CIBERSEGURIDAD Y TELECOMUNICACIONES

Valdelamar Christian Abraham.
contiverosv@outlook.com
Villaseñor Almazán Mario Alberto.
alberto_9792@hotmail.com
Sánchez Coraza Erandy Itzel.
erandy_coraza@hotmail.com

Instituto Politécnico Nacional

Abstract

We live in a time of change, where technology is gaining a lot of ground, where new generations born surrounded of appliances and innovation is our daily bread, this is what past generations call ”future”, all the people that experiments this transition is not used to handle technology carefully, and that is the first problem about this change, because criminals are also immersed in technology, looking ways to steal information from people and using it without permission. Cybersecurity is a word used to explain the actions that are implemented to shelter the System´s information by: using a lot of methods that evolve day to day, fighting to be at the forefront of the Technological revolution. This Article will explain what the Cybersecurity is, and it is importance nowadays by attending the norms, the environment in which it develops, by explaining the way we can make Cybersecurity a part of our lives, and how the organizations protect our data from the criminals.

Internet se ha convertido sin lugar a duda en un recurso para la comunicación sin precedentes en nuestros días, es lugar donde la mayor parte de la población mundial se desenvuelve, trascendiendo las limitaciones de las fronteras, permitiendo a los ciudadanos mantener una interacción con los sucesos que acontecen día con día, permitiéndoles el acceso inmediato a la información, a la vez de dárseles la oportunidad de compartir su opinión al respecto y debatir con otras personas.

Esto ha llevado a que todos los sectores económicos miren hacia este gran fenómeno y quieran enfocar su lógica de negocio en el uso de la tecnología, lo cual ha llevado a que la internet se convierta en un elemento clave para el desarrollo de la economía a lo largo y ancho del planeta.

Así mismo, esto conlleva diferentes amenazas que pueden provocar problemas al momento de realizar actividades dentro y fuera de la red, ya que, siendo la web un terreno poco explorado y a la vez con gran cantidad de movimientos económicos, es el centro de atención para los distintos criminales cibernéticos, quienes buscan llevar al sistema contra las cuerdas en todo momento, para desencadenar incidencias de cualquier índole.

Para combatir estos actos, las naciones a lo largo del planeta han tomado sus propias medidas de seguridad, a la par de que diferentes organizaciones reconocidas mundialmente, se han encargado de desarrollar estándares para el manejo de las nuevas tecnologías y la información en general, de forma que la población pueda apoyarse en estos, para evitar todos los riesgos.

La ciberseguridad, nació para solventar la constante necesidad de proteger la información recabada dentro de los sistemas que yacen en el internet, desarrollando medidas preventivas, dependiendo del contexto en el que se produzca alguna posible falla, siempre manteniéndose a la vanguardia de la tecnología y explotando al máximo su creatividad para encontrar posibles caminos que puedan poner en riesgo la integridad de la información. [1]

Los diferentes ataques a la seguridad de la información dentro de las plataformas han alentado a que los especialistas desarrollen medidas para lidiar con estos problemas, como diferentes estándares y planes de contingencia que solventarán estos riesgos, sin embargo, los atacantes también se

mantienen actualizados conforme la tecnología avanza, ya que diferentes actualizaciones se despliegan constantemente, lo cual abre y cierra oportunidades para hacerse con la información. [3]

A su vez, las naciones se han enfocado en acoplarse a este nuevo modelo de desarrollo, creando distintas leyes que ayuden a regular su uso, enfocándose en no limitar el derecho natural a la información, pero también a no exponer la integridad de las personas dejando al descubierto sus datos personales. [5]

CIBERSEGURIDAD A NIVEL PERSONAL

Dentro del entorno de la ciberseguridad podemos observar que los ataques son dirigidos a sectores específicos o al azar dependiendo el tipo de daño que se desee causar, encontrando como tal un amplio campo para el entendimiento de la ciberseguridad. Comenzando por el entendimiento de los diferentes tipos de daños posibles tomando como base los siguientes ejemplos: [7]

Dentro del entorno de la ciberseguridad podemos observar que los ataques son dirigidos a sectores específicos o al azar dependiendo el tipo de daño que se desee causar, encontrando como tal un amplio campo para el entendimiento de la ciberseguridad. Comenzando por el entendimiento de los diferentes tipos de daños posibles tomando como base los siguientes ejemplos: [7]

Gusano: Se trata de códigos dañinos calificados como independientes, al estar diseñados para reproducirse a sí mismos, es decir, realizar copias de sí mismo y enviarlas a todos aquellos ordenadores que estén conectados a través de la red. [14]

Virus: Consiste en un programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros. [9] [13]

Destinados al daño claro para los usuarios comunes dentro del ciberespacio, dañando de esta manera su equipo, robando información personal y/o suplantando a la persona dañada en cuestión.

CIBERSEGURIDAD A NIVEL EMPRESARIAL

El área empresarial es un sector más detallado y concreto, donde adoptando nuevas vertientes tecnológicas; todas las organizaciones y/o empresas buscan centralizarse mediante una estrategia de negocio haciendo uso de las TI (Tecnologías de la Información). [16]

Haciendo un enorme uso y teniendo un gran aprovechamiento de todo el entorno del ciberespacio, las empresas desarrollan y se desenvuelven en torno a las tecnologías y el correcto uso del internet; por lo que las empresas actualmente manejan una Arquitectura Empresarial (AE) la cual es un enfoque para la gestión de la estructura interna y el esparcimiento de su información; donde se toma como referencia el concepto básico de “Ciberseguridad”.

En donde a nivel empresarial la ciberseguridad: Es el conjunto de actividades centradas en mecanismos defensivos y ofensivos empleados tanto para proteger el ciberespacio contra el uso indebido del mismo, defender su infraestructura tecnológica, los servicios que prestan y la información que manejan, tomando como lineamientos específicos ciertas “NORMAS Y MARCOS DE TRABAJO”.

LINEAMIENTOS Y MARCO DE TRABAJO

A. ISO/IEC 27001. Dicha norma presenta las necesidades del sistema de gestión de seguridad de la información; dicha norma nos otorga una metodología para poder llevar acabo la correcta implementación de un sistema de gestión de seguridad de la información (SGSI) dentro de una organización. [15]

La norma consta de 4 fases internas o 4 lineamientos de aplicación que son: Planificación, implementación, revisión, mantenimiento; las cuales deben de ser implementadas en una forma constante para reducir al mínimo los riesgos en la confidencialidad, integridad y disponibilidad de la información.

B. ISO/IEC 27032. Otorga una serie de lineamientos, tomando una función como guía para mejorar el entorno de ciberseguridad, substrayendo los aspectos únicos de esta actividad y de sus dependencias en otros dominios de seguridad. [12] [15]

De manera más específica y concreta: Aspectos como la información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras criticas (CIIP). ISO 27032,

permite gestionar directrices para maximizar los estados de la ciberseguridad, resaltando aspectos únicos de dicha actividad y su dependencia de otros ámbitos de seguridad.

C. MARCO DE TRABAJO PARA MEJORAR LA CIBERSEGURIDAD DE INFRAESTRUCTURAS CRÍTICAS (CS-IC). Consta de un conjunto de especificaciones y/o directrices sobre ciberseguridad que ayuda a proteger las infraestructuras críticas, y está fundamentado en la gestión de riesgos para la ciberseguridad, el marco de trabajo consta principalmente de tres partes: Primero el núcleo del marco de trabajo, que presenta estándares de la industria, directrices y practicas; posteriormente están los niveles de aplicación del marco de trabajo, los cuales proporcionan un contexto de cómo una organización entiende el riesgo de la ciberseguridad; y por último se encuentra el perfil del marco de trabajo, que representa los resultados de observar las necesidades del negocio que se han seleccionado dentro de las categorías y sus propias subcategorías del marco de trabajo. [13]

Tomando en cuenta y basado en lo anterior las bases para la arquitectura y la creación de un estándar para las empresas en un modelo de ciberseguridad básico para el correcto funcionamiento de la empresa y la distribución de su información.

La ciberseguridad es una práctica y acción que todos debemos llevar a cabo por nuestro bienestar y el de las personas que nos rodean, sobre todo si queremos formar parte de la actual revolución tecnológica en donde siempre debemos tener un control de donde usamos nuestros datos personales, tomado así medidas para prevenir que hayan conflictos de identidad, a la vez de proteger nuestras empresas, solo revelando y distribuyendo información a los empleados de confianza, usando todos los filtros de seguridad para que ningún dato sensible se fugue.

Referencias

1. Caulkins, B., Marlowe, T., Reardon, A. (**2016**) *Skills to Address Today's Threats Cybersecurity* Compiègne, France: Springer

2. E. Niemi, S. Pekkola (**2013**) *Enterprise Architecture Quality Attributes: A Case Study, Computer Society* pp. 3878.

3. G. Peterson, S. Shenoi (**2012**) *Advances in Digital Forensics* VII, vol. 361, pp. 3-21.

4. ISO/IEC 27032:2012 (**2012**)ISO/IEC 27032:2012, ISO.

5. J. Osorio (**2010**) *Togaf y Zachman Framework* pp. 19-20.

6. J. Payette, E. Anegbe, E. Caceres, S. Muegge (**2015**) *Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects* pp. 26-34.

7. K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson (**2008**) *Systematic Mapping Studies in Software Engineering, 12Th International Conference on Evaluation and Assessment in Software Engineering.* pp. 17-10.

8. Ministerio de Justicia Derechos Humanos y Cultos (**2014**) *Código Organico Integral Penal (COIP)* Quito, Pichincha, pp. 93-95.

9. N.T. Le, D.B. Hoang, (**2016**) *Can maturity models support cyber security?.* University Technology of Sydney, Faculty of Engineering & IT.

10. OW ASP (**2014**) *Testing Guide v4.* OW ASP.

11. Sadeghi, S.H (**2018**) *Learning objectives in cyberspace.* Studies in Systems, Decision and Control, 156 pp. 55-64.

12. Sadeghi, S.H (**2018**) *Reduce and deal with injuries by training in cyberspace.*Studies in Systems, Decision and Control, 156 pp. 93-102.

13. Sadeghi, S.H (**2018**) *Training in cyberspace. Studies in Systems, Decision and Control.* 156 pp. 39-53.

14. TOGAF and SABSA Integration (**2011**) *Working Group/revista*

15. Autor (**año**) *Transforming Cybersecurity Using COBIT 5.* ISACA, 2013.

16. X. Servitja Roca (**año**) *Ciberseguridad contrainteligencia y operaciones encubiertas en el programa nuclear de iran,* IEEE, 2013.