ANALIZAR LAS POLÍTICAS Y LOS CONTROLES BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN EN FUNCIÓN DE LAS NUEVAS NECESIDADES QUE TIENEN LAS PYMES DEL SECTOR COMERCIAL EN TIEMPOS COVID-19

Gabriel Felipe Rodriguez Arteaga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2023

ANALIZAR LAS POLÍTICAS Y LOS CONTROLES BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN EN FUNCIÓN DE LAS NUEVAS NECESIDADES QUE TIENEN LAS PYMES DEL SECTOR COMERCIAL EN TIEMPOS COVID-19

Gabriel Felipe Rodriguez Arteaga

Proyecto de Grado – Monografía presentado para optar por el titulo de
ESPECIALISTA EN SEGURIDAD INFORMATICA

DANNY FERNANDO LEÓN JARAMILLO
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2023

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Mayo 31 de 2023

DEDICATORIA

Con amor dedico este trabajo a mi Madre y hermanos, que con su carisma y comprensión me acompañó en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones.

Sin ellos y su acostumbrado apoyo en cosas tan mínimas no me hubieran facilitado el desarrollo y culminación del proyecto.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

Agradezco por la metodología de autoestudio gran herramienta cognitiva usada desde el inicio de la carrera que permitió desarrollar y aprender un nuevo mecanismo y transformación en mi ambiente pedagógico y tener la capacidad analítica en mi entorno personal y laboral.

CONTENIDO

GLOSARIO

Activos: Bien material que forma parte de la riqueza de quien lo posee, activo de información como datos e información o activos tecnológicos ejem: PC, Servidor, etc.

Backdoor: Aplicado al malware, los virus de puerta trasera son aquellos en los que los hackers acceden a funciones del ordenador de manera oculta y trabajan en segundo plano.

Cadena de suministro: La cadena de suministro es una serie de elementos involucrados en el proceso de fabricación y entrega del producto al cliente final, uniendo a varias empresas entre sí para poder satisfacer al consumidor.

Ciber-Agresión: Descripción de una amplia gama de comportamientos negativos en Internet y a través de dispositivos móviles.

Ciberdelincuentes: Persona que realiza actividades delictivas en internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.

Ciberdelito: El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Ciber-Política: Analizan la profundidad y finalidad del uso de Internet para el activismo político. Abarca todas las formas del software social, lo que incluye periodismo, búsqueda de fondos, uso de blogs, construcción de organizaciones y voluntariado.

Ciberseguridad: Una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones en el ciberespacio.

Confidencialidad: Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

Controles: Es el proceso diseñado para gestionar los riesgos de acuerdo con los parámetros de la empresa y las leyes del país, el cual debe ser llevado a cabo por todo el personal.

COVID-19: El COVID-19 es la enfermedad infecciosa causada por el coronavirus que se ha descubierto más recientemente.

Disponibilidad: Es el principio fundamental de la seguridad informática que asegura la fiabilidad y el acceso oportuno a los datos y recursos por parte de los individuos o personas autorizadas.

Exploit: Un error en el software que representa una brecha de seguridad.

Firewall: Un componente de hardware o software diseñado para bloquear el acceso no autorizado.

Información: Se conoce como el conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Infraestructura Critica: Infraestructura crítica es un término utilizado por los gobiernos para describir los activos que son esenciales para el funcionamiento de una sociedad y economía.

Integridad: La garantía de exactitud y fiabilidad de la información. Asegurando la integridad de la información y los datos se consigue prevenir cualquier modificación no autorizada de esta.

Inteligencia artificial: La inteligencia artificial es la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear.

Malware: Término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos, Gusanos, keyloggers, Botnets, Ransomware, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues.

Nube: Es el uso de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software.

Pharming: Redirigir el tráfico a un sitio web falso para capturar información confidencial de los usuarios.

Phishing: Técnica utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

Politicas: **Es** el conjunto de actividades que se asocian con la toma de decisiones en grupo, u otras formas de relaciones de poder entre individuos, como la distribución de recursos o el estatus.

Pymes: El término Pyme hace referencia al grupo de empresas pequeñas y medianas con activos totales superiores a 500 SMMLV y hasta 30.000 SMMLV.

SGSI: Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas de administración de la información.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios.

Spoofing: La suplantación de identidad o spoofing en términos de seguridad de redes, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

Tecnología Disruptiva: Es una innovación tecnológica que deja totalmente obsoletas las que se estaban usando hasta ese momento.

TI: La tecnología de la información es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos

TIC: Tecnologías de la información y las comunicaciones, son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.

Vulnerabilidades: Debilidad del sistema informática que puede ser utilizada para causar algún tipo de daño.

RESUMEN

La ciberseguridad ha sido el principal enfoque y tema critico en la cuarta revolución industrial, todos los procesos laborales, productivos se basan con el procesamiento y transformación digital, permitiendo mejores tiempos de respuesta y de procesamiento en conjunto a lo esperado por los objetivos corporativos, sin embargo, la seguridad en cuanto al almacenamiento y tratamiento de la información ha sido el mayor problema que muchas organizaciones sin importar el tamaño han sido afectadas.

Como especifica John Chambers [1]CEO de Cisco “Las empresas se dividen en dos categorías: las que ha sido hackeadas y las no lo saben”, este tipo de ataque ha crecido y evolucionado de igual forma o a escala a los avances tecnológicos, nunca es obsoletos los ataques, cada día se vuelven más robustos y el riesgo siempre estará presente.

Las vulnerabilidades o debilidades identificadas gracias a las mejoras practicas existentes en la infraestructura tecnológica será la prioridad del equipo TI, en resolver y crear controles que mitigan el impacto material que pueden ocasionar, se debe crear políticas, procedimientos para analizar, evaluar y controlar la seguridad de la información y aseguramiento de las aplicaciones y servicios (disponibilidad).

Lastimosamente se viene a implementar estos procedimientos de control y continuidad cada vez que ocurra un ataque o materialización de estos, se debe concientizar desde un inicio la implementación y desarrollo de los planes de ciberseguridad de forma preventiva y reactiva para minimizar los tiempos de respuesta en la solución y la afectación mínima del servicio.

Si a lo anterior le agregamos la condición actual del COVID-19 donde obligó a las pequeñas y medianas empresas a resurgir o a cambiar su modo de operación más apoyado en las tecnologías de información, claramente el factor de seguridad informática juega un papel fundamental en la cual es nuevo para muchas organizaciones y es de vital importancia que contextualicen y robustezcan el ámbito de la seguridad informática y a su vez integrado dentro de sus estrategias organizacionales.

Ya se ha visto en los primeros meses de la COVID-19. “Los delincuentes no han dejado pasar la oportunidad y muchos de los incidentes que se vienen observando desde el inicio de la pandemia están relacionados directamente con una mala implementación de las políticas de seguridad y de una configuración incorrecta de los accesos remotos o los permisos de los usuarios en una red corporativa”, destaca

[1] PANDA SECURITY, La ciberseguridad objetivo preferente de las empresas [Sitio WEB]La entidad [18, Marzo, 2015] Disponible en: https://www.pandasecurity.com/es/mediacenter/malware/la-ciberseguridad-objetivo-preferente-de-las-empresas/?utm_source=twitter.com&utm_medium=smedia&utm_content=SM_ES_TW_PNCIBERSEGURIDAD_180315&utm_campaign=genericCampaign

el responsable de concienciación y laboratorio de Eset, Josep Albors (2020). “Con las transferencias de datos de alta velocidad, los piratas informáticos tendrán la capacidad de infectar paquetes de datos y realizar espionaje corporativo sin que se den cuenta.[2]

La implementación de políticas y controles fundamentadas en las buena prácticas y estándares como la ISO 27001 y la ISO 27002 son estrategias claves para que las PYMES se mantenga en pie y existentes, para un futuro que claramente es una nueva realidad que hace dos años no pensábamos que fuera de esta forma.

La adaptación a las nuevas herramientas tecnológicas permite una adopción a la nueva revolución industrial completamente tecnológica y que a su vez tiene sus distractores o amenazas existentes en el escenario virtual y que de cierta manera tendremos que convivir con estas amenazas, pero siempre estar prevenido y preparado para afrontarlas.

Palabras claves: Ciberseguridad, COVID-19, PYMES, Resiliencia, Seguridad, Vulnerabilidad**.**

[2] PROTEGERSE, ¿Que nos depara un futuro incierto en materia de ciberseguridad? [Sitio WEB]La entidad [4, Diciembre,2020]Disponible en: https://blogs.protegerse.com/2020/12/04/tendencias-2021-que-nos-depara-un-futuro-incierto-en-materia-de-ciberseguridad/

ABSTRACT

The Cybersecurity has been the main focus and critical issue in the fourth industrial revolution, all labor and production processes are based on digital processing and transformation, allowing better response and processing times as a whole than expected by corporate objectives, without However, security in terms of storage and treatment of information has been the biggest problem that many organizations regardless of size have been affected.

The implementation of policies and controls based on good practices and standards such as ISO 27001 and ISO 27002 are key strategies for SMEs to remain standing and existing, for a future that is clearly a new reality that two years ago we did not think. that it was this way.

The adaptation to the new technological tools allows an adoption to the new completely technological industrial revolution, which in turn has its distractors or existing threats in the virtual scenario and that in a certain way we will have to live with these threats, but always be prevented and prepared. to face them

Keywords: Cybersecurity, COVID-19, PYME, Resilience, Security, Vulnerabilit

INTRODUCCIÓN

Hoy en día toda organización cuenta con una infraestructura tecnológica basada en software y hardware que brinda los servicios necesarios para la continuidad de la operación que brinda aplicaciones y herramientas para dar cumplimiento a los objetivos organizacionales, pero en muchos casos, detrás de toda la maquinaria tecnológica hay ausencia de la administración, gestión y controles con respecto a la seguridad informática (ciberseguridad), una ausencia de tal magnitud que puede acarrear en pérdidas económicas, legales, reputacionales y operativas.

El apoyo de la tecnología en los procesos corporativos y/o organizacionales es un hecho casi que obligatorio en función a la obtención de los objetivos de la organización, pero en muchas oportunidades se descuidan ciertos parámetros o barreras de seguridad que ayudan a blindar al entorno tecnológico de ataques como el robo de información o el bloqueo (denegación) de las diferentes plataformas tecnológicas ocasionando retrasos y aspectos negativos en la rentabilidad de la organización o peor aún no lograr alcanzar las metas propuestas y fracasar en el intento misional y visional de la organización.

Con el apoyo e implementación de algunos controles basados en la ISO 27002 se puede contemplar una barrera de blindaje o contención que puede ser aprovechada para estas pequeñas y medias empresas (PYMES) que están incursionando en conjunto con las nuevas tecnologías, a raíz que tuvieron que adaptarse a la digitalización, servicios electrónicos dada la pandemia y que una vez se reestablezca a la normalidad, será la nueva normalidad de estas organizaciones.

En complemento con las metodologías, estándares de ciberseguridad y mejores prácticas, se evalúa un estatus inicial de la infraestructura tecnológica donde se refleja la situación actual con respecto a las amenazas existentes y de cierta manera se puede corregir para no llegar a una materialización cuantificada en pérdidas o en su efecto a la desaparición completa de la pequeña y mediana empresa (PYMES).

Es un ejercicio casi que obligatorio que se debe cuestionar y aplicar en toda organización pequeña y mediana (PYMES), que permitirá conocer en que se debe mejorar y aplicar cambios inmediatamente para proteger los activos más valiosos de una organización, protegiendo a estas organizaciones frente a los ciberdelincuentes que están al asecho.

Definir e implementar estas barreras de seguridad como controles, actualización de parches, implementación de reglas de firewall, implementación de antivirus y otras herramientas de orden de seguridad permiten en especial un aumento significativo en la confianza y plena garantía del funcionamiento continuo de la plataforma tecnológica y protección de los datos e información, lo más valioso que tiene una organización como los son sus activos de información e infraestructura.

Creando una estrategia robusta enfocada en ciberseguridad desde la gobernabilidad de la organización para ayudar a las organizaciones a mantener un entorno de seguridad informática sustentable en el trabajo.

Para nadie es un secreto que lo vivido en el 2020 durante el inicio y desarrollo de la pandemia el número de ataques cibernéticos crecieron exponencialmente, ataques como Phishing (Robo de Credenciales), suplantación, ataques de ransomware fueron el día a día de los ciberdelincuentes, cabe aclarar que estos ataques han estado presentes en el ciberespacio hace mucho tiempo antes de la Pandemia y sus objetivos eran las empresas u organizaciones que en su mayoría tienen un portal público web o tienen servicios web para sus clientes.

La situación de 2020 fue tan crítica que el 85% de los CISOs admitieron que sacrificaron la ciberseguridad para permitir que los empleados trabajaran de forma remota rápidamente, según una investigación de Netwrix también reveló que una de cada cuatro empresas considera que corre un mayor riesgo de ciberseguridad ahora que antes de la pandemia y el 54% de los CISOs admitieron no tener la visibilidad necesaria para garantizar una protección de datos adecuada.[3]

Con la situación actual del COVID-19, muchos se reinventaron (cambiaron su forma habitual de trabajo o de prestar el servicio) desde casa con apoyo de las tecnologías y esto permitió que estuvieran en el ojo del huracán para los ciberdelincuentes aprovechando la poca implementación de herramientas, configuraciones y bases de ciberseguridad en sus páginas web, en sus pasarelas de pagos incluso en sus procesos internos.

[3] NETWRIX, Survey: 85% of CISOs admit they sacrificed cybersecurity to enable employees to work remotely [Sitio WEB]Irvine, CA,La entidad [22, Septiembre,2020], Disponible en: https://www.netwrix.com/netwrix_survey_cisos_admit_they_sacrificed_cybersecurity_to_quickly_enable_employees_to_work_remotely.html

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La carencia de procedimientos, controles, políticas y lineamientos basados en seguridad informática sobre la infraestructura tecnológica en las organizaciones.

La vulnerabilidad de los sistemas de información e infraestructura de servicios tecnológicos.

Los incidentes que se presentaron durante el año 2013, donde los servicios de mensajería instantánea, redes sociales, los sistemas gubernamentales y militares de varios países, universidades, hospitales, divulgación de información privada fueron alguna de los miles de ataques que se produjeron, constatando que cada año los incidentes de seguridad son más en cantidad, mayormente agresivos y con un mayor impacto de criticidad a los activos informativos de los ciudadanos.[4]

Durante y posterior al desarrollo de software siempre existirán vulnerabilidades que pueden ser atacadas, estas son mitigadas o controladas por medio de actualizaciones o parches de seguridad que implica la modificación de la aplicación atreves de la red por un tercero que de igual forma puede dejar expuesta la herramienta.[5]

El ataque a las infraestructuras criticas (todo sistema de uso masivo nacional que administra o gestiona servicios básicos como la registraduría, organismos de control como los impuestos, sistemas de alertas tempranas meteorológicas, sistemas de control vial y Aero entre otras.) se ha vuelto muy recurrente este tipo de ataque y al parecer implican a los gobiernos extranjeros, una guerra ciber-política y ciber agresión.[6]

El boom de la internet de las cosas, de la interconexión de todo equipo eléctrico con internet permite una expansión de redes y dispositivos interconectados en la palma de la mano con el beneficio de controlar ciertos aspectos hogareños como el clima, luces, refrigerados incluso hasta la misma seguridad física de las locaciones, tiene sus ventajas pero de igual forma trae consigo una serie de riesgos que hoy en día los ciberdelincuentes están aprovechando sin escrúpulos, por ejemplo

[4] DE SALVADOR CARRASCO, Luis. Los problemas estructurales en el planteamiento de la ciberseguridad. En: Boletín Electrónico del Instituto español de Estudios Estratégicos, 2014, p. 1-27.

[5] STORM, Darlene. Downloading of software updates for lifesaving medical devices proves very dangerous.[en Linea][19, Junio, 2012], Disponible en: http://blogs.computerworld.com/malware-and-vulnerabilities/20554/software-updates-lifesaving-medical-devices-found-tainted-malware

[6] BAKER, Stewart. Et al. En el punto de mira: las infraestructuras críticas en la era de la ciberguerra McAffee.[en linea]Madrid España,[2010] Disponible en: http://img.en25.com/Web/McAfee/CIP_report_final_es_fnl_lores.pdf

recientemente se ha descubierto vulnerabilidades en los TV inteligentes que permiten espiar con imagen y sonidos a los usuarios.[7]

Según John Chambers CEO de Cisco, define un punto débil frente a la Ciberseguridad "siempre creeré en el poder de la tecnología de transformar los negocios y la vida de las personas, no se puede negar que las nuevas tecnologías también crean nuevos riesgos de seguridad. Hemos visto esto con el aumento de las vulneraciones de datos y temas de privacidad en años recientes. La seguridad debe ser un componente inherente de todas las estrategias de digitalización"[8]

"Ya no existen soluciones sencillas a problemas sencillos", destacó Chema Alonso, director de Datos de Telefónica, quien subrayó que es necesario aceptar la complejidad de los ataques para ser capaz de gestionar personas, tecnologías y procesos "asumiendo que vas a ser golpeado, pero resolviendo la amenaza". De hecho, según Alonso, cualquier empresa corre el riesgo de ser atacada, ya que no existe el 100% de la seguridad frente a la ciberdelincuencia: "La tecnología siempre va a tener límites. Si alguien dice que conseguirá una seguridad total, te está engañando", aseguró el responsable de Telefónica. Sin embargo, el 77% de la empresa no cuenta con plan de respuesta**.**[9]

Las pequeñas y medianas empresas ahora afrontan un boom de apoyo en relaciona las nuevas tecnologías desde la publicación de sus productos y/o servicios hasta la etapa final de la transacción del bien o servicio por medio de las plataformas tecnológicas, este nuevo paradigma ha volcado a muchas de estas empresas se enfrenten con nuevo gigante que en consecuencia trae beneficios pero que de igual forma trae consigo mismo ciertos riesgos a los que no están exentos de padecer.

Incluso el modelo de trabajo que se optó en Pandemia (Trabajo Remote Office y Home Office), abrió o expandió una brecha de seguridad, ya que muchas empresas no estaban preparadas para trabajar en esta modalidad por ausencia en controles o políticas en su infraestructura tecnológica y la cultura del empleado para trabajar en estos entornos.

El 2020 pasará a la historia como el punto de partida de la carrera digital. Para los que tenían dudas de apostar por la automatización, la nube, la inteligencia artificial

[7] NEWS, Who´s watching whom? Camera-equipped TV can be hacked, says researcher[Sitio WEB],La entidad [13, Diciembre,2012], Disponible en: https://www.nbcnews.com/technology/whos-watching-whom-camera-equipped-tv-can-be-hacked-says-1C7596675

8 El economista, Leccionesde un CEO,segun John Chambers de Cisco, [Sitio WEB], la entidad [1, Diciembre 2019], Disponible en: https://www.eleconomista.com.mx/tecnologia/Lecciones-para-un-CEO-segun-John-Chambers-de-Cisco-20191201-0009.html

9 El mundo, Hay dos tipos de empresas: a las que han atacado y las que atacaran [Sitio WEB], la entidad [3, Octubre 2018], Disponible en: https://www.elmundo.es/comunidad-valenciana/2018/10/03/5bb3acf4268e3ef5548b45af.html

y la fuerza laboral 'líquida', fuera de la oficina, el COVID-19 ha quitado una venda que muchos no querían retirar. De hecho, el 62% de las empresas ha confesado recibir más ataques desde el comienzo de la pandemia, según datos de Deloitte (2020).[10]

Es más, se han incrementado en sectores tan vulnerables, en estos momentos, como el de la sanidad, donde varias organizaciones han sufrido robos de información y ransomware (software malicioso que secuestra un dispositivo a cambio de un rescate) inutilizando sus sistemas.

La divulgación de información personal, las transacciones monetarias y hasta los accesos restringidos son las nuevas realidades a las que deben afrontar estos nuevos participantes en el ecosistema digital.

Un problema teniendo en cuenta los principales patrones de amenaza que se detectaron, gran parte fruto de errores humanos: phishing o suplantación (48%), errores de administración (27%) e intercambio inadecuado de datos por parte de los empleados (26%). Los compromisos de la cadena de suministro se tardaron más en detectar: el 55% necesitó días, semanas o incluso meses para registrar estos incidentes.[11]

Según Correios Braziliense (2020) el número de víctimas de delitos cometidos por Internet aumentó durante el período pandémico. El aumento del periodo en el que las personas pasan online y los nuevos comportamientos impuestos por el nuevo coronavirus, como la mayor adherencia de la población a las compras por Internet, han contribuido a la acción de los delincuentes. Según registros de la Policía Civil del Distrito Federal (PCDF), entre marzo y junio de 2020, los delitos de estafa cometidos por internet aumentaron un 198,95%. Los robos por fraude aumentaron un 310,97%. De marzo a junio de 2019, hubo 82 mientras que, en el mismo período de 2020, se registraron 337 ocurrencias. Según Jornal Daqui (2020) En Minas Gerais, el número de delitos cibernéticos aumentó en casi un 50% en comparación con el año pasado. Según datos de la Policía Civil, de enero a mayo de este año se registraron 3.070 casos de ciberdelito, casi 606 más que en el mismo período de 2019.[12]

[10] DELOITTE, El estado de la ciberseguridad en España: Digitalización, teletrabajo y ciberataques en tiempos de pandemia [Sitio WEB], la entidad [2020], Disponible en: www2.deloitte.com/es/es/pages/risk/arti-cles/estado-ciberseguridad.html

[11] VERA, J. M. Ciberseguridad post-Covid : ¿Qué papel jugará la ciberinteligencia frente a los cisnes negros digitales que llegarán tras la vacuna? En: Journal of Economic & Business Intelligence, 2021. 11–23.

[12] BARBOSA, J. S., Silva, D. B. e, Oliveira, D. C. de, Jesus, D. C. de, Miranda, W. F. de, Research, Society and Development. En: Protección de datos y seguridad de la información en la pandemia COVID-19: contexto nacional, 2021 Vol. 10 No. 2; e40510212557

1.2 FORMULACIÓN DEL PROBLEMA

Las PYMES en Colombia y más específicamente las del sector comercial no están preparadas para afrontar ataques de ciberseguridad, dado que hoy en día están adoptando nuevas formas de trabajo en apoyo de las herramientas tecnológicas sin considerar los riesgos existentes en el medio.

Las PYMES representan el 28% del PIB del estado, conforma el 67% del empleo y el 37% de la producción nacional, alrededor del 20% de las PYMES está en riesgo de cierre debido a la pandemia.[13]

¿Cuáles son las políticas y controles mínimas de Seguridad de la información que deben considerar las PYMES del sector comercial en Colombia frente a la nueva realidad del COVID-19 y una posterior normalidad?

Para nadie es un secreto que hoy en día las pequeñas y medianas empresas comerciales están afrontando nuevos retos frente a la Pandemia del COVID-19, incursionando en el mundo de la tecnología, la virtualidad, el comercio electrónico, herramientas que están disponibles en el momento y que tienen una gran demanda para las PYMES en estos tiempos de incertidumbre, prestando un apoyo incondicional y de cierta forma obligando a estas organizaciones a cambiar de paradigma, incluso a cambiar su esquema de organización y de operación para lograr mantenerse en el campo y subsistir.

El apoyo de la tecnología ha logrado mantener ese equilibrio de mantenerse en el mercado y no desistir o fallecer como organización, sin embargo, esta adaptabilidad a la nueva tecnología puede traer consecuencias negativas en la organización, por encontrar una solución, puede encontrarse con una gran variedad de problemas que afectan los intereses de la organización.

Esos aspectos negativos o problemáticas que pueden surgir radican de la seguridad informática de la organización, es la razón de ser de los activos, datos e información que gestiona y administra la organización. Una organización sin datos ni activos básicamente no existe.

Debido a la cuarentena impuesta por COVID-19, los datos, la protección y la seguridad de la información se han vuelto vulnerables. A toda prisa, las personas y las organizaciones tuvieron que adaptarse al trabajo remoto, debiendo lidiar con la

[13] RODRIGUEZ PINZON, É. Impacto económico, social y político de la COVID-19.[en linea] Madrid España, [30, Abril, 2020] Disponible en: https://doi.org/10.33960/ac_24.2020

logística de personal, dispositivos y otros equipos. Y así, surgieron ciberataques en la pandemia COVID-19.[14]

La tecnología es cada vez más avanzada y, durante la pandemia de COVID-19, en la que las personas y las organizaciones tuvieron que reinventar, el ciberdelito, ganaron espacio en las redes. Como resultado del aislamiento social, las personas están más conectadas y terminan asumiendo más riesgos, por lo que surgieron diferentes ciberataques durante la pandemia COVID-19.

Y claramente es entendible el aumento significativo de los ataques cibernéticos dado que las PYMES no están preparadas para afrontar estos retos y vulnerabilidades ya que no cuentan con el personal idóneo y/o las capacidades para identificar estos riesgos e implementar controles de seguridad.

Su prioridad son sus ventas y servicios se mantengan en este escenario de pérdida o desaparición total del negocio, y recurren a la tecnología para solventar esta deficiencia, pero no son conscientes que este escenario y/o espacio virtual tiene sus amenazas y que los ciberdelincuentes están al acecho para actuar aprovechando sus vulnerabilidades.

Según Gatefy (2020) Según la agencia europea, las campañas de phishing y spam se han utilizado ampliamente para recopilar credenciales y otros datos personales y confidenciales. Además, los correos electrónicos se utilizan para infectar a los usuarios con software malintencionado o malware. Con el fin de extorsionar dinero y robar datos confidenciales y personales, los piratas informáticos aprovecharon el escenario de pánico causado por el COVID-19 para distribuir malware, ransomware y aplicaciones maliciosas dirigidas a personas, empresas y otras organizaciones. En la web oscura, en el contexto de la pandemia.

Si la sofisticación de los ataques supera las capacidades defensivas de los equipos, los altercados provocarían pérdidas y daños más graves.

Para proteger a empresas y a la sociedad en general de los efectos negativos debe establecerse un marco de colaboración entre sectores públicos y privados. Se necesita la colaboración global de las autoridades para elaborar nuevas estrategias que sustituyan a las tradicionales, ya obsoletas.[15]

---

[14] BARBOSA, J. S., Silva, D. B. e, Oliveira, D. C. de, Jesus, D. C. de, Miranda, W. F. de, Research, Society and Development. En: Protección de datos y seguridad de la información en la pandemia COVID-19: contexto nacional, 2021 Vol. 10 No. 2; e40510212557

[15] PANDA SECURITY, La ciberseguridad objetivo preferente de las empresas [Sitio WEB], La entidad [18, Marzo, 2015] Disponible en: https://www.pandasecurity.com/es/mediacenter/malware/la-ciberseguridad-objetivo-preferente-de-las-empresas/?utm_source=twitter.com&utm_medium=smedia&utm_content=SM_ES_TW_PNCIBERSEGURIDAD_180315&utm_campaign=genericCampaign

Con los adelantos tecnológicos y las innovaciones frente a la seguridad tecnológica no se podría decir que una aplicación, herramienta, servicio o infraestructura está al 100% protegida de algunos de los ataques existentes, siempre existirá los riesgos dado que la tecnología avanza a pasos gigantes y muchas veces están uno o dos pasos adelante para cometer actos delictivos como el secuestro, robo de información o la denegación de servicio.

Pero toda organización incluso personalmente se deben implementar estrategias basadas en seguridad informática existentes por medio de las buenas prácticas, estándares y políticas que de cierta forma aseguren la integridad, disponibilidad y confidencialidad de la información.

La sensibilización en transmitir las bases fundamentales como la no divulgación de información personal y la importancia que tiene la seguridad de nuestras aplicaciones, nuestra información personal y laboral es super clave en la construcción y aporte para las estrategias que buscan de cierta forma no completamente blindar las infraestructuras tecnológicas

“La Ciberseguridad ya no es una opción. La dependencia de las sociedades occidentales de sus sistemas de información (públicos y privados) es de tal magnitud que no puede abordarse ningún proyecto de interés nacional que no contemple la seguridad de los sistemas de información, la información tratada y los servicios prestados, como requisitos tan importantes como la propia prestación de aquellos servicios”.[16]

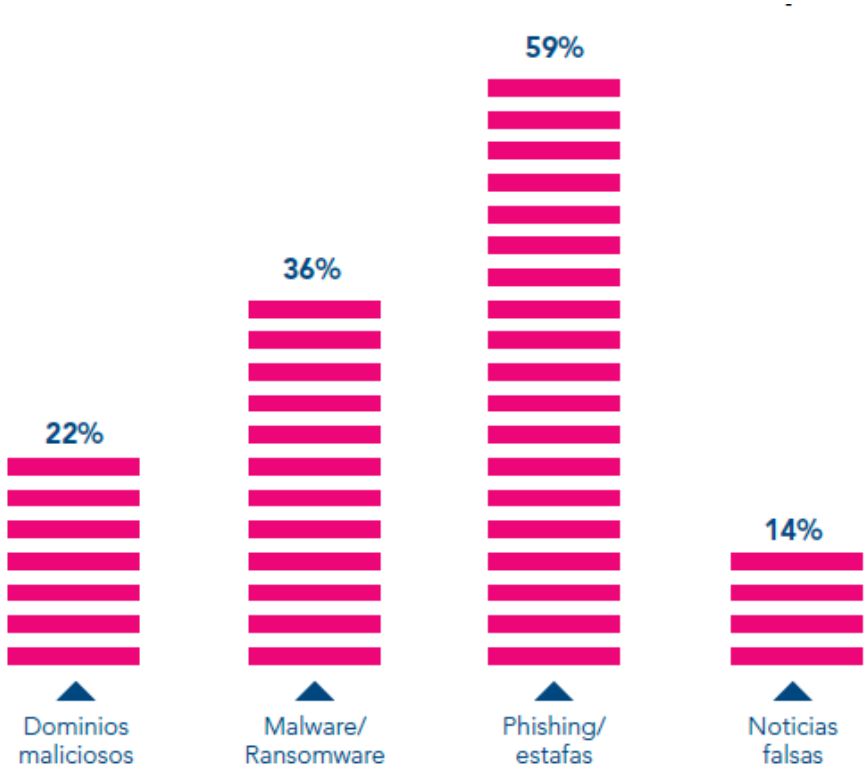
De acuerdo con la información de Diana Arias, los ciberdelitos durante el 2020 llegaron a más de 45.000 casos, un incremento del 89 % frente al año anterior. Este fue el año de mayor ascenso en cifras e impacto en Colombia. Durante el periodo denominado COVID-19 (marzo – diciembre 2020), se presentó un incremento del 101%, con más de 37.000 reportes en el número de noticias criminales instauradas ante la fiscalía general de la Nación.[17]

El delito que mayores denuncias presentó fue la suplantación de sitios web para capturar datos personales con un crecimiento del 303%, comparado con el 2019. Este delito tiene una relación directa con modalidades conocidas, tales como el Phishing, Spoofing y Pharming que sufrieron las empresas. Adicionalmente, hubo 5.440 casos denunciados donde este tipo de ataques fue utilizado por los cibercriminales para capturar datos personales o dispersar malware en las redes corporativas. “La ciberseguridad es el área que mayor atención deberá tener en el

[16] GALAN, C. M., & Galán Cordero, Derecho & Sociedad, La ciberseguridad pública como garantía del ejercicio de derechos.[en línea] 2016 (47), 293-306.Disponible en: http://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/18892

[17] ARIAS, Diana.Ciberseguridad: uno de los retos que dejo el 2020 [en linea], 28, Enero, 2021. Disponible en: https://www.enter.co/guias/lleva-tu-negocio-a-internet/ciberseguridad-uno-de-los-retos-que-dejo-el-2020/

2021, pues un gran número de colaboradores seguirán operando desde sus hogares", asegura Adriana Ceballos, directora de desarrollo de programas del Tanque de Análisis y Creatividad de las Tic (TicTac).



El segundo delito fue la violación de datos personales, con 9.487 casos registrados. Este presentó un crecimiento del 174% como consecuencia de la filtración y robo de datos, lo que generó un doble impacto que compromete aspectos operativos, así como legales y de cumplimiento por la pérdida de información sensible.

Seguido, se encuentra el hurto por medios informáticos, con un crecimiento del 37% y que registró más de 16.000 casos denunciados. Pese a tener la mayor frecuencia estadística, la modalidad más común sigue siendo el apoderamiento de credenciales para el acceso a servicios de banca online, con los cuales los cibercriminales, consiguen suplantar al titular del producto bancario y apoderarse del dinero generalmente dispuesto en cuentas bancarias.

Estos ciberataques afectaron por igual diferentes sectores productivos del país, los métodos de propagación continúan siendo las campañas de Phishing que contienen archivos adjuntos maliciosos. Las entidades de gobierno con mayor presencia de trámites en línea también se vieron afectadas, entre ellos, la Administración de

Impuestos y Aduanas, la Registraduría Nacional del Estado Civil, la Fiscalía General de la Nación y las autoridades de tránsito.[18]

[18] ARIAS, Diana. Ciberseguridad: uno de los retos que dejo el 2020 [en linea], 28, Enero, 2021. Disponible en: https://www.enter.co/guias/lleva-tu-negocio-a-internet/ciberseguridad-uno-de-los-retos-que-dejo-el-2020/

2 JUSTIFICACIÓN

La seguridad es un factor crítico en toda organización, “La perdida, manipulación, divulgación o falta de disponibilidad, causada por incidentes de seguridad, puede dar lugar a gastos, consecuencias legales”. Se requiere acciones desde la planeación y desarrollo en conjunto con las operaciones de la organización para reducir este tipo de riesgos.[19]

Un análisis de riesgo es necesario contar con “Medidas coordinadas a lo largo del tiempo”, llamadas controles de seguridad, su fin es el mantenimiento de riesgos dentro de los umbrales aceptables de la organización.[20]

La seguridad de la información tiene que ver con proteger la información del acceso no autorizado. Es parte de la gestión de riesgos de la información e implica prevenir o reducir la probabilidad de acceso, uso, divulgación, interrupción, eliminación, modificación, inspección o registros no autorizados.

La ciberseguridad es un tema pilar e importante en una organización, que al mismo tiempo se convierte en un tema de preocupación dado que “Hoy en día, es una actividad compleja, caracterizada por ataques persistentes a gran escala que permiten entrar en las redes internas empresariales, generando pérdidas económicas, robo de información crítica, caída de los servicios, e incluso llegando hasta la pérdida de la imagen y prestigio de la empresa”[21]

El impacto negativo que se tendría posterior a un ataque es considerado en perdidas financiera, legales, reputacionales, son aspectos altamente nocivos para los interés y objetivos de las organizaciones.

Toda organización incluso personalmente se deben implementar estrategias basadas en seguridad informática existentes por medio de las buenas prácticas, estándares y políticas que de cierta forma aseguren la integridad, disponibilidad y confidencialidad de la información.

La sensibilización en transmitir las bases fundamentales como la no divulgación de información personal y la importancia que tiene la seguridad de nuestras aplicaciones, nuestra información personal y laboral es super clave en la

[19] VERA, Víctor Daniel Gil; VERA, Juan Carlos Gil. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia et technica,[en linea] 2017, vol. 22, no 2, p. 193-197.

[20] RODRÍGUEZ, David E. Acosta. Categorización funcional de los diferentes tipos de controles de seguridad y su aplicabilidad en la estrategia de protección corporativa. Revista SIC: ciberseguridad, seguridad de la información y privacidad,[en linea], 2018, vol. 27, no 130, p. 122-124.

[21] REA-GUAMAN, M., Calvo-Manzano, J. A., & Feliu, T. S. (2018). Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas. (Spanish). CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 1–6.

construcción y aporte para las estrategias que buscan de cierta forma no completamente blindar las infraestructuras tecnológicas.

En la actualidad todo proceso o ejecución de funciones dentro de una organización están apoyadas de la infraestructura TI, se depende casi que completamente de la infraestructura, que si por algún motivo se comprometa en temas de seguridad como un ataque o robo, inmediatamente tendrá un repercusión en la operativa del servicio, por eso es importante blindar de cierta forma la infraestructura TI, objetos tecnológicos frente a las diferentes amenazas internas y externas, no se limita a eliminar completamente el riesgo pero si a controlarlo, minimizando en lo posible dentro del umbral definido (capacidad de la organización dispuesto a perder o asumir).

Debido a la coyuntura económica y sanitaria actual, los ciberdelincuentes son conscientes que existen puertas abiertas de números dispositivos y sistemas informáticos, coincidiendo que la ciberseguridad es una tarea pendiente de muchas empresas y especialmente para las PYMES e independientes.

Según Castellano Vega la información de las empresas está siendo tratada por trabajadores que utilizan sus propios dispositivos BYOD y la famosa internet de las cosas, donde todo esta interconectado a las redes externas lo que supone una enorme debilidad en seguridad y una llamada perfecta de acción para los ciberdelincuentes.[22]

Como era de esperar, el mayor impacto del cibercrimen a lo largo del año, según un informe de Crowd Strike (2020), ha sido por la masiva adopción del teletrabajo. Ello ha supuesto que, en el 30% de los incidentes, las soluciones de antivirus no estuvieran correctamente configuradas, tenían activada la seguridad más débil o ni siquiera protegían el entorno corporativo completo. Las soluciones tradicionales fallaron en la prevención del 40% de los incidentes, ya sea debido a errores de detección de malware o a que alguna secuencia del ataque no fue descubierta por la herramienta, destaca su informe.[23]

Los días de la seguridad fragmentada han quedado atrás y la protección digital debe ser más proactiva y preparada para el futuro si queremos superar en innovación a los atacantes.

Quizá la pandemia pase, pero la que se quedará será la pandemia cibernética fruto de conectarlo todo y a todos sin una mínima seguridad. El COVID-19 no ha hecho

[22] CASTELLANOS VEGA, Carlos Jacinto, et al. Modalidades de cibercrimen en tiempos de Pandemia Covid-19 en Bogotá (Colombia).

[23] BUSSELEN, M. Por qué el ciberdelito sigue siendo un desafío empresarial preocupante en un mundo blo-queado por COVID.[en linea] [septiembre 2020]. Disponible en: www.crowds-trike.com/blog/why-cybercrime-remains-a-worrying-business-challenge-in-a-covid-lockdown-world.

sino agudizar el preocupante estado cibernético mundial. En su "Informe de riesgos globales 2020", el Foro Económico Mundial (WEF), establece que el cibercrimen será el segundo riesgo más preocupante para el comercio mundial durante la próxima década, el séptimo riesgo con mayor probabilidad de ocurrir y el octavo con mayor impacto.[24]

En la situación actual de Pandemia, las empresas necesitan más que nunca transmitir confianza plena sobre sus servicios y forma de responder frente a las nuevas necesidades y escenarios, y los compradores desde los consumidores necesitan confianza para la toma de decisiones y seguridad al adquirir su producto o servicio. De esta forma se puede ejercer en el mercado como lo exige.[25]

Es por ello por lo que se requiere de manera urgente y prioritaria identificar de todas las normas, políticas, procedimientos existentes en las grandes empresas, sustraer los requerimientos básicos que deberían considerarse como un estándar para ser aplicados a las PYMES del sector Comercial, estas PYMES la gran mayoría carece de riesgos, controles, metodologías que permitan estar conscientes del grado de exposición al que se enfrentan.

[24] World Economic Forum. Future Series: Cibersegu-ridad, tecnología emergente y riesgo sistémico[Sitio WEB] [Noviembre, 2020], Disponible en: www.weforum.org/reports/future-series-cybersecu-rity-emerging-technology-and-systemic-risk.

[25] RISS, Boris Delgado; SÁNCHEZ, Carlos Manuel Fernández.Revista SIC: ciberseguridad, seguridad de la información y privacidad. Las mejores prácticas ISO contra el Covid-19 y crisis futuras. 2020, vol. 29, no 140, p. 94-96.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las políticas y los controles mínimos básicos de seguridad de la información por medio de una revisión documental basada en escenarios COVID-19 para controlar y minimizar impactos negativos en la seguridad de los principales activos tecnológicos de una PYME colombiana del sector comercial.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar las normas y estándares de seguridad de la información ISO 27001 y 27002 por medio de una revisión documental aplicado a escenarios COVID-19 para identificar las mejores prácticas en cuanto a procedimientos y controles.

- Identificar las políticas y controles mínimas básicas que pueden ser aplicados a una PYME colombiana del sector comercial bajo un escenario COVID-19 por medio de una revisión de casos estudio, para extractarlas como un lineamiento o base que debería implementarse como mínimo en un SGSI.

- Reconocer los diferentes ataques de ciberseguridad que tendrán mayor impacto sobre las PYMES para prepararse a una respuesta inmediata y efectiva por medio de las revisiones de casos de estudio.

- Extraer las mejores prácticas y recomendaciones en función de mantener la seguridad de los principales activos tecnológicos en las PYMES en Colombia del sector comercial en tiempos COVID-19.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

PYMES

Una de las organizaciones con mayor proyección y crecimiento, por múltiples factores, a nivel mundial con las Pequeñas y Medianas Empresas (PYME). Estas fueron creadas a mediados de los años 50 a raíz de las crisis económicas de las grandes organizaciones y en respuesta a los avances tecnológicos

Sus respuestas son más efectivas, rápidas y económicas en comparación con las grandes empresas. En este sentido, según Márquez, A. y Pérez, L (2007) comentan que estas desempeñan un importante papel ya sea mediante la dinamicidad que aporta al sistema económico, su contribución al empleo, su aporte al Producto Interno Bruto (PIB) o al enriquecimiento del proceso innovador (citado por Martínez, 2010).

Las PYMES en Colombia

De acuerdo con la ley 905 del 2004, para clasificar a las micro y las PYMES se tienen en cuenta dos criterios, el valor de los activos y el número de empleados.

Las microempresas: hasta 10 empleados y activos inferiores a los 500 salarios mínimos legales mensuales vigentes.

La pequeña empresa: Desde 11 hasta 50 empleados y sus activos rondan entre 501 y 5.000 salarios mínimos mensuales vigentes.

La mediana empresa: Desde 51 hasta 200 empleados y sus activos rondan desde los 5001 hasta 30000 salarios mínimos mensuales vigentes.[26]

Las PYMES mantienen su comportamiento en Colombia, como en la mayoría de los países de la región. En 2004 representaban el 96% de las empresas del país, generaban el 66% del empleo industrial, realizaban el 25% de las exportaciones no tradicionales y pagaban el 50% de los salarios, de acuerdo con los datos del Ministerio de Desarrollo (Velásquez, 2004).[27]

[26] BANCOLOMBIA, Conoce todo sobre las pymes en Colombia [Sitio WEB], Colombia, La entidad [18, Julio,2018], Disponible en: https://www.grupobancolombia.com/wps/portal/negocios/actualizate/legal-y-tributario/todo-sobre-las-pymes-en-colombia

[27] VELASQUEZ V., F. La estrategia, la estructura y las formas de asociación: fuentes de ventaja competitiva para las Pymes colombianas. Estudios Gerenciales. 2004 093, 73-97.

Sistemas de información

Según Calder y Watkins (2019) las organizaciones consideran implementar un buen presupuesto para invertir en los sistemas de información y con ello posicionarse en el mercado, ser modelos de la competencia y tener un acercamiento más detallado y personalizado frente a los clientes y proveedores, todo ello demarcado en el manejo de la información, este manejo contempla los tres principales pilares como la disponibilidad, integridad y confidencialidad de los datos y la información que maneje las organizaciones.[28]

Principios de seguridad de la información. Fuente: Ticsalborada.

De acuerdo con lo descrito anteriormente, la información física y digital desempeña un rol importante ya que es el activo clave de toda organización y siempre se ha considerado desde la implementación de las nuevas tecnologías, ahora todas las organizaciones sin importar su tamaño claramente tienen en su organización el apoyo de las tecnologías e indudablemente estas las vuelve participe de lo vulnerable que pueden ser.

Si una empresa no administra adecuadamente su información, estará altamente vulnerable a los riesgos lo que podría afectar la continuidad del negocio. Por ello, es importante que se establezca mecanismos de seguridad para proteger la información (Gómez y católico, 2010).[29]

Nuevamente la importancia de implementar mecanismos de seguridad es vital para mantener a las organizaciones protegidas de los ciberdelincuentes.

[28] CALDER, A. y Watkins, S. Information Security Risk Management for ISO 27001/ISO 27002.IT Governance Publishing Ltd. United Kingdom. 2019

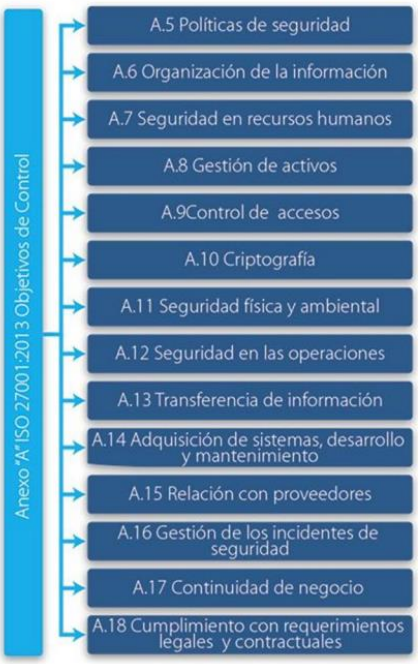
[29] GOMEZ, F. y católico, D. Relación de la presentación de información de negocios online con las variables financieras en las empresas colombianas. Revista Facultad de Ciencias Económicas: Investigación y Reflexión [en linea] (2010). Disponible en: https://bit.ly/2RtJRp3

ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.

También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.[30]



[30] 27001 ACADEMY,Que es norma ISO 27001[Sitio WEB],La entidad, Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

IMPLEMENTACION ISO 27001

De acuerdo con una investigación sobre la aplicación de la ISO 27001 y su influencia en la seguridad de la información a una empresa privada en Perú se pudo determinar:[31]

Frente a la pregunta ¿cómo influye la aplicación del ISO 27001 en la confidencialidad de la seguridad de la información de una empresa privada?, los expertos señalan que la protección de los datos y la información es la prioridad y gran diferencial con respecto a las demás organizaciones. La confidencialidad es la razón de ser de las organizaciones, la confianza que generan las organizaciones en cuanto seguro esta los datos, por ello se debe prevenir la divulgación no autorizada de la información empresarial. Es relevante que las empresas grandes, medianas o pequeñas apliquen ISO 27001 y 27002 de acuerdo con su ámbito ya que esta norma orientará como manejar los aspectos de seguridad de la información y evaluarán su situación actual y como pueden ir evolucionando en el tiempo, todo se trata de una mejora continua.

Toda empresa posee información confidencial, por lo tanto, debe resguardarla hasta de sus propios colaboradores cuando se debe aplicar los mínimos requeridos; ellos deben ser conscientes de lo relevante que es el adecuado manejo de la información que generar en sus labores diarias. Muchas empresas grandes, medianas y pequeñas aplican normas internacionales y con ello analizan su situación actual frente a una situación deseada, tomando como base los pilares de la seguridad informática como son la confidencialidad, la integridad y disponibilidad.

Con relación a la pregunta ¿cómo influye la aplicación del ISO 27001 en la integridad de la seguridad de la información?, los entrevistados afirmaron que al aplicar ISO 27001 en una organización, a través de los dominios de esta norma, se evalúa la integridad de la seguridad de la información, esto implica que deben existir mecanismos, políticas, directivas conocidas por los colaboradores de las diferentes áreas orientados a prevenir modificaciones no autorizadas de la información que se maneja.

Evidentemente, los resultados obtenidos en relación con la integridad de la seguridad de la información validan lo expuesto anteriormente; ya que, si una organización no implementa políticas o normas para el desarrollo de sus procesos, éstos marcharán a la deriva y expuestos a altos riesgos.

Finalmente, y a la consulta ¿cómo influye la aplicación del ISO 27001 en la disponibilidad de la seguridad de la información?, las afirmaciones revelan que el aplicar el ISO 27001 en una organización impacta en la disponibilidad de la

[31]RODRIGUEZ BACA, L. S., Puente de la Vega, C. F. C., Mejía Corredor, C., & Alarcón Diaz, M. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. (Spanish). Propósitos y Representaciones, 8(3), 473–483

seguridad de la información, ya que es uno de los pilares de la seguridad de la información y sostiene que es necesario que la información debe ser accedida por usuarios autorizados. Se comenta también que la información de la organización se encuentra vulnerable a ataques, modificaciones y otros tipos de daños. La disponibilidad hace referencia a que los datos, información debe estar a disposición de los usuarios de forma oportuna y según los privilegios o accesos que se les haya asignado.

De acuerdo a la investigación anterior se define y se apuesta por un evidente cambio en la implementación de los lineamientos sobre la ISO 27001 y 27002, asegurando los principales pilares de la seguridad como lo es la Disponibilidad, la integridad y disponibilidad, controles tan claros y fundamentales como proteger la información, prevenir la divulgación no autorizada y limitar la información solo a los usuarios autorizados claramente es necesario en toda organización sin importar su tamaño y debe ser considerada aún más para las PYMES que están cambiando su modelo de negocio apoyado en la tecnología.

CICLO DE MEJORA CONTINÚA EN LA NORMA ISO/IEC 27001:2013

1. Plan: Consiste en planificar acciones para hacer frente a los riesgos e identificar las oportunidades, para posteriormente evaluarlas y gestionarlas.

- Definir las políticas de seguridad de la información.
- Establecer el alcance del SGSI.
- Realizar el análisis de riesgo.
- Seleccionar los controles de seguridad.
- Definir competencias.
- Establecer el mapa de riesgos.
- Definir autoridades y responsabilidades.

2. Hacer: Indica que la organización debe de disponer los recursos necesarios para establecer, implementar y mantener el SGSI, además de dar a conocer las políticas de seguridad de la información del SGSI.

- Poner en marcha el Plan de gestión de riesgos establecido.
- Se implanta el SGSI.
- Se establecen los controles de seguridad.

3. Check - Controlar:

- Revisar internamente el SGSI.
- Realizar auditorías.
- Se revisan los indicadores y métricas del SGSI.

4. Actuar:

- Realizan las acciones correctivas.
- Realizan las acciones preventivas.

Las TIC y el teletrabajo en tiempos de Pandemia.

Según las naciones unidas, La digitalización es clave en el escenario actual donde muchas personas se vieron obligadas a trabajar desde casa, optando por la virtualidad y herramientas digitales. Asimismo, la digitalización no solo es una herramienta que le va a permitir a las PYMES adaptarse a una crisis como la que se está viviendo, sino que puede suponer un impulso para fomentar la sostenibilidad dentro de las organizaciones y una cultura de desarrollo sostenible a largo plazo.[32]

¿Qué es la ciberseguridad?, perspectiva desde un escenario de amenazas.

La ciberseguridad es un término reciente que engloba la seguridad sobre el espacio informático agrupando tecnologías, redes, protocolos, servicios y productos TI digitalmente, la ciberseguridad también se utiliza para designar diversos campos de la investigación, desarrollo e innovación relacionados con el ciberespacio desde las bases de seguridad.[33]

ISACA define la ciberseguridad como la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

En el modelo de la ciberseguridad se interrelacionan conceptos, métodos, procedimientos, herramientas y regulaciones convirtiendo a la ciberseguridad en estrategias multidisciplinarias.[34]

Las amenazas cibernéticas ocupan el lugar número 1 entre los riesgos y amenazas de la seguridad interna e internacional.[35]

---

[32] NACIONES UNIDAS (2020). Pymes y COVID 19: hacia una recuperación sostenible. Red Española del Pacto Mundial.

[33] PAYA, C.; Cremades, A. & DELGADO, J. El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad de Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. Revista Policía y Seguridad Pública [en línea] , 2016 7(1), 237-270.Disponible en: http://dx.doi.org/10.5377/rpsp.v7i1.4312

[34] GALAN, C. & GALAN C., C. La ciberseguridad pública como garantía del ejercicio de derechos. En: Derecho & Sociedad. 2016. 47, 293-306.

[35] DE TOMAS, S. Hacia una cultura de ciberseguridad: capacitación especializada para un "proyecto compartido". En: Especial referencia al ámbito universitario. ICADE. 2016 92, 14-47.

Colombia ha empezado a plantear una visión rectora consolidada en el documento CONPES 3701, el cual busca generar los lineamientos nacionales de política en Ciberseguridad orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. En este marco de referencia se define la Ciberseguridad como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.[36]

Una iniciativa interesante para la reducción de vulnerabilidades de software es el catálogo de patrones de ataque patrocinado por el DHS en Estados Unidos y de dominio público. Los patrones de ataque describen las técnicas que los atacantes emplean para romper el software, que tienen tendencia a ser pocas y bastante específicas.[37]

La OSSTMM Metodología abierta de testeo de seguridad, es una metodología para implementar pruebas de seguridad, también se le conoce como auditoría con respecto a la seguridad y un abanico de buenas prácticas basadas en pruebas a cortafuegos, pruebas a enrutamientos, es un estándar de seguridad para aquellos que necesiten una prueba de seguridad confiable en lugar de un solo reporte de cumplimiento.[38]

Controles del CIS (Centro de Seguridad para Internet), es el marco de seguridad o mejores prácticas para el ámbito informático, compuesto por 20 controles, teniendo como objetivo establecer en las diferentes capas de protección con sistemas proactivos de defensa y sistemas reactivos capaces de dar respuesta rápida cuando se detecte un problema o anomalía de seguridad, se clasifican en tres grandes grupos, los básicos cubriendo los más elementales controles en cuanto a inventario, periódicamente evaluar vulnerabilidades, establecer configuraciones seguras y mantener los registros de auditoría.[39]

[36]MINISTERIO DE LAS TICS. [Sitio WEB],La entidad, Disponible en: https://www.mintic.gov.co/portal/inicio/Micrositios/I+D+I/Nodos/6120:Ciberseguridad

[37] HOMELAND SECURITY[Sitio WEB], La entidad. Disponible en: www.dhs.gov

[38]REYDES. La OSSTTM [Sitio WEB][17, Noviembre, 2015]. Disponible en: http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual#:~:text=OSSTMM%20(Open%20Source%20Security%20Testing%20Methodology%20Manual)%20proporciona%20una%20metodolog%C3%ADa,evita%20suposiciones%20y%20evidencia%20anecd%C3%B3tica.

[39] ISEC AUDITORS. Controles del CIS [Sitio WEB] [28, noviembre, 2019]. Disponible en: https://blog.isecauditors.com/2019/11/novedades-version-7-1-controles-cis.html

4.2 MARCO CONCEPTUAL

Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.[40]

Vulnerabilidad. Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza.

Amenaza. Causa potencial de un incidente que puede causar daños a un sistema de información o a una Organización.

Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo es el impacto por la probabilidad de ocurrencia de la amenaza.

Ciberseguridad: En la actualidad, ante el gran desarrollo y difusión de los sistemas de información, y la dependencia de ellos de las sociedades modernas, el ciberespacio se presenta como un gran campo para el espionaje. Sin embargo, ésta no es la única oportunidad que brinda a los potenciales agresores, ya que puede ser empleado también como vehículo para todo tipo de actividades ilegítimas, la ciberseguridad es la acción de implementar y ejecutar controles o políticas de seguridad en un entorno completamente digital.

Infraestructuras críticas: Las infraestructuras críticas, compuestas de instituciones públicas y privadas, constituyen el sistema nervioso de las naciones desarrolladas, compuestos por toda la infraestructura tecnológica, activos de información y soluciones que administran el procesamiento digital.

La globalización de Internet hace que los centros de gravedad de un Estado sean más vulnerables a un ataque, al ser las fronteras de la red permeables. Un ataque contra el sistema informático de una infraestructura crítica puede generar muchos daños con un riesgo mínimo para el atacante.[41]

Las ciberamenazas: Hoy en día la red más grande de interconexión es la internet, un sistema globalizado de millones de conexiones desde personas a organizaciones, donde las vías o autopistas de comunicación son expuestas de igual forma a millones de usuarios permitiendo que mal intencionados roben, secuestres o actúen indiscriminadamente frente a la información que se transmite en internet o solo el hecho de alterar sistemas o servicios en línea.

---

[40] UNE 71504 UNE 71504:2008, "Metodología de análisis y gestión de riesgos para los sistemas de información

[41] MAROTO, Juan Puime. El ciber espionaje y la ciberseguridad. En *La violencia del siglo XXI. Nuevas dimensiones de la guerra*. Instituto Español de Estudios Estratégicos, 2009. p. 45-76.

Las vulnerabilidades que más amenazan el ciberespacio se encuentran en los sistemas de información de las empresas de la infraestructura crítica, y en sus estructuras de apoyo externo. Los atacantes buscan explotar vulnerabilidades surgidas durante el diseño e implementación del software, hardware, redes y protocolos. Incluso cuando las alertas están disponibles, el arreglo de algunas vulnerabilidades necesita días, semanas o incluso años de trabajo. Por ello, las vulnerabilidades en las redes críticas se deben identificar y corregir antes de que surjan las amenazas. No se pueden eliminar todas las vulnerabilidades o amenazas, pero se pueden minimizar realizando esfuerzos para:

Reducir y corregir las vulnerabilidades de software, identificando y arreglando las vulnerabilidades existentes que, si se explotasen, podrían causar la mayor parte del daño a los sistemas críticos.

Impulsar el empleo de sistemas seguros de supervisión, control y adquisición de datos.

Identificar interdependencias de la infraestructura y la mejorar la seguridad física de los sistemas vitales.

Identificar y castigar actores maliciosos, mejorando las capacidades judiciales para la prevención y persecución de los ataques en el ciberespacio.[42]

Auditoria en ciberseguridad: La auditoría forense como recurso de prevención de los riesgos de ciberseguridad que, conjugando talento humano con altos niveles de competencias, permite blindar a las organizaciones modernas frente ataques informáticos y actos indebidos, que puedan traer consecuencias graves en la continuidad del negocio y esta a su vez se vea afectada en su posición distintiva frente a los competidores, en un entorno económico y tecnológico que evoluciona a gran velocidad.

Ciberterrorismo: Es toda acción negativa por medio de ataques informáticos a las diferentes infraestructuras críticas de una nación u organización, el canal de internet es utilizado cada vez como un medio para el terrorismo, es un medio o canal de comunicación para obtener y formar fabricación de bombas, tácticas de guerrillas urbanas o milicias con la utilización de terroristas.[43]

El ciberterrorismo es una actividad criminal trasnacional que al tener lugar en un espacio virtual, no puede ser contrarrestada por políticas públicas de los territorios,

[42] MAROTO, Juan Puime. El ciber espionaje y la ciberseguridad. En *La violencia del siglo XXI. Nuevas dimensiones de la guerra*. Instituto Español de Estudios Estratégicos, 2009. p. 45-76.

[43] HERNANDEZ HERNANDEZ, Enrique. El ciberterrorismo en la actualidad AUDITORIA EN INFORMÁTICA, UN ENFOQUE METODOLÓGICO 1996

el alcance que tiene los delitos informáticos en la red es bastante amplio que se traduce en un complejo control sobre ellos, políticas internas y externas de los países han tratado de mitigar ciertos impactos o ataques de esta naturaleza pero no son suficientes con la expansión tecnológica y las redes ocultas darkweb, hacen que sea difícil contener este tipo de ataques.

El Ciber-espionaje: En los tiempos de paz, los adversarios pueden realizar reconocimientos de los sistemas de información de gobiernos, universidad, compañías privadas, identificando los objetivos claves, buscando vulnerabilidades e introduciendo puertas traseras para su empleo en tiempos de crisis o confrontación, estas acciones se consideran acciones de espionaje.[44]

Los ataques más comunes que enfrenta la Ciberseguridad en Colombia.

Las APT: Amenaza persistente avanzada consiste en un ataque sistemático, planeado con tiempo y con una infraestructura considerable donde la mayoría de sus ataques son exitosos, son persistentes dado que escanean y utilizar bastantes recursos o herramientas para conseguir su objetivo y normalmente son silenciosos, sigilosos muy difíciles de detectar.

Normalmente este tipo de ataque es utilizado en los espionajes internacionales con objetivos políticos y económicos, para robar secretos de estados, información confidencial, estrategias de estado, son usados en los gobiernos y en grandes corporaciones quienes tienen un musculo financiero capaz de financiar las diferentes herramientas.

Su implementación es en base a las vulnerabilidades de las aplicaciones o soluciones con los que se cuentan en los equipos de trabajo, al explotar la vulnerabilidad implementar un malware tipo gusano para crear una Puerta trasera Backdoor y de esta forma dejar un acceso para el atacante, para aprovechar los exploits simplemente con un correo, un adjunto le permite ejecutar la vulnerabilidad y tener el control del equipo y posteriormente realizar escalamientos a nivel de sistema.

Para la protección de este ataque es un poco complejo identificarlo de forma anticipada, dado que este tipo de ataque es sumamente silencioso y desapercibido, sin embargo existen herramientas como el monitoreo de red y con un buen análisis de recursos y trazabilidad de recursos en la red se pueden interceptar, un buen

[44] EL CIBERESPIONAJE PUIME MAROTO J. El Ciberespionaje y La Ciberseguridad.; 2009. Accessed November 30, 2020. http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.4549946ART&lang=es&site=eds-live&scope=site

análisis es fundamental y clave para encontrar estas anomalías, También la importancia de tener un buen antivirus con las actualizaciones de las ultimas firmas de malware y tener actualizado las aplicaciones ofimáticas y soluciones del negocio para minimizar las vulnerabilidades de estos.

Ransomware: Es un malware tipo criminal donde su principal objetivo es secuestrar información y posteriormente solicitar una transacción monetaria (pago) a cambio de volver a usar y disponer de la información, es un secuestro digital de la información y de los activos informáticos como servicios o software, normalmente suelen pedir montos de rescate de 100 dólares a 200 dólares u otros montos mayores de acuerdo a la naturaleza de la organización y a los valores de los activos como una entidad financiera o de servicios locales.

La materialización de este tipo de ataque se realiza por medio de alguna descarga de aplicaciones poco confiables, adjuntos de orígenes desconocidos sumado a la ausencia de un antivirus o la carencia de un firewall fácilmente pueden ser instalados en las estaciones de trabajo y en cuestión de segundos cifrar la información de rutas conocidas como escritorio, documentos e iniciar el bombardeo de mensajes donde solicitan un monto para el rescate de la información.[45]

Uno de los métodos para recuperar la información muchas veces es pagando por medios conocidos como bitcoin, Moneypak, métodos en línea, pero no aseguran el 100% de que la información será descifrada y también queda latente el riesgo de compartir los datos de las tarjetas de pago.

Una forma de blindar de alguna forma este tipo de ataque es la actualización del antivirus, la implementación de unas reglas de firewall estrictas y más aún si el entorno corporativo lo amerita y como buena práctica disponer de backups o copias de seguridad de la información que se almacena localmente.

COVID-19

Es una nueva forma de la enfermedad del Coronavirus la cual se debe al nuevo virus SARS-CoV2 que causa una infección aguda con síntomas respiratorios. (American Thoracic Society, 2020).[46]

[45] KASPERSKY. El ransomware: qué es, cómo se lo evita, cómo se elimina [Sitio WEB] Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

[46] AMERCAN THORACIC SOCIETY. ¿Qué es el COVID-19? s/n[en Linea] ATS Patient Education Series (2020)

4.3 ANTECEDENTES O ESTADO ACTUAL

Tipo de publicación: Trabajo de titulación.
Autores: Medina Ubidia, María José – Pardo Montaquiza, Ronny Joseph.
Año: 2021.
País: Ecuador.
Repositorio: http://repositorio.espe.edu.ec/bitstream/21000/24202/1/T-ESPE-044428.pdf
Título: El comercio electrónico y su incidencia en las PYMES del sector comercial, en la época del COVID-19, en la ciudad de Quito.
Resumen: Identificar si el crecimiento del comercio electrónico y servicio delivery puede llegar a influir favorablemente sobre el nivel de ventas de las PYMES comerciales en función de la pandemia ocasionada por el COVID-19.

Tipo de publicación: Tesis.
Autores: Ruiz Aranda, Andres Mauricio / Angel Rojas, John Edison.
Año: 2019.
País: Colombia.
Repositorio: https://repository.ucc.edu.co/handle/20.500.12494/13891
Título: Diseño de una guía de aseguramiento en informática para servidores en entornos Windows con base en la norma ISO 27000 SGSI en las empresas Conciving Ingenieros S.A.S y ARQ S.A, sedes Bogotá.
Resumen: Consiste en la evaluación, diagnóstico y creación de una guía para una empresa local, utilizando una metodología de Microsoft Windows Server, adaptándolo con las políticas de seguridad actuales, también se presenta un informe sobre el rendimiento y estado actual, identificando las vulnerabilidades y por último se relacionan algunas recomendaciones para solventar los hallazgos.

Tipo de publicación: Publicación Académica.
Autores: Roque Hernandez, Ramon Ventura / Juarez Ibarra, Carlos Manuel.
Año: 2018.
País: México.
Repositorio:http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072018000200005&lng=en&tlng=en
Título: Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios.
Resumen: Es una investigación realizada para identificar las falencias o ausencias en cuanto a los conocimientos de seguridad informática sobre los estudiantes universitarios de tecnología que cursan los primeros semestres, sobre la investigación arrojaron resultados positivos que motiva a implementar un programa permanente de concientización y capacitación.

Tipo de publicación: Tesis.
Autores: Andrade Chila, Juan Carlos – Chavez Loor, Carlos Erick.
Año: 2018.
País: Ecuador.
Repositorio: http://repositorio.ug.edu.ec/handle/redug/32606
Título: Generación de un plan para la gestión integral de seguridad de la información basado en el marco de la norma ISO 27001 y las mejores prácticas de seguridad de la norma ISO 27002 para la compañía international Gym Ecuaintergym S.A. de la ciudad de Guayaquil.
Resumen: Las normas ISO 27001:2013 e ISO 27002 de Seguridad de la Información, radican en comprobar el cumplimiento de los controles y las exigencias definidas por el estándar, de darse el caso de no cumplimiento de estos controles en general se realiza una auditoría para definir las no conformidades que son presentadas por un informe de un auditor. El proceso de auditoría es sistemático e independiente basándose en la verificación de los objetivos de control de las normas siendo este evidenciado. El Proyecto tecnológico que se realizó en la compañía International Gym Ecuaintergym S.A., radica en presentar un plan de gestión integral de seguridad de la información alineado en las normas ISO 27001:2013 e ISO 27002, el cual brinda seguridad a los datos con el objetivo de mantener la confidencialidad, integridad, y disponibilidad, definiendo reglas y procedimientos que aseguren tomar buenas prácticas cuando se presenten incidentes de seguridad, gestionando los riesgos y procedimientos que se realizan en la compañía

4.4 MARCO LEGAL

Marco normativo sobre ciberseguridad en Colombia

Normatividad	Descripción
Ley 527	Acceso y uso de mensajes de datos, comercio electrónico y firmas digitales, y determinación de entes certificadores (Congreso de la República de Colombia, 1999).
Ley 594	Seguridad de archivos (Congreso de la República de Colombia, 2000a).
Ley 599	Violación ilícita de comunicaciones, derechos de autor y algunos delitos informáticos en el Código Penal (Congreso de la República de Colombia, 2000b).
Ley 679	Prevención y ataque contra la explotación, la pornografía y el turismo sexual con menores (Congreso de la República de Colombia, 2001).
Ley 962	Reducción de trámites y procedimientos administrativos de entidades públicas o privadas con funciones públicas o de servicios públicos (Congreso de la República de Colombia, 2005).
Ley 1266	*Habeas data* y manejo de información de bases de datos personales (Congreso de la República de Colombia, 2008).
Ley 1273	Modificación del Código Penal para acoger la protección de la información y la preservación integral de los sistemas que usan TIC (Congreso de la República de Colombia, 2009a).
Ley 1341	Principios y conceptos sobre la sociedad de la información y la organización de las TIC y creación de la Agencia Nacional del Espectro (Congreso de la República de Colombia, 2009b).
Ley 1437	Pruebas electrónicas para tipificar los delitos en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Congreso de la República de Colombia, 2011a).
Ley 1480	Protección al consumidor por medios electrónicos y seguridad en transacciones electrónicas en el Estatuto del Consumidor (Congreso de la República de Colombia, 2011b).
Decreto-Ley 019	Reducción de trámites en el estado a través de medios electrónicos y establecimiento de criterios de seguridad (Presidencia de la República de Colombia, 2012a).
Decreto 2693	Estrategia de gobierno electrónico (Presidencia de la República de Colombia, 2012b).
Decreto 2364	Posibilidad de la firma electrónica (Presidencia de la República de Colombia, 2012c).
Decreto 2609	Posibilidad del expediente electrónico en el esquema de gestión documental estatal (Presidencia de la República de Colombia, 2012d).
Ley 1581	Regulación de la protección de datos personales de los individuos (Congreso, 2012).
Ley Estatutaria 1621	Normatividad para las labores de Inteligencia y contrainteligencia y criterios de seguridad para este rol (Congreso de la República de Colombia, 2013).
Decreto 1377	Reglamentación de la la protección de datos personales de los individuos (Presidencia de la República de Colombia, 2013a).
Decreto 1510	Contratación y compra pública por medios electrónicos (Presidencia de la República de Colombia, 2013b).
Ley 1712	Criterio de transparencia en el acceso a la información pública (Congreso de la República de Colombia, 2014).
Decreto 333	Determinación de las entidades de certificación digital (Presidencia de la República de Colombia, 2014).
Ley 1978	Modernización del sector de las tecnologías de la información y las comunicaciones (Congreso de la República de Colombia, 2019).
Decreto 620	Lineamientos generales en el uso y operación de los servicios ciudadanos digitales (Presidencia de la República de Colombia, 2020).
Conpes 3975	Política Nacional para la transformación digital e inteligencia artificial (DNP, 2019).

5 DESARROLLO DE LOS OBJETIVOS

6 Examinar las normas y estándares de seguridad de la información ISO 27001 y 27002 por medio de una revisión documental aplicado a escenarios COVID-19 para identificar las mejores prácticas en cuanto a procedimientos y controles.

Se puede aplicar las normas ISO 27001 para definir los lineamientos en las directrices y los requisitos para llegar a establecer un sistema de gestión de seguridad de la información, permiten identificar vulnerabilidades de acuerdo con los mismos conceptos declarados en las directrices.

La norma ISO 27002 define objetivos y controles para mitigar vulnerabilidades en los sistemas.

De acuerdo con los estándares ISO 27001 quien se encarga de definir los lineamientos en la directriz y los requisitos para llegar a establecer un SGSI y la norma ISO 27002 quien define los dominios, los objetivos de control y los controles a considerar para mitigar las vulnerabilidades en los sistemas.

Revisión # 1 Aplicación del estándar ISO 27001 en organizaciones para hacer frente a los riesgos y amanezcas TIC en un escenario actual y futuro.

La ciberseguridad y teletrabajo seguros con la ISO 27001 Y 27002.

A través del análisis y gestión de riesgos de los procesos de negocio/servicio de TI y sus activos de información, hardware, software, es aplicar un set de controles para mitigar dichos riesgos, de acuerdo con ello proponen la implementación de la ISO 27001 bajo algunos dominios descritos a continuación:

- El dominio A.6.2 Dispositivos móviles y teletrabajo, donde la correcta aplicación del control garantiza la seguridad en dispositivos móviles y en las condiciones del teletrabajo, a raíz de la pandemia muchas organizaciones recurrieron a la modalidad remota por medio de sus dispositivos móviles obligando a no usar dispositivos corporativos sino usar dispositivos personales propios.

- Dominio A.13 Seguridad en las comunicaciones, garantizando comunicaciones seguras a través de VPNs, asegurando la confidencialidad y privacidad de la información intercambiada con los sistemas corporativos.[47]

Las buenas prácticas abarcan los siguientes aspectos claves:

La implementación de una administración y gestión de riesgos que contemple la mitigación e implementación de controles adecuada tanto para la información, servicios y sistemas de la organización.

Revisión # 2 La Privacidad de la información: clave en la transformación digital de la era COVID-19.

Debido a la crisis del COVID-19 los datos principales activos hoy en día juegan un papel relevante durante la contingencia de la pandemia, su privacidad se vuelve el principal foco de la alerta sanitaria.

De acuerdo con Marta Aulle el escenario de pandemia ha obligado a tomar decisiones para dar continuidad y seguridad a la actividad laboral, lo que ha acelerado la adopción de soluciones TIC en las organizaciones y sus empleados, para poder trabajar en remoto (teletrabajo) a través de herramientas colaborativas

Esto ha generado a la misma velocidad riesgos en los sistemas de información de las organizaciones y sus datos, que deben ser debidamente gestionados para que su seguridad y privacidad se vean afectadas lo menos posible, y así ser productivos y eficaces cumpliendo los objetivos de negocio.[48]

Como es sabido, la ISO/IEC 27001 establece un Sistema de Gestión de Seguridad de la Información ya considerado internacionalmente como un estándar en la seguridad para las organizaciones.

El principal objetivo es implementar la ciberseguridad orientada a los procesos y objetivos de la organización, se debe implementar el análisis de riesgos de TIC para que posteriormente se implemente los más efectivos controles y procedimientos en función de minimizar los riesgos identificados inicialmente.

[47] RISS, Boris Delgado; SÁNCHEZ, Carlos Manuel Fernández. Las mejores prácticas ISO contra el Covid-19 y crisis futuras. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 2020, vol. 29, no 140, p. 94-96.

[48] ALLUE, Marta; DELGADO, Boris; FERNÁNDEZ, Carlos Manuel. Privacidad de la información: clave en la transformación digital de la era COVID-19. AENOR: Revista de la normalización y la certificación, 2020, no 362, p. 5-8.

Esta gestión eficaz de la ciberseguridad permite garantizar:

- Solo los autorizados pueden acceder a la información, con ello se asegura la confidencialidad.
- Asegurar la completitud de los datos se asegura la integridad.
- Solo los usuarios autorizados tienen acceso a la información y a sus activos respectivos asegurando la disponibilidad.

Revisión # 3 Implementado los estándares de la ISO 27001.

Según la introducción de esta norma internacional está preparada para proporcionar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un SGSI.

El hecho de adoptar un SGSI es una estrategia determinante para una organización.

Las necesidades, los objetivos y los requisitos de seguridad de la organización son las condiciones para implementar y establecer un SGSI, lo cual implica una mejora continua con el tiempo.

En la condición de escenario critico como lo es la Pandemia claramente el SGSI está enfocado en implementar procesos de seguridad que estén en la capacidad de proteger activos como los datos de cliente, información confidencial, implementar canales seguros de transferencia, estos requisitos mínimos deben ser las condiciones por las cuales se establera un SGSI.

También se tendrá en cuenta el tamaño de la organización, su modalidad de trabajo, sus equipos tecnológicos si son propios de la organización o personales, que conexión optaran para trabajar con los diferentes archivos y documentos, web o bajo una VPN que garantice confidencialidad.

Claramente es importante identificar esos activos valiosos para la organización como lo es la información, los datos, el hardware y software que utilizan diariamente para el procesamiento de las actividades, deberán ser consientes en identificar todos estos elementos.

La ventaja de implementar un SGSI ayuda a preservar la confidencialidad, integridad y disponibilidad de la información, permitiendo asegurar una correcta gestión de los riesgos.

Es de vital importancia que el SGSI se encuentre integrado en el mapa de procesos de la organización, que sea un programa transversal para todos los actividades y unidades de negocio misionales, también debe se debe contemplar los riesgos y controles.

Revisión # 4 Propuesta de diseño de una VPN para una PYME en tiempo de COVID-19.

Se puede aplicar las normas ISO 27001 para definir los lineamientos en las directrices y los requisitos para llegar a establecer un sistema de gestión de seguridad de la información, permiten identificar vulnerabilidades de acuerdo con los mismos conceptos declarados en las directrices.

La norma ISO 27002 define objetivos y controles para mitigar vulnerabilidades en los sistemas.

De acuerdo con los estándares ISO 27001 quien se encarga de definir los lineamientos en la directriz y los requisitos para llegar a establecer un SGSI y la norma ISO 27002 quien define los dominios, los objetivos de control y los controles a considerar para mitigar las vulnerabilidades en los sistemas.

En la propuesta presentada por José Daniel Rojas, se evidencia las directrices para identificar las vulnerabilidades sobre diferentes activos como en hardware, comunicaciones, software, factores ambientales, factores sociales, estas directrices son determinadas por la ISO 27001 y como solución a su problemática contempla la implementación de un VPN para que el personal de las PYMES puedan trabajar desde sus casas manteniendo una estructura de información y operación segura, esta solución se determina por los controles basados en la ISO 27002 para mitigar las vulnerabilidades identificadas.[49]

[49] ROJAS CELIS, J D., Hoyos Rodríguez, R D., y Castro Reyes.Propuesta de diseño de una VPN de acceso remoto con túneles GRE para permitir plan de continuidad tic para las mipymes del sector económico terciario, en empresas dedicadas al comercio de equipos partes y piezas electrónicas en Bogotá D.C.[en línea] Tesis de pregrado, Universidad Cooperativa de Colombia.(2020) Disponible en: http://hdl.handle.net/20.500.12494/28389

Revisión # 5 La ciberseguridad y análisis de riesgos informáticos.

La ciberseguridad se enfoca en el diseño de normas, procedimientos, métodos y técnicas que posibiliten seguridad y confiabilidad en los sistemas de información incluyendo aspectos tanto físicos (estructuras, infraestructura) y humanos (personal de la organización).[50]

Por ello, actualmente se cuenta con estándares, protocolos, métodos, reglas, herramientas y normas para minimizar los riesgos y amenazas cibernéticas, cada uno de estos pilares son dado por las normas y estándares de la industria como la ISO 27001 y la ISO 27002, brindando unas bases, lineamientos y controles tanto para identificar vulnerabilidades y recomendar algunos controles con el ánimo de mitigar el impacto de los riesgos en la organización.

No obstante, las amenazas a la seguridad informática aparecen principalmente debido a:

a) Usuarios con permisos sobredimensionados, sin restricción a accesos innecesarios.

b) Programas maliciosos.

c) Errores de programación.

d) Acceso de intrusos.

e) Generación de siniestros, robos e incendios.

f) Acceso de personal técnico interno.

g) Catástrofes naturales.

h) Ingeniería social (errores humanos, falta de precaución al compartir contraseñas, claves, códigos o por descarga de archivos).

[50] SAAVEDRA, B., y Parraguez, L. La ciberseguridad: análisis político y estratégico I. Revista Fuerzas Armadas [en linea] (2018), 91(243), 44-51

Una vez se identifique los diferentes riesgos a los que pueden estar expuestas las PYMES, se debe implementar las políticas de seguridad de información impidiendo la perdida y robo, estas políticas deben estar bajo alguna legislación normativa local y en base a lo recomendado en la ISO 27001 y 27002.[51]

Como complemento, en torno al tema de ciberseguridad se ha incorporado el proceso de análisis de activos informáticos, sus amenazas y vulnerabilidades, su probabilidad de ocurrencia y su impacto, buscando determinar los controles adecuados para evitar, minimizar y transferir el riesgo de daños o pérdidas para personas y organizaciones. Entre los muchos modelos existentes se encuentra el de Henriques, Silva, Poleto, Camara, y Cabral (2018).[52]

Marco para ciberseguridad

Función	Categoría
Identificar	• Gestión de activos • Entorno empresarial • Gobernanza • Evaluación de riesgos • Estrategia de gestión de riesgos • Gestión de riesgo de la cadena de suministro
Proteger	• Gestión de identidad y control de acceso • Conciencia y capacitación • Seguridad de datos • Procesos y procedimientos de protección de la información • Mantenimiento • Tecnología protectora
Detectar	• Anomalías y eventos • Vigilancia continua de seguridad • Procesos de detección
Recuperar	• Planificación de recuperación • Mejoras • Comunicaciones

Fuente: Barrett (2018).

53

[51] INCIBE. Protección de la información[Sitio WEB]Madrid, españa (28, noviembre 2017). Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

[52] HENRIQUEZ, A.P., Silva, M.M., Poleto, T., Camara, L., & Cabral, A.P. (2018). Cybersecurity risk analysis model using fault tree analysis and 215 Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia Rev. Crim. / Volumen 62 - Número 2 - Mayo-Agosto 2020 - pp. 199-217 - ISSN 1794-3108 - Bogotá, D. C., Colombia fuzzy decision theory. International Journal of Information Management, 43, 248-260. https:// doi.org/10.1016/j.ijinfomgt.2018.08.008

[53] BARRETT, M. P. (2018). *VEQI[SVO JSV -QTVSZMRK 'VMXMGEP Infrastructure Cybersecurity. Gaithersburg, Maryland (USA): National Institute of Standards and Technology - U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

No significa que la implementación de una ISO como la de seguridad (27001 y 27002) garantice completamente los ataques de los delitos cibernéticos, pero sí de cierta forma los SGSI son fundamentales para ellos, contribuyen a que los riesgos cibernéticos sean conocidos, asumidos, gestionados y minimizados de forma documentada, sistemática, estructurada, repetible en un escenario donde está involucrada las tecnologías.[54]

Revisión # 6 Colombia y la ISO 27001 en Pandemia

Este es el principal estándar mundial sobre seguridad de la información, con un amplio abanico de aplicación (organizaciones con o sin fines de lucro, privadas o públicas, pequeñas o grandes), que proporcionan una metodología para implementar la gestión de la seguridad de la información para reducir los riesgos hasta un nivel aceptable y dándole la posibilidad de certificarse como ha ocurrido mundialmente con muchas empresas.

Este marco brinda tranquilidad a los diversos grupos de interés sobre la protección de la integridad de sus datos y sistemas, muestra compromiso con la seguridad de su información, genera oportunidades de negocio, mejora los estándares éticos de los empleados y reduce los riesgos de fraude, pérdida de datos o divulgación de información no deseada, entre otros beneficios.

Las cifras en Colombia para el año 2019 se llegó a 30.410 delitos informáticos que fueron denunciados (54% más que en el 2018) distribuido en los siguientes ataques:[55]

- Phishing (42%)
- Suplantación de identidad (28%)
- Envió de malware (14%)
- Fraudes en medios de pago online (16%)
- El uso del ransomware aumento 500% en el país

[54] POWERDATA.Lo que debes saber sobre el reglamento general de protección de datos [Sitio WEB] España (26, agosto, 2019). Disponible en: https://www.powerdata.es/ gdpr-proteccion-datos

[55] EL TIEMPO. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia [Sitio WEB], Bogota, Colombia (30, octubre, 2019). Disponible en:https://www.eltiempo. com/tecnosfera/novedades-tecnologia/reportede-ciberataques-en-colombia-2019-de-policianacional-y-ccit-428790

Las grandes y medianas empresas reportaron cerca de 14 millones de intentos de ciberataques (correos fraudulentos, suplantación de identidad, enmascaramiento de correos e infección de sitios web).

Con la llegada de la pandemia y el confinamiento preventivo tuvo como consecuencia el aumento de la virtualización tanto laboral como personal, clases remotas, incremento en el uso de las aplicaciones de mensajería, aumento en las transacciones bancarias online, compras por internet, expedición de documentos online pero también ha traído consecuencias sobre el uso de las tecnologías como el incremento de páginas falsas, textos y noticias desinformativos, mensajes con virus adjuntos y llamadas engañosas.

Para contrarrestar los ataques descritos anteriormente el gobierno ha impulsado estrategias en su agenda "Estrategia de innovación" y muestra como la ciberseguridad se ha convertido en un eje estratégico y prioritario para proteger los recursos y activos informáticos de la nación y como las normas ISO juegan un papel clave en el desarrollo de estas estrategias que bien pueden ser aplicadas a las PYMES, implementando, fortaleciendo el diseño de políticas, procedimientos, monitoreo y asistencia técnica, usando también parámetros y modelos que propenden por la confidencialidad, la integridad y la disponibilidad de los datos.

En cuanto a los sistemas de gestión, el MINTIC público un modelo de seguridad y privacidad de la información en base a las buenas prácticas de seguridad de la ISO 27001 y la ley de protección de datos personales donde pretende preservar la confidencialidad, integridad y disponibilidad de los activos de la información.[56]

[56] OSPINA DIAZ, Milton Ricardo, & SANABRIA RANGEL, Pedro Emilio. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad [en linea],(26,noviembre, 2020) 62(2), 199-217. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=en&tlng=

Revisión # 7 La seguridad implementada por la ISO 27001[57]

La propia UNE ISO 27002 (2017) determina que existen tres fuentes donde obtener los requisitos de seguridad que nos ayuden a velar por la integridad de estos tres pilares:

• Primera fuente: Es el análisis de riesgo realizado por la propia organización. Como veremos en el capítulo siguiente, a través de una evaluación interna, se podrán averiguar las amenazas y su probabilidad de materialización, lo que ayudará a identificar las medidas de seguridad idóneas.

• Segunda fuente: Es el cumplimiento de requisitos legales, estatutarios, reglamentarias y contractuales a los que la organización se encuentre sometida. Por ejemplo, la normativa de protección de datos de carácter personal, que se explicará más adelante.

• Tercera fuente: Son los propios objetivos y requisitos del negocio que la organización se ha establecido como necesarios para dar soporte al tratamiento de la información. Es decir, las medidas internas que la organización se haya autoimpuesto.

La principal tarea de la seguridad informática es la de minimizar los riesgos, que, en este caso, provienen de muchas partes: puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir de los mismos usuarios y hasta de los protocolos que se están implementando; pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Lo que debe contemplar la seguridad se puede clasificar en tres partes:

• Usuarios: Considerados el eslabón más débil de la cadena, ya que las personas pueden cometer un error y olvidar algo o tener un accidente, y este suceso puede comprometer la información y que terceros puedan acceder a ella.

• Información: Compuesta por la interpretación de todos los datos introducidos en el sistema, es el principal objetivo de la seguridad informática, ya que es lo que se desea proteger y lo que tiene que estar a salvo; en otras palabras, se dice que es el principal activo.

[57] LEMA, Luis López. La gestión de la información durante etapas de teletrabajo en la época de la COVID-19. Perspectivas, n. 3, 2020.

• Infraestructura: Entendiéndose como todos los recursos necesarios para albergar, tratar y transmitir la información; puede ser uno de los medios más controlados para asegurar todos los procesos.

La seguridad es un problema integral; los problemas de seguridad informática no pueden ser tratados aisladamente, ya que la seguridad de todo el sistema es igual a su punto más débil. El uso de sofisticados algoritmos y métodos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo. Por otra parte, existe algo que los hackers llaman ingeniería social, que consiste simplemente en conseguir, mediante un engaño, que los usuarios autorizados revelen sus contraseñas. Por lo tanto, la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar.

En vista de estas manifestaciones, hay tres elementos principales que proteger en cualquier sistema informático: el software, el hardware y los datos.

Análisis de vulnerabilidades y metodología.

Para la correcta conjugación de los elementos anteriores, se requiere implementar una metodología de análisis de vulnerabilidades con la finalidad de tratar de mitigar o reducir los riesgos detectados dentro de los sistemas de información.

- Definir el alcance.
- Identificar los activos.
- Identificar amenazas.
- Identificar vulnerabilidades.
- Evaluar el riesgo.
- Tratar el riesgo.

7 Identificar las políticas y controles mínimas básicas que pueden ser aplicados a una PYME colombiana del sector comercial bajo un escenario COVID-19 por medio de una revisión de casos de estudio para extractarlas como lineamientos o bases que deberían implementarse como mínimo en un SGSI.

Caso de estudio # 1 Utilización de los dispositivos móviles en las PYMES

Muchas PYMES hacen uso de dispositivos móviles como el celular, un dispositivo con la funcionalidad de realizar llamadas y en muchos casos de recibir y enviar correos por ende también tiene información clasificada de la organización, información que es sensible, algunos de los controles que se pueden implementar para este tipo de hardware son:

- La protección física proteger la terminal de robo o perdida.
- No dejar la terminal sin vigilancia, deberá tratarse como si fuese una tarjeta de crédito; mantenerlo bajo control en todo momento.
- Utilizar herramientas de protección para terminales móviles que puedan bloquear, borrar o localizar el aparato a distancia.
- Configurar las opciones de geolocalización
- Apuntar el numero IMEI del teléfono o smartphone
- También existen aplicaciones gratuitas que permiten borras los datos de forma remota en caso de pérdida o robo de la terminal.

En cuanto a la protección lógica o aplicativa se recomienda los siguientes controles:

- Establecer un código PIN, para mejorar la seguridad de acceso.
- Bloquear el terminal móvil con un código o contraseña en caso de no utilizarlo tras un periodo de inactividad.
- Evitar utilizar la misma contraseña para un terminal móvil
- Utilizar los parámetros de seguridad entregados en el móvil.
- Invertir en una aplicación de seguridad móvil.

El uso de los portátiles o tabletas con conexión móvil se recomienda que en lugares públicos para el intercambio de mails o transferencia de archivos confidenciales de la empresa se emplee protocolos seguros en las redes wifi como https y SSL

Establecer políticas frente a la seguridad de la información en las pymes.

Se deben desarrollar políticas entorno al aseguramiento de todos los activos que participan en la organización, algunas de las recomendaciones para su implementación son:

Consejo # 1 Organización/entorno

Establecer o conducir un proceso periodo de evaluación de los riesgos que cubra los equipos itinerantes en la empresa.

Proporcionar los dispositivos de protección física para estos equipos a fin de evitar que sean robados en los entornos de escritorios.

Sensibilizar periódicamente a los propietarios y usuarios de la información móvil en lo que respecta a las precauciones de uso.

Identificar los dispositivos con el nombre del propietario, el nombre de la empresa, la dirección, número de teléfono de contacto, número de serie e identificación IMEI del smartphone.

La lista de estos dispositivos debe estar constantemente actualizada con la referencia de sus propietarios o usuarios para facilitar las verificaciones de inventario y auditorias de seguridad.

Consejo # 2 Establecer una protección para la conexión VPN a los terminales móviles de los usuarios itinerantes. [58]

[58] CARPENTIER, Jean-François. *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Ediciones ENI, 2016.

Caso de estudio # 2 Diseño de un esquema de seguridad informática para PYMES, contra amenazas de Ransomware utilizando los lineamientos de la norma ISO 27001

El documento que se describirá a continuación corresponde a una guía de políticas y procedimientos (controles) que brinda a las PYMES controles de seguridad informática a nivel de host frente a un escenario de ataque de Ransomware o un malware maligno para una PYME. [59]

Se desarrollo un plan de recuperación ante un ataque de Ransomware considerando la ISO 27001:2013 del dominio de control A17 Protección y continuidad de negocio, al implementar el plan se implementa también a través de políticas de seguridad en función a los dispositivos perimetrales y herramientas de software.

Para los dispositivos finales como portátiles o estaciones de trabajo se consideran las siguientes políticas y recomendaciones logrando una capa adicional de seguridad y lograr mitigar las amenazas de Malware y/o el Ransomware.

En la fase de identificación

1. Reducir cantidad de cuentas administrativas en la red.

Se recomienda delegar y configurar cuentas de usuarios con privilegios mínimos, esas cuentas deben tener unas contraseñas de alto nivel para acceder a la red o la información.

2. Permita que se visualicen las extensiones ocultas de los archivos.

Se recomienda activar la configuración de visualizar las extensiones de los archivos almacenados, esto permite detectar y visualizar algún archivo sospechoso por el ejemplo los archivos pdf.exe, muy usado por el Malware Cryptolocker.

En la fase de protección

3. Actualizar el sistema operativo de los equipos.

Los softwares vulnerables normalmente son los software desactualizado que permite abrir puertas a los atacantes, se recomienda constantemente aplicar actualizaciones y parches de seguridad para cerrar esas brechas.

[59] MONTOYA CORREA, Tatiana; MOLANO LUJÁN, Andrés. Diseño de un esquema de seguridad informática para PYMES, como la primera línea de defensa para la protección contra amenazas de Ransomware, utilizando los lineamientos de la norma ISO27001: 2013. 2018.

Es recomendable tener habilitadas las actualizaciones automáticas del sistema.

Antes de aplicar las actualizaciones es conveniente que el administrador de tecnología revise, documente y aplique las actualizaciones y parches para cerrar las diferentes vulnerabilidades, de esta forma se podrá garantizar un control de actualizaciones.

4. Restringir los derechos administrativos locales

Una protección adicional se implementa por medio de un control de dominio llevando a los usuarios a privilegios mínimos garantizando que amenazas como el Ransomware no se materialice en los sistemas, brindando una protección adicional a nivel local.

5. Restringir la iniciación de archivos ejecutables desde la carpeta descargas

Aplicando políticas de ejecución sobre archivos descargados se puede reducir el tipo y el nivel de riesgo que puede generar un usuario desprevenido

6. Educar a los empleados.

Otra medida importante que las organizaciones deben implementar es educar, capacitar, sensibilizar de forma periódica a los empleados quienes juegan un papel fundamente para la defensa ante ataques Ransomware, sensibilizarlo en cuanto a lo que navegan, descargan los convierten más conscientes de las posibles consecuencias.

Los administradores de TI siempre deberán estar actualizados con las últimas novedades, avances, riesgos y lanzamientos de seguridad, se deben programar capacitaciones con todo el grupo de trabajo. Con esta buena práctica se puede reducir en gran parte la amenaza de infección o ataque pues los usuarios son el primer filtro; y para los medios directos, de ataque como son dispositivos externos infectados o archivos en correos maliciosos, entre otros.

7. Otorgar permisos de sólo lectura a ciertas carpetas compartidas

Los recursos de red solo deberán tener permisos mínimos como de acceso de solo lectura. De esta manera se reduce la superficie de ataque del crypto Ransomware.

8. Tener un antivirus actualizado

Los diferentes equipos cliente deben tener la protección de su antivirus activada con análisis en tiempo real. Esto permite blindar los sistemas contra las amenazas continuas, como buena práctica también se debe crear rutinas ya sea semanal o mensual para realizar escaneos completos.

9. Firewall de host

Los dispositivos finales y perimetrales tienen la opción de usar sus propios firewalls los cuales conllevan a revisar tanto las conexiones entrantes como salientes, adicionalmente los diferentes firewalls que convivan en el mismo ecosistema deben trabajar en conjunto de lo contrario podrían entrar en conflicto con sus políticas conllevando a un bloqueo total o permitir todo de forma innecesaria.

10. Protección web

Los equipos de una organización se componen también de computadores portátiles que no siempre estarán dentro de la organización; por tanto, no serán protegidos por los sistemas de seguridad perimetral; es por esto por lo que deben tener activos sus sistemas de filtrado web a nivel de host, para evitar que usuarios accedan a páginas peligrosas o que no tengan que ver con el trabajo de la organización. De esta forma se evitará un posible riesgo de infección de malware, que posteriormente, al ingresar a la red interna de la compañía, sería un foco de ataque o infección para los demás equipos de la red y con esto, la pérdida de la información; por lo tanto, estos equipos deben ser revisados con periodicidad por el personal de TI, para garantizar la integridad de los que pueden estar fuera de la organización.

En la fase detectar

11. Chequeo continuo de los logs.

La consola de administración de seguridad de los dispositivos Endpoint almacena registros de eventos que permiten determinar una falla o ataque de manera amplia; una situación para facilitar la revisión de lo presentado en tiempo real. El análisis constante de los logs es fundamental en la evaluación de riesgos de seguridad, debido a que permite almacenar, catalogar, constituir y analizar, permitiendo iniciar de manera oportuna acciones de protección.

Con esto se espera el descubrimiento de vulnerabilidades, inconvenientes en el software, ataques o brechas de seguridad, generando métodos para acciones que

faciliten estar al tanto, de manera oportuna, de la gravedad del caso y/o de la existencia de equipos afectados.

El análisis de la información obtenida de los logs facilita la administración y servicio, ya que, en el momento que se presente un evento de comportamiento anormal, se está enterado de lo que va sucediendo, desde su inicio hasta la solución final de la novedad.

En la fase de responder.

12. Definir procedimiento de actuar ante un incidente.

En caso de que se presente alguna eventualidad, se deben tener claros los roles y las personas de la organización, que deben reaccionar en al evento. Adicionalmente, se debe contar con un proveedor externo, cuya función será la de ser el segundo nivel, brindando apoyo para resolver la novedad.

En la fase recuperar.

13. Realizar copias de seguridad periódicas de la información

Realizar respaldo de la información y los sistemas, de manera continua, resultan fundamentales en el momento de pérdida de datos; además, es de suma importancia el almacenamiento de las copias de seguridad.

Se debe verificar que los procedimientos de copias de seguridad se estén realizando de manera correcta, y que la restauración sea aplicable y funcional en la infraestructura de la compañía.

Se debe tener en cuenta que algunas de las soluciones actuales de copias de seguridad en nube, de igual manera son vulnerables a ataques Ransomware.

En algunas ocasiones las copias de seguridad sobrescriben la información que ya ha sido infectada por Ransomware, generando el cifrado de los datos; por tal motivo, es importante que dichas copias no sean solo locales; se debe garantizar diferentes medios de copia y lugares de almacenamiento, en especial cuando la información es sensible para la organización.

Caso estudio # 3 Desarrollo de una guía de controles de ciberseguridad para la protección integral de la PYME.

De acuerdo con un trabajo final de maestría realizado por Ratti Bittinger, Gabriela, se evidencia la identificación de los principales activos de la organización como caso de estudio, seguidamente se establece el riesgo por cada uno de ellos identificando su probabilidad de impacto para determinar su criticidad, dando a ello una serie controles a aplicar.[60]

Archivos (en computadores, teléfonos, dispositivos móviles).

1. Contraseñas de inicio de sesión y bloqueo de pantalla con contraseña (robusta y diferentes) en todos los equipos.
2. Cifrado de archivos sensibles
3. Distribución granular de permisos para accesos a archivos.
4. Copia de seguridad continua de archivos.

Computadores (Host Final- host de usuario)

1. Contraseña de inicio de sesión y bloqueo de pantalla con contraseñas robustas y diferentes en todos los equipos.
2. Soluciones de seguridad de Endpoint (antivirus, Antimalware, anti-spyware)
3. Cortafuegos basado en host (firewall)
4. Actualización de sistema operativo y programas.
5. Protección de servicios expuestos con contraseñas robustas.

Teléfonos y dispositivos móviles

1. Antivirus.
2. Restricción de instalación de apps no oficiales.
3. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña

Correo electrónico

1. Contraseña segura
2. Autenticador de doble factor.
3. Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware)
4. Configuración segura del servidor de correo, restricción de puerto 25
5. Actualización del software de correo
6. Configuración de información de recuperación.

[60] RATTI BITTINGER, Gabriela María. Desarrollo de una guía de controles de ciberseguridad para la protección integral de la PYME. 2017.

Redes sociales

1. Contraseña segura
2. Autenticación de doble factor.
3. Configuración de información de recuperación.
4. Procedimiento de baja de usuario – transferencia de responsabilidades y accesos

Wifi

1. Contraseña segura del wifi
2. Configuración segura del wifi – protocolos seguros
3. Contraseña segura del Access Point
4. Utilización de Https para envió de credenciales.

Página web

1. Actualización de CMS, plugin, plantillas.
2. Contraseña segura para los usuarios de CMS.
3. Auditoria de vulnerabilidades de la aplicación web (en caso de desarrollo propio)
4. Contraseña segura para accesos del hosting
5. Copia de seguridad del sitio web.
6. Separación de bases de datos y/o archivos sensibles del contenedor público.
7. Cortafuegos de aplicación web (WAF Web Application Firewall)

Servicios en la nube

1. Contraseña segura.
2. Autenticación de doble factor.
3. Configuración de información de recuperación

Sistemas internos.

1. Control de acceso a los sistemas con contraseñas robustas y diferentes para cada usuario.
2. Control granular de los permisos concedidos a cada usuario.
3. Copia de seguridad de los datos del sistema interno (base de datos y/o sistema de archivos)
4. Auditoria de vulnerabilidades de los sistemas internos
5. Actualización del software y demás componentes de los sistemas internos.
6. Soluciones de seguridad de endpoint en equipos que interactúan y/o alojan los sistemas internos (antivirus, antimalware, etc)
7. Cortafuego basado en host en equipos que interactuaran y/o alojan la aplicación interna.

Servidores propios

1. Soluciones de seguridad Endpoint (antivirus, antimalware, anti-spyware)
2. Cortafuegos basados en host y/o en red.
3. IDS/IPS basado en host y/o red.
4. Actualización del sistema operativo y programas.
5. Protección de servicios expuestos con contraseñas robustas.
6. Hardening de sistema operativo y de servicios expuesto.
7. Copias de seguridad continua del sistema operativo (imágenes o screenshots de S.O)
8. Redundancia lógica y/o física del servidor.

Controles transversales.

1. Educación al usuario.:
2. Utilización de gestor contraseña.

Caso de estudio # 4. Recomendaciones para las PYMES en tiempos de COVID-19 perspectivas de Lema, Luis López[61]

Recomendaciones para las organizaciones: cualquier empleador, bien sea una institución pública o bien sea una institución privada, deberá velar por implantar medidas de seguridad.

Para ello, entre otras acciones, deberá:

Realizar un análisis de riesgo detallado, así como el protocolo pertinente para efectuar análisis periódicos con el fin de detectar nuevas vulneraciones.

- Asegurarse una conexión segura entre el dispositivo del usuario y el sistema de información de la organización. Para ello, es recomendable contar con redes VPN (de sus siglas en inglés Virtual Private Network) corporativas que admitan una gran cantidad de conexiones simultáneas y con la finalidad de conectarse a uno o más ordenadores de una red privada utilizando Internet.

- Establecer un listado de aplicaciones y software autorizado por la organización, para evitar que el personal decida e instale soluciones informáticas que puedan comprometer la información corporativa. Además, es importante que el departamento de informática se encargue de realizar dichas instalaciones.

- Establecer sistemas de acceso con protocolos de identificación y autenticación con claves robustas (mezclando mayúsculas, minúsculas, números y símbolos) para acceder a los sistemas de información corporativos. Y, además, obligar su modificación de forma periódica.

- Proporcionar, cuando sea posible, ordenadores o dispositivos informáticos al personal que lo requiera, asegurándose de que tengan el sistema operativo y software de seguridad.

- En el caso de que no sea posible proporcionar dichos recursos, se deberá establecer políticas BYOD (concepto que deriva de sus siglas en inglés Bring Your Own Devi-ce) que regulen el uso de los dispositivos particulares de los empleados que se autorizan para un uso corporativo. En dicha política, se establecerá, entre otros aspectos, en qué condiciones se permiten su uso, cómo se accede a la información corporativa, qué configuraciones de seguridad serán necesarias para poder utilizarlos, etc.

[61] LEMA, Luis López. La gestión de la información durante etapas de teletrabajo en la época de la COVID-19. Perspectivas, n. 3, 2020.

- Formar al personal sobre principios básicos y fundamentales de seguridad de la información, así como establecer un programa de formación continua para reforzar e instruir a todo el personal ante los nuevos riesgos y amenazas que aparezcan.

- Definir una política para responder a incidentes y violaciones de seguridad.

- Asignar una dotación presupuestaria para reforzar la seguridad informática de la organización.

Recomendaciones para el personal para realizar sus funciones fuera de las dependencias de la organización: cualquier trabajador debe aplicar las medidas de seguridad idónea o sustitutivas a las que aplica durante el desempeño de su trabajo

- Utilizar preferiblemente equipos informáticos corporativos, en vez de utilizar equipos personales, a menos que la organización haya establecido una política BYOD y en la medida de lo posible, no mezclar en el dispositivo el trabajo y las actividades de ocio.

- No compartir el dispositivo con el resto de las personas que residan en el mismo domicilio.

- Conectarse a Internet a través de redes seguras, evitando las redes abiertas/libres, y mucho menos utilizar de forma fraudulenta redes wifi. Con una conexión insegura, las personas que se encuentren conectadas a la misma red pueden tener acceso al tráfico que se genera allí. Por ello, deberán activar un protocolo seguro o cifrado.

- Evitar el intercambio de información corporativa confidencial (por ejemplo, por correo electrónico) a través de conexiones posiblemente inseguras, como las redes wifi de cafeterías, vecinos del mismo edificio, etc.

- En la medida de lo posible, utilizar los recursos de la intranet corporativa para compartir archivos de trabajo. Por un lado, esto garantiza que los archivos de trabajo estén actualizados y, al mismo tiempo, se evita el intercambio de información confidencial entre dispositivos locales.

- Tener especial cuidado con la apertura de correos electrónicos, sobre todo, aquellos que hacen referencia a productos o comunicaciones referentes a la COVID-19, ya que pueden ser intentos de phishing o estafas. También, mantener especial atención a la dirección completa del emisor del correo

electrónico y comprobar la identidad en aquellos casos en los que se requiera un pago o transferencia bancaria. En caso de duda sobre la legitimidad de un correo electrónico, comunicarlo al responsable de la organización.

- Tener el sistema operativo, antivirus y de las aplicaciones utilizadas actualizadas a la última versión disponible para reducir los fallos de seguridad y contar, en la medida de lo posible, con todos los parches de seguridad oportunos.

- Bloquear la pantalla al ausentarse del ordenador si se trabaja en un espacio compartido.

- No compartir las URL de las reuniones virtuales en las redes sociales u otros canales públicos para evitar que personas ajenas a la organización o terceros no autorizados pueden acceder a reuniones privadas.

8 Reconocer los diferentes ataques de ciberseguridad que tendrá mayor impacto sobre las PYMES para prepararse a una respuesta inmediata y efectiva por medio de las revisiones de caso de estudio.

Un plan de gestión de ciberseguridad que contemple efectivos procedimientos y controles en función a los procesos, la tecnología y las personas es un esfuerzo que toda organización debe implementar considerando el escenario de hoy en día, un mundo cada vez más digital e interconectado con tecnologías disruptivas y tiempos de implementación muy exigentes donde los riesgos y la exposición de recibir un ataque de ciberseguridad es solo cuestión de tiempo[62]

La importancia de identificar los ataques de ciberseguridad existentes y los que pueden aprovecharse de infraestructuras vulnerables como las que se encuentran en las PYMES, son importantes para establecer y definir estrategias tácticas para contener dichos ataques y desarrollar mecanismos, controles más efectivos.

Debido a la crisis del COVID-19, la improvisación y adaptación de la infraestructura informática de las PYMES dio como resultado una exposición bastante alta en cuanto los temas de ciberseguridad, dejando descubierto ciertas vulnerabilidades, precipitando riesgos en cuanto a seguridad informática y un ataque se hace tan probable de realizarse.

La repentina adopción del teletrabajo por millones de personas en todo el mundo ha dado a los cibercriminales la oportunidad de buscar y explotar millones de vectores de ataque[63]

Las cifras en Colombia para el año 2019 se llegó a 30.410 delitos informáticos que fueron denunciados (54% más que en el 2018) distribuyendo en los siguientes ataques: [64]

- Phishing (42%)
- Suplantación de identidad (28%)
- Envió de malware (14%)
- Fraudes en medios de pago online (16%)

[62] MARIANO DÍAZ, Rodrigo. La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad. 2020.

[63] Reporte de Europol. Catching the virus: cybercrime, disinformation and the COVID-19 pandemic. Abril 3, 2020.

[64] EL TIEMPO. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia [Sitio WEB], Bogota, Colombia (30, octubre, 2019). Disponible en:https://www.eltiempo. com/tecnosfera/novedades-tecnologia/reportede-ciberataques-en-colombia-2019-de-policianacional-y-ccit-428790

- El uso del ransomware aumento 500% en el país

Antes de identificar los ataques más recurrentes que se están viendo en la actualidad y que posiblemente sean más certeros en una nueva realidad (post-COVID-19), se listaran las modalidades más denunciadas en el 2020 en Bogotá en orden de mayor a menor, de acuerdo con las cifras y reportes de la alcaldía de Bogotá.

Internet, Suplantación de sitios web, pagos en línea, correo electrónico y redes sociales, software malicioso, extracción de datos personales, cajeros automáticos, ingeniería social, banca móvil, transacciones electrónicas, audio respuestas, secuestro de información, keylogger[65]

Lo anterior se dio en empresas pequeñas y medianas como las PYMES, donde efectivamente muchas de ellas no tienen políticas ni controles establecidos para contener dichos ataques, dado que se adoptaron a una nueva realidad y su priorización son sus servicios dejando en segundo plano la seguridad de los datos, la disponibilidad e integridad.

Los ataques que pueden tomar un alto grado de relevación y proliferación son:

1. Malware: Se denomina de esta manera, por los términos en inglés malicius software, a cualquier tipo de código escrito en lenguaje informático, que al ejecutarse realiza acciones dañinas en un sistema de manera intencional y sin el conocimiento del usuario o propietario de dicho sistema. Algunos de los virus más comunes son: Gusanos, troyanos, Adware, Spyware, Keylogger, Ransomware.

2. Ataques de ingeniería social: Son aquellas acciones orientadas a manipular a las personas para realizar ciertas acciones en un sistema informático, o divulgar información confidencial con fines fraudulentos. Comúnmente los ataques de ingeniería social ocurren por correo electrónico o llamados telefónicos, existiendo algunas otras técnicas. Se clasifican de la siguiente manera: Vishing, pretextos, redes sociales, phishing.

Si bien en los últimos tiempos se han visto muchas víctimas de ransomware de distribución masiva mediante técnicas de phishing, la industria del cibercrimen ha mejorado sus resultados mediante el uso de una técnica mixta, compuesta por un primer paso con técnicas de descubrimiento masivo de potenciales

[65] CASTELLANOS VEGA, Carlos Jacinto, et al. Modalidades de cibercrimen en tiempos de Pandemia Covid-19 en Bogotá (Colombia).

vulnerabilidades, que una vez descubiertas son explotadas de manera dirigida, usando procedimientos y herramientas tradicionales. También se ha visto un considerable aumento en la personalización de los contenidos utilizados en las técnicas de ingeniería social, mediante la explotación de datos filtrados en eventos relacionados con fuga de información.[66]

Aunque empezó afectando a grandes empresas e instituciones, como son los casos conocidos de UBER en 2016, o los ataques WannaCry y NotPetya en mayo de 2018, actualmente lo están sufriendo PYMES, instituciones públicas y privadas, y particulares.[67]

Los ataques cibernéticos a organizaciones de atención médica como hospitales, centros médicos y otros no son nuevos. En muchos países, las organizaciones de atención médica se consideran infraestructuras críticas. Desafortunadamente, la pandemia ha dado a los cibercriminales nuevas razones para aumentar sus actividades maliciosas para maximizar el impacto y aumentar sus ganancias.

Un tipo de ataque comúnmente utilizado en hospitales y muchas otras organizaciones es el que involucra “Ransomware”; es un tipo de software malicioso que los delincuentes utilizan para tomar archivos de un dispositivo como rehén, encriptando los datos y posteriormente rechazando el acceso a ellos hasta que la víctima pague un rescate. Como declaró recientemente Europol, la pandemia ha acelerado el uso de este tipo de malware. Afirmaron que “el período entre la infección inicial con ransomware y la activación del ataque de ransomware es más corto.

1. El phishing e ingeniería social.

Los ciberdelincuentes usan técnicas y herramientas para suplantar páginas web transaccionales donde se solicita credenciales o en su efecto número de tarjetas de crédito, son herramientas falsas para engañar a la víctima, claramente las PYMES utilizan sus sistemas transaccionales en línea y es el principal foco de exposición para robos financieros.

2. Ataque de denegación de servicio (DOS)

Este tipo de ataque impide la prestación de un servicio digital o web, bloqueando la web dejándola no disponible. Son virus distribuidos en diferentes equipos (red

[66] MARIANO DÍAZ, Rodrigo. La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad. 2020.

[67] BALLESTEROS, F. (2020). LA CIBERSEGURIDAD EN TIEMPOS DIFÍCILES: ¿Nos ocupamos de ella o nos preocupamos por ella? Boletin Económico de ICE, 3122, 39–48. https://doi-org.bibliotecavirtual.unad.edu.co/10.32796/bice.2020.3122.6993

botnet o zombie) que esperan una orden para actuar y, cuando se produce, intentan acceder simultáneamente todos a la dirección de destino objetivo bloqueándola sin permitir el acceso a los usuarios.

Parece ser que durante lo que llevamos de 2020, los ciberataques por excelencia han sido aquellos de tipo phishing, que han usado la pandemia ocasionada por la COVID-19 como gancho. “Hemos detectado que los cibercriminales, en lugar de inventar nuevos esquemas, han adaptado las estafas tradicionales de phishing al momento actual, centrándolas en el virus para llamar la atención y, por lo general, para instalar malware en el dispositivo de la víctima”, advierte el director general de Kaspersky Iberia

Recientemente se ha descubierto que las plataformas de streaming se han convertido en un importante gancho para los atacantes, motivado por su creciente popularidad. Según los datos de Kaspersky, entre enero de 2019 y abril de 2020 se produjeron un total de 5.577 intentos de ataque a usuarios mientras intentaban acceder a estas plataformas por medios no oficiales, a través de archivos que utilizaban sus nombres como anzuelo[68]

[68] RODRIGUEZ, J. (2020). Ciberseguridad: ¿son conscientes las empresas del peligro del teletrabajo para su integridad online? *Especial Directivos*, *1785*, 68–73.

9 Establecer las mejores prácticas y recomendaciones en función de mantener la seguridad de los principales activos tecnológicos en las PYMES en Colombia del sector comercial en tiempos post COVID-19.

Estas son 10 recomendaciones para empresarios y personas en seguridad de la información en tiempos de COVID-19.

1. Proteja la información sensible y confidencial con firmas digitales, firmas electrónicas, cifrado, claves, contraseñas o con alguna herramienta. Utilice correos seguros como Protonmail. También es recomendable mecanismos de doble autenticación como Google Authenticator.

2. No deje los enlaces públicos de plataformas como Zoom en el momento de convocar una reunión o webinar. Así mismo, en las opciones de seguridad configure las opciones avanzadas de restringir compartir pantalla. Los crackers buscan eventos que tienen públicas las sesiones sin registro previo.

3. Documente de forma empresarial políticas de seguridad de la información para el teletrabajo. Tenga claro desde qué dispositivo ingresa el empleado, ajuste las políticas de continuidad del negocio, revise las políticas de protección de datos personales. Estos reglamentos deben ser más que un documento en Word. Deben tener controles técnicos y herramientas de seguridad informática.

4. Utilice escritorios seguros en la nube que son herramientas para controlar el trabajo remoto.

5. Realice pruebas de Ethical Hacking y análisis de vulnerabilidades a los sistemas que manejen información sensible. Las pruebas técnicas no mienten y muestran la verdad sobre la seguridad de aplicaciones en distintas plataformas.

6. Genere procesos de formación y capacitación en temas de seguridad y privacidad. La cultura es la mejor herramienta para la seguridad y la protección de los datos.

7. Compruebe la seguridad y la configuración de herramientas como chats corporativos, VPN, conexiones remotas, Dropbox, Drive, accesos a plataformas empresariales, entre otras.

8. Realice un monitoreo de los usuarios que pueden tener un riesgo alto en el manejo de información. Clasifique a sus empleados por riesgo de acuerdo con la información que manejan y que tan atractivos pueden ser para ciberdelincuentes. No es lo mismo el riesgo de la persona que hace los pagos y tiene acceso a las cuentas bancarias que alguien que solo maneja archivos en Word.

9. Documente dentro de los contratos de teletrabajo los aspectos de seguridad de la información o modifique los contratos para el trabajo en casa con cláusulas de protección de la información.

10. Desconfié de noticias falsas, enlaces extraños, promociones falsas, los cuales pueden llevar a temas de phishing, spam, malware, virus, etc. Compruebe la fuente de un correo, una noticia o un WhatsApp. Puede ingresar a los boletines informativos del CSIRT de la policía nacional para estar informado de posibles riesgos.

Los 10 errores de seguridad que las PYMES no deben cometer

- Reconocer que hay riesgos: La importancia de identificar y ser conscientes de los posibles riesgos que conlleva utilizar las diferentes tecnologías para uso empresarial.
- No dedicar suficientes recursos: Es importante desde el inicio una planeación financiera y de recursos humanos capacitados en mantener un sistema de gestión de riesgos y de ciberseguridad.
- No mantener actualizado el software: Es la practica estándar a ser aplicada para evitar vulnerabilidades y cerrar la brecha de seguridad.
- No tener en cuenta los riesgos que generan sus empleados: Los empleados o actores internes es el eslabón más débil de la cadena en las organizaciones, por eso su importancia de capacitar y concientizar una cultura de seguridad.
- No capacitar a los empleados: Culturizar y capacitar a los empleados evita en cierta medida la materialización de riesgos tan simples como la ingeniería social
- No tener software de seguridad: Es importante contar con herramientas de seguridad como mínimo un antivirus.
- No estar pendiente de los equipos de sus empleados: Importante asegurar cada uno de los activos tecnológicos de los empleados, llevando un inventario y control en cuanto a los paquetes de software instalado y un control de versiones para minimizar vulnerabilidades conocidas.
- No proteger bien los datos: Proteger el activo de información mas valioso que puede tener las organizaciones, su protección asegura el éxito de los objetivos corporativos.
- No manejar bien los backups: Las estrategias de recuperación de datos es de vital importancia en función a la disponibilidad, confidencialidad e integridad, pilares de la seguridad de la información, un mal manejo

ocasionaría perdidas económicas, reputacionales y legales para la organización.

- No tener listo un plan de respuesta: Definir Planes de contingencias, un plan de respuesta frente a amenazas persistentes de ciberseguridad es de vital importancia para contener y minimizar impactos, de igual forma estos planes y respuestas de deben poner en práctica para sensibilizar a todos los colaboradores y estar prestos atender un escenario real.

Algunas recomendaciones para ser aplicadas en el programa de seguridad de información en PYMES:

1. Actualizar totalmente los equipos y contar con las últimas versiones de los sistemas operativos.
2. Verificar el uso y envío adecuado de la información teniendo en cuenta sus canales y receptores.
3. Configurar los equipos y la nube para facilitar la creación de copias de seguridad. Esta herramienta es una buena opción para las PYMES que no tienen los recursos para invertir en una infraestructura física y cuya seguridad no pueden garantizar de manera óptima.
4. Reportar inmediatamente cualquier actividad inusual asociada con un posible ataque que afecte los documentos electrónicos.
5. En caso de sospecha de un ataque se debe inspeccionar los activos susceptibles a ataques: discos duros, USB, computadores, dispositivos móviles y en general la información que pudo perderse, encriptarse o publicarse.
6. Evaluar los daños frente a un experto forense digital.
7. Revisar si ha ocurrido algún tipo de fuga en la información: se debe validar si la causa fue interna o externa.
8. Monitorear los incidentes generados.
9. Realizar seguimiento al incidente: es necesario crear un espacio de participación en la identificación de la brecha.

Acciones de prevención y mejora.[69]

[69] ENTER.CO La alternancia creará más vulnerabilidades en las empresas ¿Qué hacer? [Sitio WEB], (23, febrero,2021) Disponible en: https://www.enter.co/empresas/la-alternancia-creara-mas-vulnerabilidades-en-los-dispositivos/

10 CONCLUSIONES

Políticas como la administración y gestión de perfiles, política gestión de acceso y de privilegios, políticas en cuanto a los requerimientos mínimos como un antivirus actualizado, una conexión segura sobre internet (VPN) permiten definir lineamientos de cumplimiento obligatorio en las PYMES conllevando a la implementación y ejecución de una barrera por defecto básica para asegurar los principales activos tecnológicos de la organización en un escenario de COVID-19 y posterior a las nuevas necesidades de la resiliencia.

Se identificaron algunas políticas claves a implementar en las PYMES:

- Políticas de teletrabajo, indicando las condiciones idóneas mínimas para realizar la conexión y trabajar de forma remota.

- Políticas para definir las diferentes categorías de datos que se gestionaran en las PYMES, permiten un pertinente manejo en cuanto a la manipulación y transmisión de información.

- Políticas frente a la protección de datos.

- Políticas en cuanto a la formalización de documentos (firmas digitales), certificados de seguridad.

También controles claves, donde su implementación mitiga en cierta manera la materialización de algunos riesgos:

- Controles como la implementación de firmas digitales, certificados de seguridad.

- Controles en cuanto a la parametrización de herramientas colaborativos, restringiendo ciertas características susceptibles a la fuga de información.

- Controles periódicos como la ejecución de pruebas de penetración, pruebas Ethical hacking, para identificar vulnerabilidades y proceder aplicar correctivos en función de cerrar brechas de seguridad.

- Controles preventivos en cuanto a la sensibilización de la cultura de seguridad de la información y ciberseguridad por medio de capacitaciones.

Tras un análisis del objetivo general y específicos previamente revisados en capítulos anteriormente, se procede a resaltar y resumir los siguientes aspectos:

Analizar las políticas y los controles mínimos básicos de seguridad de la información por medio de una revisión documental basada en escenarios COVID-19 para controlar y minimizar impactos negativos en la seguridad de los principales activos tecnológicos de una PYME colombiana del sector comercial.

La revisión documental nos permite identificar las bases en cuanto a políticas, procedimientos y controles las cuales fueron determinadas por el uso común y repetitivo en las diferentes revisiones las cuales permitieron determinar los aspectos mínimos que se deben aplicar y que deben considerar a las PYMES del sector comercial en Colombia, controles y procedimientos tan básicos como la implementación de VPN para el trabajo remoto, el cifrado de información en la transmisión de correos electrónicos, la implementación de un antivirus, la implantación de políticas de seguridad, entre otros son las claves para un mínimo de defensa que deben tener considerar las PYMES del sector comercial, siendo este uno de los más afectados durante la Pandemia del COVID-19, su modelo de negocio era uno de los que más estaban lejos de las automatizaciones y de la tecnología 2.0 y fueron obligado a transformarse de una manera muy rápida para la continuidad de sus operaciones donde su costo de impacto negativo fue demasiado alto porque no consideraron las barreras de seguridad mínimas que deberían haberse implementado una vez iniciara la pandemia.

La ISO 27001 y la ISO 27002 son los principales estándares de la seguridad de la información, son los que permiten definir los lineamientos, objetivos y controles para mitigar diferentes vulnerabilidades en los sistemas internos y externos de las organizaciones, también permiten reducir los riesgos previamente identificados por medio de un análisis de riesgos y llevarlos a un nivel de riesgo aceptables. Tanto los lineamientos como el análisis de riesgo conforman un Sistema de Gestión de Seguridad de la Información que están determinante e importante para las organizaciones, para nuestra revisión es totalmente aplicable en las PYMES, implementar un SGSI que cubre los lineamientos, procedimientos y controles en función de los usuarios, la información y la infraestructura.

La improvisación de muchas PYMES acelero los ataques de ciberseguridad, ataques que a la fecha anterior siempre han estado latentes en grandes compañías pero en un bajo porcentaje de visibilidad, a raíz de la pandemia las PYMES del sector comercial migraron sus operaciones a un entono virtual apoyado de herramientas tecnológicas pero no fueron consecuentes en desarrollar políticas, procedimientos y controles para aplicar a todo el ecosistema que integra las PYMES (activos y funcionarios) como producto de la falencia, las vulnerabilidades y debilidades crecieron exponencialmente y los ataques ya conocidos como: el phishing, la suplantación de identidad, el malware, los fraudes, el ramsonware, la ingeniería social, los ataques de denegación de servicio aprovecharon esa brecha de seguridad no contemplada en la nueva realidad.

Por ultimo las mejores prácticas que se abordaron en la monografía brindan una seguridad idónea en la infraestructura tecnológica como también en la información y en el personal de las PYMES logrando un ecosistema seguro y sobre todo predispuesto a dar respuesta y mitigar las amenazas existentes, no asegura ni garantiza que los controles serán 100% efectivos contra las amenazas sin embargo existen algunas bases de primera línea capaces de responder y prevenir ataques simples y como esto es un SGSI siempre estará dispuesto a la mejora continua de acuerdo al entorno que este expuesta la PYME.

De acuerdo con la revisión documental realizada se puede identificar en gran medida la importancia de conocer las diferentes normas y estándares de seguridad de la información como la ISO 27001 contextualizando las mejores prácticas y recomendaciones a implementar en un sistema de gestión en Seguridad informática contemplando un abanico de opciones desde lo más esencial hasta lo más detallado posible en función a procedimientos y controles.

Las PYMES siempre se han caracterizado como negocios emergentes, apoyándose en las últimas tecnologías para cumplir con los objetivos corporativos y empresariales, pero al hacer uso de estas herramientas no muchas veces contemplan la barrera de seguridad o los procedimientos que deben implementarse para hacer uso de la tecnología, ese desconocimiento o ausencia de implementación en procedimientos y controles, conlleva a que se materialice eventos de ciberseguridad, afectando la disponibilidad, integridad y confidencialidad del activo mas importante que pueda tener cualquier empresa o PYME como son los datos o información.

A causa de la pandemia COVID-19 muchas de estas empresas, se vieron obligadas a reaccionar y responder en el momento, sin tener una planeación bien definida en cuanto a la continuidad de servicios tan básicos y elementales que gracias a la tecnología se pueden implementar fácilmente, pero descuidan el borde o esa barrera de seguridad, la cual es el desconocimiento y la posible materialización del riesgo latente de muchas PYMES.

Con ayuda de la documentación ya existe de mejores prácticas como la ISO 27001 y de las diferentes revisiones documentales se identificó políticas, procedimientos y controles básicos que se pueden implementar a las diferentes tecnologías (hardware y software) actuales.

11 RECOMENDACIONES

Identificar los principales activos que tiene las PYMES es lo primero que se debe realizar para determinar su criticidad en función a la probabilidad e impacto y con ello establecer los controles básicos a implementar, algunos controles que como mínimo se deben implementar de acuerdo con la revisión son:

- Invertir en aplicaciones de seguridad
- Utilizar protocolos seguros en redes wifi públicas como https y SLS.
- Utilizar VPN para realizar conexiones seguras.
- Realizar sensibilizaciones en cuanto a la seguridad de la información y los diferentes ataques de ciberseguridad.
- Reducir cuentas de administrador.
- Actualización del Sistema Operativo y software en general
- Chequeo continuo de logs
- Establecer procedimientos para actuar frente a incidentes de ciberseguridad.
- Realizar copias de seguridad.

La importancia de reconocer también los diferentes vectores de ataque en ciberseguridad en cuanto a su modo operandi, su forma de impactar, su funcionamiento permite de cierta forma implementar procedimientos estándares por defecto que también deben ser contemplados por las PYMES como parte de esas acciones emergentes y rápidas en la que se comportan.

A continuación, se enumeran una serie de recomendaciones cuya posible implementación son vitales para mejorar y reforzar el mínimo de bases, controles, procedimientos y políticas aplicar en las PYMES del sector Comercial de Colombia.

Al tratarse de un SGSI siempre la mejora continua estará presente, se deberá identificar las nuevas modalidades de ataques como también la implementación de otras herramientas tecnológicas de detección y de respuesta acorde a la situación.

Al implementar políticas se recomienda hacerlo con el apoyo y visibilidad de la alta gerencia, que genere sensibilización e importancia para toda la organización.

Se debe sensibilizar el programa de Ciberseguridad, de igual forma capacitar y entrar en razón los aspectos de seguridad, las políticas y los controles.

Contemplar los controles de seguridad de la información aplicados a las terceras partes o proveedores que conforman la cadena de suministro, es vital revisar que cuenten con buenas medidas de mitigación y evaluar efectividad.

Se recomienda siempre actualizar los sistemas, sistemas operativos, sistemas ofimáticos, servidores, servicios web a las ultimas actualizaciones, parches de seguridad que mejoran vulnerabilidades o bugs detectados, etc.

Realizar pruebas a los controles, a los procedimientos, a las respuestas ante eventos de crisis en escenarios de ciberseguridad, con ello se mide la efectividad y eficiencia de los procedimientos y controles establecidos.

12 BIBLIOGRAFÍA

27001 ACADEMY. ¿Qué es norma ISO 27001? [Sitio WEB], La entidad, Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

ALLUE, Marta; DELGADO, Boris; FERNÁNDEZ, Carlos Manuel. Privacidad de la información: clave en la transformación digital de la era COVID-19. AENOR: Revista de la normalización y la certificación, 2020, no 362, p. 5-8.

AMERCAN THORACIC SOCIETY. ¿Qué es el COVID-19? s/n [en Línea] ATS Patient Education Series (2020)

ARIAS, Diana. Ciberseguridad: uno de los retos que dejo el 2020 [en línea], 28, enero, 2021. Disponible en: https://www.enter.co/guias/lleva-tu-negocio-a-internet/ciberseguridad-uno-de-los-retos-que-dejo-el-2020/

BAKER, Stewart. Et al. En el punto de mira: las infraestructuras críticas en la era de la ciberguerra McAfee. [en línea]Madrid España, [2010] Disponible en: http://img.en25.com/Web/McAfee/CIP_report_final_es_fnl_lores.pdf

BALLESTEROS, F. (2020). LA CIBERSEGURIDAD EN TIEMPOS DIFÍCILES: ¿Nos ocupamos de ella o nos preocupamos por ella? Boletín Económico de ICE, 3122, 39–48. https://doi-org.bibliotecavirtual.unad.edu.co/10.32796/bice.2020.3122.6993

BANCOLOMBIA, Conoce todo sobre las pymes en Colombia [Sitio WEB], Colombia, La entidad [18, Julio,2018], Disponible en: https://www.grupobancolombia.com/wps/portal/negocios/actualizate/legal-y-tributario/todo-sobre-las-pymes-en-colombia

Barbosa, J. S., Silva, D. B. e, Oliveira, D. C. de, Jesús, D. C. de, Miranda, W. F. de, Research, Society and Development. En: Protección de datos y seguridad de la información en la pandemia COVID-19: contexto nacional, 2021 Vol. 10 No. 2; e40510212557

BARRETT, M. P. (2018). *VEQI SVO JSV -QTVSZMRK 'VMXMGEP Infrastructure Cybersecurity. Gaithersburg, Maryland (USA): Nacional Institute of Standards and Technology - U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

BUSSELEN, M. Por qué el ciberdelito sigue siendo un desafío empresarial preocupante en un mundo bloqueado por COVID. [en línea] [septiembre 2020]. Disponible en: www.crowds-trike.com/blog/why-cybercrime-remains-a-worrying-business-challenge-in-a-covid-lockdown-world.

CALDER, A. y Watkins, S. Information Security Risk Management for ISO 27001/ISO 27002.IT Governance Publishing Ltd. United Kingdom. 2019

CARPENTIER, Jean-François. La seguridad informática en la PYME: Situación actual y mejores prácticas. Ediciones ENI, 2016.

CASTELLANOS VEGA, Carlos Jacinto, et al. Modalidades de cibercrimen en tiempos de Pandemia Covid-19 en Bogotá (Colombia).

COVID-19 pandemic. Abril 3, 2020.
DE SALVADOR CARRASCO, Luis. Los problemas estructurales en el planteamiento de la ciberseguridad. En: Boletín Electrónico del Instituto español de Estudios Estratégicos, 2014, p. 1-27.

DE TOMAS, S. Hacia una cultura de ciberseguridad: capacitación especializada para un "proyecto compartido". En: Especial referencia al ámbito universitario. ICADE. 2016 92, 14-47.

Deloitte, El estado de la ciberseguridad en España: Digitalización, teletrabajo y ciberataques en tiempos de pandemia [Sitio WEB], la entidad [2020], Disponible en: www2.deloitte.com/es/es/pages/risk/arti-cles/estado-ciberseguridad.html

EL CIBERESPIONAJE PUIME MAROTO J. El Ciber espionaje y La Ciberseguridad.; 2009. Accessed November 30, 2020. http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.4549946ART&lang=es&site=eds-live&scope=site

El economista, Lecciones de un CEO, según John Chambers de Cisco, [Sitio WEB], la entidad [1, diciembre 2019], Disponible en: https://www.eleconomista.com.mx/tecnologia/Lecciones-para-un-CEO-segun-John-Chambers-de-Cisco-20191201-0009.html

El mundo, Hay dos tipos de empresas: a las que han atacado y las que atacaran [Sitio WEB], la entidad [3, octubre 2018], Disponible en: https://www.elmundo.es/comunidad-valenciana/2018/10/03/5bb3acf4268e3ef5548b45af.html

EL TIEMPO. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia [Sitio WEB], Bogotá, Colombia (30, octubre, 2019). Disponible en: https://www.eltiempo. com/tecnosfera/novedades-tecnologia/reportede-ciberataques-en-colombia-2019-de-policianacional-y-ccit-428790

ENTER.CO La alternancia creará más vulnerabilidades en las empresas ¿Qué hacer? [Sitio WEB], (23, febrero,2021) Disponible en: https://www.enter.co/empresas/la-alternancia-creara-mas-vulnerabilidades-en-los-dispositivos/

GALAN, C. & GALAN C., C. La ciberseguridad pública como garantía del ejercicio de derechos. En: Derecho & Sociedad. 2016. 47, 293-306.

GALAN, C. M., & Galán Cordero, Derecho & Sociedad, La ciberseguridad pública como garantía del ejercicio de derechos. [en línea] 2016 (47), 293-306.Disponible en: http://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/18892

GOMEZ, F. y católico, D. Relación de la presentación de información de negocios online con las variables financieras en las empresas colombianas. Revista Facultad de Ciencias Económicas: Investigación y Reflexión [en línea] (2010). Disponible en: https://bit.ly/2RtJRp3

HENRIQUEZ, A.P., Silva, M.M., Poleto, T., Camara, L., & Cabral, A.P. (2018). Cybersecurity risk analysis model using fault tree analysis and 215 Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia Rev. Crim. / Volumen 62 - Número 2 - mayo-Agosto 2020 - pp. 199-217 - ISSN 1794-3108 - Bogotá, D. C., Colombia fuzzy decision theory. International Journal of Information Management, 43, 248-260. https:// doi.org/10.1016/j.ijinfomgt.2018.08.008

HERNANDEZ, Enrique. El ciberterrorismo en la actualidad AUDITORIA EN INFORMÁTICA, UN ENFOQUE METODOLÓGICO 1996

HOMELAND SECURITY [Sitio WEB], La entidad. Disponible en: www.dhs.gov
INCIBE. Protección de la información [Sitio WEB]Madrid, España (28, noviembre 2017). Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

ISEC AUDITORS. Controles del CIS [Sitio WEB] [28, noviembre, 2019]. Disponible en: https://blog.isecauditors.com/2019/11/novedades-version-7-1-controles-cis.html

KASPERSKY. El ransomware: qué es, cómo se lo evita, cómo se elimina [Sitio WEB] Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

LEMA, Luis López. La gestión de la información durante etapas de teletrabajo en la época de la COVID-19. Perspectivas, n. 3, 2020.

MARIANO DÍAZ, Rodrigo. La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciber inmunidad. 2020.

MAROTO, Juan Puime. El ciber espionaje y la ciberseguridad. En La violencia del siglo XXI. Nuevas dimensiones de la guerra. Instituto Español de Estudios Estratégicos, 2009. p. 45-76.

MAROTO, Juan Puime. El ciber espionaje y la ciberseguridad. En La violencia del siglo XXI. Nuevas dimensiones de la guerra. Instituto Español de Estudios Estratégicos, 2009. p. 45-76.

MINISTERIO DE LAS TICS. [Sitio WEB], La entidad, Disponible en: https://www.mintic.gov.co/portal/inicio/Micrositios/I+D+I/Nodos/6120:Ciberseguridad

MONTOYA CORREA, Tatiana; MOLANO LUJÁN, Andrés. Diseño de un esquema de seguridad informática para PYMES, como la primera línea de defensa para la protección contra amenazas de Ransomware, utilizando los lineamientos de la norma ISO27001: 2013. 2018.

NACIONES UNIDAS (2020). Pymes y COVID 19: hacia una recuperación sostenible. Red Española del Pacto Mundial.

NETWRIX, Survey: 85% of CISOs admit they sacrificed cybersecurity to enable employees to work remotely [Sitio WEB]Irvine, CA,La entidad [22, Septiembre,2020], Disponible en: https://www.netwrix.com/netwrix_survey_cisos_admit_they_sacrificed_cybersecurity_to_quickly_enable_employees_to_work_remotely.html

NEWS, Who´s watching whom? Camera-equipped TV can be hacked, says researcher[Sitio WEB],La entidad [13, Diciembre,2012], Disponible en: https://www.nbcnews.com/technology/whos-watching-whom-camera-equipped-tv-can-be-hacked-says-1C7596675

OSPINA DIAZ, Milton Ricardo, & SANABRIA RANGEL, Pedro Emilio. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad [en línea],(26,noviembre, 2020) 62(2), 199-217. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=en&tlng=

PANDA SECURITY, La ciberseguridad objetivo preferente de las empresas [Sitio WEB]La entidad [18, Marzo, 2015] Disponible en: https://www.pandasecurity.com/es/mediacenter/malware/la-ciberseguridad-objetivo-preferente-de-las-

empresas/?utm_source=twitter.com&utm_medium=smedia&utm_content=SM_ES_TW_PNCIBERSEGURIDAD_180315&utm_campaign=genericCampaign

PAYA, C.; Cremades, A. & DELGADO, J. El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad de Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. Revista Policía y Seguridad Pública [en línea], 2016 7(1), 237-270.Disponible en: http://dx.doi.org/10.5377/rpsp.v7i1.4312

POWERDATA. Lo que debes saber sobre el reglamento general de protección de datos [Sitio WEB] España (26, agosto, 2019). Disponible en: https://www.powerdata.es/ gdpr-proteccion-datos

PROTEGERSE, ¿Que nos depara un futuro incierto en materia de ciberseguridad? [Sitio WEB]La entidad [4, diciembre,2020]Disponible en: https://blogs.protegerse.com/2020/12/04/tendencias-2021-que-nos-depara-un-futuro-incierto-en-materia-de-ciberseguridad/

RATTI BITTINGER, Gabriela María. Desarrollo de una guía de controles de ciberseguridad para la protección integral de la PYME. 2017.

REA-GUAMAN, M., Calvo-Manzano, J. A., & Feliu, T. S. (2018). Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas. (Spanish). CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 1–6.

Reporte de Europol. Catching the virus: cybercrime, disinformation and the
REYDES. La OSSTTM [Sitio WEB][17, Noviembre, 2015]. Disponible en: http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual#:~:text=OSSTMM%20(Open%20Source%20Security%20Testing%20Methodology%20Manual)%20proporciona%20una%20metodolog%C3%ADa,evita%20suposiciones%20y%20evidencia%20anecd%C3%B3tica.
RISS, Boris Delgado; SÁNCHEZ, Carlos Manuel Fernández. Las mejores prácticas ISO contra el Covid-19 y crisis futuras. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 2020, vol. 29, no 140, p. 94-96.

RISS, Boris Delgado; SÁNCHEZ, Carlos Manuel Fernández. Revista SIC: ciberseguridad, seguridad de la información y privacidad. Las mejores prácticas ISO contra el Covid-19 y crisis futuras. 2020, vol. 29, no 140, p. 94-96.
Rodríguez Pinzón, É. Impacto económico, social y político de la COVID-19. [en línea] Madrid España, [30, abril, 2020] Disponible en: https://doi.org/10.33960/ac_24.2020

RODRIGUEZ BACA, L. S., Puente de la Vega, C. F. C., Mejía Corredor, C., & Alarcón Diaz, M. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad

de la información de una empresa privada peruana. (Spanish). Propósitos y Representaciones, 8(3), 473–483

RODRÍGUEZ, David E. Acosta. Categorización funcional de los diferentes tipos de controles de seguridad y su aplicabilidad en la estrategia de protección corporativa. Revista SIC: ciberseguridad, seguridad de la información y privacidad, [en línea], 2018, vol. 27, no 130, p. 122-124.

RODRIGUEZ, J. (2020). Ciberseguridad: ¿son conscientes las empresas del peligro del teletrabajo para su integridad online? Especial Directivos, 1785, 68–73.
ROJAS CELIS, J D., Hoyos Rodríguez, R D., y Castro Reyes.Propuesta de diseño de una VPN de acceso remoto con túneles GRE para permitir plan de continuidad tic para las mipymes del sector económico terciario, en empresas dedicadas al comercio de equipos partes y piezas electrónicas en Bogotá D.C. [en línea] Tesis de pregrado, Universidad Cooperativa de Colombia. (2020) Disponible en: http://hdl.handle.net/20.500.12494/28389

SAAVEDRA, B., y Parraguez, L. La ciberseguridad: análisis político y estratégico I. Revista Fuerzas Armadas [en línea] (2018), 91(243), 44-51

STORM, Darlene. Downloading of software updates for lifesaving medical devices proves very dangerous.[en Linea][19, Junio, 2012], Disponible en: http://blogs.computerworld.com/malware-and-vulnerabilities/20554/software-updates-lifesaving-medical-devices-found-tainted-malware

UNE 71504 UNE 71504:2008, “Metodología de análisis y gestión de riesgos para los sistemas de información

VELASQUEZ V., F. La estrategia, la estructura y las formas de asociación: fuentes de ventaja competitiva para las Pymes colombianas. Estudios Gerenciales. 2004 093, 73-97.

Vera, J. M. Ciberseguridad post-COVID : ¿Qué papel jugará la ciber inteligencia frente a los cisnes negros digitales que llegarán tras la vacuna? En: Journal of Economic & Business Intelligence, 2021. 11–23.

VERA, Víctor Daniel Gil; VERA, Juan Carlos Gil. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia et técnica, [en línea] 2017, vol. 22, no 2, p. 193-197.

World Economic Forum. Future Series: Ciberseguridad, tecnología emergente y riesgo sistémico [Sitio WEB] [noviembre, 2020], Disponible en: www.weforum.org/reports/future-series-cybersecu-rity-emerging-technology-and-systemic-risk.