Análisis Documental para la Creación de un Equipo de Respuestas a Incidentes Informáticos orientado a Pequeñas y Medianas Empresas del Sector Económico Colombiano

Katherin Andrea Franco Suarez y Luis Fernando Zambrano Hernández

Universidad Nacional Abierta Y A Distancia - UNAD
Escuela De Ciencias Administrativas, Contables, Económicas Y De Negocios - ECACEN
Maestría En Administración De Organizaciones
Octubre De 2021

Página De Aceptación

_____

Sebastián Rodríguez Ramírez

Director Trabajo de Grado

_____ _____

Jurado Jurado

Bogotá - 2021

Agradecimientos

Al profesor Sebastián Rodríguez Ramírez, director de esta monografía por su intención y contribución desde su experiencia y conocimiento para la construcción de este documento monográfico. Al equipo docente de la Maestría en Administración de Organizaciones, al profesor Héctor Martínez por haber compartido con nosotros sus experiencias profesionales.

Dedicatoria

A nuestras familias por estar siempre presentes a través de su constante apoyo, esfuerzo y dedicación. Motivándonos alcanzar nuestros objetivos y seguir construyendo nuestro proyecto de vida profesional. Gratitud total.

Resumen

Actualmente las Tecnologías de la Información y la Comunicación se han transformado en un sector transversal de todos los sistemas modernos. Según el diario El País, para el año 2018 en Colombia un 96% de empresas utiliza este medio para el desarrollo de sus actividades (País, 2018). La hipótesis de este estudio monográfico plantea que, si las organizaciones no se anticipan ante potenciales riesgos de ciberseguridad se verán afectadas en su infraestructura tecnológica, ocasionada por un evento o incidente informático, el cual genera pérdidas financieras y reputacionales, acciones legales y la afectación en la continuidad de su negocio.

En virtud de lo anterior, este documento se construye teniendo como referente una metodología de investigación cualitativa, planteada a través de cuatro capítulos incluyendo los objetivos propuestos: 1. El desarrollo metodológico; 2. El estado actual de la gestión de la ciberseguridad y de la protección de los datos en las PyMES colombianas; 3. un plan estratégico que contribuya al robustecimiento de las capacidades del aseguramiento digital; 4. una propuesta tecnológica para la gestión de un evento de ciberseguridad.

Lo antes citado conlleva a la viabilidad de la creación de un Equipo de Respuesta a Incidentes Informáticos – CSIRT[1], que brinde servicios estratégicos para la gestión de eventos de ciberseguridad a PyMES.

Este documento está dirigido a las PyMES del sector económico colombiano, Empresas del sector de la seguridad de la información, comunidades académicas y todas las partes interesadas que estén involucradas en la reducción de brechas digitales, aportando en el desarrollo de capacidades de Ciberseguridad, fortaleciendo la sostenibilidad y la continuidad del negocio.

[1] CSIRT: Sigla que significa Centro o Equipo de Respuesta a Incidentes Informáticos, que tiene como propósito la coordinación de tares de respuesta a eventos o incidentes informáticos

Palabras claves: Brechas digitales, desarrollo de capacidades, negocio, protección de datos, tecnologías de la información.

Abstract

Nowadays, the information and communication technologies have become a transversal sector of all modern systems. According to the newspaper El País, in 2018 96% of Colombian companies use this medium to develop their activities (País, 2018).

The hypothesis presented for this monographic study pretend to evidence that if small and médium organizations do not anticípate in face of potential cybersecurity risks can be affected in their technological infrastructure caused by a system incident, which generates financial and reputational losses, legal actions and impact in business continuity along time.

This document is structured doing a reference to the qualitative research methodology, giving to the reader the develop of the subject in four chapters. Included this objectives: 1. Methodological development. 2. The current state of cybersecurity management and data protection in Colombian SMEs. 3. a strategic plan that contributes to the strengthening digital assurance capabilities. 4. a technological proposal to manage a cybersecurity event.

The results are concentrated in showing the viability of creating a Computer Incident Response Team - CSIRT, which provides strategic services to manage cybersecurity events in SMEs.

This document is aimed at SMEs in the Colombian economic sector, information from companies in the security sector, the academic community and all stakeholders that are involved in reducing digital gaps, contributing to the development of Cybersecurity capacities and strengthening sustainability. and business continuity.

Keywords digital gap, business capacity development, data protection, information technology.

Prólogo

Teniendo presente la disrupción generada por la Pandemia a partir del año 2020, y la necesidad de aportar en el desarrollo de capacidades que contribuyan en mejorar entornos digitales seguros, este documento monográfico surge dada la necesidad de abordar dos factores fundamentales. UNO: El aportar al sector de las Pequeñas y Medianas Empresas del Sector Económico Colombiano, información con el fin de reconocer cual es el estado actual de las capacidades en ciberseguridad con las que cuentan, y como podrían mejorar la seguridad informática y la protección de datos; DOS: Presentar al sector de la Ciberseguridad información relacionada con la viabilidad de poder crear un CSIRT, que brinde soporte a PyMES a partir de una línea de negocio enfocada en Ciberseguridad.

Durante el desarrollo de esta propuesta, se presentaron dificultades que poco a poco se convirtieron en oportunidades. Una de estas fue el contar con pocos recursos en términos de datos estadísticos que permitiera para los años 2019 – 2020, determinar cuál es el comportamiento de las organizaciones colombianas en términos de estrategias relacionadas con ciberseguridad. En este ejercicio se evidenció la necesidad de indagar como las organizaciones, llevan a cabo procesos de aseguramiento de su infraestructura tecnológica y su información. Esta acción contribuirá en la construcción de un entorno digital que aporte en mejorar prácticas de gobierno de TI y su impacto en la gestión del conocimiento.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Introducción

Las Pequeñas y Medianas Empresas del sector colombiano vienen migrando sus servicios a la virtualidad, lo cual ha generado grandes oportunidades relacionadas con la proyección y ampliación de sus mercados, trayendo consigo el mejorar su competitividad y su reputación. No obstante, el hecho de implementar estas estrategias genera riesgos latentes asociados a sus activos de información, los cuales pueden convertirse en eventos adversos que afecten la continuidad del negocio. Hoy en día el adoptar estrategias que permitan reducir el riesgo a los cuales están expuestas las organizaciones, representa el contar con talento humano capacitado, infraestructura tecnológica o aliados estratégicos que suplan estas tareas de prevención o remediación ante un evento o incidente informático. Desafortunadamente este escenario, no es el común denominador en las PyMES puesto que en la proyección de sus presupuestos se estima un bajo recurso para la implementación de tecnologías que permitan reducir el riesgo.

La metodología de investigación cualitativa usada para el desarrollo de esta monografía, se construye a partir de cuatro capítulos: Primero se aborda el desarrollo metodológico; Seguido a esto, se establece el estado actual de la gestión de la ciberseguridad y de la protección de los datos en las PyMES colombianas; En el tercer capítulo, se presenta un plan estratégico que contribuye al robustecimiento de las capacidades del aseguramiento digital; Y, finalmente se plantea una propuesta tecnológica para la gestión de un evento de ciberseguridad.

Lo anterior da respuesta a la pregunta problema, la hipótesis y cada uno de los objetivos específicos propuestos.

De esta forma, las Pequeñas y Medianas Empresas del Sector productivo colombiano, el sector de la Ciberseguridad y sus partes interesadas podrán contar con este referente académico,

que plantea la viabilidad de la creación de un Equipo de Respuestas a Incidentes Informáticos teniendo presente el análisis de factores económicos, tecnológicos, políticos y sociales.

Planteamiento del Problema

Debido a la crisis sanitaria que atraviesa el mundo, específicamente en Colombia desde el mes de marzo de 2020 (Minsalud, 2020), hizo que muchas empresas que desarrollaban sus actividades administrativas y directivas de forma física tuvieran que migrar de forma forzada al uso de la virtualidad como canal de comunicación y el teletrabajo como estrategia para reducir un impacto económico (Mundo, 2020). Según reporte del Centro Cibernético de la Policía[2] de junio de 2020, se indica que la propagación de la pandemia ha demandado un exponencial incremento en el uso de las tecnologías de la información, que a su vez genera espacios vulnerables a ataques informáticos (CECIP, 2020). Lo anterior se ve reflejado en: pérdida de información propia y de sus partes interesadas, daño a la imagen corporativa y a su reputación y daño en sus activos de información tangibles e intangibles, los cuales hacen impacto de forma directa en pérdidas económicas.

La revista Dinero indica que la pandemia ha generado un crecimiento en la mejora de las Tecnologías de la Información, debido a que es una alternativa de operatividad de forma remota, e indica que la inversión destinada para tecnología hace 5 años era de no más de un 5% en su presupuesto, y hoy en día oscila entre un 12 y un 18% (Dinero, 2020). Según el Banco Interamericano de Desarrollo[3], para el año 2017 las empresas de orden público y privado del país señalaban que se sentían preparadas para dar respuesta a un ataque informático. Sin embargo, se considera que se deben hacer esfuerzos en temas de inversión en la seguridad digital, ya que las empresas destinan pocos recursos para la seguridad digital (BID, MINTIC, & OEA, 2017).

---

[2] El Centro Cibernético de la Policía es una iniciativa del estado colombiano que tiene como objetivo el recopilar y dar respuesta a denuncias de orden cibernético

[3] El Banco Interamericano de Desarrollo – BID, es la fuente de financiación más importante que impulsa el desarrollo económico, social e institucional para América latina

Por otra parte, el Informe de Tendencias de Ciber Crimen Para Colombia del año 2019 – 2020 presentado por la Cámara Colombiana de Informática y Telecomunicaciones[4] - CCIT y la Policía Nacional – PONAL (CCIT & PONAL, 2019), señala que los delitos más denunciados en su orden son los de: hurto por medios informáticos, violación de datos personales, acceso abusivo a sistemas informáticos y transferencia no consentida de activos, e indica que los cibercriminales están direccionando su actuar delictivo hacia las pequeñas y medianas empresas, entidades financieras y grandes compañías, especialmente las que se encuentran localizadas en las principales ciudades como Bogotá, Cali, Medellín, Barranquilla y Bucaramanga.

Debido a lo anteriormente expuesto, se plantea la pregunta problema que será el eje para el desarrollo de este estudio monográfico.

Pregunta Problema

¿De qué forma un Equipo de Respuestas a Incidentes Informáticos puede contribuir en la mejora continua de los procesos de ciberseguridad y continuidad de negocio para una Pequeña o Mediana Empresa del Sector Económico Colombiano?

[4] La Cámara Colombiana de Informática y Telecomunicaciones es una entidad gremial que agrupa el sector de las telecomunicaciones y la informática en Colombia

Hipótesis

Las organizaciones que no se anticipan ante potenciales riesgos de ciberseguridad, se verán afectadas en su infraestructura tecnológica ocasionada por un evento o incidente informático, el cual genera pérdidas financieras y reputacionales, acciones legales y la afectación en la continuidad del negocio.

Justificación

Uno de los activos más importantes en una organización es la información. Es por esta razón, que salvaguardar toda la infraestructura tecnológica que apalanca este proceso es necesario. Para el año 2017 la empresa B2B expone que las empresas con un equipo de respuesta a incidentes informáticos estiman su daño financiero en un 50% menos que el costo que puede generar un incidente cibernético si no se cuenta con este. (Kaspersky, 2017).

Establecer un Equipo de Respuestas a Incidentes Informáticos o un Centro de Operaciones de Seguridad - SOC[5] implica comprar herramientas tecnológicas, crear políticas, procesos y procedimientos y contar con un equipo de trabajo que realice las acciones de gestionar y actuar, a partir de eventos o incidentes de ciberseguridad presentados. Teniendo en cuenta esto, poner en marcha este tipo de iniciativas constituye un desafío para cualquier negocio ya que se requiere tiempo y presupuesto, recursos que, por lo general los líderes de seguridad encuentran difíciles de justificar.

Es por esto, que presentar la viabilidad de crear un Equipo de Respuestas a Incidentes Informáticos orientado a pequeñas y medianas empresas del sector económico colombiano, constituye una alternativa que brinda a estas organizaciones una reducción de costos en la implementación de un equipo en cada organización, y contribuye en la generación de estrategias para que el sector de las PyMES pueda afrontar estratégicamente un evento cibernético que amenace con afectar su continuidad de negocio.

[5] El Centro de Operaciones de Seguridad - SOC, tiene como propósito monitorear, analizar y responder a incidentes de ciberseguridad a partir de la conjunción de herramientas tecnológicas, procesos de finidos para la atención de incidentes y talento humano capacitado

Objetivos

Objetivo General

Analizar los factores económicos, tecnológicos y administrativos que den soporte para la creación de un equipo de respuestas a incidentes informáticos, para una Pequeña o Mediana Empresa del sector económico en Colombia

Objetivos Específicos

Recopilar información que permita establecer cuál es el estado actual de la gestión de la ciberseguridad en Pequeñas y Medianas Empresas del Sector Económico Colombiano.

Establecer un plan estratégico que contribuya en el robustecimiento de las capacidades de ciberseguridad que aporte en la continuidad de negocio – BCP.

Esquematizar una propuesta tecnológica que sirva como infraestructura lógica y física para la gestión de un evento de ciberseguridad.

Capítulo I

Metodología

Teniendo presente la línea de investigación “Gestión de las Organizaciones” y a partir de la sub línea “Planeación de las Organizaciones” (ECACEN, 2017), este estudio monográfico se construye con el fin de contribuir al reconocimiento de mejores prácticas de gobierno de TI y el impacto que estas puedan aportar a la gestión del conocimiento de una organización. Por tal motivo, como soporte metodológico para analizar los factores políticos, económicos, sociales y tecnológicos para la Creación de un Equipo de Respuestas a Incidentes Informáticos orientado a Pymes colombianas, se plantea la aplicación de la investigación Cualitativa. En relación con ello en el año de 1996 Taylor & Bogdan, indicaban que esta permite aplicar un conjunto de técnicas para recoger datos donde todos los escenarios son dignos de estudio y todos los puntos de vista son importantes. Es preciso también mencionar lo expuesto en el año 2002 por Fernández, quien platea que la investigación cualitativa intenta identificar la naturaleza profunda de una realidad, las relaciones que pueden existir y la estructura dinámica que pueda presentar.

Es así como la recopilación de información a partir de boletines generados por organizaciones que estudian la ciberseguridad, estándares y normativas planteadas por entes certificadores y estados, documentos emanados de la academia y el juicio de expertos[6], permite establecer un panorama que determine: el estado actual de la gestión de la seguridad en organizaciones, plantear un plan estratégico que contribuya en el robustecimiento de las capacidades de la seguridad de la información y de la protección de datos de una PyME y esquematizar un

[6] Se constituye como un conjunto de observaciones u opiniones que plantea un experto de una disciplina determinada

propuesta tecnológica que sirva como base para la gestión de un evento de ciberseguridad. Esto con el fin de plantear la creación de un Equipo de Respuestas a Incidentes Informáticos para el Sector de las Pequeñas y Medianas empresas del país.

En este orden de ideas la metodología de investigación se desarrolla a partir de cuatro capítulos los cuales dan respuesta a la pregunta problema, a la hipótesis y al objetivo general.

Tabla 1.

Capítulos y recursos utilizados para la construcción del documento

Capítulo	Actividad	Recurso utilizado
1	Desarrollo metodológico	Teoría fundamentada
2	Recopilar información	Valoración interpretativa de textos
3	Establecer plan estratégico	Fuentes documentales y estadísticas
4	Esquematizar propuesta tecnológica	Fuentes documentales y estadísticas

Fuente*:* El Autor

Lo anterior permite interpretar la información consultada, con el fin obtener una conceptualización cercana al tema de estudio.

Marco Conceptual

A continuación, se relacionan algunos conceptos que son claves para poder abordar la construcción de este documento monográfico.

Activo de Información: Persona o elemento relacionado con el tratamiento de la información, que presenta valor para una organización. (INCIBE, 2017).

Amenaza: Evento no favorable, que tiene consecuencias negativas sobre un activo de información ocasionando la no disponibilidad o el mal funcionamiento (INCIBE, 2017).

Incidente de seguridad: Suceso que afecta a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa (INCIBE, 2017).

Plan de contingencia: Plan estratégico construido en fases y que abarca un conjunto de recursos que permiten respaldar un proceso. (INCIBE, 2017).

Política de seguridad: Medidas de seguridad que una organización decide adoptar, para garantizar la seguridad de los sistemas de información (INCIBE, 2017).

SGSI: Un Sistema de Gestión de la seguridad de la Información (SGSI), es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001 (INCIBE, 2017).

Vulnerabilidad: Fallos que se presentan en un sistema y que puede ser usado para acciones no legitimas con el fin de acceder a la información (INCIBE, 2017).

Ataques Business Email Compromise – BEC: Tipo de ataque informatico que busca secuestrar cuentas empresariales, con el fin de interceptar o redireccionar las transacciones financieras propias de la organización.

Ransomware: Es un tipo de malware que busca robar información de equipos exigiendo rescate por su recuperación.

Malware: Son ataques que se apoyan de programas maliciosos y que tiene como objetivo realizar acciones dañinas en un sistema informático, con el animo de robar información o dañar el equipo para obtener asi un beneficio economico. (OSI - INCIBE, 2018):

SIM Swapping – Secuestro de Cambio de SIM CARD: Práctica fraudulenta que realizan ciberdelincuentes a partir del reconocimiento de un dato personal como número de celular, fecha de nacimiento, dirección de la residencia, con el fin de realizar una acción de suplantación para asi poder solicitar copia de una tarjeta telefónicoa - SIM (Scotiabank Colpatria, 2021)

CryptoJacking – Minería de criptomonedas: Conjunto de acciones que se requieren para validar y procesos las transacciones de una criptomoneda (ESET, 2018).

Siglas y Abreviaciones:

CSIRT: Equipos de Respuestas ante Incidentesde Seguridad (en inglés, Computer Security Incident Response Team)

SOC: Centro de operaciones de seguridad

Marco Teórico

Freyre, señala que el papel de la ciberseguridad no es solamente prevenir amenazas que se puedan presentar al interior de una organización. Indica, además, que se requieren profesionales que puedan gestionar de forma acertada los sistemas de información y de seguridad de la información desde la planificación e implementación de políticas y procedimientos que se relacionan con los recursos y los procesos que lleva a cabo una organización (Freyre, 2019).

Hoy en día Colombia cuenta con varios equipos de ciberseguridad reconocidos por el Foro Global de Incidentes de Respuesta y Equipos de Seguridad FIRTS[7]. Esta organización asigna una membresia a equipos como lo son los SOC o CSIRT, indicando que estos cuentan con una experiencia y alianzas con semejantes para dar respuesta a un evento o incidente informático.

Es importante indicar que los Equipos de Respuesta a Incidentes Informáticos se enfocan en ambitos de actuación. En este estudio monografico se abordará el CSIRT de PyMES.

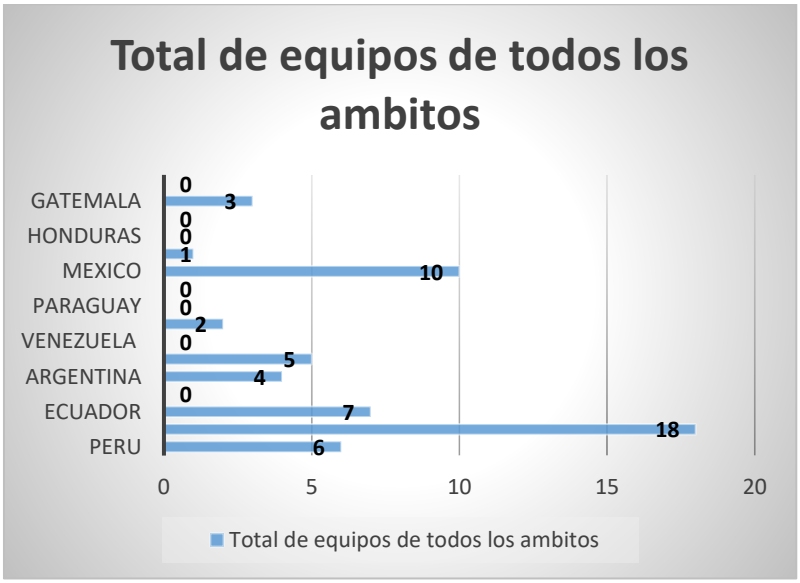
Debido al tamaño y naturaleza de estas organizaciones, es dificil implementar al interior un equipo que dé respuesta a las necesidades generadas en su entorno digital y salvaguarde la información. Por tal motivo, estos equipos deben entender y responder a las necesidades que surgen en el desarrollo de las activadades de este sector de la economía con el fin de ser un aliado estratégico para el aseguramiento de su información.

La siguiente figura presenta el total de equipos de respuesta reconocidos por FIRST a fecha 5 de agosto de 2021.

[7] El Foro de Respuesta de Incidentes y Equipos de Seguridad – FIRST es un ente que posibilita la interacción entre equipos de respuesta con el fin de simular la rápida reacción a incidentes y compartir información que permitan plantear mejores practicas

Figura 1.

Relación de Equipos de Respuesta Reconocidos por FIRST en Latinoamérica



Nota*:* El gráfico representa el número de equipos reconocidos por FIRTS en Latinoamérica

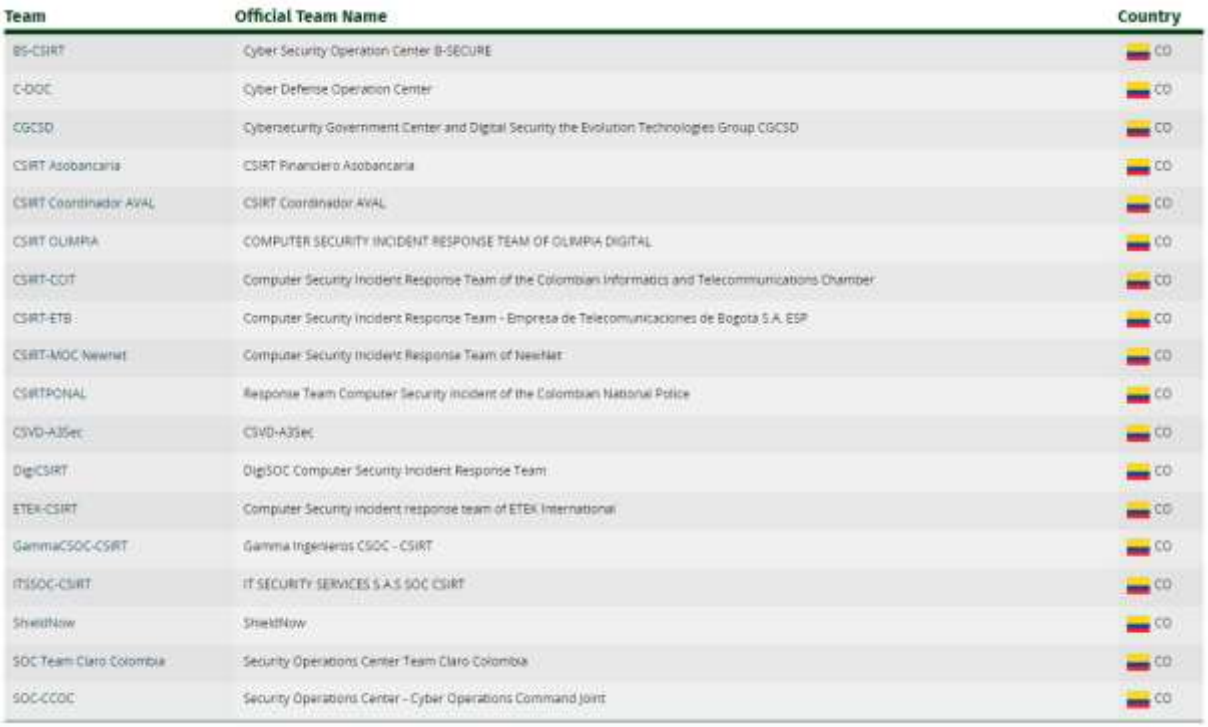
Fuente: FIRST, 2021

Los datos anteriormente expuestos indican que Colombia es el país que cuenta con más equipos de respuesta a incidientes informáticos de toda latinoamérica. Sin embargo, estos datos no son favorables para el sector de las PyMES. De los 18 equipos que relaciona el Foro Global solo 7 ofertan servicios a este sector de la economía, permitiendo evidenciar en un primer momento la necesidad de vincularse o asociarse a un equipo de respuestas a incidentes informáticos, teniendo presente su infraestrucutra tecnológica, servicios y su presupuesto.

A continuación, se relacionan los 18 equipos de respuesta que hacen presencia en Colombia:

Figura 2.

Equipos de respuesta reconocidos por FIRST en Colombia



Team	Official Team Name	Country
BS-CSIRT	Cyber Security Operation Center B-SECURE	CO
C-DOC	Cyber Defense Operation Center	CO
CGCSD	Cybersecurity Government Center and Digital Security the Evolution Technologies Group CGCSD	CO
CSIRT Asobancaria	CSIRT Financiero Asobancaria	CO
CSIRT Coordinador AVAL	CSIRT Coordinador AVAL	CO
CSIRT OLIMPIA	COMPUTER SECURITY INCIDENT RESPONSE TEAM OF OLIMPIA DIGITAL	CO
CSIRT-CCIT	Computer Security Incident Response Team of the Colombian Informatics and Telecommunications Chamber	CO
CSIRT-ETB	Computer Security Incident Response Team - Empresa de Telecomunicaciones de Bogota S.A. ESP	CO
CSIRT-MOC Newnet	Computer Security Incident Response Team of Newnet	CO
CSIRTPONAL	Response Team Computer Security Incident of the Colombian National Police	CO
CSVD-A3Sec	CSVD-A3Sec	CO
DigiCSIRT	DigiSOC Computer Security Incident Response Team	CO
ETEK-CSIRT	Computer Security Incident response team of ETEK International	CO
GammaCSOC-CSIRT	Gamma Ingenieros CSOC - CSIRT	CO
ITSSOC-CSIRT	IT SECURITY SERVICES S.A.S SOC CSIRT	CO
ShieldNow	ShieldNow	CO
SOC Team Claro Colombia	Security Operations Center Team Claro Colombia	CO
SOC-CCOC	Security Operations Center - Cyber Operations Command Joint	CO

Nota. El gráfico representa el número de equipos en Colombia reconocidos por First. Fuente: FIRST 2021

Teniendo presente lo anterior y dando una mirada al contexto local en términos de ciberseguridad, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia propone la Guía para la gestión y clasificación de incidentes de seguridad de la información donde se tiene como objetivo: "*tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información"* (MINTIC, 2016)

Así mismo, el reporte de la Cámara Colombiana de Informática y Telecomunicaciones en conjunto con el CAI Virtual presentan al año 2020 las tendencias de cibercrimen en Colombia

donde se relacionan los ataques más presentados en el país entre el año 2019 y 2020 y las tendencias de los ataques para el 2021. Para el caso particular de las PyMES, se presenta un incremento en los ataques informáticos a partir de las siguientes técnicas:

Ataques Business Email Compromise – BEC: son ataques que a través de correo electrónico donde se busca comprometer la información del negocio. Los principales vectores de engaño usados por esta técnica para el año 2019 son: correos fraudulentos personalizados (Spear Phishing), enmascaramiento de correos (Spoofing), suplantación de identidad e infección de sistemas frecuentemente visitados por empleados (Watering Hole).

El FBI, indica que para el año 2019 en Estados Unidos, se presentaron perdidas en organizaciones por un valor de 3.5 billones de dólares (FBI, Internet Crime Report, 2019).

En Colombia las cifras de pérdidas por ataques oscilan entre 300 y 5000 millones de pesos, según el tamaño de la empresa afectada (CECIP, 2020). Las modalidades que más usan los ciberdelincuentes son: Estafa de CEO (Suplantación de Gerente) y suplantación de clientes.

Ransomware: Colombia recibió el 30% de los ataques de Secuestro de datos en Latinoamérica en el último año estando por encima de países como México, Brasil y Argentina. El impacto se crea en pequeñas y medianas empresas – PyMES, teniendo en cuenta que es en estas organizaciones donde los niveles de seguridad suelen ser bajos. Para el año 2019, setecientas diecisiete (717) empresas reportaron este tipo de ataque, siendo los vectores más comunes el uso de información falsa relacionada con: embargos judiciales, reportes a centrales de riesgos, alarmas de transferencias no consentidas, foto comparendos y citaciones a diligencias judiciales.

Ataque de Denegación de Servicios Distribuido – DdoS: Para el año 2019, 170 empresas reportaron indisponibilidad de sus servicios en línea debido a ataques de DDoS logrando

interrumpir el servicio a sus clientes. (CCIT & PONAL, 2019). Los factores más comunes que se presentan en este tipo de ataque son: reconocimiento y escaneo de los servicios de la organización que se pretende afectar, uso de botnet[8] para dirigir ataques a los servicios online, interrupción de servicios para las partes interesadas, solicitud de pagos a través de criptomoneda e identificación de la infraestructura tecnológica y de seguridad de la organización.

Malware: El 57% de los ciberdelitos reportados en Colombia, corresponde al robo a través de medios informáticos. (CCIT & PONAL, 2019). Los métodos de distribución de malware más comunes son (CCIT & PONAL, 2019): correo con notificaciones suplantando entidades públicas, 63%, redireccionamiento hacia sitios web que esta infectados por el ciberdelincuente 32%, descarga de aplicaciones móviles que se encuentra infectadas con malware 5%. En el orden organizacional, de 99 casos reportados en el año 2018, pasaron a ser 705 casos reportados en el año 2019.

SIM Swapping – Secuestro de Cambio de SIM CARD: Este ataque tiene como propósito principal acceder a cuentas financieras que usen dos factores de autenticación, uno de ellos a través de mensaje de texto. El objetivo es tomar posesión de la línea de la víctima por medio de la suplantación de identidad en el operador móvil donde se encuentre registrado el servicio. (CCIT & PONAL, 2019). Es importante resaltar que cerca del 90% de ataques presentados a organizaciones colombianas se generan a partir de técnicas de Ingeniería Social como esta.

CryptoJacking – Minería de criptomonedas: El Centro Cibernético de la Policía – CCP, indica que muestras encontradas en correos electrónicos corporativos permiten identificar el malware Trojan.Nymeria.12 (CCIT & PONAL, 2019).

[8] Una Botnet es una red de computadores que son infectados con software malicioso, permitiendo el acceso indebido

La estadística anterior refleja los indicadores presentados por el Índice Global de Ciberseguridad[9] el cual, a través de un marco de cooperación internacional busca el fomento y colaboración entre estados y organizaciones público-privadas para el mejoramiento de Ciberseguridad en los siguientes pilares (GCA, 2020):

Medidas legales: Mide las leyes y normativa sobre ciberdelito y ciberseguridad.

Medidas técnicas y de procedimiento: Mide la implementación de capacidades técnicas a través de agencias nacionales y sectoriales.

Estructuras organizacionales: Mide las estrategias y organizaciones que implementan seguridad cibernética.

Creación de capacidades: Mide a partir de la concienciación, campañas, formación, educación e incentivos, capacidades desarrolladas en torno a la ciberseguridad

Cooperación internacional: Mide el grado de asociación entre agencias, empresas, y países.

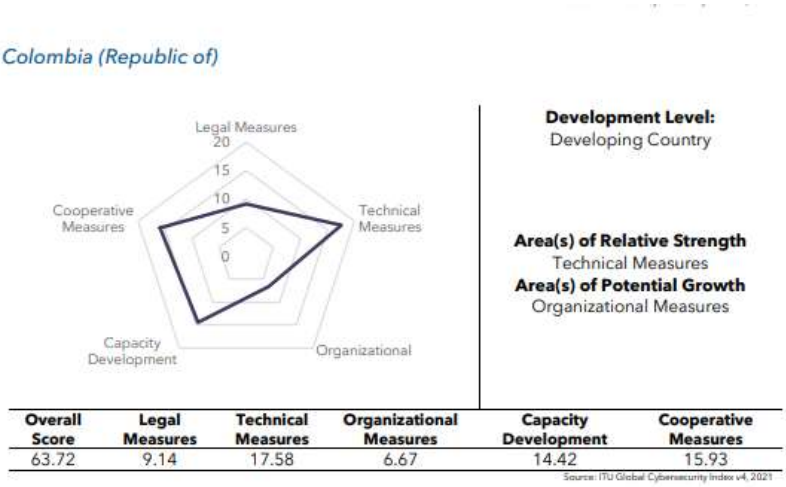
En este reporte, Colombia se presenta como el país 81 en la escala mundial y 9 en Latinoamérica evidenciando una desmejora con respecto al su posicionamiento para el año 2018.

La figura 3, presenta el puntaje obtenido por Colombia en la evaluación de los 5 pilares:

[9] El índice global de ciberseguridad es un instrumento que publica la Unión Internacional de telecomunicaciones donde muestra el monitoreo del compromiso con la ciberseguridad de los 194 países miembros

Figura 3.

Puntaje obtenido en la evaluación de los 5 pilares



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
63.72	9.14	17.58	6.67	14.42	15.93

Source: ITU Global Cybersecurity Index v4, 2021

Nota*:* Puntaje obtenido asociado a las capacidades legales, técnicas, organizacionales, capacidades de desarrollo y cooperación que se deben tener en cuenta en Colombia respecto a su entorno digital. Fuente: MyITU, 2021

La imagen anterior sirve como referente para definir las medidas organizacionales y legales que deben tenerse presente en la agenda nacional para ser revisadas con el ánimo de mejorar. Para el caso particular de las PyMES, estos dos pilares afectan de forma directa, ya que se relacionan con la legislación que se debe cumplir en términos de aseguramiento y tratamiento de la información y las capacidades organizacionales que miden las acciones estratégicas a implementar, en términos de ciberseguridad (ITU, 2020).

Marco Tecnológico

Principales proveedores de seguridad informática de orden mundial.

Con el fin de conocer un poco más las empresas que proveen servicios de seguridad digital, a continuación, se relacionan los líderes en el mercado mundial que ofrecen las soluciones en seguridad, pero que debido a los costos en sus soluciones no se adaptan a las necesidades del mercado colombiano en términos de pequeñas y medianas empresas (Tecnozero, 2020).

Palo Alto Networks

Fortinet

Cisco

Check Point Software Technologies

Es preciso indicar que este sector de la economía requiere de expertos en seguridad digital que en la actualidad son escasos (Candeltey, 2020) o sus salarios son elevados dificultando la puesta en marcha de políticas y legislación que se viene planteando para el sector. Además, es complejo para las PyMES contratar servicios que no favorezcan o se adapten a sus presupuestos. Teniendo en cuenta la información anterior y con el objetivo de presentar algunas de las empresas o equipos de respuesta a incidentes que hacen presencia en Colombia, se debe reconocer cuales son los servicios que un CSIRT podría ofrecer a sus partes interesadas. (OEA, 2021).

Tabla 2.

Servicios ofertados por un Equipo de Respuestas a Incidentes Informáticos

Servicio	Tipo	Descripción
Servicios Proactivos	Servicio de monitoreo y alertas Servicios de Investigación y Desarrollo	Están relacionados con el monitoreo y las alertas, a partir de la implementación de sistemas que ayudan a detectar eventos de seguridad
Servicios reactivos	Gestión de incidentes Respuesta Vulnerabilidades Respuesta a artefactos maliciosos	El objetivo de este servicio es el de contribuir en la mejora de los procesos de infraestructura y seguridad de la comunidad objetivo, con el fin de prevenir incidentes de seguridad
Servicios de valor agregado	Capacitación y educación Concientización Análisis de riesgos y continuidad de negocio	El objetivo de este servicio es ofrecer a las partes interesadas o comunidades objetivo, procesos de educación y apoyo a emprendimientos relacionados con ciberseguridad

Fuente*:* El Autor

A continuación, se relacionan los equipos de respuesta reconocidos por FIRST que hacen presencia en Colombia y que ofrecen sus servicios a pequeñas y medianas empresas (FIRST, 2020).

Tabla 3.

Relación de algunas empresas reconocidas por FIRST que hacen presencia en Colombia, donde se mencionan algunos de sus equipos

Empresa	Servicio ofrecido
Cyber Security Operation Center B-SECURE	•Ciberseguridad, Seguridad Cloud, Datos, Identidad y acceso, Infraestructura y aplicaciones, Gobierno Riesgo y Cumplimiento.
CSVD-A3Sec	•Ciberseguridad, Monitorización
DigiSOC Computer Security Incident Response Team	•Detección y Respuesta de incidentes, Servicios de seguridad gestionados, Exposición digital, Seguridad en la nube
Computer Security incident response team of ETEK International	•Gestión de amenazas, Respuesta a incidentes, Monitoreo de seguridad, Educación, Servicios proactivos a partir de: hacking ético, pruebas de equipos rojos, inteligencia cibernética, gestión de vulnerabilidades.

Fuente: El Autor

Marco Legal

Teniendo en cuenta la normatividad Internacional y Colombiana, se relacionan las leyes, estándares y metodologías que permiten soportar los factores económicos, tecnologicos y administrativos que pueden apalancar el desarrollo de las activiaddes de un equipo de respuestas a incidentes informáticos.

Tabla 4.

Normatividad Colombiana relacionada con el proyecto

Norma	Contenido
Ley 527 de 1999 (Comercio Electrónico)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales.
Ley 1266 de 2008 (Habeas Data)	Contempla las disposiciones generales con relación al derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 1273 de 2009 (Delitos Cibernéticos)	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC”.
Ley 1341 de 2009 (Sector TIC)	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC.
Ley 1480 de 2011	(Estatuto del Consumidor - Comercio electrónico y publicidad) Se incluye en la definición de las ventas a distancia, aquellas que se realizan a través del comercio electrónico.
Ley 1581 de 2012 (Habeas Data)	Por la cual se dictan disposiciones generales para la protección de datos.

Resolución SIC No. 76434 de 2012 (Habeas Data)	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales
Decreto 886 de 2014 (Registro Nacional de Base de Datos)	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al registro nacional de bases de datos

Fuente*:* El Autor

Estándares internacionales que plantean buenas prácticas para la gestion de los riesgos de ciberseguridad:

NTC ISO 27001:2013: Norma que se presenta como el manual de auditoria de un Sistema de Gestión de Seguridad de la Información

NTC ISO 27031: Norma que se presenta como Continuidad de Negocio basadas en las tecnologias de la información y la comunicación.

NTC ISO 27032: Norma que se presente para el apoyo de la Ciberseguridad, presentando marcos para el intercambio seguro de la información

Otros documentos:

Modelo de Gestión de Riesgos de Seguridad Digital – MGRSD

Lineamientos de Politicas para la Cibsresegudidad y Ciberdefensa – CONPES 3701

Política Nacional de Seguridad Digital – CONPES 3854

Política Nacional de Confinaza y Seguridad Digital – CONPES 3995.

Capítulo II

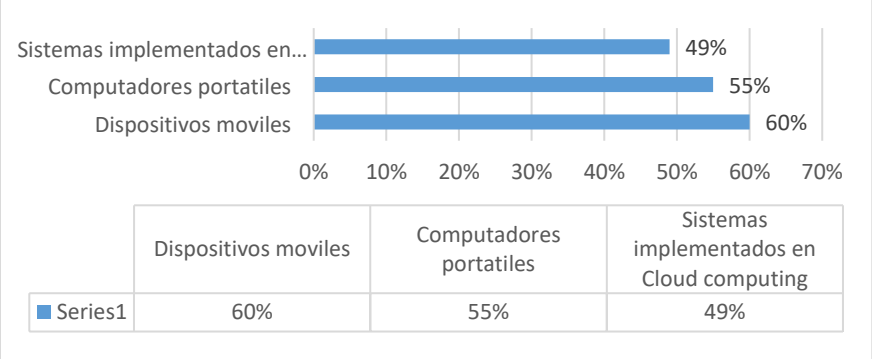
Objetivo 1. Recopilar información que permita establecer cuál es el estado actual de la gestión de la ciberseguridad en Pequeñas y Medianas Empresas del Sector TI en Colombia

En los últimos cinco años las PyMES del mundo han venido reportando un aumento significativo en eventos o incidentes relacionados con su ciberseguridad, siendo los sistemas o activos de información los más vulnerados (PONEMON, 2019).

La figura 4, presenta datos recopilados por la organización PONEMON en el informe de resultados del estado global de la ciberseguridad para el 2019 en PyMES de todo el mundo patrocinadas por Keep Security. Este informe se enfocó en realizar encuestas a empresas con nóminas entre 100 y 1000 trabajadores, la encuesta fue realizada a 2176 empleados de países como Estados Unidos, Reino Unido, Alemania, Suiza, entre otros y tuvo como propósito trazar las tendencias en ciberataques y violación de datos.

Figura 4.

Activos de Información Más Vulnerados en Pymes en el Mundo



Nota**.** Informe de investigación asociado a el estado de ciberseguridad en las pequeñas y medianas empresas. Fuente: Institute, 2019

La empresa Kaspersky LAB, en informe de 2017 indicó que independientemente del Retorno sobre la Inversión – ROI, las organizaciones latinoamericanas vienen inviertiendo en ciberseguridad. Indicó ademas que las brechas de inseguridad que mas costos elevados presenta son las que se generan a partir de fallas ocasionadas por servicios de terceros ocasionando que las empresas piensen en su propia protección y en la de sus socios. Aunque el informe revela datos de crecimiento respecto a la importancia que presentan las organizaciones en temas de ciberseguridad, en Latinoamérica estas vienen reduciendo sus presupuestos y recursos para gestionar o afrontar un incidente cibernético. Sin embargo, para micro y pequeña empresa el presupuesto de seguridad poco a poco se viene teniendo en cuenta (Kaspersky, 2017).

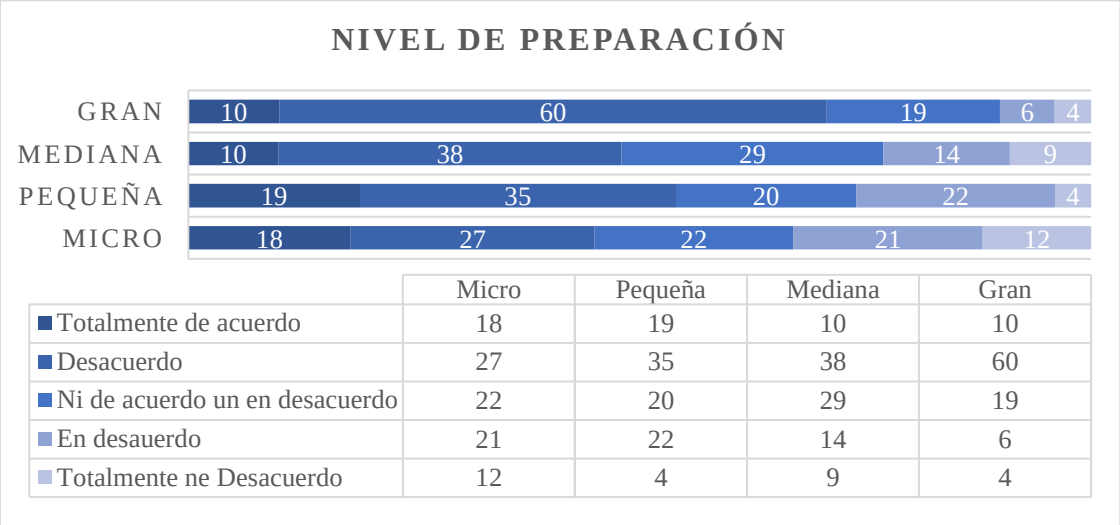
La realidad de la gestión de la ciberseguridad en Colombia es un poco alentadora, sin embargo, es preciso construir estrategias que permitan dar respuesta a posibles eventos o incidentes digitales que afecten contra la continuidad de negocio de las organizaciones.

Estado Actual de la Ciberseguridad en Colombia

A continuación, se relacionan algunos datos estadísticos de la situación que presentó a 2017 el sector de las PyMES en términos de Ciberseguridad en Colombia (BID, MINTIC, & OEA, 2017). Esto teniendo presente que para el año 2020 no se presentaron reportes similares que pudiesen establecer los datos actualizados.

Figura 5.

Nivel de Preparación Para Hacer Frente a un Incidente Digital en las PyMES Colombianas



	Micro	Pequeña	Mediana	Gran
Totalmente de acuerdo	18	19	10	10
Desacuerdo	27	35	38	60
Ni de acuerdo un en desacuerdo	22	20	29	19
En desauerdo	21	22	14	6
Totalmente ne Desacuerdo	12	4	9	4

Nota*:* Impacto de los incidentes de seguridad digital. Fuente: BID 2017

La figura 5, refleja cómo se preparan las empresas colombianas para hacer frente a un incidente digital. El 55% de las microempresas no se sienten preparadas para enfrentar un evento de Ciberseguridad, al igual que el 44% de las pequeñas empresas y el 52% de las medianas empresas.

Esto puede traer como consecuencia un gasto alto que sobrepasa lo presupuestado para dar continuidad al negocio, ya que la recuperación después de un fallo de seguridad crece de forma considerable (Kaspersky, 2017).

La figura 6, presenta la aplicación de prácticas de seguridad digital en las empresas colombianas. Esta se convierte en un factor trascendental para garantizar la educación y cultura del talento humano de las PyMES.

Figura 6.

Aplicación de Prácticas de Seguridad Digital

Nota. Prácticas en seguridad digital. Fuente: BID, 2017

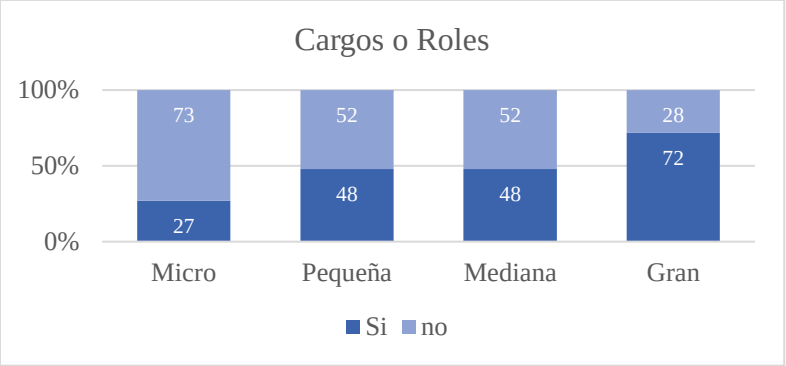
La figura 6 muestra que las micro y pequeñas empresas, generan poco uso de estándares y medidas organizacionales para la gestión de los incidentes digitales. Sin embargo, el uso de políticas y medidas técnicas empieza a tomar relevancia para el desarrollo de las actividades propias de la gestión de la información. Respecto a la mediana empresa, el uso de políticas se presenta como una medida a adoptar teniendo en cuenta que estas tienen como propósito: presentar los lineamientos que contribuyen en la realización de su misión, visión y objetivos propuestos.

Una de las debilidades en las Pymes es la asignación de bajos recursos para el talento humano que gestiona la seguridad de la información. Para este punto es preciso indicar que, aunque los sistemas de información vienen realizando tareas de recolección y análisis de datos, el talento humano se torna como factor diferenciador en términos de toma de decisiones.

A continuación, se presenta el índice de participación promedio sobre el total de cargos o roles posibles, dedicados a la seguridad en las organizaciones colombianas.

Figura 7.

Índice de participación sobre el total de Cargos o Roles Dedicados a la Seguridad Digital en Empresas Colombianas

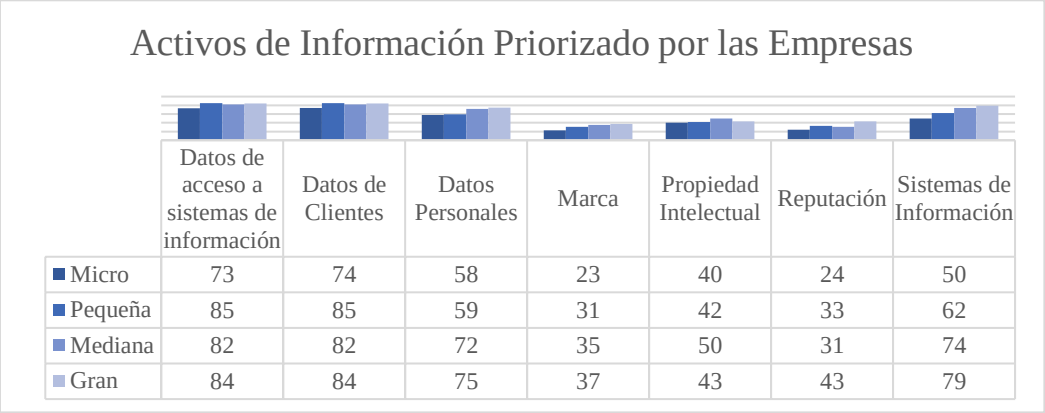


Nota*:* Prácticas en seguridad digital. Fuente: BID, 2017

Se puede observar en la figura 7, que las microempresas cuentan con un porcentaje bajo respecto a cargos o roles relacionados con áreas para la gestión de los incidentes digitales. Las pequeñas y medianas empresas en promedio cuentan con áreas, cargos o roles para la gestión de los incidentes digitales y las grandes empresas en su mayoría, cuentan con áreas, cargos o roles para la gestión de los incidentes digitales.

Figura 8.

Activos de Información Priorizado por las Empresas



	Datos de acceso a sistemas de información	Datos de Clientes	Datos Personales	Marca	Propiedad Intelectual	Reputación	Sistemas de Información
Micro	73	74	58	23	40	24	50
Pequeña	85	85	59	31	42	33	62
Mediana	82	82	72	35	50	31	74
Gran	84	84	75	37	43	43	79

Nota. Activos de información. Fuente: BID, 2017.

La figura 8, muestra que los datos y los activos que priorizan las micro, pequeñas y medianas empresas colombianas son los de: datos de acceso a sistemas informáticos, datos de clientes y datos personales. Se presenta poca atención en activos como: marca, propiedad intelectual y reputación.

Esto lleva a concluir que la importancia recaba en activos tangibles. Los activos que no son visibles para estas organizaciones pasan desapercibidos por desconocimiento o por no considerarse necesarios para el desarrollo de las actividades operacionales de este tipo de empresas.

Tabla 5.

Inversión anual que hacen las empresas por tamaño para la seguridad digital

Tamaño de la Empresa	Inversión en Pesos Colombianos
Microempresa	$ 500.000 a $ 1.000.000
Pequeña Empresa	$ 5.000.000 a $10.000.000
Empresa Mediana	$ 15.000.000 a $ 25.000.000

Nota*:* Datos obtenidos en el informe de seguridad digital presentado por el Banco Interamericano de Desarrollo. Fuente: BID, 2017.

En la tabla 5, Aunque se evidencia que las organizaciones presupuestan un valor para la seguridad digital, el informe indica que el presupuesto estimado no alcanza a ser el 1%.

Tabla 6.

Inversión Anual que Hacen las Empresas por Sector Económico Para la Seguridad Digital

Sector Económico	Inversión en Pesos Colombianos
Comercio	$ 5.000.000 a $ 10.000.000
Industria	$ 45.000.000 a $ 60.000.000
Servicios	$ 5.000.000 a $10.000.000

Nota*:* Datos obtenidos en el informe de seguridad digital presentado por el Banco Interamericano de Desarrollo. Fuente BID, 2017

La tabla 6, permite visualizar por sector económico cual es la inversión aproximada que realizan las PyMES en ciberseguridad siendo los sectores de servicios y comercio los que adoptan en sus presupuestos un menor rubro, este es aproximadamente 6 veces menos que el sector Industrial. Se debe considerar que esto se puede dar debido al desarrollo de patentes y de prototipos de confidencialidad.

La siguiente tabla presenta el presupuesto asignado para la seguridad digital en una organización. En esta se puede evidenciar que el rubro presupuestal mas alto se destina a plataformas y medios tecnológicos, mientras que para la generación de capacidades, proceso en donde se se planifican las estrategias de ciberseguridad, su inversión es baja.

Tabla 7.

Presupuesto Asignado Para Seguridad Digital

Categoría	Porcentaje
Talento Humano (Empleados, contratistas)	25%
Plataformas y medios tecnológicos (Hardware y Software)	47%
Generación de capacidades (Capacitación, concientización, investigación)	11%
Servicios especializados (Gestión de seguridad, externalización, soporte)	17%

Nota. Datos obtenidos en el informe de seguridad digital presentado por el Banco Interamericano de Desarrollo. Fuente: BID, 2017

En la tabla 7, se evidencia que el porcentaje asignado para la generación de capacidades de educación y cultura es el más bajo del presupuesto. Las empresas le apuntan a la adquisición o compra de plataformas y medios tecnológicos para la gestión de la seguridad digital. Es de tener presente que este rubro se verá afectado en la depreciación de los activos de Hardware y Software a corto o mediano plazo.

El Banco de Desarrollo Interamericano - BID indicó que para el año 2019 las empresas perderían hasta $ 4.000 millones de pesos por ataques informáticos, esto asociado a la masificación de nuevas amenazas (BID, 2017).

Desde el año 2016 en Colombia, se está estructurando una serie de políticas y lineamientos en cuanto a ciberseguridad y ciberdefensa. En el sector público colombiano las amenazas informáticas no son la excepción, por esta razón, el estado emite el CONPES 3701 de 2011 que

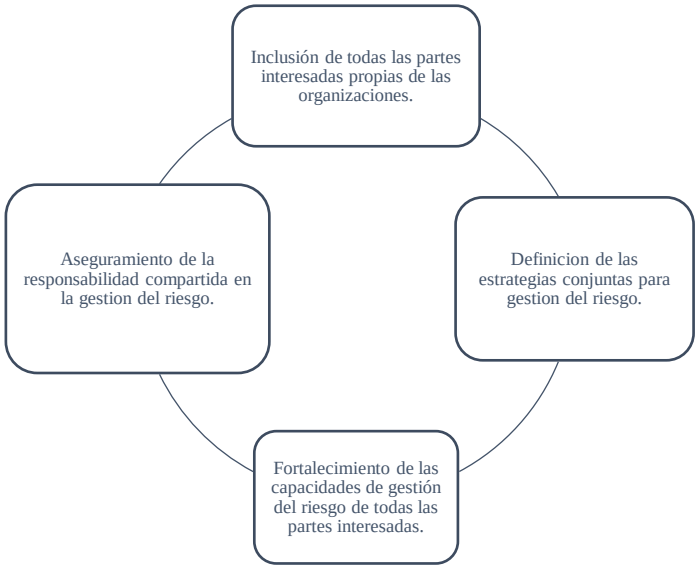
cual tiene como propósito dar los *"lineamientos para la seguridad y ciberdefensa*" y el CONPES 3854 de 2016 plantea una *"Política Nacional de Seguridad Digital"*, que buscan mitigar los riesgos inherentes a las actividades considerando una buena gestión de riesgos en el entorno digital.

Para esto, se establecieron principios fundamentales en la gestión de riesgos informáticos con el fin que esto no sea una actividad particular, sino que se involucre de forma integral a toda la organización y su entorno, con un marco de trabajo para gestionar el riesgo de las actividades económicas y sociales que sea lo más transparente y explícito posible.

"*Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital sean apropiadas para los objetivos económicos y sociales en juego abordados desde la perspectiva estratégica de la organización*" (DNP, 2016).

Figura 9.

Principios Fundamentales en la Gestión de la Seguridad Digital para las Pymes



Fuente*:* El Autor

La gestión de riesgos tiene como finalidad el aseguramiento digital el cual gira en torno a: "*alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y valores fundamentales frente a las amenazas de seguridad digital*" (DNP, 2016).

Lo anterior, permite realizar desde un plan de tratamiento para los riesgos su eliminación, aceptación, transferencia o mitigación a partir de controles propuestos por estándares como lo es la norma ISO 27001:2013[10] anexo A (MINTIC, 2017) o marco de trabajo NIST[11] 800-53 Rev. 5 (NIST, 2021).

Las ciber amenazas a las que se enfrentan las Pymes según estudio de Tic Tac y Safe presentado por la (Revista Dinero, 2020), permite hacer la identificación de los ataques más comunes. Mediante este recurso se presenta la caracterización de cada uno de estos con el fin de identificar los escenarios donde se pueden materializar estos riesgos y aplicar los debidos controles en los mapas de riesgos de seguridad digital que un equipo de respuestas puede ofrecer al sector de PyMES, de tal forma que a través de este planteamiento se desarrollen medidas de seguridad digital así como un estudio de costos mediante el modelo de Retorno de Inversión de la Seguridad de la Información ROSI[12].

[10] La norma ISO 27001:2013 proporciona lineamientos para el aseguramiento, la confidencialidad e integridad de los datos y de la información a partir de la implementación de un Sistema de Gestión de la Seguridad de la Información - SGSI

[11] NIST es el Instituto de Estándares y tecnología que tiene como propósito promover la innovación y la competencia industrial

[12] El ROSI se define como el cálculo del retorno sobre la inversión en seguridad de la información, el cual permite realizar una medición del retorno de inversión en seguridad desde el análisis de beneficios económicos partir del análisis de los eventos o incidentes que se puedan presentar en una organización y el impacto económico que estos puedan generar.

Capítulo III

Objetivo2. Establecer un plan estratégico que contribuya en el robustecimiento de las capacidades de ciberseguridad que aporte en la continuidad de negocio – BCP

Basado en la información recopilada en el capítulo anterior, donde se expone el estado actual de la ciberseguridad y el modelo para la gestión del riesgo de la seguridad digital propuesto por MINTIC, los Planes Director de Seguridad – PDS o Planes Estratégicos de Seguridad de la Información – PESI tienen como propósito definir y priorizar una serie de proyectos que permitan reducir los riesgos a los que está expuesta una organización hasta concretar o llegar a niveles aceptables del entorno digital teniendo en cuenta la situación actual. En este orden de ideas, es importante tener claro que el PDS debe estar alienado con los objetivos estratégicos de la organización desde el planteamiento de un alcance que incorpore buenas prácticas de seguridad para el cumplimento de estas por parte del equipo de trabajo y las partes interesadas.

Para realizar esta acción, es importante mencionar que un PDS estará siempre basado en un proceso de mejora continua con el fin realizar procesos cíclicos en su desarrollo y conocer los siguientes aspectos relacionados con la organización: su tamaño, el nivel de madurez tecnológica, el sector al que pertenece, el contexto legal que regula las actividades de la organización, la naturaleza de la información que se maneja y el alcance del proyecto.

Con el fin de establecer un plan estratégico que contribuya en el robustecimiento de las capacidades de ciberseguridad que aporte en la continuidad de negocio – BCP de una organización, a continuación, se presentan 6 Fases propuestas por el Instituto de Ciberseguridad de España para la construcción de un PDS (INCIBE, 2020).

Fase I:

Conocer la situación actual de la organización en términos de ciberseguridad realizando un análisis de orden técnico, organizativo, regulatorio y normativo. En esta fase es de gran importancia contar con el apoyo de la alta dirección.

- Establecer el alcance, donde se determine la magnitud de los trabajos y el foco principal de la mejora después de la aplicación del PDS.
- Definir los responsables de la gestión de los activos con el fin de facilitar la realización de seguimientos de las iniciativas a implantar.
- Realizar una valoración Inicial tomando como referencia algún estándar o marco de trabajo. Por lo generar en Colombia el marco de trabajo o estándar más conocido y aplicado es la ISO 27002:2015 *"Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información"* (ISO, 2015).
- Implementar un modelo que determine el grado de madurez de los controles.

Establecer los objetivos que la empresa quiere lograr en materia de ciberseguridad. En este punto se podrán determinar los ámbitos que requieren mejora e identificar los aspectos en los cuales se debe focalizar esfuerzos. Para esto se sugiere trabajar a partir de un análisis de brechas o GAP, donde se defina cual es el estado actual, cual es el objetivo y cuál es el estado óptimo de los controles de seguridad que se están aplicando.

Figura 10.

Resultado de un análisis GAP a la implementación de controles del anexo A de la norma ISO 27001:2013 en una organización

Nota. Plan director de seguridad. Fuente: Plan Director de Seguridad, 2019

Realizar un análisis técnico de seguridad, donde quede cubierto mediante la valoración del grado de implantación y madurez de los controles más relacionados con los sistemas de información empleados por la organización para almacenar y gestionar la información (INCIBE, 2017):

Fase II:

En el desarrollo de la fase II se debe conocer la situación actual de la organización y el empezar a considerar cuales son los proyectos que se están desarrollando y los que se van a desarrollar teniendo presente la previsión de crecimiento y los cambios en la organización debido

a reorganizaciones. Dependiendo de la naturaleza de los proyectos que se quieran desarrollar, las áreas estratégicas deben hacer un inventario de las áreas involucradas y los activos de información que se manejan. Esto para identificar las brechas, riesgos y rubros que se requieren para establecer los controles que deben implementarse durante la ejecución de los proyectos propuestos durante la vigencia.

Fase III:

Definir los proyectos que permitan mejorar el entorno digital de la organización. Esto permitirá alcanzar el nivel de seguridad que la organización requiere. Para esto es preciso:

- Definir las iniciativas dirigidas a mejorar los métodos de trabajo actuales, para que contemplen los controles establecidos por el marco normativo y regulatorio.
- Poner en marcha un conjunto de acciones relacionadas con los controles a implementar que permitan reducir el riesgo, cuya ausencia o insuficiencia se hayan detectado.
- Definir la estrategia a seguir, así como los proyectos más adecuados para gestionar los riesgos por encima del riesgo aceptado por la organización (apetito por el riesgo[13]).

Es de anotar que los proyectos relacionados con ciberseguridad deben proyectarse en su ejecución a máximo tres años. Esto debido al cambio tecnológico o a otros factores relacionados con la evolución de las ciber amenazas.

[13] El apetito por el riesgo es el nivel de aceptación del riesgo que una organización asume, con el fin de dar cumplimiento a sus objetivos estratégicos

Tabla 8.

Ejemplo de proyectos que Pueden Ser Desarrollados en un PDS

Proyecto	Descripción
Desarrollar e implementar una política de seguridad	Desarrollar e implementar una política

Nota. Plan director de seguridad. Fuente: (Plan director de seguridad, 2019)

Fase IV

Esta fase tiene la tarea de clasificar y priorizar los proyectos de la fase anterior. Para esto se debe considerar:

- Agrupar las iniciativas o dividir las propuestas para homogeneizar el conjunto de proyectos que se han definido
- Considerar como criterio el origen de estas, es decir, derivadas de la evaluación del cumplimiento normativo y regulatorio, análisis técnico o análisis de riesgos.
- Organizar los proyectos atendiendo al esfuerzo que requieren y a su costo temporal. De este modo se establecen proyectos a corto, medio y largo plazo.
- Crear un grupo que reúna aquellos proyectos cuya consecución requiere poco esfuerzo, pero su resultado produce mejoras sustanciales en la seguridad (quick wins[14]).

Fase V:

[14] El quick wins hace referencia a la búsqueda de resultados de forma rápida con una inversión baja

La aprobación del Plan Director de Seguridad es fundamental para el establecimiento de una estrategia que contribuya en la mejora del entorno digital. Por consiguiente, en esta fase se debe contar con una versión preliminar del PDS para su revisión y aprobación teniendo presente que se pueden presentar modificaciones al alcance o el cambio en la priorización de algunos proyectos.

Fase VI:

En esta fase se pone en marcha el PDS, es importante aplicar alguna metodología para la gestión de proyectos con el fin de favorecer el éxito del plan y la consecución de los objetivos propuestos.

La norma ISO 21500:2012, sirve como orientación para la gestión de proyectos y es referente para las organizaciones para ser adoptada. (Gestión de Proyectos según la ISO 21500, 2015). Esta norma es presentada a las organizaciones desde de la necesidad de estas para la ejecución de proyectos de forma exitosa, teniendo presente la reducción de tiempos y costos y por la necesidad de establecer principios, procedimientos y prácticas comunes para la gestión de proyectos (Rojas, Moreira, Marín, & Torres, 2019).

La ISO 21500:2012 se dirige a directivos de organizaciones y directores de proyectos y presenta características de universalidad, integradora, sencilla y flexible ya que define que debe considerarse para dar gestión de forma efectiva de un proyecto, teniendo presente que cada empresa adopta el estándar y lo aplica de la forma que mejor considere con el fin de dar cumplimiento a los objetivos propuestos.

La norma ISO 21500:2012 está basada en los estándares de PMBOK y PRINCE 2. A continuación se presentan aspectos claves para su cumplimiento

Inicio:

- Desarrollar el acta de constitución del proyecto, es aquí donde se presentan los requisitos iniciales y las expectativas de los interesados.
- Establecer el equipo del proyecto, teniendo presente conseguir el recurso necesario para dar puesta en marcha al proyecto
- Determinar las fases del proyecto, las funciones y el tipo de recursos requeridos
- Identificar las partes interesadas, involucrando a cualquier grupo que pueda verse afectado de cualquier forma en la ejecución y culminación del proyecto. Es preciso para este punto recoger y analizar información que permita determinar los intereses relacionados con el proyecto.

Planificación:

- Definir el alcance indicando información detallada del proyecto y los productos o servicios a entregar. Para esto se puede tener presente los criterios de aceptación del proyecto desde la propuesta de objetivos y criterios de aceptación.
- Crear la estructura de desglose de trabajo donde se presente una separación jerárquica que permita que el producto o servicio emanado del proyecto pueda ser ejecutado por el equipo, cumpliendo con los objetivos propuestos.
- Definir las actividades y lista de actividades identificando los productos entregables incluyendo todas las actividades que se planificaron desde el cronograma, realizando la descripción de cada una de las fases.
- Secuenciar las actividades y estimar su duración identificando la interrelación entre actividades.
- Desarrollar un cronograma de actividades, a partir de un diagrama de Gantt.
- Desarrollar el presupuesto, estimando cada una de las fases del proyecto

- Planificar la calidad, asegurando la misma, desde el compromiso del equipo de trabajo, haciendo detección de forma oportuna a los errores o situaciones anómalas. Esto tiene como fin determinar los requisitos de calidad desde las normas que aplican al proyecto teniendo presente sus entregables.
- Identificar y evaluar los riesgos determinando que amenazas se pueden presentar, sus vulnerabilidades y como estas podrían ser mitigadas.
- Planificar las comunicaciones determinando la necesidad de información y comunicación de las partes interesadas.

Implementación:

- Direccionar el trabajo del proyecto: siendo responsable el director del proyecto, teniendo presente las actividades planificadas.
- Gestionar las partes interesadas: siendo el director de proyecto quien establece comunicación con las mismas para satisfacer sus requerimientos y enfrentar los problemas en la medida que se van presentando.
- Realizar el aseguramiento de la calidad, cumpliendo los requisitos de calidad dados por la organización y por el cliente
- Seleccionar los proveedores, planteando para los mismos criterios de ponderación para su selección definidos en el plan de adquisiciones
- Distribuir la Información, siendo el director del proyecto quien garantiza que las dependencias correctas sean quienes reciben la información de forma integra
- Gestionar el Equipo de trabajo, asegurando que el rendimiento en las actividades sea el óptimo generando espacios motivacionales que conduzcan a un comportamiento responsable desde el respeto hacia las normas de la organización y al equipo de trabajo.

Control:

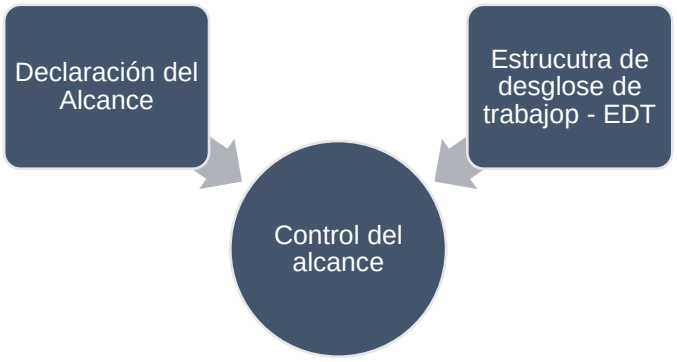
•Controlar las actividades planificadas, realizándose esta acción a lo largo del proyecto, garantizando el desempeño de estas respecto a los tiempos, costos y calidad.

•Controlar los cambios, desde las solicitudes presentadas en el desarrollo de las fases del proyecto. Esta debe ser gestionada en el menor tiempo posible. Los cambios en un proyecto pueden conllevar implicaciones como las ventajas y consecuencias en el alcance, tiempo, costos, recursos entre otros factores que afectarían de forma positiva o negativa el proyecto

•Controlar el alcance, realizando monitoreos al alcance del proyecto y los productos o servicios asociados este. Es preciso destacar dos líneas base relacionada con el alcance derivadas de la documentación:

Figura 11.

Líneas de base para realizar control al alcance

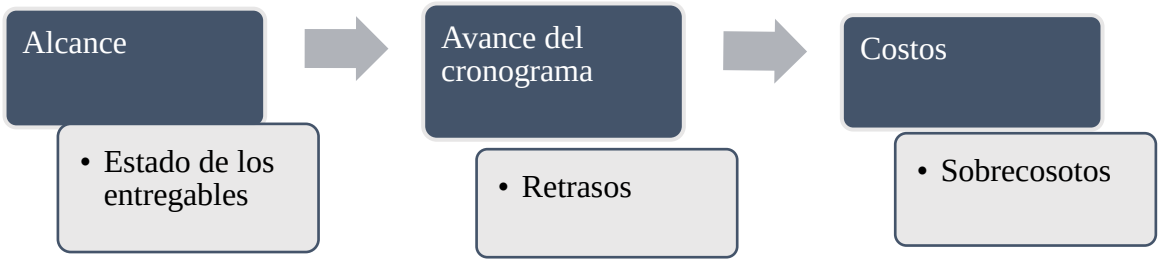


Fuente: El Autor

•Controlar los recursos, haciendo una trazabilidad a las reuniones semanales del equipo de trabajo verificando los informes de rendimiento reales del proyecto con la línea de bases desde las siguientes variables.

Figura 12.

Control de recursos en un Proyecto



Fuente: El Autor

- Gestionar el equipo del proyecto, realizando evaluaciones de desempeño de forma periódica
- Controlar el cronograma, determinando el estado actual del proyecto con el fin de dar actualización y avance al mismo gestionando los cambios que se presenten.
- Controlar los costos, actualizando el presupuesto y gestionando los posibles cambios que se presenten.
- Controlar los riesgos, permitiendo verificar si se han materializado, también para actualizar el registro teniendo presente el avance del proyecto, desde la identificación de nuevos riegos.

Cierre:

- Cerrar las fases del proyecto, teniendo en cuenta que el director dará revisión a todos los informes generados del cierre de cada una de las fases, garantizando la completitud del trabajo.
- Recopilar las lecciones aprendidas, haciendo un recorrido a todo el clico de vida del proyecto, identificando las experiencias obtenidas relacionadas con aspectos técnicos, administrativos entre otros.

A continuación, se relacionan los principales documentos que se generan en el desarrollo de un proyecto a partir del uso de la norma ISO 21500:2012

Tabla 9.

Relación de los principales documentos que se relacionan en un proyecto

Inicio	•Proyecto nuevo ○Caso de negocio ○Contacto ○Enunciado de trabajo ○Documentación de fase previa •Acta de constitución de proyecto
Planificación	•Planes de Proyecto •Lecciones aprendidas de los proyectos previos
Implementación	•Lecciones aprendidas
Control	•Cambios aprobados •Informes de avances •Acciones correctivas
Cierre	•Informe cierre de los proyectos o fase de proyecto

Fuente: El Autor

La norma ISO 21500:2012, desde su aplicación evidencia que esta actividad (Gestión de Proyectos según la ISO 21500, 2015) Impulsa la transferencia de conocimiento entre proyectos con el fin de establecer mejoras en ejecución de estos.

Análisis Político, Económico, Social y Tecnológico

Es aquí donde se debe asociar la recopilación de la información relacionada con el estado actual de la seguridad de la información en Pequeñas y Medianas Empresas con el establecimiento de un plan estratégico que contribuya en el robustecimiento de las capacidades de ciberseguridad. Para esto se presenta a continuación matriz PEST la cual analiza los factores políticos, económicos, sociales y tecnológicos, que tiene como propósito el evidenciar variables que deban ser consideradas en la creación de un CSIRT con el fin de identificar algún tipo de impacto que pueda afectar el desarrollo de sus servicios.

Figura 13.

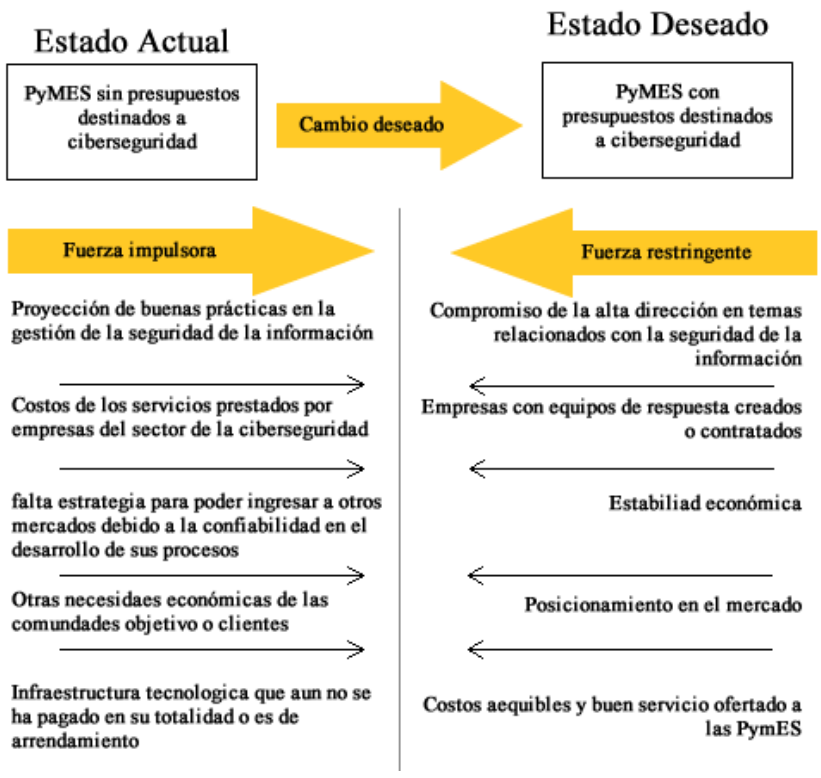
Matriz PEST que analiza la creación de un Equipo de Respuestas a Incidentes Informáticos orientado a Pequeñas y Medianas Empresas del Sector Económico Colombiano

Fuente: El Autor

A continuación, se presenta un análisis de campo de fuerza el cual muestra la necesidad de consolidar un Equipo de Respuestas a Incidentes Informáticos orientado a Pequeñas y Medianas Empresas. Es de tener presente que este análisis tiene como propósito identificar factores que contribuyen en facilitar el cambio en un proyecto, permitiendo visibilizar hasta donde este puede ser difícil.

Figura 14.

Análisis de campo de Fuerzas

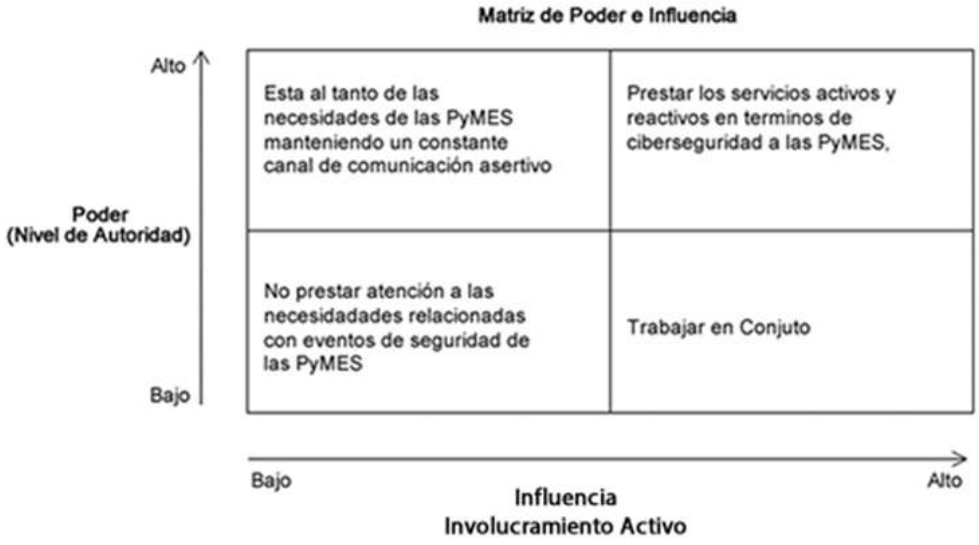


Fuente: El Autor

La Matriz de Poder y de Influencia, agrupa las partes interesadas basándose en el nivel de autoridad y en la capacidad de participar de forma activa en un proyecto de ciberseguridad (MDAP, 2016).

Figura 15.

Mapa de Poder e Influencia para la creación de un CSIRT que dé respuesta a las necesidades del sector de las PyMES en Colombia.

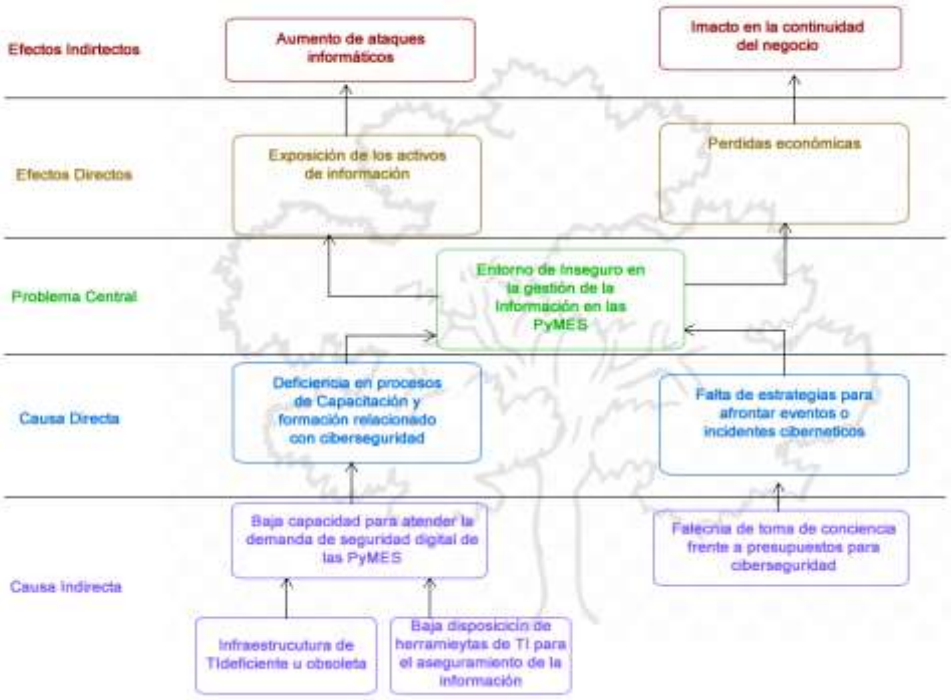


Fuente: El Autor

A continuación, se presenta el diagrama de árbol de problemas el cual tiene como propósito aplicar una técnica que permita identificar situaciones negativas a partir de un problema central. Estos deben ser analizados teniendo en cuenta relaciones de causa efecto. (UNESCO, s.f.). Para el análisis la causa raíz identificada es: Entorno Inseguro en la Gestión de la información en las PyMES

Figura 16.

Análisis de Árbol de Problemas

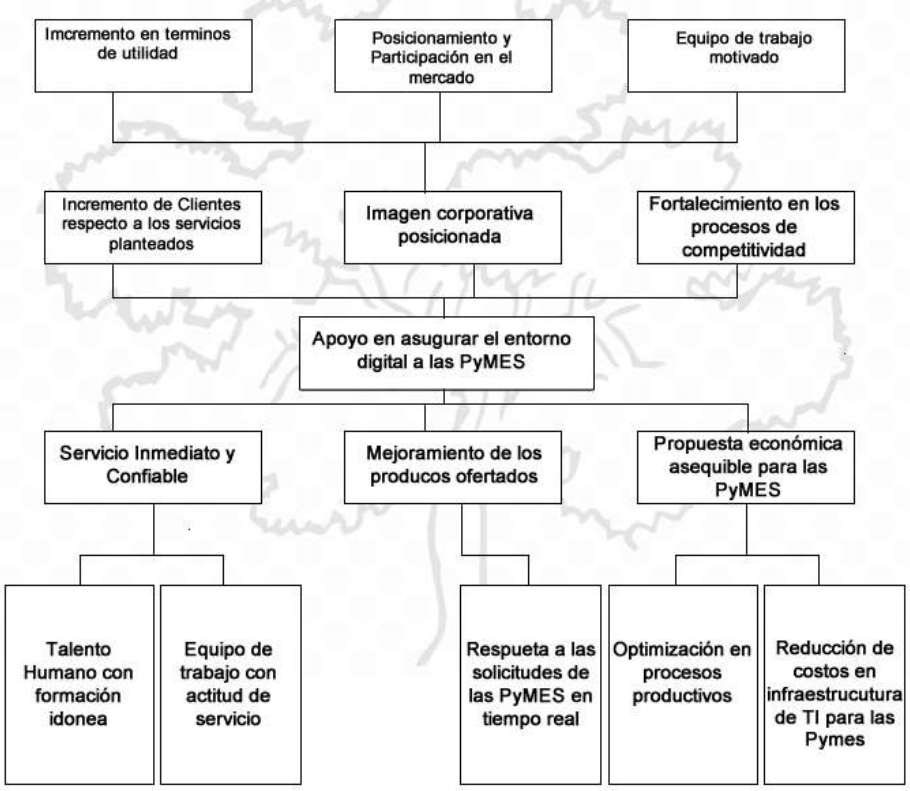


Fuente*:* El Autor

De igual forma, se construye el Árbol de objetivos que tiene como propósito reunir o presentar medios y alternativas que den solución a la pregunta problema, con el fin de lograr un panorama positivo de las situaciones que se presentaron en el Árbol de Problemas.

Figura 17.

Árbol de Objetivos propuesto para la creación de un Equipo de Respuestas a Incidentes Informáticos orientado a Pequeñas y Medianas Empresas del Sector Económico Colombiano



Fuente: El Autor.

Análisis de Partes Interesadas

Teniendo presente que las partes interesadas analizadas para la creación de un Equipo de Respuestas a Incidentes Informáticos son las Pequeñas y Medianas Empresas del sector económico del país, a continuación, se plantea un esquema que pueda permitir identificar la dependencia tecnológica de una organización. Para este punto se puede tener en cuenta lo

planteado por INCIBE en 2015 que aún sigue vigente en termino de análisis de partes interesadas a partir del tipo de dependencia tecnológica con la que puede contar una organización (INCIBE, 2015):

Dependencia Baja: Se pueden catalogar a las empresas que en sus quehaceres diarios usan:

- Computadores para trabajos administrativos
- Bases de datos de forma local
- Internet para realizar búsquedas de información
- Correo electrónico como una canal más de comunicación
- Puede contar con una página web informativa
- Tiene establecida una red de datos local para compartir procesos administrativos

Dependencia Media: Se pueden catalogar empresas que usan en su quehacer diario:

- Herramientas colaborativas para la gestión del modelo de negocio
    1. Procesos
    2. Talento Humano
    3. Gestión de clientes
- Internet como herramienta de mercadeo para potencializar el negocio
- Cuenta con servidor de correo configurado en su red o subcontratado
- Hacen copias de seguridad en sitios remotos para salvaguardar la información
- Cuentan con una red local para compartir procesos administrativos o información utilizando como infraestructura servidores propios
- La página web presenta contenido dinámico y actualizado

- Pueden hacer uso de dispositivos móviles o portables para tener acceso a la información a través de la red corporativa

Dependencia Alta: Se pueden catalogar a las empresas que en sus quehaceres diarios usan

- Diferentes tipos de red para desarrollar su modelo de negocio
    1. Internet
    2. Intranet
    3. Extranet
- Puede contar con plataformas o sistemas de ventas en internet
- Realiza intercambios de forma electrónica para dar desarrollo al modelo de negocio
    1. Contratación
    2. Facturación
- Hace uso de herramientas colaborativas haciendo uso de sus plataformas web.
- Cuenta con talento humano para resolver eventos o incidentes informáticos.
- Dispone del recurso para seleccionar herramientas de trabajo digital para solventar sus necesidades.

Con base en la información que se relacionó anteriormente, es preciso plantear el nivel de interés que puedan presentar las partes interesadas y como el Equipo de Respuestas puede influir en el desarrollo de actividades seguras de las PyMES

Figura 18.

Matriz de Influencia e Interés de partes interesadas respecto aun CSIRT

Fuente: El Autor

La figura 18, permite evidenciar la influencia y el interés que puede presentar una PyME respecto a los servicios proporcionados por un Equipo de Respuesta. En este se aprecia que el mantener un contacto cercano genera satisfacción entre las partes interesadas.

Capítulo IV

Objetivo 3. Esquematizar una propuesta tecnológica que sirva como infraestructura lógica y física para la gestión de un evento de ciberseguridad.

Para el desarrollo de las actividades de un equipo de respuesta es necesario contar con una infraestructura que permita dar respuesta a los eventos informáticos o servicios que puedan ser ofertados a las PyMES. A continuación, se presenta un esquema de herramientas de software y de talento humano mínimos para la creación de un CSIRT.

Talento humano

La OEA en el documento denominado "*Buenas Prácticas para establecer un CSIRT nacional*" (OEA, 2021), propone los siguientes roles y perfiles mínimos con los que debe contar un CSIRT para el desarrollo de sus actividades. Es importante resaltar la importancia de este ítem, ya que la metodología para el desarrollo de proyectos ISO 21500:2012 lo contempla como una de sus actividades fundamentales para la realización de un proyecto (ISO-21500, 2018).

Para esta actividad se requiere tener:

Director: Este rol se encarga de direccionar de forma estratégica al equipo de respuestas

- Supervisa el trabajo y las actividades del equipo
- Realiza las entrevistas del talento humano para los roles requeridos por el equipo y hace la respectiva contratación
- Es quien asiste a las sesiones del consejo asesor de seguridad en la organización

Gerente de Triage: Rol que se encarga de clasificar y priorizar los eventos que pueda presentar la parte interesada.

- Realiza la asignación de personal técnico

Gestor de Incidentes: Rol que se encarga de analizar los incidentes, monitorearlos registrarlos y dar respuesta a estos

- Coordina la respuesta a incidentes al interior del equipo
- Contribuye a partir de la resolución de incidentes con otros equipos de respuesta

Clasificador de eventos: Rol que brinda apoyo inicial en la respuesta a un evento o incidente

- Tiene la responsabilidad de clasificar y priorizar la información recibida de un caso por parte de la parte interesada.

Analista – Investigador: Rol que trabaja en procesos de I+D en temas relacionados con ciberseguridad

- Apoya de forma técnica las iniciativas del equipo de trabajo
- Realizar procesos de monitoreo
- Tiene la capacidad para el desarrollo de herramientas enfocadas en procesos de ciberseguridad

Gerente de comunicaciones: Diseña y publica documentos correspondientes al equipo de respuestas

- Gestiona el sitio web del equipo y sus redes sociales

Administrador de red: Mantiene y administra la red de comunicaciones del equipo de trabajo

- Apoya los procesos de respuesta en temas relacionados con las redes de datos

Administrador de sistemas: Administra y gestiona a partir del mantenimiento los sistemas informáticos del equipo de respuestas

- Apoya los procesos de respuesta en temas relacionados con sistemas de información
- Tiene como responsabilidad gestionar el privilegio de accesos a la información

Representante: Representa al Equipo de respuestas en eventos y podría llegar a realizar procesos de capacitación con otros actores

Vocero: Es el rol autorizado para interactuar o generar comunicación con diferentes medios (prensa, tv, entre otros)

Custodio de registro: Tiene el rol de custodiar el acceso a repositorios seguros de información

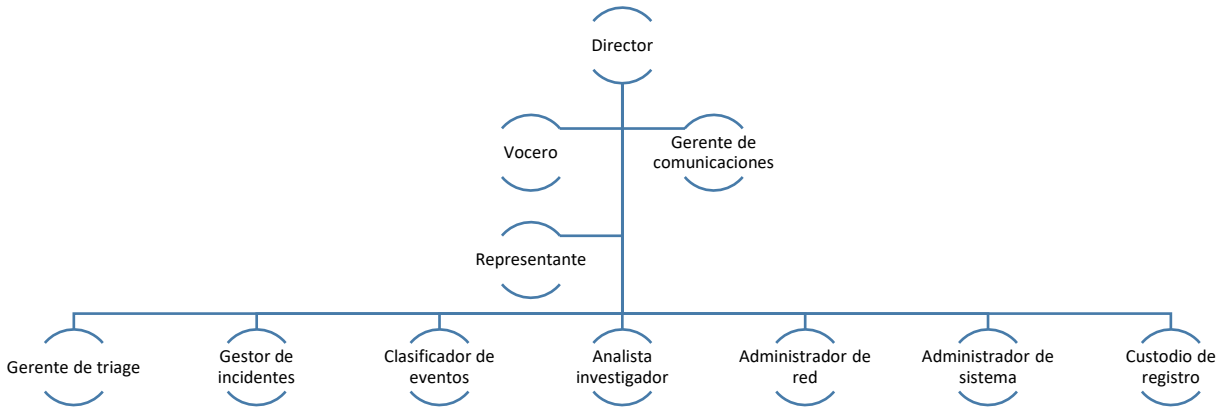
Asistente: Realiza la acción de asistir al talento humano del equipo de respuesta a partir de las tareas que sean asignadas

Es preciso indicar que estos roles y sus respectivas funciones se distribuyen con los diferentes actores del equipo de trabajo generando así que una misma persona ejerza varias funciones o roles a la vez. Es por esto por lo que para estos casos debe existir una política que sea lo suficientemente clara respecto a la separación o segregación de funciones.

La figura 19 plantea un posible organigrama funcional a partir de los roles que fueron expuestos:

Figura 19.

Propuesta de organigrama para un equipo de respuesta a incidentes que brinde apoyo a medianas y pequeñas empresas



Fuente: El Autor

Herramientas tecnológicas

Las herramientas tecnológicas relacionadas con software para apalancar las necesidades de un equipo de respuesta, pueden ser consideradas teniendo presente si son de licencia, es decir requieren algún tipo de pago, o si se trabajara con infraestructura de licencias Publicas Generales – GNU - GPL [15], esto indica que es una licencia de derechos de autor que brinda a los usuarios finales hacer uso de forma libre para estudiar, compartir o modificar el software según sea el caso, siempre protegiendo el software de intentos de apropiación (Mozilla, 2020).

A continuación, se presenta un esquema básico de uso de infraestructura lógica para el desarrollo de las actividades de un equipo de respuesta. Los datos presentados hacen parte de los

[15] GNU - GPL hace referencia a licencia publica general o licencia de software libre que permite la libertad de usar, modificar y compartir el código fuente de una aplicación

informes publicados por la empresa consultoría e investigación en TI, Gartner entre los años 2020 – 2021 (RICOH, 2021).

En la figura 20 se presente el cuadrante mágico de Gartner, el cual muestra la culminación que se da a partir de la investigación de un mercado puntual de tecnología con el fin de proporcionar una visión global de los actores de desarrollo tecnológico más relevantes del mercado.

El método de valoración se realiza a partir de la construcción de un gráfico con dos ejes:

Figura 20.

Esquema del cuadrante de Gartner

Nota. Explicación del cuadrante de Gartner. Fuente: RICOH, 2021.

- Eje Vertical: presenta las empresas con más conocimiento del mercado
- Eje Horizontal: presenta las empresas que demuestran mejores habilidades para el uso de sus productos.

Vale la pena mencionar que entre más a la derecha de la gráfica este el producto, este será más completo y entre más arriba se ubique, será más fácil de usar.

Los cuadrantes que se encuentran en su interior presentan a los proveedores de TI mejor posicionados teniendo en cuenta las siguientes capacidades (ISC, 2019):

- Aspirantes: Son las empresas o servicios de TI que brindan una buena ejecución del negocio y tienen la capacidad de dominar un vasto segmento del mercado, pero no han logrado demostrar un entendimiento real de este.
- Líderes: Son las empresas o servicios de TI que hacen un buen desarrollo de su negocio y que se encuentran bien posicionados para resolver lo que se presente.
- Jugadores de nicho especifico: Son las empresas o servicios que se están enfocando en tener éxito en un segmento de mercado puntual, pero que aún no han adquirido una visión global del negocio o no se han caracterizado por presentar grandes innovaciones o por superar a la competencia.
- Visionarios: Son las empresas o servicios que interpretan hacia donde puede ir el mercado con el fin de poder plantear cambios en sus ideas o en las reglas y sus paradigmas pero que aún no tienen la capacidad de desarrollar con éxito sus ideas.

Propuesta de infraestructura lógica básica para el desarrollo de las actividades de un Equipo de Respuestas

Servicio de Gestión de incidentes

Servicio de prevención: Permite generar alertas a partir de la valoración de eventos teniendo presente la importancia de este y su gravedad.

Producto: SIEM[16] - Software: Splunk - Tipo de licencia: Pago

[16] Un SIEM es un Sistema Gestor de eventos de Información de Ciberseguridad el cual brinda información acerca de potenciales amenazas al interior de una organización

Figura 21.

Cuadrante de Gartner para soluciones de SIEM 2020

Nota. Cuadrado mágico de Gartner. Fuente: IT, 2020

Alternativa de código abierto (GNU - GPL)

Software: Elasticsearch / Kibana - Tipo de licencia: libre

Servicio de detección: Permite analizar los incidentes a partir de su identificación y análisis

Producto: SIEM - Software: Splunk - Tipo de licencia: Pago

Figura 22.

Cuadrante de Gartner para soluciones de soluciones de SIEM 2020

Nota. Cuadrado mágico de Gartner. Fuente: IT, 2020

Alternativa de código abierto

Software: Elasticsearch / Kibana / Wazuh -Tipo de licencia: libre

Servicio de Contención y Respuesta: Permite dar soporte a la respuesta de incidentes a partir del monitoreo y la generación de reportes y envío de documentación técnica que brinda pautas para resolver un incidente

Producto: Herramienta de monitoreo de infraestructura tecnológica - Software: Palo Alto - Tipo de licencia: Pago

Figura 23.

Cuadrante de Gartner para soluciones de UTM[17] según Gartner 2020

Nota. Cuadrado mágico de Gartner. Fuente: Palo alto, 2020

Alternativa de código abierto - Software: PfSense – Suricata - Tipo de licencia: libre

Servicios de Gestión de Vulnerabilidades

Servicios de descubrimiento: Permite identificar activos de información que puedan ser requeridos para procesos de identificación de vulnerabilidades

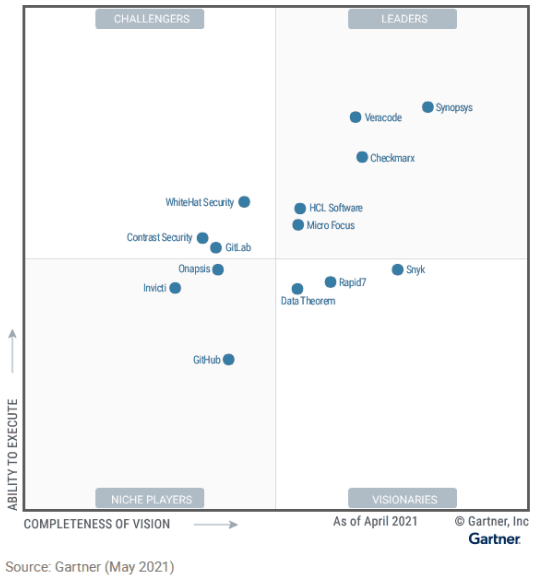
Servicios de Detección y Análisis: Permite la recopilación de información que se relaciona con los activos de información

[17] Un UTM (Gestión Unificad de Amenazas), es un software que permite unificar las amenazas de una organización en un solo sistema

Producto: Herramienta para gestión de vulnerabilidades y monitoreo - Software: Synopsys - Tipo de licencia: Pago

Figura 24.

Cuadrante de Gartner para soluciones de Gestión de vulnerabilidades 2021



Nota. Cuadrado mágico de Gartner. Fuente: Synopsys, 2021

Alternativa de código abierto - Software: Openvas (Greenbone) - Tipo de licencia: libre

Servicio de Formación, Educación y Concienciación

Servicios: Plataforma E-learning para el desarrollo de programas de formación y concienciación - Software: Moodle - Tipo de licencia: libre

Servicio de Auditorias Técnicas

Servicios de Auditorias forenses: Servicio que se oferta después de presentado un evento o incidente de seguridad con el fin de identificar su origen

Hacking Ético: Se presentan como actividades que apoyan el proceso de auditoría, con el fin de identificar vulnerabilidades de sistemas de información.

Software: Kali Linux - BackBox – Parrot Security OS - Tipo de licencia: libre

Es importante resaltar que el uso de las herramientas planteadas se relaciona con tecnologías 4.0, las cuales contribuyen en la generación de Business Intelligence – BI.

- Big Data: Esta tecnología permite extraer información que debe ser analizada y que sea relevante para las decisiones del negocio Ejemplo:
  - Diseño modelos predictivos para la prevención y mejora de un entorno digital seguro
  - Obtención de capacidades para dar respuesta a eventos o incidentes cibernéticos o la reducción en su impacto debido a la materialización de estos.
  - Información para dar respuesta de forma rápida y acertada teniendo presente lecciones aprendidas y la recopilación e intercambio de información con otros equipos de respuesta.
- Tecnología Blockchain: Esta tecnología permite documentar datos administrados por un grupo de computadoras el cual genera datos inmutables, compatibles y con un registro de marca a través del tiempo (Delgado, 2019), esta tecnología aporta en garantizar las dimensiones de la seguridad de la información[18] de una organización y de los datos que gestiona un equipo de respuesta. A continuación, se relacionan las dimensiones (ENS, 2013):
- Disponibilidad: "*disposición de los servicios a ser usados cuando sea necesario"*
- Integridad: "*mantenimiento de las características de completitud y corrección de los datos"*
- Confidencialidad: "que la información llegue solamente a las personas autorizadas"

[18] Las dimensiones de seguridad de la información son los pilares fundamentes que se deben tener en cuenta en el momento de salvaguardar la información. Disponibilidad: la información debe estar disponible cunado se necesite. Integridad: la información no su sufre de cambios indeseados. Confidencialidad: la información solo está disponible para personas autorizadas

Blockchain: Contribuye en la construcción de una estrategia que permite que el esquema de seguridad de un Equipo de Respuestas y de sus partes interesadas sea más segura a partir de la priorización de los controles que se implementen con el fin de reducir amenazas conocidas y emergentes, con una búsqueda constante de inteligencia de amenazas y de conocimiento para identificar conductas que puedan afectar a partes interesadas y resilientes, lo cual permitirá tener la capacidad de poderse recuperar y de minimizar el impacto de algún evento o incidente cibernético (Piscin & Dalton).

Infraestructura Física

En 2012 El registro de direcciones de internet de América latina y el caribe, presenta una propuesta para la infraestructura física que sirve para dar respuesta a un evento de seguridad. Esta aún permanece vigente (LACNIC, 2012):

Espacio físico: debe contar con las siguientes condiciones: espacio y movilidad, espacios para el tratamiento acústico, equipos para el control del ambiente climático, instalaciones eléctricas y equipos para el manejo de picos y ruidos electromagnéticos y cableado de red.

Es recomendable que el equipo de respuesta brinde sus servicios en un espacio locativo diferente al de alguno de las partes interesadas, esto teniendo presente posibles amenazas de tipo de intrusión o situaciones hostiles, asalto o desastres naturales.

Respecto a la infraestructura Tecnológica, a continuación, se relacionan los equipos mínimos con los que el Equipo de respuestas podría iniciar sus actividades:

Tabla 10.

Infraestructura tecnología de inicio de actividades

Descripción	Cantidad
Servidor de aplicaciones relacionada con los servicios de CSIRT (intranet)	1
Servidor de pruebas	1
Servidor para el SIEM - agente de monitoreo - correlación - búsqueda de eventos	1
Servidor de Logs y almacenamiento - Servidor para monitoreo de red - uso del PRTG	1
SAN - Sistema de almacenamiento	1
Switch y Router	3

Fuente: El Autor

La figura 25, está construida con Software de uso libre, este puede abarcar las necesidades básicas para iniciar las alternativas de un equipo de respuestas y permite reducir el uso de infraestructura tecnológica o de hardware a partir de tecnología como lo es la de gestor de contenedores[19] o hipervisores[20].

[19] Aplicaciones que permiten hacer un despliegue rápido de infraestructuras lógicas o de software. Un de los más usados en el sector de TI es Docker

[20] Software que permite la creación de máquinas virtuales, permitiendo administrar los recursos de hardware entre dos o más de dos sistemas operativos

Figura 25.

Esquema de herramientas de software libre para la implementación básica de un equipo de respuestas

Fuente: El Autor

La figura anterior plantea herramientas de software libre que permiten:

Proxmox o Docker: Despliega los servicios estratégicos de un centro de respuestas a incidentes informáticos, los cuales pueden apalancar procesos de virtualización de sistemas

PfSense: Gestiona el filtrado de información entrante y saliente de una red con el fin de controlar las operaciones que se realizan en el quehacer diario de una organización

OpenVPN: Permite crear redes virtuales privadas que aseguran la comunicación de dispositivos que se encuentran fuera de la red de datos y que deben o pueden acceder a la información que se encuentra al interior de estas.

Openvas - Greenbone: permite la identificación y gestión de vulnerabilidades en un sistema de información digital con el fin de ser tratadas de forma preventiva y correctiva

Elasticsearch – Kibana – Wazuh: Permite centralizar y correlacionar los diferentes registros de información generados por los sistemas de información usados al interior de una PyME.

Nagios: permite realizar el seguimiento y la trazabilidad del flujo de datos a través de una red de comunicación.

Estas herramientas son de uso libre y permiten ser configuradas como infraestructura lógica para el despliegue de servicios de un Equipo de Respuesta a Incidentes Informáticos enfocado las necesidades de ciberseguridad de una Pequeña y Mediana Empresa, permitiendo así realizar una inversión económica mínima en software en comparación con la adquisición de una solución comercial.

Conclusiones

La hipótesis señalada “Las organizaciones que no se anticipan ante potenciales riesgos de ciberseguridad se ven afectadas en su infraestructura tecnológica ocasionada por un evento o incidente informático, el cual genera pérdidas financieras y reputacionales, acciones legales y la afectación en la continuidad del negocio.”, se comprueba teniendo presente lo expuesto en el capítulo uno, ya que a partir de la fundamentación teórica planteada en los marcos y el desarrollo del capítulo dos, se puede evidenciar que las pérdidas económicas debido a ataques informáticos para el año 2019 oscilaba entre 300 y 5000 millones de pesos, indicando además que la baja capacidad en recursos como talento humano capacitado y la poca inversión en ciberseguridad que las PyMES asignan en sus presupuestos es una realidad. Esto sin duda alguna afecta la continuidad del negocio ocasionando pérdidas económicas y reputacionales.

El capítulo tres, se establece un plan estratégico que contribuye en el robustecimiento de las capacidades de ciberseguridad, que aporta a la continuidad de negocio a partir del diseño de un Plan Director de Seguridad y que se integra con una metodología para el desarrollo de proyectos como la ISO 21500. En este plan, se brindan lineamientos claros para que una organización o para que un equipo de respuestas a incidentes informáticos, cuenten con un talento humano capacitado con unos procesos definidos para la gestión de la información y la protección de los datos y con el uso de tecnologías que permitan mejorar el aseguramiento de sus entornos digitales.

Así mismo, este capítulo, soporta la necesidad de consolidar un equipo de respuestas a incidentes informáticos que brinde servicios a PyMES, teniendo presente lo planteado en la matriz de análisis de factores políticos, sociales, económicos y tecnológicos, evidenciando en

esta, la necesidad de ampliar un modelo de negocio en la línea de la ciberseguridad, que impacte a las pequeñas y medianas empresas a partir del despliegue de servicios acorde a sus presupuestos y necesidades, que acompañen a este sector de la economía en el cumplimiento de la legislación y normatividad y que fortalezca como servicio externo sus infraestructuras tecnológicas con el ánimo de mejorar el estado de la ciberseguridad.

El capítulo 4, esquematiza una propuesta que sirva como infraestructura tecnológica y física para el despliegue de los servicios de un CSIRT de PyMES. Esta infraestructura se proyecta teniendo presente: Uno: Recursos mínimos locativos que permitan tener un espacio físico para la prestación de sus servicios. DOS: Recursos mínimos de hardware los cuales pueden ser considerados en un presupuesto a un costo bajo en su adquisición. TRES: El uso de herramientas de software libre lo cual termina siendo el valor agregado en términos de inversión. Es por esto por lo que un Equipo de respuestas orientado a PyMES no solo se implementa con el fin de dar cumplimiento a las exigencias normativas que se imponen en torno a la seguridad digital, sino que permite abarcar estratégicamente las necesidades de una Pequeña y Mediana Empresa con el fin de contribuir en la mejora de prácticas de gobierno de TI, generando impacto en la competitividad de la organización y en su entorno digital.

Recomendaciones

La implementación de un CSIRT es una tarea que debe ser prioritaria en las organizaciones por los beneficios que se obtienen a largo plazo en cuanto a la construcción de una cultura adecuada de prevención y cuidado de los activos de información. Para lograrlo, es prioritario el levantamiento de los activos de información de cada empresa y de acuerdo con esto, implementar las estrategias y política del manejo de esta misma con el fin de mitigar la materialización de riesgos existentes. Para esto, se recomienda continuar trabajando en las estrategias que buscan hacer accesible a estas empresas orientadas hacia la identificación de la vulnerabilidad por medio de metodologías para que la solución sea conveniente y de fácil implementación y puesta en marcha de estas actividades.

Se recomienda a futuro, continuar esta iniciativa efectuando estudios documentales o de investigación para abordar temas relacionados con estimación de costos relacionados con eventos o incidentes presentados en un entorno digital y como poder establecer la valoración de un activo de información de tal forma que se pueda definir el retorno de inversión de la seguridad de la información - ROSI.

Así mismo es preciso realizar estudios que aporten como establecer procesos para el despliegue de servicios con partes interesadas o comunidades objetivos y como establecer un plan de negocio que plantee estrategias relacionada con el proceso de ventas y la proyección de su catálogo de servicios.

Bibliografía

agoraSIC. (2019). *CSIRTS: Al pie del cañon.* Centro de Conocimeinto en Ciberseguridad: https://www.first.org/newsroom/releases/FIRST-Press-Release-20201118.pdf

BID. (2017). *Impacto de los incidentes de seguridad digital.* https://publications.iadb.org/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf

BÖHME. (2010). *Security metrics and security investment models.* Universidad de Berkeley: http://lyle.smu.edu/~tylerm/courses/econsec/reading/lnsesecinv2.pdf

Bortnik, S. (2010). *Retorno de inversión en seguridad.* ESET: https://www.welivesecurity.com/la-es/2010/04/06/retorno-de-inversion-en-seguridad/

Candeltey, D. (18 de 02 de 2020). *La ciberseguridad, sinónimo de empleo: se necesitan 350.000 trabajadores en Europa*. Universidad de la Rioja: https://www.unir.net/ingenieria/revista/la-ciberseguridad-sinonimo-de-empleo-se-necesitan-350-000-trabajadores-en-europa/

CCIT, & PONAL. (29 de Octubre de 2019). *Tendencias Cibercrimen Colombia 2019 - 2020*. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

CECIP. (2020). *Balance Cibercrimen 2020.* Bogotá.

Charla norma 21500. (28 de 05 de 2014). Notas: Plan director de seguridad (Plan director de seguridad, s.f.)

Ciberseguridad.com. (2020). *ciberseguridad*. https://ciberseguridad.com/empresas/colombia/

Delgado, P. (24 de 4 de 2019). *Tecnologico de Monterey.* https://observatorio.tec.mx/edu-news/que-es-blockchain

Descuadrando. (s.f.). *Análisis PEST.* Descuadrando: http://descuadrando.com/An%C3%A1lisis_PEST

Dinero. (24 de Julio de 2020). *La ciberseguridad, cada vez más relevante para las organizaciones*. https://www.dinero.com/hablan-las-marcas/articulo/la-ciberseguridad--cada-vez-mas-relevante-para-las-organizaciones/293516

DNP. (2016). *Política Nacional de Seguridad Digital.* Departamento Nacional de Plaeación: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

ECACEN. (2017). *Escuela de Ciencas Administrativas, Contables, Económicas y de Negocio.* Universidad Nacional Abierta y a Distancia: https://academia.unad.edu.co/ecacen/investigacion-y-productividad/lineas

ECURED. (s.f). *ECURED.* CMM: https://www.ecured.cu/CMM

ENS. (2013). *Metodología de Analisis y Gestión de Riesgos de los Sistemas de Información.* Centro Criptologico Nacional de España: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

ESET. (2018). *Minería de criptomonedas: respuesta a tres de las preguntas más frecuentes.* Welivesecurity: https://www.welivesecurity.com/la-es/2018/06/22/mineria-criptomonedas-respuesta-tres-preguntas-frecuentes/

Espino , & Martínez . (2017). *Análisis predictivo: técnicas y modelos utilizados y aplicaciones del mismo - herramientas Open Sourceque permiten su uso.* UOC: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/59565/6/caresptimTFG0117mem%C3%B2ria.pdf

FBI. (2019). *Internet Crime Report*. https://pdf.ic3.gov/2019_IC3Report.pdf

Fernández, S. (2002). *Investigación cuantitativa y cualitativa.* . Coruña España: Cad Aten primaria complejo Hospitalario Juan Canalejo.

FIRST. (2020). *FIRST Teams.* Foro de Respuesta a Incidentes y Equipos de Seguridad: https://www.first.org/members/teams/?#

Fregoso, c. (17 de 03 de 2021). *INTERUS*. Estrategias de marketing digital: https://blog.interius.com.mx/quick-wins-para-empezar-automatizar-procesos-empresa

Freyre, C. (11 de Marzo de 2019). *El papel de la ciberseguridad en las organizaciones*. Escuela Argentina de Negocios: http://www.ean.edu.ar/nota/299-el-papel-de-la-ciberseguridad-en-las-organizaciones

GCA. (2020). *Global Cybersecurity Agenda (GCA).* https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

GORDON, & LOEB. (2002). *The economics of information security* . https://dl.acm.org/citation.cfm?id=581274

INCIBE. (2015). *Taxonomía de Soluciones de Ciberseguridad.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/taxonomia_ciberseguridad.pdf

INCIBE. (2017). Glosario de términos de ciberseguridad: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

INCIBE. (2017). *¡Fácil y sencillo! Análisis de riesgos en 6 pasos.* https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE. (2020). *Plan Director de Seguridad.* Instituo Nacional de Ciberseguridad: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

Institute, P. (2019). https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf

ISC. (2019). *Ingeniería, Servicios y Comunicaciones.*

ISO. (2015). *GTC-ISO-IEC 27002:2015.* TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN: https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/normavw.aspx?ID=308

ISO-21500. (2018). *ISO 21500.* http://www.iso-21500.es/sites/default/files/ficheros_guia_iso21500/p01-guia_de_gestion_de_los_recursos_0.pdf

IT, p. (2020). *Splunk por séptimo año consecutivo líder en el cuadrante mágico de Gartner en SIEM*. https://panoramait.com/splunk-por-septimo-ano-consecutivo-en-el-cuadrante-magico-de-gartner-en-siem/

ITU. (2020). *Global Cybersecurity Index 2020.* https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020

Kaspersky. (28 de Noviembre de 2017). *las brechas de seguridad ocasionadas por terceros representan un costo mayor para las empresas*. https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-security-breaches

LACNIC. (2012). *Manual báscio de: Gestión de Incidentes de Seguridad Informática.* https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

MDAP. (2016). *Excecutive Master Project Management.* https://uv-mdap.com/matriz-poder-influencia-interesados/

Minsalud. (03 de 2020). *Ministerio de Salud de Colombia*. https://www.minsalud.gov.co/CC/Noticias/2020/03/Paginas/Historico-Noticias.aspx

MINTIC. (2016). *Fortalecimiento de Gestiòn TI en el Estado*. https://www.mintic.gov.co/gestionti/615/w3-article-5482.html?_noredirect=1

MINTIC. (2017). *Controles de Seguridad y Privacidad de la Información.* Seguridad y Privacidad de la Información: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

MINTIC. (27 de 03 de 2020). *Ministerio de tecnologias de la información y las telecomunicaciones*. https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126374:Top-de-herramientas-digitales-para-que-las-mipyme-trabajen-en-linea

MNEMO. (s.f.). https://cert.mnemo.com/fraude-bec-la-amenaza-silenciosa-que-afecta-a-areas-financieras-de-empresas-mexicanas/

Mozilla. (2020). *MDN Web Docs.* https://developer.mozilla.org/es/docs/Glossary/GPL

Mundo, E. (23 de Marzo de 2020). *Diario El Mundo*. https://www.elmundo.es/economia/2020/03/23/5e7773bf21efa0ec658b4634.html

MyITU. (2021). https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020

NIST. (2021). *SP 800-53 Rev. 5.* Security and Privacy Controls for Information Systems and Organizations: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

OEA. (2021). *Semillero Ceros y Unos.* Semillero Ceros y Unos: https://semillerocerosyunos.com/index.php/2021/07/02/buenas-practicas-para-establecer-un-csirt-nacional/

OSI - INCIBE. (2018). *Guía de ciberataques. Todo lo que debes saber a nivel usuario.* Oficina de Seguridad del Internauta: https://www.osi.es/es/guia-ciberataques

País, E. (18 de 01 de 2018). *Diario el País*. https://www.elpais.com.co/tecnologia/el-96-de-las-empresas-en-colombia-utilizan-internet.html

Palo alto. (2020). *A 2020 Gartner Magic Quadrant Leader for Network Firewalls.* https://start.paloaltonetworks.com/2020-gartner-mq-for-firewalls.html

Panda Security. (s.f.). *¿Qué es un Ransomware?* https://www.pandasecurity.com/es/mediacenter/malware/que-es-un-ransomware/

Piscin, E., & Dalton, D. (s.f.). *Blockchain & Ciberseguridad.* https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Blockchain&%20CiberseguridadESP%20(1).pdf

Plan director de seguridad. (2019). https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

PONEMON. (2019). *Exclusive Research Report 2019 Global State of cybersecurity iun small and medium-size businesses*. https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf

RAE. (s.f.). *RAE*. https://dle.rae.es/taxonom%C3%ADa

Revista Dinero. (2020). Ciberataques en América Latina: ¿están expuestas las empresas colombianas? *Revista DInero*.

RICOH. (2021). *Cuadrante mágico de Gardner*. https://digital.ricoh.es/que-es-cuadrante-magico-gartner/

Rojas, Moreira, Marín, & Torres. (2019). *Revista ULatina.* https://revistas.ulatina.ac.cr/index.php/tecnologiavital/article/view/231/238

Scotiabank Colpatria. (2021). *Te contamos qué es SIM Swapping, una modalidad de robo.* https://www.scotiabankcolpatria.com/: https://www.scotiabankcolpatria.com/seguridad-bancaria/swapping

Synopsys. (2021). *https://www.synopsys.com/.* https://www.synopsys.com/software-integrity/resources/analyst-reports/gartner-magic-quadrant-appsec.html

Taylor, S., & Bogdan, R. (1996). *Introducción a los métodos cualitativos de investigación.* Barcelona: Ediciones Paidos Ibérica, S. A.

Tecnozero. (2020). *Cuadrante Mágico de Gartner 2019 para Firewalls de Red.* https://www.tecnozero.com/firewall/cuadrante-magico-de-gartner-2019-para-firewalls-de-red/

UNESCO. (s.f.). *Expresiones culturales.* Organizacion de las Naciones Undas para la Educación la Ciencia y la Cultura: http://www.unesco.org/new/es/culture/themes/%20cultural-diversity/diversity-of-cultural%20expressions/tools/policy-guide/planificar/diagnosticar/arbol-de-problemas/

Vargas, P. (2019). *Análisis Predictivo.* http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.FFCA5910&lang=es&site=eds-live&scope=site

VIrtual, CAI; CCIT;. (Octubre de 2019). *Tendencias del Cibercrimen en Colombia 2019-2020.* https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Zambrano, Moreno, Peña, Tamayo. (2020). *Propuesta para la Creación y Consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD.* https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180