¿Existen políticas de privacidad basado en normas ISO para el manejo de la información?

¿Qué normas aplica en la institución?

☐ Normas internas de una empresa

☐ Normas ISO

¿Qué tipo de normas ISO aplica?

☐ ISO 27001

☐ ISO 27002

☐ ISO 27003

☐ ISO 27004

☐ ISO 27005

☐ ISO 27006

☐ ISO 27007

☐ Otro

¿La identificación, protección, almacenamiento, recuperación y manejo de registros están protegidos por una metodología adecuada?

¿Quién es responsable de instalar y mantener el software de seguridad en los equipos?

☐ Empleados

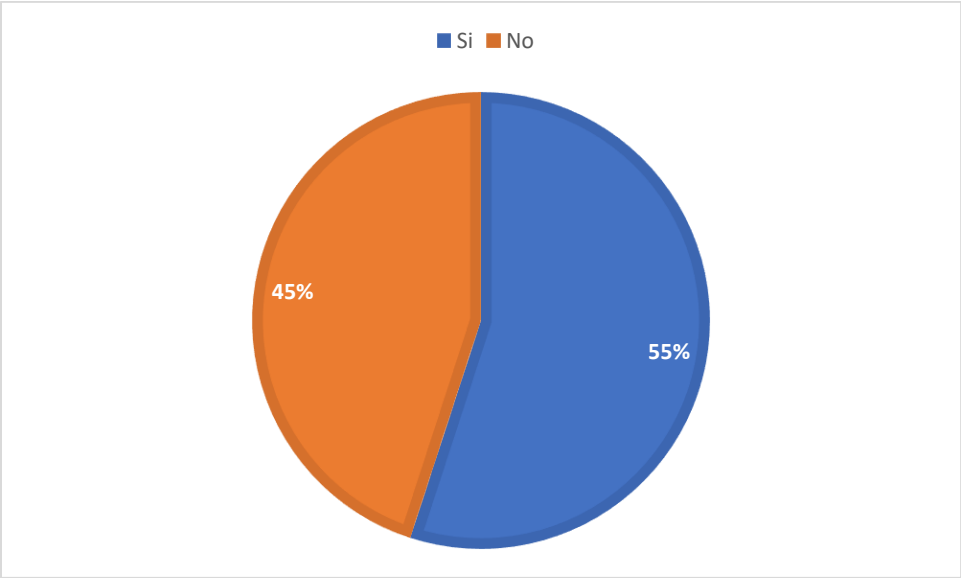
☐ Administrador

☐ Personal de TI

RESULTADOS

Relacionado con: NORMAS ISO DE SEGURIDAD DE LA INFORMACIÓN Y SUS UTILIDADES EN EL AREA DE TI

1. ¿Tiene conocimiento de los estándares ISO?

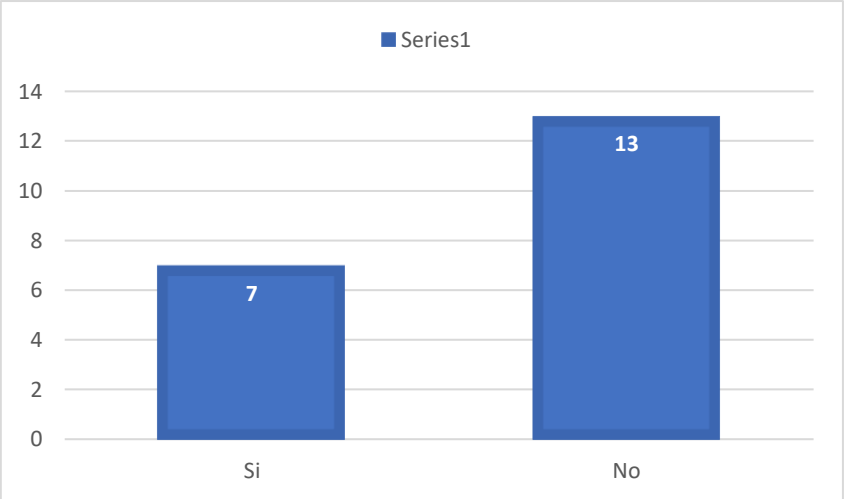


Alternativa	Frecuencia	%
Si	11	55%
No	9	45%

TOTAL	20	100%

Con el resultado obtenido se denota en la pregunta 1 que el 55% dijo que si tienen conocimiento de estos estándares y un 45% no conocen. Dado los resultados nos podemos percatar que si tienen conocimiento acerca de las normas ISO de seguridad de información en TI.

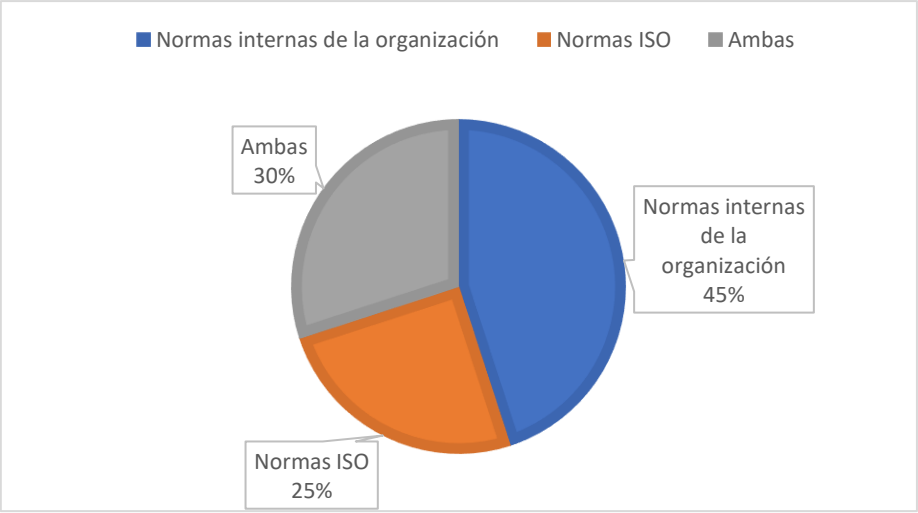
2. ¿Existen políticas de privacidad basado en normas ISO para el manejo de la información?



Alternativa	Frecuencia	%
Si	7	35%
No	13	65%
TOTAL	20	100%

Analizando este resultado vemos que un 35% que si aplican políticas de privacidad basado en normas ISO y un 65% no aplican.

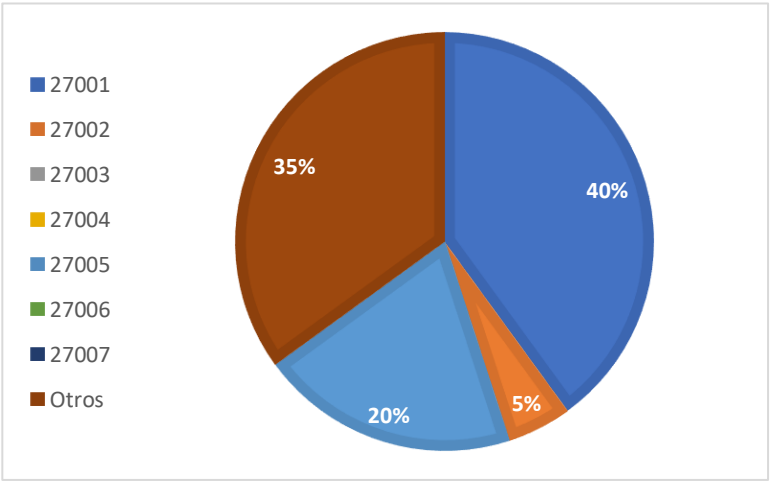
3. ¿Qué normas aplica en la institución?



Alternativa	Frecuencia	%
Normas internas de la organización	9	45%
Normas ISO	5	25%
Ambas	6	30%
TOTAL	20	100%

El resultado demostró que un 45% aplican políticas internas de la organización, el 25% aplican políticas basado en normas ISO y finalmente el 30% aplican ambas normas tanto ISO como normas internas.

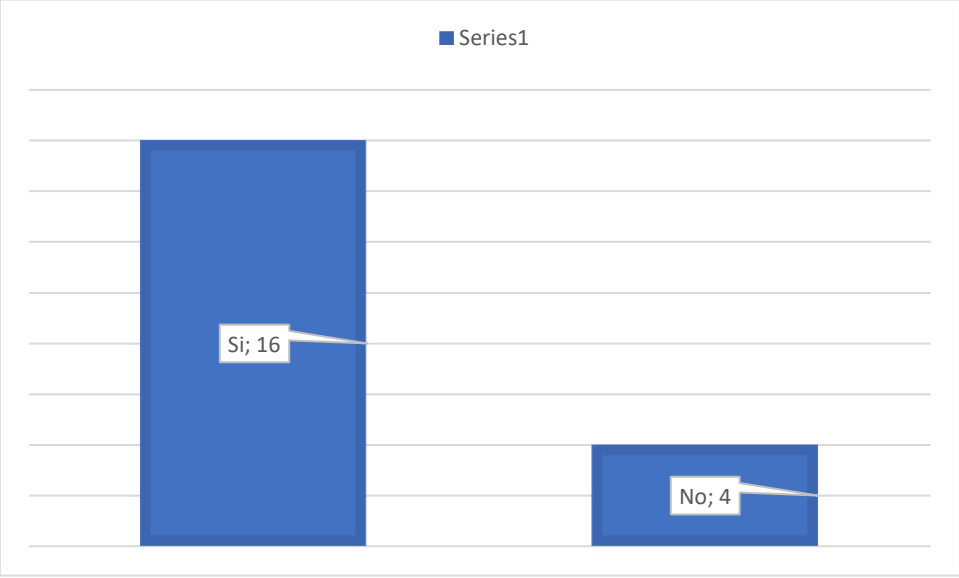
4. ¿Qué tipo de normas ISO aplica?



Alternativa	Frecuencia	%
27001	8	40%
27002	1	5%
27003	0	0
27004	0	0
27005	4	20%
27006	0	0
27007	0	0
Otros	7	35%
TOTAL	20	100%

Según los datos obtenidos en esta pregunta, el 40% aplica la norma 27001, el 35% aplica otro tipo de normas, el 20% aplica la norma 27005 y el 5% aplica la norma 27002.

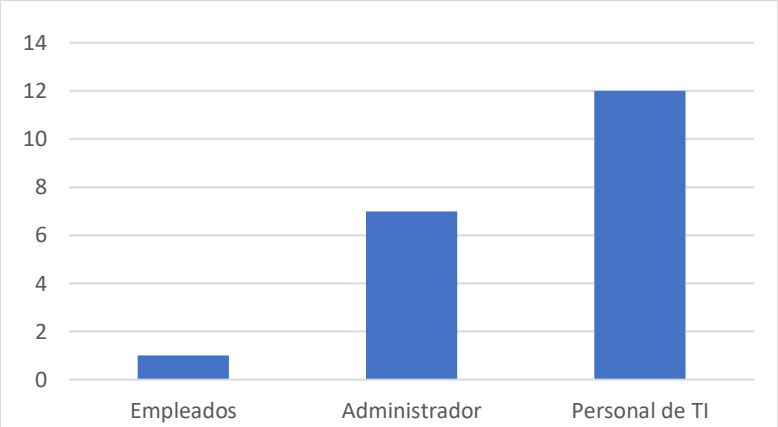
5. ¿La identificación, protección, almacenamiento, recuperación y manejo de registros están protegidos por una metodología adecuada?



Alternativa	Frecuencia	%
Si	16	80%
No	4	20%
TOTAL	20	100%

Con el resultado obtenido nos indica que un 80% que si usan metodología para mantener la información y un 20% no aplican metodologías.

6. ¿Quién es responsable de instalar y mantener el software de seguridad en los equipos?



Alternativa	Frecuencia	%
Empleados	1	5%
Administrador	7	35%
Personal de TI	12	60%
TOTAL	20	100%

En esta pregunta nos refleja como resultado los responsables de mantener la seguridad en los equipos un 60% al personal de TI, un 35% al administrador y finalmente el 5% a los empleados.

Luego de obtener estos resultados, las Normas ISO han sido de gran utilidad para las empresas u organizaciones ya que han manifestado la mejoría de los resultados de las empresas que brindan un mejor rendimiento de las actividades para gestionar de manera correcta la seguridad de la información, por otra parte, la mayoría de las empresas no cuentan con conocimientos precisos para el uso adecuado de gestionar la seguridad de información.