TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLALNEPANTLA

INSTITUTO TECNOLÓGICO DE TLALNEPANTLA.

TECNOLOGÍAS DE SEGURIDAD EN SOFTWARE.

DOCENTE: DÍAZ RINCÓN HILDA.

ALUMNO Y N^{o} CONTROL:

ALDAMA MÁRQUEZ JOEL JAIR - 15251870.

GRUPO: T91.

ACTIVIDAD: 3.3 ESTÁNDARES NACIONALES E INTERNACIONALES.

INDICE

INTRODUCCIÓN

En el presente documento, se llevara a cabo un análisis de los diferentes estándares relacionados con la ciberseguridad o seguridad informática en las Tecnologías de la Información y Comunicaciones (TICs) con ayuda de ciertas páginas web y se generará un listado de los estándares localizados, integrando como mínimo el nombre del estándar, descripción, tipo del estándar (si es especificado), el área de aplicación del estándar, y comentarios personales.

DESARROLLO

Primero, debemos saber que es un marco de ciberseguridad, un marco de ciberseguridad es un sistema de estándares, pautas y buenas prácticas para gestionar los riesgos que surgen en el mundo digital. Por lo general, coinciden con los objetivos de seguridad de tu empresa, como evitar el acceso no autorizado al sistema con controles.

Los marcos de ciberseguridad adoptan el enfoque de marco al mundo del aseguramiento de activos digitales.

A menudo se usan de manera obligatoria en las empresas que desean cumplir con regulaciones estatales, industriales y de ciberseguridad internacional.

Tipos de marcos de ciberseguridad

- Marcos de Control
  - Descripción: Desarrollar una estrategia básica para el equipo de seguridad, proporcionar un conjunto de controles básicos, evaluar el estado técnico actual, priorizar la implementación de controles.
  - En donde se aplica: A cualquier tipo de organización.
  - Comentario: Este es un marco muy importante para la seguridad básica de cualquier organización y es importante que se implemente si no se tiene algún sistema de seguridad incorporado.

- Marcos programáticos:
  - Descripción: Evaluar el estado del programa de seguridad, construir un programa integral de seguridad, medir la seguridad del programa / análisis competitivo, simplificar la comunicación entre el equipo de seguridad y los líderes de empresa.
  - En donde se aplica: A cualquier tipo de organización.

- Comentario: Es importante que se lleve a cabo la implementación del marco programático en las empresas u organizaciones que emplean la programación, ya que se debe desarrollar para ilustrar el vínculo entre los insumos, productos y resultados de los programas y tanto, el monitoreo y la evaluación del progreso así como los logros de la organización están integrados en los ciclos de vida del programa y del proyecto.

❖ Marcos de riesgo.

- Descripción: Definir pasos clave del proceso para evaluar / gestionar el riesgo, estructurar el programa para la gestión del riesgo, identificar, medir y cuantificar el riesgo, priorizar las actividades de seguridad
- En donde se aplica: A cualquier tipo de organización.
- Comentario: La implementación del marco de riesgo en las organizaciones debe ser fundamental para que se pueda realizar un análisis de todos los riesgos o posibles riesgos que se encuentren dentro de la organización y ayudar a la organización en integrar la gestión de riesgos en todas sus actividades y funciones, para conocer e implementar las acciones necesarias.

❖ Norma ISO/IEC 27001:

- Descripción: Es un estándar internacional que ayuda a las organizaciones a gestionar la seguridad de sus activos de información. Proporciona un marco de gestión para implementar un SGSI (sistema de gestión de seguridad de la información) para garantizar la confidencialidad, integridad y disponibilidad de todos los datos corporativos
- Tipo: ISO
- En donde se aplica: A cualquier tipo de organización y en especial a las empresas y agencias gubernamentales.
- Comentario: Es una de las normas más importantes que se deben implementar en las organizaciones, ya que si cuenta con esta norma puede permitir presentar un nivel

de calidad para los usuarios, siendo una herramienta sumamente efectiva y además otorga un certificado que hace que sea aún más serio su implementación.

- Norma ISO/IEC 27002:
  - Descripción: Sirve como un documento de orientación, que proporciona una guía de mejores prácticas sobre la aplicación de los controles enumerados en el Anexo A de ISO 27001. Apoya, y debe leerse junto con, ISO 27001.
  - Tipo: ISO
  - En donde se aplica: A todo tipo de empresas, independientemente del tamaño, tipo o naturaleza.
  - Comentario: Es un punto de información muy importante para el conjunto de las normas ISO 27000 y al igual que la norma ISO 27001, ISO 27002 proporciona un marco de referencia de gestión y seguridad a las organizaciones en las que sea implementado y al manejar esta norma se comprende de recomendaciones y buenas practicas.

- Marco NIST de ciberseguridad:
  - Descripción: Está destinado a ser utilizado para proteger infraestructura crítica como plantas de energía y represas de ataques ciberneticos. Sin embargo, sus principios pueden aplicarse a cualquier organización que busque una mejor seguridad. Es uno de varios estándares NIST que cubren la ciberseguridad.
  - Tipo: NIST
  - En donde se aplica: A cualquier organización/negocio que busque una mejor seguridad.
  - Comentario: Este marco es importante para cualquier información, ya que ayuda a los negocios sin importar el tamaño, pero además para que estos negocios puedan conocer con mayor efectividad los posibles riesgos de ciberseguridad a los que se enfrenta y de esta forma poder reducir los riesgos y proteger datos.
- CIS:

- Descripción: Tiene como objetivo crear un marco para proteger a las empresas de las amenazas de ciberseguridad.
- En donde se aplica: Funciona bien para organizaciones que desean dar pequeños pasos.
- Comentario: Es una muy buena incorporación la implementación de estar herramienta y más para las organizaciones pequeñas o que van empezando y quieran tener una eficaz herramienta de ciberseguridad.

❖ Ciclo PDCA:

- Descripción: Es un método de gestión empresarial que se centra en 4 pasos principales que deben implementarse continuamente a medida que se considera el cambio en la empresa. Los cuatro pasos son: Planear, hacer, verificar, actuar.
- Tipo: Gestión empresarial.
- En donde se aplica: Las empresas y agencias gubernamentales.
- Comentario: El ciclo PDCA es muy utilizado a nivel mundial, con un gran numero de empresas desde pequeñas hasta grandes y para poder conseguir una gestión exitosa es mas sencillo con el apoyo de esta metodología PDCA

❖ COBIT:

- Descripción: Es un marco de control para los sistemas de TI utilizados en la contabilidad financiera. Es una parte fundamental del cumplimiento de la Ley Sarbanes-Oxley.
- Tipo: Marco de control.
- En donde se aplica: En la contabilidad financiera.
- Comentario: El modelo COBIT es reconocido internacionalmente y esto habla de su importancia y se puede implementar utilizando prácticas de proceso y gracias a este modelo es importante que podamos asegurar que los objetivos de las Tecnologías de la Información y los objetivos de la empresa estén sincronizados, permitiendo un buen control de los recursos que se utilizaran y tener una gestión de riesgos.

- HIPAA:
  - Descripción: Es una ley diseñada para proteger la privacidad de los pacientes, comprende tanto un conjunto de regulaciones como un marco, de manera muy similar a PCI DSS. Es un conjunto específico de requisitos de control que se combinan con un proceso de certificación para dar fe del compliance.
  - Tipo: Ley.
  - En donde se aplica: En general a cualquier prestador de servicios médicos.
  - Comentario: La implementación del cumplimiento HIPAA es importante para cualquier organización que se ocupe de información médica protegida, ya que HIPAA asegura la privacidad y seguridad de los datos de los usuarios y esto es de lo más importante que deben de implementar las organizaciones médicas.

- Norma GDPR:
  - Descripción: Protege la información personal es algo más suave en su naturaleza. Las reglas son bastante claras, pero el compliance no está certificado por ninguna entidad específica, sino que debe ser auditado en muchos casos por los propios usuarios.
  - En donde se aplica: A controladores y procesadores, donde un controlador es cualquier empresa u organización y el procesador sería una empresa TI que realice el procesamiento de datos real.
  - Comentario: Esta es muy importante para aclarar las relaciones y ganar más responsabilidad en base al suministro, almacenamiento y al uso y procesamiento de datos.

- UNE 320001:
  - Descripción: Fija los requisitos básicos y define el marco de referencia en este sentido. La certificación de ciberseguridad según el estándar LINCE permite mejorar la seguridad del producto que se evalúa. Pero también realizarse en un

tiempo y esfuerzo acotados. De esta manera, estos productos son accesibles a todo tipo de desarrolladores.

- Tipo: Referencia.
- En donde se aplica: En la seguridad lógica.
- Comentario: UNE 320001 es muy buena para lograr la mejora en seguridad de los productos a evaluar y es muy interesante que sea un estándar que se basa en la metodología LINCE para la evaluación de ciberseguridad.

❖ Estándar FITCEM:

- Descripción: No se conoce mucho, ya que su aprobación se espera en los próximos meses, pero sus siglas quieren decir Fixed-Time Cybersecurity Evaluation Methodology for ICT products y es desarrollado por CEN/CENELEC JTC13 WG3

❖ Norma UNE 320002. Arquitecturas de confianza para el intercambio de Inteligencia de Ciberamenazas:

- Descripción: Contempla unos conceptos y procesos de diseño, gobierno y monitorización de arquitecturas de compartición en este sentido. Estos conceptos posibilitan la creación de un ecosistema de garantías y confianza para las entidades que componen la Red.
- Tipo: Marco de referencia genérico
- En donde se aplica: Empresas y organizaciones
- Comentario:

❖ Norma ISO/IEC 27000

- Descripción: Es un conjunto de estándares internacionales sobre la Seguridad de la Información. La familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información.
- Tipo: ISO

- En donde se aplica: A todo tipo de empresas, independientemente del tamaño, tipo o naturaleza.
- Comentario: Este conjunto de estándares es de los más reconocidos y de los más importantes de implementar para la seguridad de la información, tanto el ISO 27001 como el ISO 27002 y los demás estándares de este conjunto son de mucha ayuda en la ciberseguridad, pero ambos son muy valiosos, tanto que en la norma ISO 27001 se obtiene un certificado, haciendo que su implementación sea de gran importancia y seriedad.

❖ ISO/IEC 27032:2012 Directrices para ciberseguridad

- Descripción: Proporciona una guía para analizar y mejorar el estado de la ciberseguridad, destacando los aspectos específicos de esta actividad y sus dependencias y relaciones con la seguridad de la información, la seguridad de las redes, la seguridad en internet y la protección de infraestructura de información crítica de una organización.
- Tipo: ISO.
- En donde se aplica: Organización
- Comentario: Esta norma hace que sea más factible la contribución segura e íntegra para la protección de la privacidad de las personas, ya que ayuda a detectar y luchar contra los ataques cibernéticos.

❖ ISO/IEC TR 27103:2018 Ciberseguridad y estándares ISO e IEC.

- Descripción: Proporciona una guía sobre cómo aprovechar los estándares existentes en un marco de ciberseguridad.
- Tipo: ISO.
- En donde se aplica:
- Comentario: La utilización de la norma ISO/IEC 27013 trae muchas ventajas para la ciberseguridad y que son aplicables a la implementación, como pueden ser

estratégicos, de gestión, económicos operacionales y logísticos, haciendo que estas ventajas sean de gran importancia en la seguridad informática.

- UNE 320001:2021.
  - Descripción: Especifica los pasos necesarios para realizar una evaluación de seguridad básica de productos TIC. Pretende dar respuesta a la necesidad de evaluación de productos cuyo despliegue está previsto en entornos en los cuales el nivel de amenaza es de tipo básico o substancial comprendiendo, además, un alcance limitado dentro de un tiempo y esfuerzo acotado.
  - Tipo: UNE
  - En donde se aplica: Toda organización, cualquiera sea su tipo, tamaño o naturaleza
  - Comentario: Esta metodología de evaluación LINCE es de gran ayuda ya que especifica bien el procedimiento para la evaluación básica de la seguridad, que es de gran ayuda a cualquier tipo de organización.

CONCLUSION

El uso de los estándares es de suma importancia, ya que gracias a estos se puede lograr una muy buena seguridad informática en las organizaciones.

Como podemos ver, existen un gran número de estándares que se puedan implementar, y hay algunos que van más orientado a un tipo de organización o empresa, aunque también existen muchos otros que pueden ser implementados sin importar de que empresa u organización se trate, así que es muy bueno y recomendable aplicar las máximas posibles para lograr una buena seguridad, calidad y control dentro del sistema al cual se implementa.

Aunque considero que sin importar cuantos estándares o mecanismos de defensa se implementen, nunca se podrá asegurar al 100% que se esté libre de amenazas o ataques, o que estemos libres de problemas en corto o largo plazo, pero si ayudan en gran medida a estar mucho mejor protegidos y tener mayor calidad y seguridad

BIBLIOGRAFÍA

- Gutiérrez., N. (2020, 28 julio). *Marcos de Ciberseguridad: La Guía Definitiva*. The Missing Report. https://preyproject.com/blog/es/marcos-de-ciberseguridad-la-guia-definitiva/
- Asociación Española de Normalización (UNE). (2021, 2 febrero). *Así es el primer estándar español basado en LINCE para evaluar la ciberseguridad de los productos TIC*. Redseguridad. https://www.redseguridad.com/actualidad/asi-es-el-primer-estandar-espanol-basado-en-lince-para-evaluar-la-ciberseguridad-de-los-productos-tic_20210202.html
- UNE. (2021, 2 marzo). *Publicado el primer estándar mundial sobre intercambio de inteligencia de ciberamenazas*. Redseguridad. https://www.redseguridad.com/actualidad/ciberseguridad/publicado-el-primer-estandar-mundial-sobre-intercambio-de-inteligencia-de-ciberamenazas_20210302.html
- García., P. (2018, 3 mayo). *Ciberseguridad y estándares europeos*. UNE. https://revista.une.org/3/estandares-europeos-en-ciberseguridad.html
- UNE. (s. f.). *UNE 320001:2021 Metodología de evaluación LINCE para la cibers. . .* https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0065212
- *ISO 27000 y el conjunto de estÃ¡ndares de Seguridad de la InformaciÃ³n*. (2015, 1 septiembre). intedya. https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjunto-de-estandares-de-seguridad-de-la-informacion.html

- *Interpretación ISO/IEC 27032:2012. Directrices para la ciberseguridad (Colombia).* (s. f.). Academy - Internet Security Auditors. Recuperado 31 de mayo de 2021, de https://academy.isecauditors.com/interpretacion-ISO27032-directrices-ciberseguridad