“ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO”

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

CARRERA DE SOFTWARE

SOFTWARE DE TIEMPO REAL

Estudiante:

John Cuvi

Código: 6680

Semestre: Séptimo Semestre

Docente: Ing. Jaime Camacho

Actividad: Normas ISO 27000 SGSI

Riobamba – Ecuador

13/10/2022

OBJETIVOS

- Realizar una investigación sobre las Normas ISO 27000 que permita complementar la información vista durante las clases.

INTRODUCCIÓN

A medida que la sociedad continúa desarrollándose automatizando todos los procesos, diseña mecanismos para proteger los datos o información que la sociedad no debería conocer y ser protegidos. Para proteger estos datos, se vio obligado a desarrollar diversas reglas, mecanismos y elementos que lo ayudaran a proteger esta información. Desde la llegada de la tecnología en el siglo pasado, en los años 80 y 90, la sociedad se ha visto inundada por el constante desarrollo de los sistemas de seguridad informática, donde se han descubierto nuevas formas de almacenar la información, pero cuanto más se desarrolla la tecnología, más vulnerable se vuelve.

En general, la seguridad de los datos se refiere a las protecciones de privacidad digital utilizadas para evitar el acceso no autorizado a los datos que pueden residir en computadoras, servidores, bases de datos, sitios web, etc. La seguridad de datos también protege los datos de posibles daños.

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

En concreto la familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad que proporciona un marco para la gestión de la seguridad.

DESARROLLO

Normas ISO 27000

Es un conjunto de estándares denominada familia ISO/IEC 27000 que reúne prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

ISO	Criterio	Característica
ISO 27001	Esta norma nos proporciona requisitos para el establecimiento, implantación, mantenimiento y mejora continua de un SGSI. El proceso de mejora continua se basa en el conocido Ciclo Deming o PDCA.	Posee 4 Fases 1. Planificar 2. Hacer 3. Verificar 4. Actuar
ISO 27002	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información haciendo que su aplicación sea lo más exacto posible.	1. Contiene 39 objetivos de control. 2. Contiene 113 controles. 3. Agrupados en 11 dominios.
ISO 27003	Es una guía que nos brinda una ayuda en la implementación de un **SGSI**. Sirve como apoyo a la norma 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI. Además nos incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.	Tiene 5 fases 1. Obtener la aprobación gerencial para iniciar un proyecto SGSI. 2. Definir el alcance del SGSI y la política del SGSI. 3. Realizar un análisis de la organización. 4. Valorar los requisitos de seguridad para la información. 5. Riesgo y planificar el tratamiento del riesgo. 6. Diseñar el SGSI.

ISO 27004	En este estándar se nos especifican las técnicas de medida y las métricas que son aplicables a la determinación de la eficacia de un Sistema de Gestión de Seguridad de la Información y los controles relacionados.	Tiene 6 etapas 1. Elegir los objetivos y procesos de medición. 2. Describir las líneas principales. 3. Elegir los datos. 4. Desarrollo del sistema de medición. 5. Interpretar los valores medidos. 6. Notificar dichos valores.
ISO 27005	Esta normativa establece las diferentes directrices para la gestión de los Riesgos en la Seguridad de la Información. Se trata de una norma de apoyo a los conceptos generales que vienen especificados en la ISO 27001 y se encuentra diseñada para ayudar a aplicar, de una forma satisfactoria, la seguridad de la información basada en un enfoque de gestión de riesgos.	Tiene 14 Secciones 1. Prefacio. 2. Introducción. 3. Referencias normativas. 4. Términos y definiciones. 5. Estructura. 6. Fondo. 7. Descripción del proceso de ISRM. 8. Establecimiento Contexto. 9. Información sobre la evaluación de riesgos de seguridad (ISRA). 10. Tratamiento de Riesgos Seguridad de la Información. 11. Admisión de Riesgos Seguridad de la información. 12. Comunicación de riesgos de seguridad de información. 13. Información de seguridad Seguimiento de Riesgos y Revisión. 14. Anexos
ISO 27006	Esta norma específica requisitos para la certificación de SGSI y es usada en	Contiene 5 Requisitos 1. Monitoreo, medición, análisis y

	conjunto con la norma 17021-1, la norma genérica de acreditación.	evaluación del SGSI, 2. Seguridad de información, 3. Sistemas de gestión, 4. Principios de auditoría, y 5. Conocimiento técnico de los sistemas a auditar.
ISO 27007	Es un manual de auditoría de un Sistema de Gestión de Seguridad de la Información. Incluso nos proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).	3 aspectos específicos 1. Administración del programa de auditoría del Sistema de Gestión de Seguridad de la Información. 2. Realización de una auditoría 3. Gestión de auditores del Sistema de Gestión de Seguridad de la Información
ISO 27032	Es un texto relativo a la ciber-seguridad. Se trata de un estándar que garantiza directrices de seguridad que desde la organización ISO han asegurado que "proporcionará una colaboración general entre las múltiples partes interesadas para reducir riesgos en Internet". Más concretamente, ISO/IEC 27032 proporciona un marco seguro para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos.	4 puntos estratégicos más importantes 1. La Seguridad en la Redes 2. Seguridad en Internet 3. Seguridad de la información 4. la Seguridad de las Aplicaciones

CONCLUCIONES

- La seguridad de la información que uno de los puntos mas fundamentales en la actualidad y con el avance de la tecnología por lo que tomar medidas de seguridad para su seguridad es importante para la empresa. Por ello es

importante realizarlo con el apoyo de una norma ISO 27000 con sus diferentes variantes ya que aportaría a la empresa una serie de procedimientos que ayudan a que regular el funcionamiento de las distintas áreas de estas, al proveer un idioma de calidad común.

- Sin importar el tipo de empresa que sea desde pequeña hasta empresas multinacionales la aplicación de esta norma incluso de vuelve una necesidad ya que puede aplicarlo con el fin de proporcionar un marco de trabajo y administración de la seguridad de la información y además ayudan a reducir el impacto de los riesgos que de no administrarlos pueden convertirse en serias amenazas que afecten la continuidad del negocio de la empresa, lo que podría llevar a perdidas de distintas oportunidades de negocio en el mercado.

REFERENCIAS

- Alonso, C. (2022, 24 mayo). *ISO 27000 y el conjunto de estándares de Seguridad de la Información*. GlobalSuite Solutions. Recuperado 13 de octubre de 2022, de https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/
- editorE. (2015, 10 abril). *La familia de normas ISO 27000*. Software ISO. Recuperado 13 de octubre de 2022, de https://www.isotools.org/2015/01/21/familia-normas-iso-27000/
- *Desarrollo de la familia de normas ISO 27000*. (2014, 29 abril). PMG SSI - ISO 27001. Recuperado 13 de octubre de 2022, de https://www.pmg-ssi.com/2014/04/desarrollo-de-la-familia-de-normas-iso-27000/