CIBERSEGURIDAD, SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

V. E. Gonzalez Ortiz

7690-13-11075 Universidad Mariano Gálvez

Seminario de Tecnologías de la Investigación

vgonzalezo@miumg.edu.gt

1. Resumen

En la era digital actual, la ciberseguridad, la seguridad informática y la seguridad de la información se han convertido en pilares fundamentales para proteger los datos de organizaciones y personas. Estos conceptos, aunque relacionados, tienen enfoques y ámbitos de aplicación distintos pero complementarios. Este artículo ofrece una visión integral de cada uno de estos términos, destacando su importancia, los riesgos asociados y las estrategias para mitigar amenazas en un entorno cada vez más interconectado. Asimismo, se abordan temas relacionados como la gestión de riesgos, la privacidad de los datos y la normativa vigente.

2. Palabras clave

Datos, Infraestructura, Dispositivos, Servidores, Cifrado, Politicas, ISO, Integridad, Confidencialidad, Disponibilidad, Normas, riesgos, gestion, privacidad.

3. Desarrollo del tema

Considerando la implementación y ampliación de la tecnología en gran parte de la vida diaria, como en el trabajo, la educación, la salud, las comunicaciones, entre otras muchas áreas, se deben tener en cuenta las amenazas que esto conlleva, como la integridad de la información que se consulta, la confidencialidad de la información personal o privada, y la accesibilidad o disponibilidad a la información crítica. A raíz de estas amenazas, ahora se tiene un enfoque en poder proteger los datos que la tecnología procesa.

3.1. Temas relacionadosl

Se detallan a continuacion una serie de subtemas relacionados que apoyan al mejor entendimiento de la informacion de los temas principales, mencionando a su vez la relacion que tienen con los mismos.

Redes de telecomunicaciones

Son sistemas compuestos por diversas tecnologias y equipos que permiten la transmision de la informacion a larga distancia utilizando señales electromagneticas y opticas. Dado que hoy en dia la mayor parte de la informacion es transmitida a travez de datos utilizando redes de telecomunicaciones, es importante tener conocimiento de su concepto y que conjunto de practicas pueden ser aplicadas para su proteccion.

Politicas y normas ISO

Las normas ISO son un conjunto de normas y estandares detalladas estandarizadas de forma internacional desarrolladas y administradas por la Organizacion Internacional de Normalizacion (ISO por sus siglas en ingles), estas normas son un conjunto de estandares agrupadas y enumeradas en base a su funcion y propositos, Para las politicas relacionadas a la seguridad se tiene la familia de normas ISO 27000 la cuales se enfocan en las normas de seguridad de la informacion.

SGSI

Sistema de gestion de seguridad de la informacion, por sus siglas en ingles, es un sistema con el objetivo de gestionar la informacion dentro de las diversas organizaciones.

Cultura organizacion

Esto se enfoca en la forma de pensar, sentir y actuar de las personas de forma colectiva que se relacionan dentro de la organizacion. Se puede mencionar el **individualismo/colectivo** que busca entender la relacion de los individuos con los grupos.

Modelo de riesgos

Es un modelo que abarca una serie de politicas, pasos y herramientas necesarias para poder detectar y solventar las posibles vulneabilidades que un sistema informatico pueda ser utilizado de forma maliciosa o incorrecta

Modelo CIA

POr sus siglas CIA (Confidencialidad, Integridad y Disponibilidad), es un modelo o politica de seguridad importante que aplica dentro de la seguridad de la informacion. La **Confidencialidad** asegura que solamente las personas que fueron previamente establecidas tenga acceso a la informacion, la **Integridad** garantiza que los datos previamente almacenados mantengan su formato original, es decir, que no sea alterada de manera incorrecta, de forma maliciosa o sin previo consentimiento, y la **Disponibilidad** se enfoca que los datos esten disponibles en el momento en el que se necesita.

3.2. Ciberseguridad

Se comprende como ciberseguridad a todas las practicas herramientas y uso de las mismas a la proteccion de los datos informaticos, aplicando a los dispositivos, como lo es, las computadoras, servidores, dispositivos moviles como tambien a las tecnologias involucradas como sistemas de software, redes de telecomunicaciones y todo programa digital, de ataques maliciosos que quieran dañar, obtener o utilizar de forma incorrecta estos datos.

Amenazas Ciberneticas

Las amenazas ciberneticas es cualquier amenaza o acto mal intencionado que pretenda afectar un sistema informatico.

Protecciones Ciberneticas

Son todas las medidas, practicas y herramientas, entre las cuales se pueden mensionar un sistema o software de antivirus, la implementacion de firewalls dentro de las redes de telecomunicaciones, sistema de deteccion de intrusos o personas no autorizadas, capacitacion continua al personal de la organizacion sobre los diversos ataques o amenazas que puede ser de forma individual como de ingenieria social.

3.3. Seguridad Informatica

La seguridad informática es una categoría que se centra en la protección de los sistemas y de toda la infraestructura de comunicaciones que manejan los datos de información. Algunas de las técnicas más utilizadas en la seguridad son el cifrado de datos, la autenticación de usuarios, el control de acceso a los datos y las copias de seguridad.

Proteccion de sistemas y redes

El enfoque de la seguridad informática está en garantizar que los sistemas sean resilientes a ataques y que los datos estén protegidos en tránsito y en reposo. La implementación de redes seguras y la correcta configuración de los sistemas son aspectos críticos.

Gestión de Vulnerabilidades

La gestión de vulnerabilidades implica la identificación, evaluación y mitigación de posibles puntos débiles en los sistemas. Esta gestión es esencial para prevenir la explotación de vulnerabilidades por parte de atacantes.

3.4. Seguridad de la Informacion

La seguridad de la informacion es una categoria que se expande a un enfoque mayor ya que no solo aplica a la informacion de datos de informacion, esta categoria aplica a toda la proteccion de la informacion en sus diversas formas, como digital o fisica. Adicional a aplicar practicas de de proteccion de la informacion, se puede aplicar politicas, procedimientos, controles y tecnicas para controla y salvaguardar toda la informacion que una organizacion o persona individual tiene a su disposicion segun la disponibilidad de accesibilidad previamente establecida.

Normativa y Cumplimiento

Las organizaciones deben cumplir con diversas normativas relacionadas con la protección de la información, como el GDPR en Europa o la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos. Estas normativas establecen requisitos estrictos para la protección de datos personales y la privacidad.

4. Observaciones y comentarios

1. El creciente uso y dependencia de la tecnología en el manejo de la información ha hecho necesaria la implementación de medidas de seguridad sobre los datos gestionados, desglosándose en tres primordiales categorías para una mejor comprensión e implementación de las diferentes normas y prácticas especializadas para cada escenario.

2. La importancia de la politica de seguridad robutsas y la implementacion de una cultura organizacion en base a la seguridad es clave para poder hacer frente a las diferentes amenazas y ataques sobre los datos.

5. Conclusiones

1. Los temas relacionados a la serguridad incluyen su formato dijital resguardada con la ciberseguridad y seguridad informatica y de forma fisica con la seguridad de la informacion.

2. La gestion efectiva de estas areas no solo protegen los datos sensibles sino tambien fortalece la confianza de los usuarios y clientes entre las organizaciones

3. Es de vital importancia que las organizaciones y personas individuales adopten un enfoque de seguridad proactivo y de cumplimiento de politicas de seguridad.

6. Bibliografia

* Kaspersky. (n.d.). What is cyber security? Kaspersky Latam. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

* PMG-SSI. (2021, marzo 29). ¿Qué es la seguridad de la información y cuántos tipos hay? PMG-SSI. https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

* Hewlett Packard Enterprise. (n.d.). What is IT security? Hewlett Packard Enterprise. https://www.hpe.com/lamerica/es/what-is/it-security.html

* ISACA. (2021). Organizational culture for information security. ISACA Journal, Volume 3. https://www.isaca.org/es-es/resources/isaca-journal/issues/2021/volume-3/organizational-culture-for-information-security

* Pirani Risk. (n.d.). ISO 27001: ¿Qué es y cómo implementarla? Pirani Risk. https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implement~:text=La%20norma%20ISO%2027001%20establece,tus%20clientes%2C%20proveedo20y%20empleados

* NFON. (n.d.). Redes de telecomunicaciones. NFON. https://www.nfon.com/es/get-started/cloud-telephony/lexicon/base-de-conocimiento-destacar/redes-de-telecomunicaciones#:~:text=Las%20redes%20de%20telecomunicacione20son,v%C3%ADdeo%20o%20de%20otros%20tipos

https://github.com/UMGVg/SDTDI_Foro_Acad-mico1