Guía metodológica para obtener una certificación de entidades regulatorias para lograr una estabilidad en la seguridad de la información del sector comercial
Methodological guide to obtain a certification from regulatory entities to achieve stability in the security of information in the commercial sector

Diego José Esquivel Quirós
Universidad Latina, Costa Rica
djeq1995@hotmail.com

Recibido 12/oct/2020
Aprobado 20/nov/2020

Resumen-
Este artículo trata del desarrollo de una guía inicial para las empresas que quieran implementar seguridad en sus sistemas respecto a la ISO 27002 dentro del sector de comercial y que sean parte del comercio electrónico, para que puedan evaluar diferentes medidas con la idea de que más adelante puedan escoger y mejorar sus controles de seguridad. Se establecen en cinco capítulos, el primero se trata del marco introductorio en donde básicamente de los objetivos del proyecto y todos los temas relacionados a la organización del proyecto como del porqué se escogió ese tema y esa norma, seguidamente el siguiente capítulo, el marco teórico como su nombre lo dice, es donde se va a plantear toda la teoría del proyecto para formalizar y tener una base teórica. El marco metodológico será el capitulo en el cual se enfoca en la información y el instrumento para conseguir convertir datos en información. Una vez concluido la siguiente sección es el análisis de la información donde precisamente pasan de ser datos a información. Por último, encontramos la propuesta que es la información interpretada en un conjunto de medidas e ideas de como se debe de formalizar la seguridad en el sector seleccionado.

Palabras Claves: *Metodología, seguridad, certificación, ISO 27002.*

Abstract Context:
This article deals with the development of an initial guide for companies that want to implement security in their systems with respect to ISO 27002 within the commercial sector and that are part of electronic commerce, so that they can evaluate different

measures with the idea that later They can choose and improve their security controls. They are established in five chapters, the first is the introductory framework where basically the objectives of the project and all the issues related to the organization of the project as well as why that topic and that standard were chosen, then the next chapter, the theoretical framework as its name says, it is where the entire theory of the project will be raised to formalize and have a theoretical basis. The methodological framework will be the chapter in which it focuses on the information and the instrument to convert data into information. Once the next section is concluded, it is the analysis of the information where precisely they go from being data to information. Finally, we find the proposal that is the information interpreted in a set of measures and ideas on how security should be formalized in the selected sector.

Keywords: *Methodology, security, certification, ISO 27002.*

I. INTRODUCCIÓN

Dentro del sector comercial de Costa Rica existen muchas fisuras en la seguridad para demostrarlas se realizó una encuesta para demostrar que el nivel de seguridad en el comercio electrónico del país difiere con los protocolos que sugieren las normas de seguridad de la información. Siguiendo en contexto del proyecto para dejar en evidencia los posibles que tienden a generar las empresas con el manejo de información se utilizo la norma ISO 27002 que es la representante en las buenas prácticas del manejo de la información, por ello se utilizo para crear una especie de guía en la cual será un base para que futuras empresas puedan crear y continuar creando medidas de protección de información como bien se detallo en la sinopsis el trabajo se dividen en cinco áreas introductorio, teórico, metodológico, análisis y propuesta, en cada uno de ellos se desarrollan puntos clave en la investigación por lo tanto cada capítulo está integrado en una forma que genera un avance importante en la investigación de protocolos de seguridad, además de orientar a las empresas a complementar un nivel satisfactorio en las áreas que se mencionaron en el proyecto. Sin embargo, es ideal que esto se tomen como los primeros pasos que las empresas deben de seguir, pero no quedarse atacados solo con este documento, sino gracias a este documento crecer y mejorar sus controles de seguridad para el resguardo de la información.

II. CONTEXTO DE SEGURIDAD EN LAS EMPRESAS DE COSTA RICA PARA EL SECTOR DEL COMERCIO ELECTRÓNICO

El objetivo general de esta investigación Diseñar una guía metodológica para obtener una certificación de entidades regulatorias para lograr una estabilidad en la seguridad de la información del sector de comercio electrónico, basados en las buenas prácticas del ISO 27002, en Costa Rica en el año 2021.

Antes de que se mencione la metodología es importante señalar definición es la norma que se utiliza en el documento es la (Organización Internacional de Normalización) INTE ISO IEC 27002 del año 2016.

Respecto a la metodología seleccionada se pensó en la idea de recolectar datos directamente de diferentes tipos de negocios sin embargo, se tenía una condición independientemente del producto o servicio que ofrecía debía de ser un negocio que fuera parte del comercio electrónico, una vez cumplida esa condición, se observo que la mejor herramienta era la encuesta porque podía brindar un camino especifico que nos ayudaría a preguntar cuestiones muy

específicas de la seguridad, por supuesto que tenían que realizarse anónimas ya que, si la información caía en manos equivocadas las empresas podía ser victimas de ataques y resolver un problema no es crear uno diferente, una vez enviadas las encuestas se recogen los datos y se interpretan con diferentes opciones junto con la norma para crear un respuesta ante la situación que los datos se van revelando hasta que se vuelven información un ejemplo sencillo es que una de las preguntas que se solicito si el negocio posee alguna medida para mitigar un evento, el 70% no poseía una respuesta ante incidentes evidentemente es preocupante pero ayudara mucho para crear luego un conjunto de protocolos para que los negocios puedan mejorar su seguridad.

III. RESULTADOS

3

Es importante resaltar que una de las mejores opciones era la enseñanza de la seguridad por las buenas practicas que genera en las empresas que pueden implementar esta medida.

4

Si tenemos en cuenta que del 70% no posee una medida de seguridad para un evento es precisamente se busca visualizar los posibles peligros que pueden ocurrir.

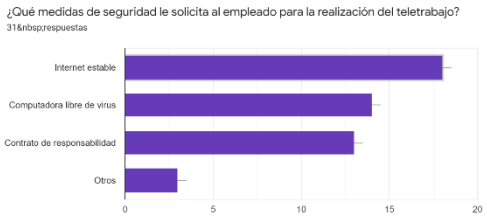
Pregunta 5

Esta pregunta nos ayudara a comprender la necesidad de un control de seguridad ante algún proveedor.

6

Más de lo mismo la delicada situación de no poseer un procedimiento ante algún robo de información puede llegar a perjudicar gravemente a la empresa.

7



Se refleja que si se conoce requisitos mínimos para ofrecer la modalidad de teletrabajo.

8

Se debe de desarrollar de manera urgente contratos que la empresa pueda usar para salvaguardarse a ella y a la información.

Pregunta 10

Esta sin duda es preocupante porque si un empleado encuentra algún problema por cual medio podrá reportar la avería para mejorar la empresa.

IV. DISCUSIÓN

En esta sección es donde se interpreta los datos recibidos de las encuestas, se debe definir primeramente que la discusión se fragmentó en siete partes con la intensión de cubrir todos los puntos de las investigaciones los siete puntos son: las buenas prácticas, controles de acceso, Documentación de proveedores, seguridad en teletrabajo, Acuerdos de no divulgación, inventario de activos y reporte de eventos. Estos puntos son los que se desarrollan a lo largo de la investigación como parte de generar los niveles de seguridad de cada uno de esos objetivos del trabajo. Como primer punto de las buenas prácticas se menciona el trabajo de (Mejía et al, 2016) que nos refleja la idea de cuales son las practicas que en una empresa deberían de ser totalmente normales, se menciona el uso de antivirus y una parte imprescindible que es el uso de software legal para que se tenga una idea de lo que es, básicamente es comprar el software y instalar en la empresa un programa pirata porque puede provocar problemas, otro punto fundamental que toca es la actualización de equipos, el uso de backups, el noble uso de las contraseñas seguras y el cifrado de datos. Por otra parte, la Organización Internacional de Normalización (ISO, 2016) menciona todos esos puntos y resalta la importancia de cada uno de ellos en especial el uso de contraseñas seguras y los controles criptográficos necesarios para la protección contra los códigos maliciosos. Como el siguiente objetivo de la interpretación de datos los controles de acceso, (Figueroa et al,2018) nos comenta de la importancia de los tres pilares de la información que son la confidencialidad, la integridad y la disponibilidad haciendo hincapié de que una falta de controles de acceso puede provocar una filtración de información y precisamente la pregunta a la que está arraigada a este punto varias empresas pueden ser vulneradas en cualquier momento.

De acuerdo con (ISO, 2016) nos hablan sobre la necesidad de estos controles y que no solo es digital sino también física por lo tanto nos brinda varios puntos como roles de acceso y la existencia de un registro en el cual se documenten todos los accesos ya sean debidos como indebidos. Dentro de la parte tres la documentación de los proveedores, (ISO, 2016) nos brinda maneras de como establecer una conexión con los proveedores y nos mencionan por ejemplo el realizar siempre un nivel de desempeño con el proveedor o bien registrar toda la documentación brindada por ellos. La siguiente parte la seguridad del teletrabajo es una realidad que en 2021 es común ver muchas empresas ejercer esta modalidad en buena parte gasta menos dinero en emplear eso, sin embargo la (ISO, 2016) deja claro que un contrato o bien una mala

gestión de permisos en el teletrabajo puede provocar que dicha empresa pierda más dinero y reputación de lo que pueden creer pero, también nos da los tips para crear controles óptimos que se pueden establecer en los contratos y las medidas que debe optar el negocio para disminuir un problema en esa área. En la quinta parte los acuerdos de no divulgación en el sector del comercio electrónico es fundamental tener estos tipos de contratos para evitar que información se filtre en la competencia por ello, el (ISO, 2016) nos menciona la importancia de estos conceptos y el como incluirlos en los contratos, además de respaldarlas con políticas para que la empresa tenga herramientas para defenderse de ese tipo de problemas. En este punto el numero seis el inventario de activos nos importante hacerlos, pero, el (ISO, 2016) dice que no es la único que se debe de hacer, debe existir documentación del cuando se realizó, el tener un control de los activos nos ayudara a visualizar si por ejemplo un equipo no posee garantía o si se tiene algún problema. Como ultimo punto y termina uniendo a todos los demás el reporte de fallos se encuentra en cada uno de los puntos anteriores por la simple finalidad de que es indispensable para mantener medidas de seguridad precisamente el reporte de fallos es una medida en pura regla y como podemos observar la última pregunta contenía este herramienta de seguridad y muchas empresas no tenían por ello, el (ISO, 2016) nos desarrolla la idea de que un problema se puede efectuar de diferentes maneras y dice la importancia de aplicarlo en cada una de las áreas en que se desarrolle la empresa para poder optar por un conjunto de controles de seguridad que ayuden a levantarse a la empresa cuando ocurra algún evento que intente dañar al negocio.

V. Conclusión

La investigación concluye que las necesidades de diferentes empresas del sector del comercio electrónico requieren atención desde el punto de vista de seguridad, se demuestra como existen empresas sin controles mínimos de seguridad por diferentes razones ya sea tiempo o dinero se abren muchas brechas a la seguridad y eso ocurre que atacantes vea posibles flancos por donde adentrarse y sustraer información para así venderla después, se discuten desde diferentes puntos de vistas y en conjunto con la norma ISO 27002 acerca de los diferentes reglas o políticas que debería tener una empresa para solventar un problema con la seguridad. De igual forma se logra recabar datos con encuestas que posterior de conseguir los datos se procesan para obtener la información con la que se desarrolla un conjunto de consejos que le brinda una oportunidad para que negocios que quieran salvaguardar la información lo puedan realizar en menor medida y menor costo sin embargo, al ser solo el comienzo se recomienda a las empresas utilizar esta guía para poder eventualmente crear sus propias políticas y mejorar para lograr un nivel por encima de la media.

VI. REFERENCIAS

accensit. (Agosto de 2017). accensit. Recuperado de www.accensit.com: https://www.accensit.com/blog/seguridad-perimetral-informatica-informacion-necesaria/

akamai. (s.f.). akamai. Recuperado de www.akamai.com: https://www.akamai.com/es/es/resources/cyber-attacks.jsp

BIBLIOGRAPHY Arteaga, G. (Octubre de 2020). www.testsiteforme.com. Obtenido de Una guía completa de técnicas de investigación cuantitativa: https://www.testsiteforme.com/tecnicas-de-investigacion-cuantitativa/

Business Platform. (s.f.). sistel. Recuperado de www.sistel.es: https://www.sistel.es/seguridad-gsuite-como-protege-google-mis-datos

caser. (2018). caser. Recuperado de www.caser.es: https://www.caser.es/seguros-empresas/articulos/que-es-un-ciberataque-y-tipos

Caurin, J. (Junio de 2018). emprendepyme. Recuperado de www.emprendepyme.net: https://www.emprendepyme.net/politicas-de-seguridad.html

cetmetacom. (s.f.). Metacom. Recuperado de cetmetacom.cl: https://cetmetacom.cl/ftecnicas/estandar-tia-942.pdf

cisco. (s.f.). cisco. Recuperado de www.cisco.com: https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html

computing. (Diciembre de 2018). computing. Recuperado de www.computing.es: https://www.computing.es/infraestructuras/noticias/1109344001801/importancia-del-software-de-monitoreo-de-red-empresa.1.html

Daccach, J. C. (s.f.). Estructura Informática. Obtenido de www.deltaasesores.com: https://www.deltaasesores.com/estructura-informatica/#:~:text=La%20estructura%20inform%C3%A1tica%20de%20una,nivel%20de%20complejidad%20y%20beneficio.

DAVANTISEDITOR. (Enero de 2019). davantis. Recuperado de www.davantis.com: https://www.davantis.com/es/content/blog/que-es-la-seguridad-perimetral-y-cuales-son-sus-beneficios

econectia. (Agosto de 2018). econectia. Recuperado de www.econectia.com: https://www.econectia.com/blog/mejores-herramientas-seguridad-informatica

Equipo de Expertos. (Setiembre de 2018). universidadviu. Recuperado de www.universidadviu.com: https://www.universidadviu.com/seguridad-digital-nivel-global-y-definiciones/

ESIC Business & Marketing School. (Enero de 2018). esic. Recuperado de www.esic.edu: https://www.esic.edu/rethink/tecnologia/tipos-de-seguridad-informatica-cuales-existen

Figueroa-Suárez, J., Rodríguez-Andrade, R., Bone-Obando, C., & Saltos-Gómez, J. (2018). La seguridad informática y la seguridad de la información. Polo del Conocimiento, 2(12), 145-155. doi: HYPERLINK "http://dx.doi.org/10.23857/pc.v2i12.420" http://dx.doi.org/10.23857/pc.v2i12.420

gbadvisors. (Abril de 2019). gb-advisors. Recuperado de www.gb-advisors.com: https://www.gb-advisors.com/es/comprar-software-de-seguridad-informatica/

hacknoid. (s.f.). hacknoid. Recuperado de hacknoid.com: https://hacknoid.com/hacknoid/importancia-de-la-seguridad-informatica-de-las-empresas/

Hernandez, C. (Julio de 2020). Instituto Nacional de contadores publicos. Recuperado de www.incp.org: https://www.incp.org.co/que-tipos-de-ciberataques-existen/

Hernandez, M. (Septiembre de 2019). hiberus. Recuperado de /www.hiberus.com: https://www.hiberus.com/crecemos-contigo/uso-de-los-apm-monitoreo-del-rendimiento-de-aplicaciones/

INCIBE. (Enero de 2019). incibe. Recuperado de www.incibe.es: https://www.incibe.es/protege-tu-empresa/blog/sabes-mejorar-ciberseguridad-tu-organizacion-implanta-plan-director

INCIBE. (s.f.). incibe. Recuperado de www.incibe.es: https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

isotools. (Junio de 2019). isotools. Recuperado de www.isotools.org: https://www.isotools.org/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/

isotools. (s.f.). isotools. Recuperado de www.isotools.org: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

itdigitalsecurity. (Septiembre de 2018). itdigitalsecurity. Recuperado de www.itdigitalsecurity.es: https://www.itdigitalsecurity.es/vulnerabilidades/2018/09/los-ciberataques-internos-preocupan-a-casi-la-mitad-de-los-responsables-de-seguridad

Jiménez, J. (Mayo de 2020). redeszone. Recuperado de www.redeszone.net: https://www.redeszone.net/tutoriales/seguridad/consejos-mantener-segura-red-empresarial/

Jiménez, K. C. (Noviembre de 2016). elfinancierocr. Recuperado de www.elfinancierocr.com: https://www.elfinancierocr.com/tecnologia/las-claves-de-israel-para-resguardar-su-seguridad-informatica/UQVWGZNCRNGOLGZQVNSMST3A4U/story/

LASKURAIN, A. (Enero de 2017). captio. Recuperado de www.captio.net: https://www.captio.net/blog/recomendaciones-al-aplicar-politicas-de-seguridad-en-los-viajes-de-empresa

Macía, B. (Junio de 2019). neamaster. Recuperado de www.neamaster.com: https://www.neamaster.com/importancia-de-la-seguridad-informatica/

Mejía.A, Mejía.A.F, Bernal.A.F."Buenas prácticas de seguridad informática en microempresas colombianas". Revista CIES,Vol.7,pp. 15-26. 2016.

http://www.escolme.edu.co/revista/index.php/cies/article/view/72/69

Mercado, R. B. (Agosto de 2018). Seguridad Física de TI. Obtenido de www.rberny.com: https://www.rberny.com/gestion-de-ti/seguridad-fisica-de-ti/

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2017). micitt. Recuperado de https://micitt.go.cr: https://micitt.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

Organización Internacional de Normalización. (2016). INTE/ISO/IEC 27002:2016 Técnicas de seguridad. Código de buenas prácticas para controles de seguridad de la información. (Obra original publicada en 2016)

Otzen, Tamara, & Manterola, Carlos. (2017). Técnicas de Muestreo sobre una Población a Estudio. International Journal of Morphology, 35(1), 227-232. HYPERLINK "https://dx.doi.org/10.4067/S0717-95022017000100037" https://dx.doi.org/10.4067/S0717-95022017000100037

Pacheco, J. (Octubre de 2019). www.webyempresas.com. Obtenido de Método Comparativo (definición, usos, características): https://www.webyempresas.com/metodo-comparativo/

Raffino, M. E. (Agosto de 2020). https://concepto.de/. Obtenido de ¿Qué es el método analítico?: https://concepto.de/metodo-analitico/#:~:text=Caracter%C3%ADsticas%20del%20m%C3%A9todo%20anal%C3%ADtico,Verificable%20emp%C3%ADricamente.

Ramíres, I. (Mayo de 2020). xataka. Recuperado de www.xataka.com: https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

riesgoscero. (s.f.). riesgoscero. Recuperado de www.riesgoscero.com: https://www.riesgoscero.com/academia/especiales/guia-para-gestionar-un-plan-de-continuidad-de-negocio-segun-la-iso-22301

Rivas, G. (Enero de 2019). gb-advisors. Recuperado de www.gb-advisors.com: https://www.gb-advisors.com/es/seguridad-digital-frente-a-las-amenazas/

Roldán, P. N. (Diciembre de 2016). economipedia. Recuperado de https://economipedia.com/: https://economipedia.com/definiciones/equilibrio-de-nash.html

Sánchez-Paredes.G, Montenegro-Ramírez.G,Medina-Chicaiza.P."Teletrabajo una propuesta de innovación en productividad 9 empresarial". 593 Digital Publisher CEIT, ISSN-e 2588-0705, Vol. 4, Nº. 5-1, 2019,págs. 91-107

https://dialnet.unirioja.es/servlet/articulo?codigo=7144041

si-mad. (Noviembre de 2017). actualización de equipos informaticos. Obtenido de www.si-mad.com: http://www.si-mad.com/actualizacion-de-equipos-informaticos/

seguridadcra. (s.f.). seguridadcra. Recuperado de www.seguridadcra.com: https://www.seguridadcra.com/control-de-acceso/?gclid=CjwKCAjw1ej5BRBhEiwAfHyh1GAQtMj35PMmTDswxJXYrsdqAQlzhoC5WG20d2CEAYFkqI0X47-PfhoCAOIQAvD_BwE

Torres, M., Paz, K., y Salazar, F. G. (s.f.). Métodos de recolección de datos para una investigación. Recuperado de http://fgsalazar.net/LANDIVAR/ING-PRIMERO/boletin03/URL_03_BAS01.pdf

Unir. (Mayo de 2020). unir. Recuperado de www.unir.net: https://www.unir.net/ingenieria/revista/noticias/politicas-seguridad-informatica/549204996232/

urbisegur. (Marzo de 2020). urbisegur. Recuperado de urbisegur.com: https://urbisegur.com/vigilante-de-seguridad-funciones/