ESTUDIO MONOGRÁFICO SOBRE CASOS MÁS COMUNES DE CIBERCRIMEN EN LAS PYMES COLOMBIANAS

ANA MILENA MARIN GUINEME
OSCAR JAVIER CARVAJAL CARVAJAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

ESTUDIO MONOGRÁFICO SOBRE CASOS MÁS COMUNES DE CIBERCRIMEN EN LAS PYMES COLOMBIANAS

ANA MILENA MARIN GUINEME
OSCAR JAVIER CARVAJAL CARVAJAL

Trabajo de Grado para optar por el título
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de Proyecto
Esp. Ing. MARTIN CANCELADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá Noviembre del 2019

DEDICATORIA

Dios, familia, amigos, y demás personas especiales en mi vida, no son nada más y nada menos que un hermoso conjunto que me han apoyado en todos los momentos alegres y de dificultades en mi vida. No podría sentirme más alegre con la confianza que han puesto en mí, especialmente cuando siempre he contado con su apoyo desde que tengo memoria.

Este nuevo logro es en gran parte gracias a todos ustedes; he logrado concluir con éxito un proyecto que en su inicio parecía un proyecto imposible e interminable. Por lo que quisiera dedicar este proyecto a ustedes, personas buenas, seres de amor, que siempre están conmigo.

AGRADECIMIENTOS

Primero quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi existencia y a mi familia por haber sido mi apoyo a lo largo de toda mi carrera universitaria y a lo largo de mi vida. A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano.

Me gustaría agradecer en estas líneas la ayuda que muchas personas y amigos me han prestado durante el proceso de investigación y redacción de este trabajo. En primer lugar, quisiera agradecer a mis padres que me han ayudado y apoyado en todo mi producto, y a mi tutor, por haberme orientado en todos los momentos que necesité sus consejos.

Agradecemos a nuestros docentes de la UNAD, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, a los directamente relacionados con nuestro proyecto quienes nos han acompañado con su paciencia, y su rectitud como docentes y guías, y por todos los implicados por su valioso aporte para nuestra investigación.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

- AMENAZA: Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización[1].

- CIBERDELITO (Cibercrimen): Actividad delictiva donde servicios o aplicaciones en el ciberespacio se utilizan o son el objetivo de un crimen o donde le ciberespacio es la fuente, herramienta, blanco o el lugar del delito.[2]

- CIBERESPACIO (the Cyberspace): entorno complejo que resulta del a interacción de las personas, el software y los servicios a través de internet, por medio de dispositivos tecnológicos y redes conectados al mismo, que no existe en forma física alguna[3].

- CIBERINTRUSO (cyber-squatter): personas u organizaciones que se registran y mantiene en direcciones URL que se asemejan al a referencias o nombre de otras organizaciones en el mundo real o ciberespacio.[4]

- CIBERPROTECCIÓN (cybersafety): Condición de estar protegido contra consecuencias físicas, sociales, espirituales, financieras, políticas, emocionales, laborales, psicológicas, educacionales u otro tipo de consecuencias por falla, daño, error, accidente, o cualquier evento en el ciberespacio que podría ser considerado no deseable.[5]

- CIBERSEGURIDAD (Cybersecurity /Cyberspace security): Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.[6]

- INTERNET: interconexión de redes o una colección de redes interconectadas.[7]

- PIRATERÍA INFORMÁTICA (hacking): Acceso intencional a un sistema informático sin la autorización del usuario o el propietario.[8]

[1] AMENAZA, NTC ISO 27032, Norma Colombiana, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[2] CIBERDELITO, NTC ISO 27032, Norma Colombiana, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[3] CIBERESPACIO, NTC ISO 27032, Norma Colombiana, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[4]CIBERINTRUSO, NTC ISO 27032, Norma Colombiana, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[5]CIBERPROTECCION, NTC ISO 27032, Norma, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[6] CIBERSEGURIDAD, NTC ISO 27032, Norma Colombiana, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[7] INTERNET, NTC ISO 27032, Norma Colombiana, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[8] PIRATERIA INFORMATICA, NTC ISO 27032, Norma 1ª Ed Icontec: Bogotá 2018-10-05, p18

- SEGURIDAD EN INTERNET[9]: Perseveración de la confidencialidad la integridad y la disponibilidad del a información en la Internet.

- SOFTWARE ENGAÑOSO (deceptive software) Software que realiza actividades en la computadora de un usuario sin notificarle o pedirle autorización para las acciones que el software pretende ejecutar.[10]

- SOFTWARE MALICIOSO: Software diseñado con malas intenciones que contiene características o capacidades que potencialmente pueden causar daño directa o indirectamente al usuario o al sistema informático del usuario. [11]

- SOFTWARE potencialmente no deseado: software engañoso, que incluye el programa maligno, y no malicioso que muestra las características de software engañoso.[12]

- SUPLANTACIÓN DE IDENTIDAD (Phishing): Proceso fraudulento, en una comunicación electrónica, para intentar adquirí información privada o confidencial, de manera enmascarada, haciéndose pasar por una entidad confiable.[13]

- TROYANO (TROJAN/ TROJAN HORSE) Software malintencionado que aparenta realizar una función deseable[14].

- VULNERABILIDAD (vulnerability): Debilidad de un activo o control que puede ser aprovechado por una amenaza.[15]

[9] SEGURIDAD EN INTERNET, NTC ISO 27032, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[10] SOFTWARE ENGAÑOSO, NTC ISO 27032, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[11] SOFTWARE MALICIOSO, NTC ISO 27032, Norma, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[12] SOFTWARE; NTC ISO 27032, Norma Colombiana, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[13] SUPLANTACIÓN DE IDENTIDAD; NTC ISO 27032, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[14] TROYANO; NTC ISO 27032, Norma, 1ª Ed Icontec: Bogotá 2018-10-05, p18
[15] VULNERABILIDAD (vulnerability): Debilidad de un activo o control que puede ser aprovechado por una amenaza

1. INTRODUCCIÓN

Esta monografía pretende analizar las principales técnicas, herramientas y amenazas a las que se ven expuestas las pymes o empresas que no cuentan con infraestructuras de seguridad o malas prácticas en las mismas, se busca documentar las principales medidas y desafíos que enfrenta el país de manera informativa contribuyendo con un documento que esté acorde a la realidad y de manera acertada para Colombia ya que es necesario estar en contexto en el área de ciberseguridad respecto a la región.

En síntesis, mostrar un análisis sobre los últimos riesgos cibernéticos que amenazan a las pequeñas y medianas empresas en Colombia que se adopte el tema con más compromiso dejando de verlo como un asunto externo al que se es ajeno; comparar Colombia en materia de seguridad respecto a la región y qué medidas se están implementando en las empresas emergentes que no cuenten con suficientes recursos para cubrir una infraestructura robusta.

2. PLANTEAMIENTO DEL PROBLEMA

El desarrollo tecnológico en Colombia está contribuyendo con el crecimiento de las pymes[16] Aun así no hay un uso responsable de las tecnologías el hecho de usar sus propios recursos para la protección de la información crea una brecha que las convierte en blanco predilecto para los delincuentes ya que el 80% de las compañías en Colombia son vulnerables a los ataques informáticos.[17]

Al desarrollar un estudio de seguridad informática en empresas emergentes en Colombia, de acuerdo a las leyes de seguridad de la información locales y a los estándares internacionales[18] , es necesario contar con material informativo sobre ciberseguridad en situaciones reales pudiendo desempeñar plan completo desde la parte administrativa, técnica y demás partes que se vean involucradas, que tipo de software muestra más garantías o presenta mayor oportunidad de configurar técnicamente los recursos que se dispongan también se busca documentar la brecha que hoy existe entre organizaciones gubernamentales y pequeñas empresas que están emergiendo en ámbitos de ciberseguridad y ciberdefensa.[19],[20].

Las buenas prácticas desde básicas hasta el uso de infraestructura tecnológica avanzada deben ser entendidas y los procesos que estas comprenden; entonces él lo que refiere a Colombia. ¿Cuáles son los casos más frecuentes y que tan preparadas están las pymes de Colombia frente al cibercrimen?

Colocar en contexto sobre las consecuencias más graves sobre un posible incidente de ciberseguridad la pérdida, daño o mal uso de los datos en las empresas es el problema que se requiere abordar con este proyecto aparte de documentar las buenas prácticas también es reflejar el panorama actual en el campo de la seguridad informática a nivel nacional ya que la ciberseguridad no es

[16]Las empresas colombianas se adaptan rápido al cambio tecnológico, [En línea]. En: Periódico Portafolio, Julio, 17, 2017.,1 p. recuperado de http://www.portafolio.co/innovacion/empresas-colombianas-se-adaptan-rapido-al-cambio-tecnologico-507825

[17] CONTRERAS, Nicolás, Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos, [En línea]. En: Radio Caracol, junio,9, 2016., 1 p Recuperado de http://caracol.com.co/radio/2016/06/09/tecnologia/1465469190_389745.html

[18] COBARRUBIAS, Pedro, Estándares Internacionales de Seguridad Informática, [En línea], septiembre,12, 2013., 1 p. Recuperado de https://es.slideshare.net/PedroCobarrubias/seguridad-informtica-26154937

[19] Altos estándares de seguridad pueden cerrar la puerta al cibercrimen [En línea]. En: Periódico Portafolio, septiembre,29, 2017., 1 p. Recuperado de http://blogs.portafolio.co/seguridad-informatica-certicamara-sa/altos-estandares-seguridad-pueden-cerrar-la-puerta-al-cibercrimen/

[20] El 2015 fue un año de “altas y bajas” para la seguridad informática, [En línea]. En: Periódico Dinero.enero,5, 2016.,1 p. Recuperado de https://www.dinero.com/pais/articulo/informe-certicamara-sobre-seguridad-informatica-colombia-para-2016/217635

algo que aún se tome en cuenta con la prioridad que esta debe tener actualmente[21].

[21]Las empresas en Colombia no invierten en seguridad digital, [En línea]. En: Rev. Semana, junio, 9, 2017., 1 p. Recuperado de https://www.semana.com/tecnologia/articulo/colombia-no-invierte-en-seguridad-digital/492724

3. OBJETIVOS

OBJETIVO GENERAL

- Realizar un estudio monográfico sobre los casos más comunes de cibercrimen en las pymes colombianas.

OBJETIVOS ESPECÍFICOS

- Realizar un estudio sobre las técnicas más usadas por los ciberdelincuentes en las pymes de Colombia.
- Identificar las medidas de seguridad informática de las pymes de Colombia frente a las pymes de Latinoamérica.
- Aportar un análisis sobre las medidas que se están tomando para prevenir ciberataques en las pymes de Colombia.

4. JUSTIFICACION

La documentación sobre los ataques informáticos en el campo de las pymes en Colombia no cuenta con suficiente soporte por lo que este documento permitirá abordar algunas temáticas con mayor profundidad respecto a la investigación cibernética en las pymes.

Como se sabe unos de los activos más importante de las empresas es la información y depende como esta se trata, esto puede marcar una diferencia grande en el mercado con la competencia por lo que es de relevancia absoluta el uso correcto de los sistemas de información, datos y todos los procesos que involucren la privacidad de este activo[22].

En Colombia esto se ve un poco más reflejado en las ciudades capitales pero aún hay muchas empresas en regiones apartadas en el sector rural que están emergiendo y adoptando nuevas tecnologías eso es muy positivo en cuestión de desarrollo, pero deben haber documentos guía que acompañen tanto a empresarios como a usuarios finales a tener más claro los riesgos cibernéticos a los que se pueden ver expuestos, en muchos rincones de Colombia se sigue desconociendo el tema y compromiso con la seguridad informática[23].

El contexto de la idea principal es contribuir con un documento que ayude a tener presente los riesgos que actualmente poseen las pymes como pérdida, modificación, divulgación de información, pérdida de acceso a la misma y las afectaciones que pueden tener en los procesos de la compañía comprendiendo estos riesgos que también se relacionan en los objetivos de esta monografía se puede hacer un uso más responsable de los medios tecnológicos que se están implementado en el desarrollo empresarial colombiano..

[22] GANDINI, Gregorio, El 43% de las empresas colombianas no están preparadas contra los ciberataques, [en línea]. En: Rev. Dinero. Junio, 8, 2016., 1 p. Referenciado de, https://www.dinero.com/pais/articulo/colombia-tuvo-perdidas-de-1-billon-por-ciberataques/224404.

[23] Colombia, el sexto país con más ciberataques en 2017, [en línea]. En: Periódico El colombiano, abril, 12, 2016., 1 p. Referenciado de http://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174

5. MARCO REFERENCIAL

MARCO TEORICO

El gobierno nacional ha llegado a un punto de inflexión en materia de ciberseguridad en alianzas con compañías internacionales, pero también se hace necesaria una revisión activa al sector privado de las pymes ya que su crecimiento es proporcional a los riesgos que conlleva este desarrollo en materia, de seguridad digital es imperante tener presente los posibles vectores de incidencias.

Colombia en materia de seguridad si bien no es el referente en Latinoamérica ha venido adoptando medidas sobre todo en el área de capacitación, el ministerio de las telecomunicaciones ha tomado más en serio incluso impulsando el crecimiento de profesionales en área de tecnologías, aun así hay una brecha grande por cubrir respecto a otros países, el uso de nuevas tecnologías como blockchain o IA (inteligencia artificial) en la región de Latinoamérica es cada día más frecuente, se debe ser consciente de las ventajas y riesgos que esto traerá para las empresas y usuarios, se busca generar un documento competente que pueda beneficiar a empresas pequeñas y grandes al ponerlas en contexto sobre la situación actual en el campo de riesgos cibernéticos[24].

5.1 ANTECEDENTES DEL CIBERCRIMEN EN COLOMBIA

Colombia en el 2015 fue uno de los mejores países del mundo en manejo de la ciberseguridad, ubicado en la quinta posición entre los países de Latinoamérica según ranking de la UIT (Union Internacional de Telecomunicaciones), este resultado es basado en estrategias que el gobierno implemento que busca proteger a los colombianos del ciberespacio en temas como manejo de información, suplantación de identidad, ataques cibernéticos, etc.[25]

Durante el periodo del 2014 al 2016 se recibieron cerca de 13.774 denuncias de violación a la ley 1273 de 2009, en el transcurso del año 2017 aumento este número a 15.565. En el 2016 fueron capturados 18 personas de nacionalidad

[24]LUNA, David, Colombia es fuerte en Ciberseguridad, [EN LINEA]. Ministerios de las Tecnologías de la información y las telecomunicaciones, diciembre, 30, 2015., Tomado de http://www.mintic.gov.co/portal/604/w3-article-14433.html

[25]Colombia entre los mejores del mundo en manejo de ciberseguridad según ranking global de la UIT, EN LINEA]. Ministerios de las Tecnologías de la información y las telecomunicaciones, enero,8 ,2015; tomado de https://www.mintic.gov.co/portal/604/w3-article-8148.html

extranjera por delitos cibernéticos realizados en Colombia. Según el Centro Cibernético Policial y en alianza con la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), las denuncias más frecuentes son las del ciudadano común con un porcentaje 66% de los incidentes siendo una modalidad que afecta fuertemente a Colombia. `12 La estafa que más se presenta es la que se realiza a nivel de ofertas publicadas en una página web o plataformas ecomerce, estas denuncias son originadas por el incumplimiento del algunas de las partes involucradas en la compra del producto.
Se calcula en $9.100 millones al año por perdidas de tipo ataque phishing a nivel mundial solo Colombia se reportó 1.400 incidencias de este tipo.[26], [27]

El fácil acceso al mercado ilegal de tecnología permite que sea difícil el rastreo de estas actividades de tipo ilícito, usando la “Dark Net” o por medio de criptomonedas generando un panorama inseguro y débil para la persecución penal. En Colombia existen 8 aspectos comunes que caracterizan un delito informático que son:

1. El cambio de realizar ataques al ciudadano común a empresas del sector tanto público como privado, donde estadísticas indican que 2014 al 2016 las denuncias atendidas fueron de 92% disminuyendo al 35%, en cambio el sector de las pymes ha incrementado desde 5 al 28% en los mismos reportes atendidos, estas cifras fueron tomadas del documento “IOCTA 2016 (Internet Organised Crime Threat Assesment) del Europeran Law Enforcement Agency de Europol”.

2. La creación de plataformas de phishing donde el ciudadano es quien más reporta este incidente, aun siendo plataformas reconocidas como MercadoLibre, OLX, entre otras.

3. El uso de servicios de correo como vector de ataque para distribuir software malicioso o extraer información los cibercriminales encontraron plataformas estratégicas que servían para distribuir sus ataques algunos llegaron a usar correo falso de la Fiscalía General de la Nación, Dian, Simit, Avianca para atraer la atención de los usuarios a atacar, este incidente creció 114,4% en el país, en los últimos años.[28]

[26] CCIT, El Centro Cibernético de la Policía Nacional y la CCIT presentaron el Primer Informe sobre el Cibercrimen en Colombia. [EN LINEA], Cámara Colombiana de Informática y Telecomunicaciones. Marzo, 31, 2017., p,1 Tomado de: http://www.ccit.org.co/noticias/centro-cibernetico-la-policia-nacional-la-ccit-presentaron-primer-informe-cibercrimen-colombia/

[27] 13CCIT. Óp. Cit., p.1. http://www.ccit.org.co/noticias/centro-cibernetico-la-policia-nacional-la-ccit-presentaron-primer-informe-cibercrimen-colombia/

[28]SEMANA, Mitos y realidades. [EN LINEA], Cámara Colombiana de Informática y Telecomunicaciones.
Marzo, 10, 2001., p,1 Tomado de: https://www.semana.com/tecnologia/articulo/correos-falsos-de-la-fiscalia/48943

Las APT´S (Amenazas Persistentes Avanzadas) donde el delincuente informático emplea diferentes técnicas como el uso de malware, insiders o ingeniería social para explotar los fallos o vulnerabilidades en los sistemas, se recibieron 48 denuncias de este tipo de incidentes en el 2015 y 286 en el 2016, así mismo el ransomware en el año 2017 tuvo un incremento del 500% comparado con el 2016 y 2015 donde han reportado 86 denuncias siendo otras de las principales tendencias del cibercrimen.

4. BEC es una estafa cuyo fin está destinada a las pymes o quienes trabajan con proveedores locales o extranjeros, en el cual el tipo de pago es a través de transferencias bancarias que suplantan o redirigen a través de ingeniería social lo cual implica cuentas de correo electrónico de negocios.[29]

5. En cajeros automáticos ATM el delincuente a través de skimmers realiza copia magnética correspondiente a una tarjeta y recopila la información de las cuentas habientes cuyo fin es desocupar las cuentas bancarias.

6. Deep Web es el internet que no ha sido indexado por ningún buscador, por lo cual la única forma de llegar a este tipo información es con dirección exacta, y con configuraciones especiales sean proxys, red tor, freenet, red I2P, extensiones en navegadores comunes y recomendable uso de vpn actualmente hay 30 mil sitios activos, permitiendo que los ciberdelincuentes puedan realizar cualquier tipo acciones ilícitas.

7. EL uso del internet donde MINTIC arrojo una cifra de más 13 millones de usuarios inscritos para uso de la red, el ciberdelincuente realiza mal uso del internet logrando realizar delitos conocido como sexting, cyberbullying, apología del delito, grooming, entre otros más.

8. Uso de criptomonedas como pago, donde ha alcanzado una variedad de más 175 tipos diferentes como el bitcoin estos activos no están regulados por ninguna entidad financiera, por lo cual su valor es inestable. Este tipo de criptomonedas se convierte una opción para los cibercriminales para cobrar el desembolso de sus víctimas sin ser registrado y evitar que las autoridades rastreen transacciones.[30], [31].

[29] LUZARDO, Ana María, EL NUEVO BLANCO DE LOS CIBERCRIMINALES EN COLOMBIA SON LAS EMPRESAS, [en línea]. En: Rev. Entre. Marzo, 31, 2017., 1 p. Referenciado de http://www.enter.co/chips-bits/seguridad/empresas-el-nuevo-blanco-de-los-cibercriminales-en-colombia/

[30]MENDOZA, Miguel, ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia, En: welivesecurity [En línea], junio, 2016., Tomado de: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/ /

[31] MENDOZA, Óp. Cit., p.1.

En la tabla 1 se muestra un análisis comparativo de 15.565 denuncias recibidas entre el año 2014 y 2017 mediante el centro cibernético Policial donde se caracteriza individualmente los sectores predilectos o más frecuentes en denunciar estos incidentes como se aprecia el ciudadano promedio es aún el más afectado a pesar de su considerable reducción de denuncias esto no quiere decir que sea el más beneficioso para los delincuentes ya que un mayor volumen de ataques a objetivos con menor nivel de protección no siempre es beneficioso, por eso se observa en segundo y tercer lugar el sector financiero y sector industrial han venido mostrando un aumento . Este análisis respecto a los años y objetivos pone en contexto la cantidad de denuncias y sectores más afectados

Tabla 1 Cuadro comparativo de víctimas del cibercrimen en los últimos años

Víctimas del cibercrimen	Año 2014	Año 2015	Año 2016	Año 2017
Hacia ciudadano	92%	63%	57%	66%
Sector Financiero	5%	15%	14%	12%
Sector Industrial	3%	5%	7%	5%
Tecnología	3%	4%	2%	6%
Gobierno	3%	6%	4%	3%
Educación	3%	3%	4%	3%
Medios de comunicación	3%	2%	3%	3%
Menor de edad	3%	2%	1%	2%
Salud	3%	0%	0%	0%

Fuente :

Para contrarrestar el cibercrimen es utilizado el concepto de ciberseguridad, donde se busca proteger la información en formato digital, este concepto refiere a las técnicas o mecanismos usados para preservar la información que se encuentra interconectada, su propósito es el de asegurar los activos de la información a través del tratamiento de amenazas que ponen en riesgo dicha información y sus medios de transporte, almacenamiento y procesamiento en los sistemas de que participan en el tratamiento de datos.[32]

El estado tiene la capacidad de minimizar el riesgo al que están expuestos los ciudadanos y las pymes ante amenazas o incidentes de naturaleza cibernética, para ello existe el documento CONPES 3701, genera los lineamientos nacionales de la política en materia de ciberseguridad busca contrarrestar el incremento de

[32] MENDOZA, Miguel, ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia, En: welivesecurity [En línea], junio, 2016., Disponible En: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

incidencias de delitos informáticos. [33]¿Pero qué es un delito informático? Un delito informático se le conoce como una actividad ilícita que se vale de técnicas, metodologías y herramientas para sacar provecho o atentar contra el funcionamiento de los sistemas de información independiente del tipo de técnica usada. Vulnerar, atacar, eliminar, alterar o extraer información ya sea de personas o empresas constituye un delito, todas las formas de delito cibernético involucran tanto a las Tics (tecnologías de la información) como a una víctima específica

La delincuencia informática es aquella que tiene como acción realizar un acto o conducta ilegal que pueda ser categorizada como un crimen que involucre medios tecnológicos, esta va dirigida a destruir, manipular, extraer, alterar, cualquier tipo de información de un sistema informático cuya finalidad es causar un daño y beneficio propio.[34] Para ello fue necesario clasificar los tipos de delitos informáticos:

- **Fraudes cometidos mediante manipulación de computadores:** donde el ciberdelincuente manipula sistemas de información mediante conexiones de entrada como de salida y donde su finalidad es la intrusión y manipulación de los datos de cualquier modo.

- **Daños a datos computarizados:** En este tipo de delito se clasifican toda clase de virus, troyanos, gusanos, acceso no autorizado, entre otros; donde forman parte de la acción del delincuente para dañar la información del sistema víctima o de la organización.

- **Falsificaciones Informáticas:** Se suplanta o se ofrece un servicio o dato, mediante scams, dispositivos o técnicas de ingeniería social que permitan obtener provecho de los falsos servicios ofrecidos o alterados.

5.2 TIPO DE DELITOS INFORMÁTICOS

Existen diversos comportamientos que hace que una acción se convierta en algo ilícito donde depende de factores como la imaginación, conocimiento técnico, recursos del posible delincuente y las vulnerabilidades existentes en el sistema informático objetivo. Por ello hubo la necesidad de realizar una lista de tipos delitos informáticos con el objetivo de poder tratar de manera legal estas conductas delictivas; tales resultados han sido satisfactorios en áreas como derecho civil, comercial o de tipo laboral; pero ha sido una constante lucha aplicarla al derecho penal ya que la ley asume que aquello que no está prohibido

[33] ACURIO DEL PINO, Santiago, Delitos Informáticos: Generalidades,, [EN LINEA], Profesor de la PUCE., 326, 22p., Referenciado http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.
[34] ACURIO DEL PINO, Óp. Cit., p.22.

es permitido, de este modo se impide a ley misma aplicar sanciones o castigos en proporción a este tipo de delitos.

Los tipos de delitos son:

- **Fraude informático:** Es la utilización de medios tecnológicos con el fin de alterar, extraer o ingresar a datos privados o públicos sin autorización, buscando beneficio económico, político, militar, académico etc. Mediante cualquier técnica disponible.

- **Sabotaje informático:** El ciberdelincuente altera o manipula sin autorización sistemas de información con la intención de interrumpir el comportamiento normal del sistema atacado.

- **Espionaje informático y hurto de software:** La exposición o divulgación no autorizada de información confidencial, es considerado como un espionaje industrial, para ello es importante el pilar de la confidencialidad el cual lleva el uso del concepto de criptografía, el hurto de software es apropiarse de códigos fuentes o de activación mediante cualquier medio sea físico o digital de forma ilegal.

- **Robo de servicios:** Refiere al empleo de técnicas que se aprovechan de fallos o malas configuraciones donde se accede a módulos o servicios privilegiados también pueden valerse de su perfil o posición dentro de una organización y manipular o extraer datos que cambien las características de servicios específicos.

- **Acceso no autorizado a servicios informáticos:** las Puertas Falsas TRAP DOORS es ingresar obstáculos en la lógica del software cuyo fin es indagar que procesos existen, si los alcances intermedios son correctos, ejecutar salidas de control con el mismo objetivo de obtener la información deseada, para luego analizarla[35]

Estos son otros tipos de técnicas y ataques más usados en la actualidad por los cibercriminales:

- Ingeniería social.
- Cracking.
- Phreaking.
- Ransomware.
- MITM (Man in the middle).
- Phishing.
- Ataque Ddos.

[35] ACURIO DEL PINO, Santiago, Delitos Informáticos: Generalidades,, [EN LINEA], Profesor de la PUCE., 326, 22p., Referenciado http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

5.3 LOS DELITOS MÁS COMUNES EN COLOMBIA SON

Actualmente el cibercrimen en Colombia va creciendo de manera exponencial ya que la tecnología actual permite que se creen nuevas formas de cometer delitos tecnológicos, la más usual es método phishing y algunos de los más comunes son:

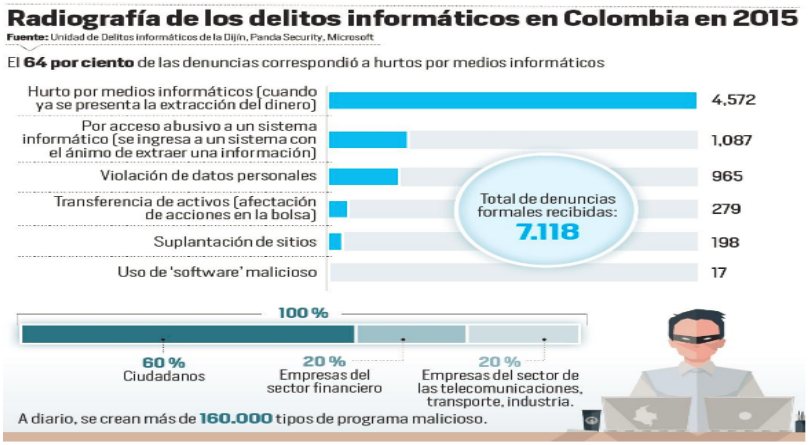
- Transferencia de activos.
- Suplantación de sitios.
- Software malicioso.
- Violación de datos.
- Acceso no autorizado (extracción de información).[36]
- Ciber acoso
- Pornografía infantil
- Ciber inducción al daño físico
- Suplantación de identidad financiera[37]

En la figura 1 se muestra un análisis de los delitos informáticos que más tuvieron denuncias en Colombia durante el 2015 se formalizaron 7.118 denuncias por delitos informáticos más de 40 por ciento más que en 2014 de los cuales el 15% referente a acceso abusivo a sistemas informáticos, el 13.5% violación de datos personales,3,9 % manipulación indebida de activos para beneficio del delincuente, 2,7% correspondiente a phishing y el 0,2% corresponde creación de software malicioso, la siguiente figura representa dichos porcentajes respecto a número de denuncias.

[36] Redacción Tecnosfera, 27 de enero 2016, En 2015, cibercrimen generó pérdidas por US$ 600 millones en Colombia Disponible [EN LINEA:] http://www.eltiempo.com/archivo/documento/CMS-16493604

[37]Pamela López, 15 de febrero de 2018, Colombia se rajó por falta de civismo y fraude en la red Disponible [EN LINEA:] https://www.publimetro.co/co/bogota/2018/02/15/delitos-informaticos-que-mas-se-cometen-en-colombia.html

Figura 1 Delitos en Colombia 2015



Fuente: http://www.eltiempo.com/archivo/documento/CMS-16493604

También es importante dar una definición de que es Seguridad de la Información para entender con claridad cómo funciona y que tan importante es actualmente en una organización. La seguridad de la información requiere de mejoras preventivas y correctivas en las empresas y tecnologías que permitan garantizar y proteger la información sobre los pilares de seguridad CIDA. La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas,[38] análisis de riesgos, la integridad, confidencialidad, recuperación y análisis de los riesgos. En la segunda guerra mundial la seguridad de la información fue evolucionando y empezando a tomar interés en ser una carrera con demanda. Existen muchas ramas en el campo de la seguridad de la información aquellas donde se incluye, auditorías, planificación de continuidad del negocio, normatividad, políticas de seguridad, matrices de riesgo, metodologías y demás componentes que infieren en la seguridad de la información, su acceso tiene posibilidades estratégicas en una compañía como pueden ser, tener restricción a ciertos privilegios de información dependiendo de su contenido, ésta se clasifica como:

•Crítica: El negocio no podría continuar
•Valiosa: Activo de la empresa y muy valioso.
•Sensible: Se debe concienciar y capacitar a las personas autorizadas de manejar la información[39]

Según un estudio realizado por la empresa ESET Smart Security en el año 2011 se entrevistaron más de 3200 profesionales de seguridad en diferentes organizaciones donde mostraron más preocupación en la perdida de datos y fuga de información con un 42.52%, en segundo lugar, el malware con 35.36% en

[38] OCCIDENTE Los servicios de seguridad Informática brindan una opción al alcance de las necesidades de cada empresa, [en Línea], mes del incidente., Tomado de: http://mesdeoccidente.com/service/seguridad-informatica/
[39]OCCIDENTE, Óp. Cit., p.1.

tercer lugar el fraude y estafas con 29.35% y muy cerca están las vulnerabilidades de sistemas operativos y software como se aprecia en la figura 2.

Figura 2 Principales preocupaciones en ámbitos de seguridad de la información. (diciembre 2011)

Fuente:

En la seguridad de la información se quiere garantizar que haya un uso correcto y gestión de la información, esto se establece con un término conocido como CID (CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD), sin estos tres pilares no es posible garantizar que la gestión de la información sea segura y es probable enfrentar un incidente de seguridad de la información de forma considerable. La norma ISO 7498 define la seguridad como un "mecanismo que minimiza los riesgos de bienes y recursos de una organización" así mismo se puede articular con la propuesta que define la seguridad informática, Glosary INFOSEC: Seguridad informática son las medidas y controles que aseguran la confidencialidad, Integridad y disponibilidad de los activos de información incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican" Hay premisas importantes, como por ejemplo; no todos los sistemas son seguros independiente de los recursos empleados para proteger la información siempre van a haber factores de riesgo dentro de la operación y manipulación de información.[40],[41]

Para estos fines la seguridad de la información se ocupará de crear y diseñar normas o métodos destinados a que un sistema de información sea seguro y confiable para afrontar diferentes amenazas, para un sistema de gestión de

[40]GOMEZ VIEITES, Álvaro, SUAREZ REY, Carlos, SISTEMAS DE INFORMACIÓN. HERRAMIENTAS PRÁCTICAS PARA LA GESTIÓN EMPRESARIAL. 4ª EDICION AMPLIADA Y ACTUALIZADA [en línea], ED RA-MA , 2011., p,370.,Tomado de: http://www.ra-ma.es/libros/SISTEMAS-DE-INFORMACION-HERRAMIENTAS-PRACTICAS-PARA-LA-GESTION-EMPRESARIAL-4-EDICION-AMPLIADA/66891/978-84-9964-122-5

[41] GOMEZ VIEITES, SUAREZ REY, Óp. Cit., p.39

seguridad de la información es necesario conocer cuáles son los elementos que componen e interactúan con la información para ello se realiza la recolección de información con los responsables de la organización, en esta actividad es posible medir riesgos y clasificarlos según su caso bajo la metodología que permita abordar los factores críticos que se abordaran en orden jerárquico, estas medidas también son importantes y estos elementos se usan normalmente para medir, prevenir, reducir o controlar potenciales riesgos y así poder llegar a tomar decisiones sobre cómo afrontar los riesgos y en qué medida tendrán impacto las vulnerabilidades encontradas.

Como se mencionó anteriormente la información puede verse comprometida de muchas maneras es por eso por lo que la seguridad informática y la seguridad de la información convergen en pro de su protección velando con sus tres pilares que son:

- Integridad
- Confidencialidad
- Disponibilidad

Para que haya una sinergia correcta en el manejo de la información y datos deben coexistir los tres pilares mencionados, con la importancia de cada uno por igual.

5.4 DELITOS INFORMÁTICOS EN LA LEGISLACIÓN COLOMBIANA

En el marco legal de Colombia las leyes que rigen el tratamiento de información personal y de las organizaciones que usen datos eh información son respectivamente las leyes: Ley 527 de 1999, Ley 1266 de 2008, Ley 1273 de 2009, Ley 1621 de 2013 Ley 1581 de 2012, Ley 1712 de 2014 entre otros varios decretos y circulares, son los mecanismos gubernamentales que velan por el correcto tratamiento y manejo de datos, distribución, procedimientos, mecanismos, técnicas y factores externos que involucren la información y sus cadenas de suministro en Colombia.

La Ley 1273 del 2009

“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

tecnologías de la información y las comunicaciones, entre otras disposiciones.[42],[43]

El constante avance de la tecnología es proporcional a la ciberdelincuencia a nivel mundial, en Colombia este permanente cambio también hace que existan grandes brechas en el sector público y privado pero las pymes son las más afectadas debido a sus recursos o desconocimiento de la importancia del tema de seguridad informática, esta situación de desventaja económica, tecnológica y de conocimientos crea el escenario propicio para un posible ataque informático o perdida de datos.

Este escenario referente al crecimiento tecnológico en Colombia ha hecho que las leyes se adapten a estos entornos tecnológicos como el cibercrimen como lo demuestra la última década con leyes como: Ley1341 de 2009, Ley 1581 de 2012, Ley 1621 de 2013, Ley 1712 de 2014, además de decretos circulares y requisitos para empresas y proveedores que se vuelven más exigentes en materia de manejo de información como la circular 007 de la superintendencia financiera.

En la actualidad ante la mejora de modalidades en los delitos cibernéticos y permanente cambio es objetivo plantear la duda si en realidad la ley actual está cumpliendo con su objetivo inicial o si por el contrario se debe realizar nuevas leyes o replantear términos y que se ajusten con la situación actual y la era de inteligencia artificial que se aproxima.[44]

En el siguiente artículo encontramos los siguientes tipos de delitos informáticos que abarca la ley 1273.

- Artículo 269ª: Acceso abusivo a un sistema informático, acceso informático de manera no autorizada por el delincuente.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicaciones.
- Artículo 269C: Interceptación de datos informáticos, interceptación en el transporte de datos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva:

CAPITULO. II

[42] Alcaldía de Bogotá, Ley 1273 de 2009 Nivel Nacional [EN LINEA], enero, 5, 2009., 1p., Tomado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
[43] Alcaldía Bogotá, Op .cit.,p 1 http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
[44]Alcaldía Bogotá, Op .cit.,p 1 http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

- Artículo 269I Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos.

5.5¿QUÉ PAÍSES LIDERAN LA LUCHA CONTRA EL CIBERCRIMEN EN LATINOAMÉRICA?

En Latinoamérica un estudio por ICG (Ciberseguridad Global) 2017, reveló que el primer país en tener más compromiso a nivel de ciberseguridad es México, gracias a las herramientas usadas para mitigar el impacto de las amenazas actuales cibernéticas, con un porcentaje de 0.66%, el cual lo ubica en Latinoamérica en lugar 28 a nivel de otros países del mundo como Bélgica que tiene un 0.671% y para el resto de la Organización OCDE que contiene una calificación de 0.65%.

Otros países en Latinoamérica como se muestra en la tabla 2 también se encuentran dentro del top 5 de los 5 mejores de la región de Latinoamérica se encuentra Uruguay en el 29, Brasil en el 38, Colombia en el 46 y finalmente Panamá en el 61. Algunos países no se encuentran en top de las 5 mejores, pero empiezan a ganar puestos en este ranking como lo son Chile con el80, Perú con el 78, Argentina con el 62.[45]

Tabla 2 Raking latinoamericano en ciberseguridad

Región de Latinoamérica		
País	PUNTAJE	RANKIGN GLOBAL
México	0.660	28
Uruguay	0.647	29
Brasil	0.593	38
Colombia	0.569	46
Panamá	0.485	61
Argentina	0.482	62
Ecuador	.0.466	65
Perú	0.374	78
Venezuela	0.372	79

Fuente: Nuestra Diseño basado y Referenciado de:

[45] AETecno QUÉ PAÍSES LIDERAN LA LUCHA CONTRA EL CIBERCRIMEN EN LATINOAMÉRICA?[en linea], Agosto,9 de 2017., 1p.,https://tecno.americaeconomia.com/articulos/que-paises-lideran-la-lucha-contra-el-cibercrimen-en-latinoamerica

6. TÉCNICAS MÁS USADAS POR CIBERDELICUENTES EN LAS PYMES COLOMBIANAS

Las amenazas cibernéticas se convierten en una importante preocupación de seguridad en Colombia. Los incidentes van desde motivación política hasta intervenciones ilegales a medios y dispositivos electrónicos, los motivos financieros también se han vuelto clave a medida que el crecimiento tecnológico se convierte en la piedra angular de muchas empresas emergentes o las que adoptan la transformación digital como medio de competencia dentro del mercado actual. Según un estudio de seguridad de Intel, el 15% de los delitos contra empresas en Colombia están asociados con el delito cibernético, generando pérdidas de aproximadamente US $ 600 millones al año.[46]

Los retos contra el cibercrimen en Colombia se convierten en uno de los principales desafíos para el sector privado y público, por ejemplo, durante el primer semestre de 2011, el autodenominado grupo hacktivista Anonymous atacó los portales de la Presidencia de la República, el Senado, el Gobierno en línea y los ministerios de Interior, Justicia, Cultura y Defensa. El ataque fue llevado a cabo para protestar contra un proyecto de ley presentado en abril de 2011 por el entonces ministro del Interior y Justicia, Germán Vargas Lleras, que buscaba regular "la responsabilidad por violaciones del derecho de autor y los derechos de Internet relacionados."[47]

En la región de Latinoamérica el perfeccionamiento de técnicas y perfilamiento de objetivos ha sido clave en el incremento de incidentes de tipo digital, Colombia en 2013 se clasifico como el peor país de América Latina y el octavo del mundo por técnicas como phishing y spear phishing según un informe del servicio de seguridad de EMC Corporation.[48]

Estas razones como el crecimiento y perfeccionamiento de técnicas en el cibercrimen hacen necesaria la inversión en infraestructura y profesionales de la seguridad convirtiéndose en una demanda constante en el presente y futuro de las pymes que buscan familiarizarse con el mercado digital que es cada día más competitivo y proporcional a los riesgos que representa. El desarrollo tecnológico en el sector industrial es considerablemente mayor frente a otras industrias como del sector textil o construcción por otro lado los sectores en los que se ha invertido

[46] PRIETO GOMEZ, Wilmer, practice manager foundstone consulting Latín América 42., Disponible en:https://sistemas.uniandes.edu.co/images/forosisis/foros/fsi2016/Intel_SeguridadDigital_Ciudadania_.pdf

[47] Anonymous ataca a Juan Manuel Santos y Álvaro Uribe, [En línea]. En: Revista El Mundo. noviembre, 20, 2017., 1 p. Disponible en http://www.elmundo.es/america/2011/07/20/colombia/1311194120.html

[48] 2013 a YEAR IN REVIEW [EN LINEA], RSA, 2017.,4p. Disponible en: https://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf

más en tecnología son la minería, la electricidad, el petróleo, el gas, y sectores de alimentos y bebidas.[49]

Por esta razón la inversión en infraestructura y profesionales de la seguridad se convierte en una demanda constante en el presente y futuro de las pymes que buscan familiarizarse con el mercado digital que es cada día más competitivo y proporcional a los riesgos que representa.

6.1 LAS PRINCIPALES TÉCNICAS EMPLEADAS POR LOS CIBERDELINCUENTES EN COLOMBIA.

Las técnicas del cibercrimen en Colombia no son muy diferentes a las empleadas nivel mundial sin embargo las técnicas más comunes empleadas para afectar las pymes o start-up parten de las mismas vulnerabilidades a las que se encuentran expuestas.

- Vishing (estafa por llamada telefónica): Este tipo de ataque se ha convertido en uno de los más usados ya que por medio de la ingeniería social y con voces automatizadas que simulan entidades financieras buscan obtener suficiente información que comprometa la vida financiera de las personas, las pymes también se han visto afectadas con este tipo de técnicas con llamadas de supuestos clientes o proveedores. Durante el 2017 la policía recibió 1055 casos de vishing con cifras cercanas a los $2.132.000.000.[50]

- Spears-• Spears-Phishing (Estafa por correo electrónico): Esta dirigida a personas específicas de compañías diferencia del phishing tradicional este está más elaborado y requiere de ingeniería social para mejor desarrollo de este. Colombia en el 2018 aumento su indicador respecto al año anterior y se ubica detrás de México en la región.

- Fraude por WhatsApp falso (Ingeniería social): Los delincuentes se hacen pasar por tiendas virtuales y simulan chats con ofertas buscando comprometer la información u obtener pago por productos que no envían. Las autoridades reciben entre 3 y 5 denuncias diarias por este delito.

- BEC (Suplantación de correo corporativo): La suplantación e intervención de correos electrónicos corporativos o personales; recopila información para construir un ataque que puede ir desde fraude a gerentes, fraudes de facturas,

[49] Industrias colombianas podrían ser blanco de ciberataques [En línea]. En: Periódico Espectador. Abril, 9, 2014., 1 p. Disponible en https://www.elespectador.com/noticias/economia/industrias-colombianas-podrian-ser-blanco-de-ciberataqu-articulo-486877

[50] informe_cibercrimen_2017, diciembre, 2017,12p. Disponible en https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

robo de datos y escalamiento de ataques a posibles clientes de la compañía o empleados de la misma.

- Fuga de información: La fuga de información en las compañías también representa uno de los mayores factores de lucro para los delincuentes; que al valerse de ingeniería social o comprometer usuarios y contraseñas para acceder a bases de datos, sistemas de información o archivos confidenciales de compañías, para la posterior venta de estas bases de datos y así poder adelantar o preparar mejores ataques con esta información obtenida.[51]

6.2 IMPACTO DE LOS INCIDENTES, AMENAZAS Y ATAQUES CIBERNÉTICOS EN COLOMBIA.

6.2.1 ANÁLISIS DEL CIBERCRIMEN EN COLOMBIA

En Colombia las principales ciudades con mayor número de reportes de incidentes informáticos son: Bogotá 9709, Medellín 691, Cali 475, Barranquilla 240 y Bucaramanga 12930, las principales ciudades con mayores denuncias por Ley 1273 son: Bogotá 2607, Cali 1607, Medellín 998, Bucaramanga 594, Ibagué 448 y Barranquilla 398. Lo anterior, debido a que en estas ciudades se encuentra más del 75% de suscriptores de internet fijo dedicado y por índice de habitantes por ciudad en el país[52] Colombia en el 2017 registró un total de 1.200.000 delitos con un mayor impacto de los ciberdelitos, según los estudios de la empresa de seguridad informática Digiware en 2017 Colombia participó con el 8,05% del total de los delitos informáticos de América Latina, lo que equivale a pérdidas más de US$6.179 millones, de acuerdo a estas cifras Colombia es quinto en la clasificación latinoamericana en materia de ataques informáticos.[53]

En el sector empresarial en Colombia los sectores más afectados de acuerdo con estas cifras se producen en promedio 542.465 ataques informáticos al día. Así se distribuyen los ataques por sectores económicos:

[51]GOMEZ MONTES, Julián, ¿Es un buen negocio comprar bases de datos?, Revista LR la republica [en línea], Julio,205, 2016., 1 p. Tomado de https://www.larepublica.co/alta-gerencia/es-un-buen-negocio-comprar-bases-de-datos-2391421

[52] Colombia en el 2017 registró un total de 1.200.000 delitos con un mayor impacto de los ciberdelitos, según los estudios de la empresa de seguridad informática Digiware en 2017 Colombia participó con el 8,05% del total de los delitos informáticos de América Latina, lo que equivale a pérdidas más de US$6.179 millones, de acuerdo a estas cifras Colombia es quinto en la clasificación latinoamericana en materia de ataques informáticos

[53]Los sectores económicos más impactados por el cibercrimen en Colombia, [En línea]. En: Periódico Dinero. Septiembre, 26, 2017., 1 p. Disponible en https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

- El sector financiero: 214.600 ataques por día (39,56%).
- Telecomunicaciones: 138.329 ataques por día (25,5%).
- El sector Gobierno: 83.756 ataques por día (15,44%)
- Sector energético: 19.583 ataques por día (3,61%)
- Industria: 51.263 ataques por día (9,45%).
- Retail: 34.934 (6,44%

Los sectores más afectados por ciberataques en Colombia son el financiero, con 214.000 ataques por día (39,6%) y el de telecomunicaciones, con 138.329 ataques por día (25,50%) adicional a esto también una investigación aplicada a más de 500 empresas que operan en el país y según el cual el 80% de los fraudes en las organizaciones es perpetrado por los mismos empleados.

El impacto financiero de esta serie de hechos delictivos es alto. Según el análisis de la policía nacional, el 45% de las empresas en Colombia logró cuantificar el monto defraudado en un valor de hasta US$10.000. Otro 20%, tuvo pérdidas entre los US$10.000 y los US$50.000, mientras que un 23% reportó un detrimento superior a los US$50.000 y con un tope de hasta US$500.000.

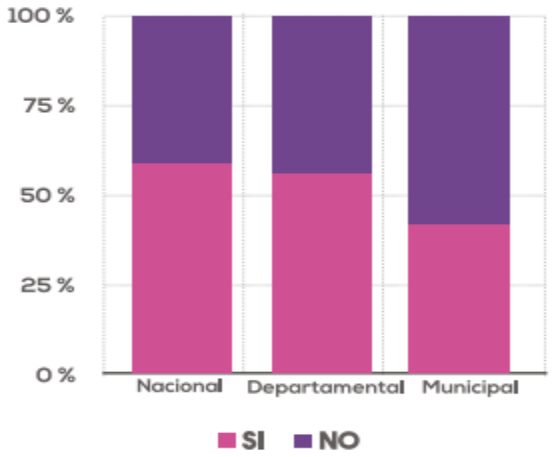
- **Los más vulnerables**

Las áreas internas de las empresas que son más vulnerables a los delitos son: operaciones y producción, ventas y atención al cliente, alta gerencia, tesorería, compras y bodega. Por su parte, cuando se analiza la naturaleza de quién comete el ilícito, se encuentra que en el 25% de las situaciones es un colaborador interno de la empresa, complicidad entre empleados (18%), supervisor (9%), alianzas entre colaborador y proveedor (7%) y alguien de la alta gerencia (7%). En tanto, al revisar el promedio de antigüedad de las personas que cometen estos delitos, el 38% llevaba entre tres y cinco años, seguido por quienes llevaban más de 10 años (16%).[54]

Durante el año 2016 como se aprecia en la figura 3 hubo un porcentaje similar en cuanto a denuncias en el área nacional y departamental mientras que en los municipios se observa un menor índice de denuncias; esto corresponde al impacto de los incidentes presentados ya que no se denuncia una fuga de información con la misma severidad de un sabotaje a la infraestructura en un municipio.

Figura 3 Entidades del gobierno que identificaron incidentes digitales en el 2016

[54]Top 10 de los fraudes y la corrupción contra las empresas en Colombia, [En línea]. En: Periódico Dinero. Agosto, 31, 2018., 1 p. Disponible en https://www.dinero.com/empresas/articulo/estudio-de-kpmg-encuesta-sobre-fraude-en-colombia-2017/261575



Fuente: https://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

6.2.2 PRINCIPALES TÉCNICAS QUE AFECTA LAS PYMES COLOMBIANAS

La mayor y más frecuente técnica utilizada contra las empresas en Colombia sigue siendo el Business Email Compromise Attacks (BEC). Los reportes de ataques cibernéticos en el sector empresarial crecieron del 5 al 28% del total de delitos denunciados, a diferencia que en ciudadanos particulares descendió de 57 a 35%, de igual manera la suplantación de identidad (Phishing) y la infiltración de programas informáticos maliciosos (Malware) son sólo algunos de los incidentes que afectan a los 13 millones de suscriptores de internet registrados en Colombia[55]

Un ejemplo de un ataque de esta modalidad es suplantando el correo de un alto ejecutivo o de un comprador encargado en una empresa ya sea bajo técnicas de Spoofing, phishing, robo de contraseñas, envenenamiento de redes con metasploit o ingeniería social; cualquiera de estas técnicas se usan para obtener, cambiar o usurpar una cuenta de correo de alguien encargado de realizar pedidos, recibir facturación, procesar cuentas de cobro o cualquier tipo de actividad que realice la victima que acaba siendo afectada con consecuencias económicas y de reputación considerables.

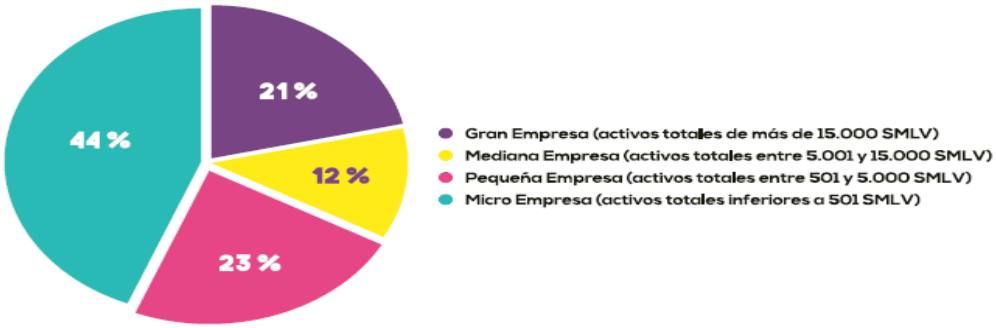
6.3 ANÁLISIS EN SECTOR PRIVADO

[55]Aumenta número de empresas víctimas de delitos cibernéticos en Colombia, [En línea]. En: Periódico Semana. marzo, 3, 2017., 1 p. Disponible en https://www.semana.com/nacion/articulo/presentan-informe-sobre-el-cibercrimen-en-colombia/520236

6.3.1 PERFIL DE LAS EMPRESAS

Según encuesta realizadas en el sector privado el 44% de las empresas, indican que solo el 23% pertenece al sector de las pymes, el 12% y el 21% están en el sector de empresas medianas y grandes, el 84% pertenece al sector privado y el 16% es del sector mixto y público según se aprecia en la figura 4.

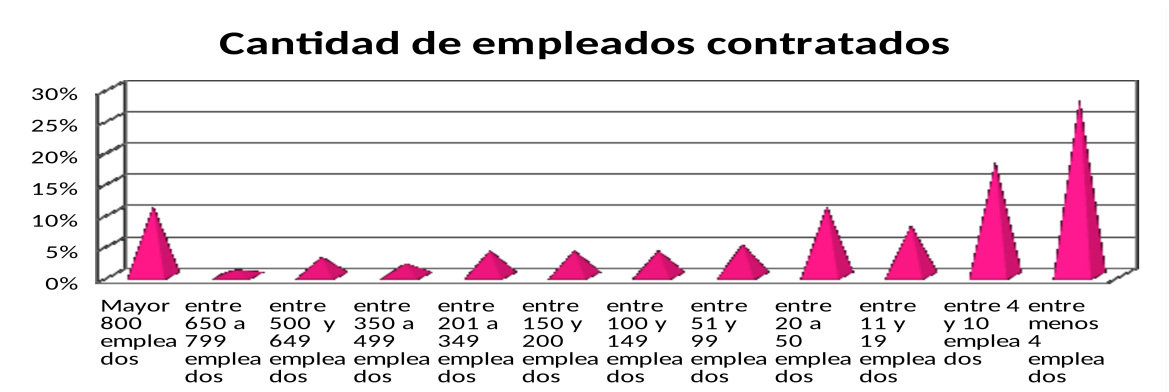
Figura 4 Perfil de empresas sector privado



Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

A nivel de empleados contratados la encuesta arroja que el 28% de las empresas tiene menos de 4 empleados contratados, 60, menos de 800 empleados, y cerca de un 11% tiene superior a 800 como se muestra en la figura 5

Figura 5 Cantidad de empleados en las empresas colombiana



Fuente:

También según la encuesta se observa el porcentaje de personas que tiene acceso a internet de la compañía, como se observa en la figura 6, gran parte de los empelados tiene acceso a medios informáticos y a internet para el ejercicio de sus funciones.

Figura 6 Cantidad de empleados que tiene acceso a internet en su empresa

Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

Ya teniendo claro el sector privado como está conformado y que tanto acceso tienen a una red se plantea el cuestionamiento, ¿qué porcentaje de incidentes digitales se ha identificado en las empresas durante los últimos años?

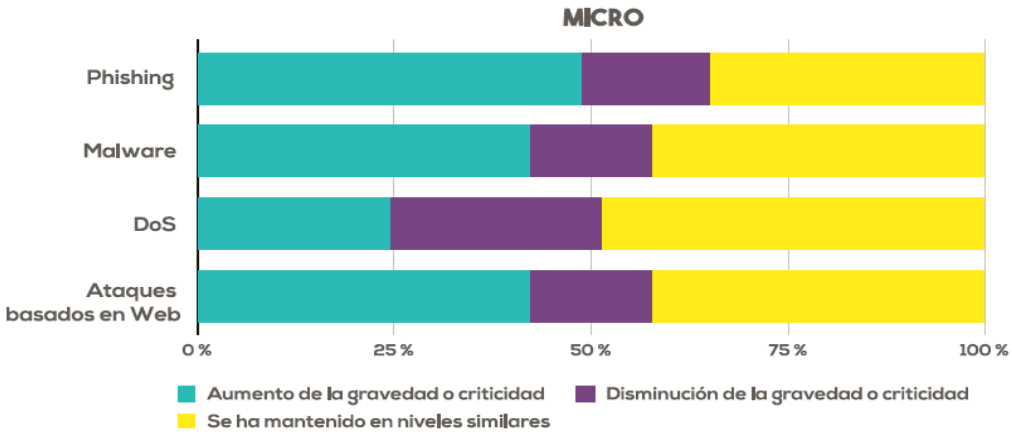
6.3.2 INCIDENTES DIGITALES EN LAS EMPRESAS

Según el estudio de impacto de los incidentes digitales en Colombia realizado por el ministerio de las telecomunicaciones el 70 % de las micro pymes no han identificado un incidente digital como tampoco el 60% de las empresas pequeñas, en cambio en la empresa catalogadas como medias y grandes esta entre 51% y 63% quien indica que si se ha presentado un incidente digital.

El malware y phishing son los incidentes más usuales, se evidencia que el 50% de quienes participaron en la encuesta del ministerio de telecomunicaciones de donde sacaron estas estadísticas notaron un aumento en este tipo de incidentes.[56] En las microempresas se ubica el malware con 47 % de tipo phishing 49% y el 39% de ataques de tipo web y 18% en DoS, como se muestra en la figura 7.

Figura 7 Microempresa

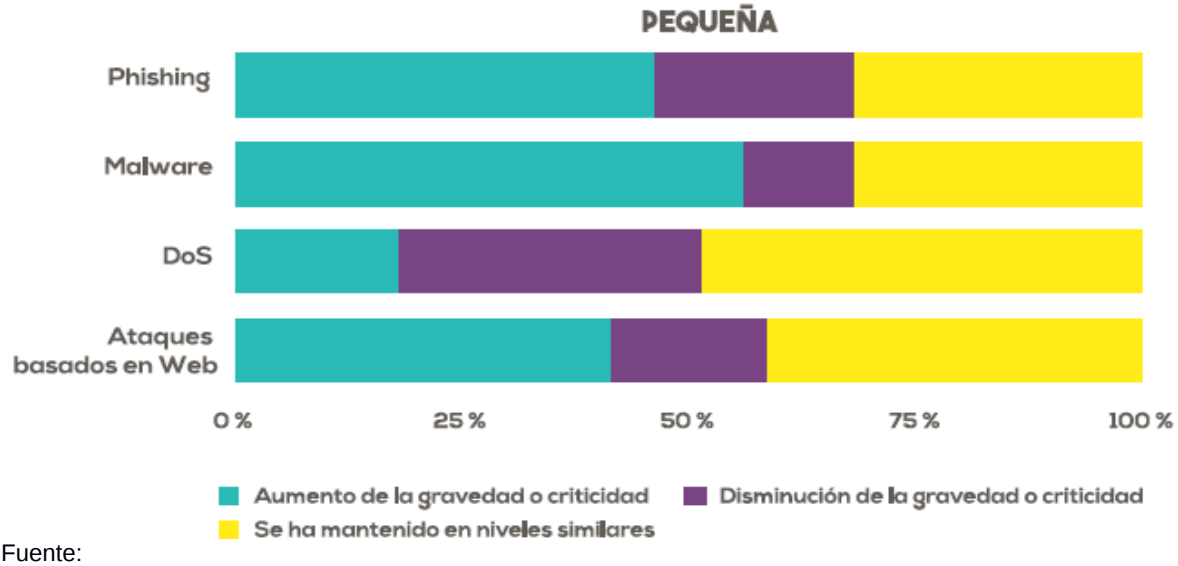
[56] Impactos de los incidentes de la seguridad Digital, [en línea]MINTIC, OEA, 2017, Disponible en https://publications.iadb.org/handle/11319/8552?locale-attribute=es



Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

En otro tipo de empresas como las de sector comercial se evidencio que el 53% reportaron en incidentes de malware y el 41% en phishing y 37% en ataques de tipo web como se muestra en la figura 8, permaneciendo el malware en primer lugar en el sector comercial.

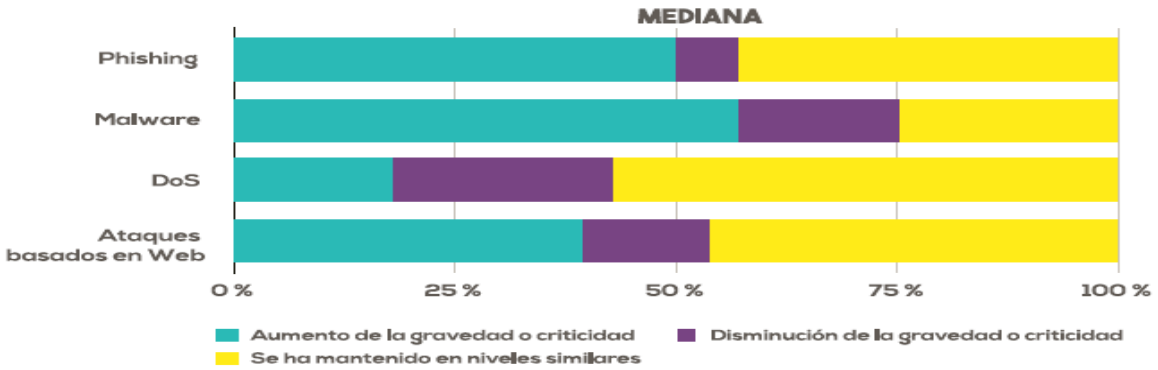
Figura 8 Pequeña empresa



Fuente:

En el sector industrial el porcentaje es más notable ya que el 67% es basado en ataques de tipo malware y el 59% en ataque phishing como se relaciona en la figura 9, es considerablemente más alta la afectación al sector industrial en Colombia por el malware.

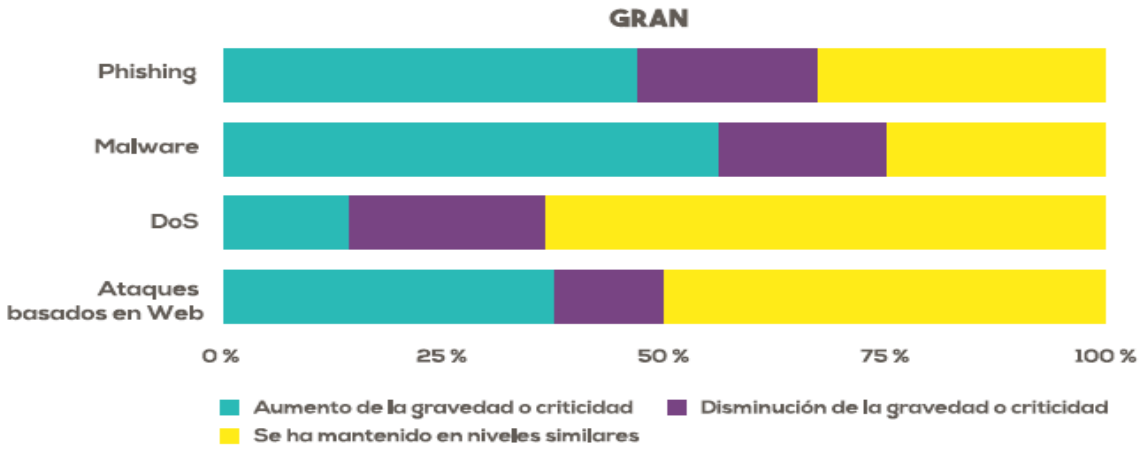
Figura 9 Mediana empresa



Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

Finalmente, en las grandes empresas la tendencia no difiere notablemente ya que el malware sigue en primer lugar con más del 67 % y el phishing con 50% y la tendencia en ataques de tipo web se mantiene con cerca del 37% en relación a los demás tipos de empresas relacionados anteriormente como se aprecia en la figura 10.

Figura 10 Grande empresa



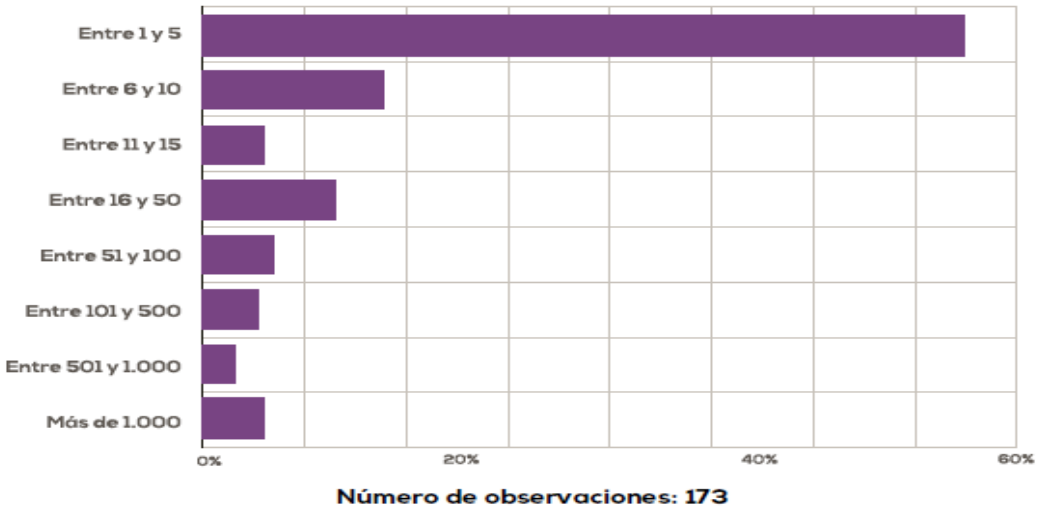
Fuente:

Ya teniendo un poco más claro el porcentaje de incidentes presentados en el sector privado y basado en el artículo de la policía CPP de Colombia, en el último año se han incrementado las denuncias cibernéticas donde se evidencia que en Colombia una de las principales técnicas es el phishing, BEC, uso de software malicioso o suplantación de sitios web para obtener información de usuarios. Por lo cual este estudio también permite ver que del 2016-2017 aumentaron estas

incidencias (phishing, malware, suplantación de sitios web) de un 5% al 20% según denuncias recibidas.

En las entrevistas realizadas a las entidades se les consulta ¿a quiénes se les notifica cuando ocurre una incidencia digital en dentro de la organización? El 87% informo que no notificó a una autoridad y el 80% que se avisó a la compañía a sus jefes. En el 2016 también el 50% de las empresas registran entre 1 a 5 incidentes y solo el 30% entre 6 y 100 incidentes. Por último y aún más importante a pesar del poco porcentaje el 5% de las organizaciones reportaron más de 1.000 y 100 mil incidentes digitales en el transcurso del año como se relaciona en la figura 11.

Figura 11 Número de incidentes digitales identificados por las empresas (2016)



Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

6.3.3 COSTOS Y PÉRDIDAS DE LOS INCIDENTES DIGITALES EN LAS EMPRESAS

Del 100% de las compañías, el 79% de las empresas no tiene un costo estimado en pérdidas como consecuencia de incidentes digitales, solo el 21% de las empresas si cuentan con este costo económico cuando ocurren incidentes digitales como se relaciona en la figura 12.

Figura 12 Costo económico

Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

Teniendo en cuenta el 21% de estas compañías se realiza un estudio de la distribución de costo con referente al tema en forma de 5 categorías.

- Interrupción operacional.
- Daños en infraestructura y activos.
- Gastos en términos legales.
- Daño de imagen empresarial.
- Perdida de información confidencial.

Estas cinco categorías se tienen en cuenta como consecuencia de un incidente, una incidencia digital puede ir desde robo de información en una compañía, interrupción laboral de actividades diarias generando pérdidas en producción y más si la empresa es prestadora de un servicio continuo, atacar la red y sus sistemas de infraestructura con el objetivo de usarla para beneficio propio del ciberdelincuente incurre en gastos legales para la compañía en compensación a clientes por ataques de malware o daño de imagen al realizar mala publicidad o perdida de datos generando una mala imagen al cliente.

Se referencian algunas estadísticas en costos empresariales según la OEA y la MINTIC con referencia a los impactos de los incidentes de seguridad digital publicado en el 2016.[57], [58]

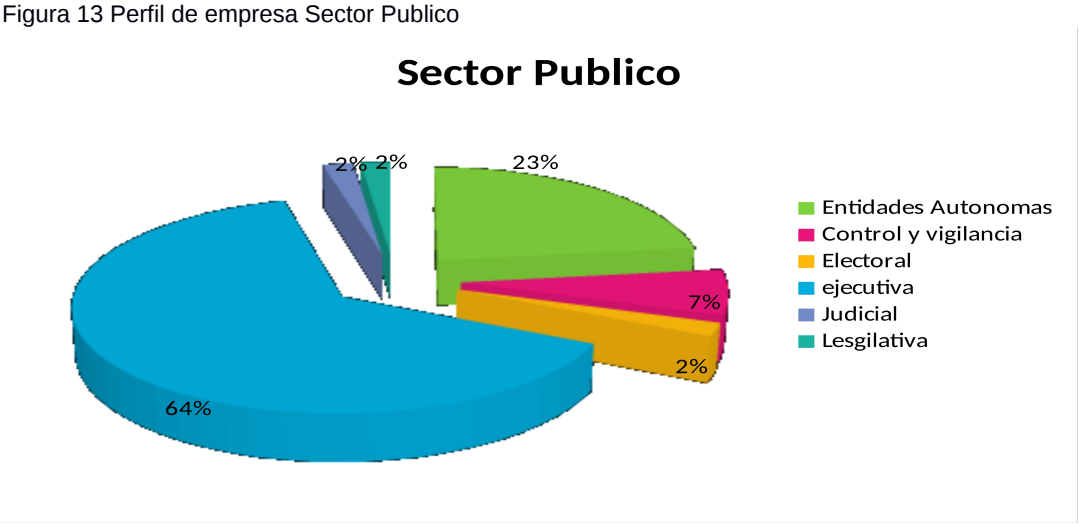
6.4 ANALISIS DE SECTOR PÚBLICO

[57] Impacto de los incidentes de seguridad digital en Colombia 2017, [en línea]MINTIC, OEA, 2017, Disponible en https://publications.iadb.org/handle/11319/8552?locale-attribute=es
[58] CCIT. Óp. Cit., p.64.

6.4.1 PERFIL DE LAS EMPRESAS

Según encuestas realizadas por Mintic en el sector público el 64% se encuentra en la rama ejecutiva, indican que solo el 23% eran tipo autónomas el 13% se dividen en diferentes organismos de control y vigilancia, rama legislativa y judicial como se aprecia en la figura 13.

Figura 13 Perfil de empresa Sector Publico



Fuente:

En esa anterior división de empresas del sector público el 52% viene del sector municipal, frente al 36% a entidades nacionales y 12% departamental mostrando predominancia el sector municipal por lo tanto entidades de orden y control como se aprecia en la figura 14.

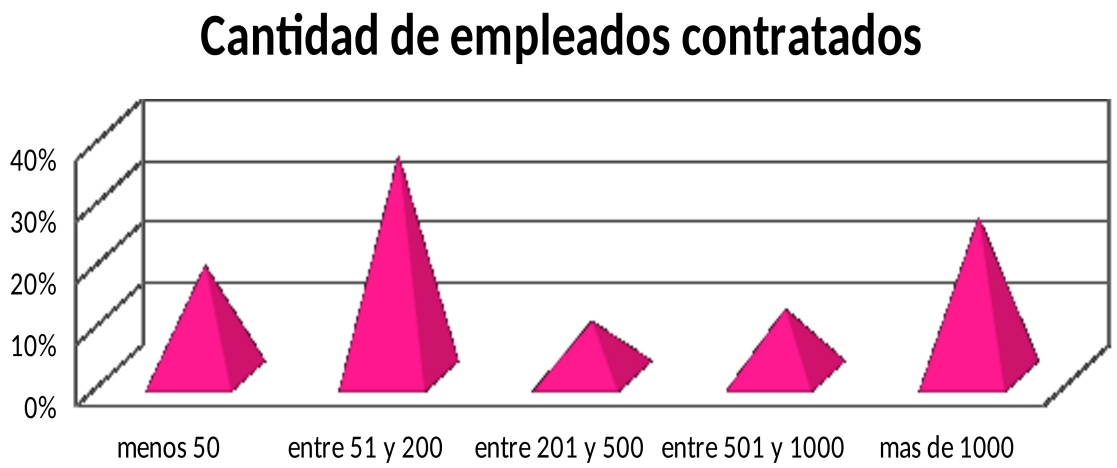
Figura 14 Ubicación de entidad

Fuente:

A nivel de empleados contratados la encuesta arroja que el 18% de las empresas tiene menos de 50 empleados contratados, 36%, menos de 200 empleados, y

cerca de un 9% tiene superior a 500 empleados, 26% más de 1000 empleados como se aprecia en la figura 15.

Figura 15 Cantidad de empleados en las empresas colombiana en sector publico



Fuente:

También según la encuesta se observa el porcentaje de personas tiene acceso a internet dentro de la compañía como se aprecia en la figura 16 la cantidad de empleados que cuenta con acceso a internet. Prevalece la conexión a internet entre los empleados.

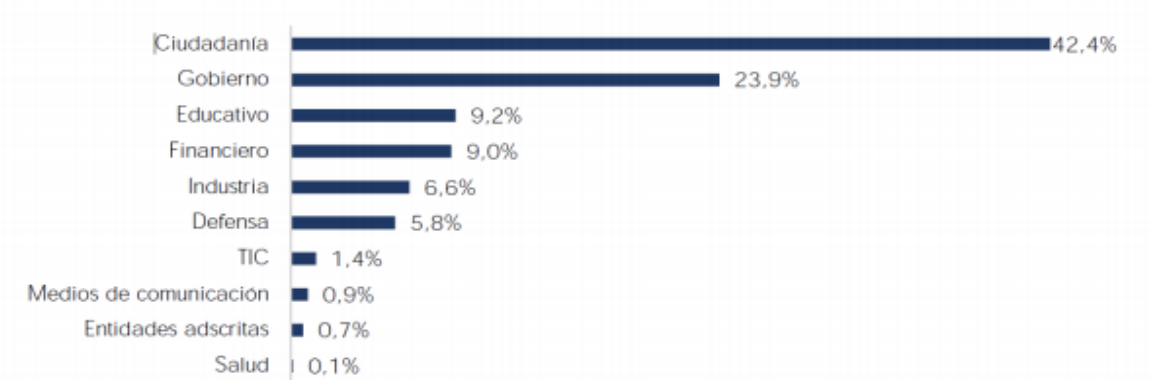
Figura 16 Cantidad de empleados que tiene acceso a internet en su empresa entidades publicas

Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

6.4.2 INCIDENTES DIGITALES EN LAS EMPRESAS SECTOR PÚBLICO

En el año 2016 se identificaron incidentes digitales en las empresas estatales, de orden nacional en un 59% y de tipo entidad departamental 56% en cuanto territorio municipal el 42% de las empresas también evidenciaron incidentes digitales. Como entidades soportadas y respaldadas por el sector gubernamental deben contar con políticas y recursos más exigentes es por eso por lo que se espera que sector público este mejor preparado sin embargo sigue siendo el segundo sector más afectado después de la ciudadanía en general como se aprecia en la figura 17.

Figura 17 Perfil de empresa Sector Publico



Fuente: https://repository.unimilitar.edu.co/bitstream/10654/15354/3/GuerraSalcedoJuanDavid2016.pdf

Con la anterior información también se aprecia la demanda de seguridad en el sector público. Se aprecia como aumenta de manera exponencial sin importar el presupuesto con el que cuente y los esfuerzos que se usan para implementar una política pública con las necesidades de ciberseguridad en el país.[59]

6.4.3 COSTO Y PÉRDIDAS DE LOS INCIDENTES DIGITALES EN LAS EMPRESAS

El costo del cibercrimen en Colombia en 2013 subió a 461.000 dólares en un año algo como 873 millones de pesos por año según el informe de Symantec con el 42% de la población como víctima de algún delito de este tipo alguna vez en su vida, tendencia que va en aumento según las amenazas a dispositivos móviles Según se aprecia en la figura 18 correspondiente a datos de Colombia.[60]

[59] Ciberdefensa y Ciberseguridad: de la política pública a las acciones concretas, [en línea], ASOBANCARIA, OCTUBRE,3,2016,.11p, Disponible en http://www.asobancaria.com/wp-content/uploads/2018/02/1062.pdf

[60]BECARES, Barbara, El coste del cibercrimen en Colombia sube a 461.000 dólares en un año, [en línea]. Octubre, 9, 2013, Disponible enhttps://www.siliconweek.com/cloud/el-coste-del-cibercrimen-en-colombia-sube-461-000-dolares-en-un-ano-47219?print=pdf

Colombia en 2016 reportó pérdidas por 5.700 millones de dólares, que significan un aumento del 4 % con respecto al 2015[61]

Figura 18 Costo del Cibercrimen

Fuente:

El 20% de las entidades del estado tuvieron pérdidas más altas respecto a daños en sus activos en 2016 no obstante el otro 80 % representan perdidas notables y de la misma cuantía representada en daños a la infraestructura como se aprecia en la figura 19 en porcentaje y costos.

Figura 19 Costo del Cibercrimen Activos e infraestructura

Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

7. IDENTIFICAR LAS MEDIDAS DE SEGURIDAD INFORMÁTICA DE LAS PYMES DE COLOMBIA FRENTE A LAS PYMES DE LATINOAMÉRICA.

[61] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, REPÚBLICA DE COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN, [en línea] CONPES3584, ABRIL,11,2016 Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Las pymes que se toman en serio la seguridad de sus activos y que no cuentan con presupuestos o infraestructuras grandes se valen de diferentes estrategias para cumplir con los estándares mínimos ya sea la implementación de un SGSI, buenas prácticas en uso de información, soluciones endpoint por suscripción, herramientas open source para gestión de la seguridad, personal capacitado para administrar estas herramientas, algunas opciones en el mercado también están disponibles para agregar una capa de abstracción que permita gestionar de una manera más organizada la infraestructura estas soluciones puedes ser IaaS, PaaS, SaaS.[62]
También se puede optar dependiendo del mercado y presupuesto por implementar normativas más exigentes como, por ejemplo:

Si bien todas las compañías no cuentan con la capacidad económica y recursos de infraestructura para implementar todos los requisitos de la Circular Externa 007 de 2018 se pueden implementar algunos de los requisitos exigidos ya sea implementación de soluciones perimetrales como firewall open source, FIM(File integrity monitor),SIEM(AlientVault) entre otras herramientas Open Source que cumplan las exigencias no solo de esta circular sino que se integren al SGSI basadas en otras normas ya sea ISO 27001 o PCI DSS. La circular 007 es evidencia de las medidas que implementa Colombia en ciberseguridad respecto a la región de Latinoamérica; esta circular se expidió teniendo en cuenta el auge de la digitalización de los servicios financieros, con la mayor interconectividad de los agentes tecnológicos que convergen en el manejo de la información llámense usuarios, redes, protocolos, sistemas La masificación en el uso de canales electrónicos entre otros mecanismos que interactúan con información financiera y complementa las normas existentes con relación a la administración de los riesgos operativos y la seguridad de la información.

A pesar de la creciente amenaza de los ataques cibernéticos y la mejora en las técnicas de ataque, la importancia que se les da a estas amenazas aún es baja entre las pymes en Colombia, de ahí la importancia que se apliquen recursos para el área de la seguridad informática[63].

Estas pequeñas y medianas empresas representan el 80% del empleo en el país, así como aportan el 35% al PIB. Datos del Ministerio de Tecnologías de la

[62] RATTIBITTINGER, Gabriela, LOZANO, Moreno; Desarrollo de una guía de controles de ciberseguridad, [en línea]MISTIC, DICIEMBRE, 2017, Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72887/8/grattibTFM0118memoria.pdf
[63]SUPERFINANCIERA FORTALECE LA PROTECCIÓN DE LA INFORMACIÓN DE LOS CONSUMIDORES FINANCIEROS ANTE RIESGOS DE CIBERSEGURIDAD Y LA REALIZACIÓN DE OPERACIONES EN PASARELAS DE PAGO CIRCULAR EXTERNA 007 DE 2018, superintendencia financiera de Colombia, junio 05, 2018., Disponible en https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00

Información y las Comunicaciones (Min Tic) revelan que las Pymes incrementaron en un 60% su adopción de tecnologías en el 2017.[64]

Algunos de los puntos más importantes que se plantean en la circular externa de 2018 de la superintendencia financiera de Colombia son: la actualización permanente en las nuevas modalidades de ciberataques, centralizar la información en una unidad que gestione los riesgos de seguridad de la información, monitorear diferentes fuentes de información como: sitios web, blogs y redes sociales, y tener mecanismos para análisis de incidentes informáticos, entre otros.

Todas las entidades vigiladas por la Superintendencia financiera deben cumplir los requisitos exigidos en está circular como lo son establecer una política de seguridad de la información, evaluación del riesgo y servicios prestados por la entidad, documentar las responsabilidades, procesos, procedimientos, etapas y la gestión que se realiza frente a la ciberseguridad, las entidades deben contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad. Sin embargo, para que Colombia tenga un entorno digital más seguro, es necesario trabajar fuertemente no solo en entidades públicas y financieras donde ha estado el máximo esfuerzo del Gobierno, sino ampliar las medidas y lineamientos a empresas privadas como las Pymes; según afirma Julio César Barreto Baena, desarrollador de negocios en Gamma Ingenieros, compañía experta en ciberseguridad.

A pesar de que Colombia tiene políticas y lineamientos de ciberseguridad y ciberdefensa, algunos países latinoamericanos cuentan con medidas mucho más avanzadas. Por ejemplo, Venezuela, que tiene un amplio espectro de ataques cibernéticos, ha desarrollado una fundamentación tecnológica robusta para su monitoreo, alerta miento y control con apoyo de Rusia.

En Colombia y en Latinoamérica los últimos años el Internet se ha utilizado cada vez más con fines delictivos. Desde 2007, Colombia ha estado construyendo una estrategia nacional para combatir el delito cibernético, centrándose en la defensa y la seguridad cibernéticas.[65]

8. LA ESTRATEGIA DE COLOMBIA SE SOPORTA SOBRE TRES PILARES

[64] ACIS, Aumenta en 30% la inversión de las Pymes en ciberseguridad Bogotá, julio, 2018, Disponible en http://acis.org.co/portal/content/NoticiaDelSector/aumenta-en-30-la-inversi%C3%B3n-de-las-pymes-en-ciberseguridad

[65] Chaves, M. ALVARO. (2016, 27 septiembre). Seguridad cibernética en Colombia https://dialogo-americas.com/es/articles/cyber-security-south-america

- Pilar 1: Adopción de un marco institucional apropiado para monitorear amenazas y prevenir ataques, coordinar respuestas y generar recomendaciones para enfrentar amenazas y riesgos en el ciberespacio.

- Pilar 2: Capacitar al personal en seguridad de la información y ampliar la investigación sobre defensa y seguridad cibernética.

- Pilar 3: Fortalecer la legislación, la cooperación internacional y avanzar en la adhesión a los instrumentos internacionales para combatir el delito cibernético.

8.2 PARA DESARROLLAR ESTAS ESTRATEGIAS, COLOMBIA DISEÑÓ E IMPLEMENTÓ CINCO ENTIDADES:

- Comisión intersectorial: Establece la visión estratégica de la gestión de la información y las directrices políticas para la infraestructura tecnológica, la información pública y la seguridad cibernética y la ciberseguridad.

- Equipo de preparación informática de Colombia (colcert): Coordina los aspectos nacionales de la defensa y la seguridad cibernética.

- Comando cibernético conjunto Comando general de las fuerzas armadas: defiende contra las amenazas cibernéticas, en particular la protección de la infraestructura crítica nacional y el sector de defensa contra las amenazas cibernéticas.

- Centro cibernético de la policía: Apoya y protege contra los delitos cibernéticos a través de la estrategia integral contra los delitos cibernéticos.

- Centro de Capacidades para la Ciberseguridad ‘C4’: Se trata del centro estratégico más grande de Latinoamérica, cuya inversión en tecnología superó los 5 mil millones de pesos y maneja cuatro enfoques: prevención, ciber investigación, forense y relacionamiento estratégico[66]

8.2.1 LA ESTRATEGIA PLANIFICADA CUMPLE TRES OBJETIVOS:

Mejora la cobertura y las capacidades técnicas mediante la creación de unidades especializadas. Empareja y asegura la participación activa de las partes interesadas en la estrategia a través de su administración, articula la estrategia al

[66] Chaves, M. ALVARO. (2016, 27 septiembre). Ciberseguridad en Sudamérica. Recuperado de https://dialogo-americas.com/en/articles/cyber-security-south-america

sector privado, fortalece la educación ciudadana y mejora todos los niveles de prevención a través de las redes sociales y otros canales.

Alerta de las estructuras criminales a través de análisis exhaustivos de delitos, investiga e impide la economía cibernética vinculando a la policía nacional con diferentes escenarios internacionales, todos alineados con el documento de política nacional que define las pautas de seguridad cibernética y defensa.

La estrategia nacional de delitos cibernéticos de Colombia se implementó a través del Ministerio de Defensa Nacional. Si bien estos esfuerzos reconocen la importancia del tema a nivel internacional, es importante que el gobierno nacional fortalezca su liderazgo y construya una visión general nueva y clara para un enfoque integrado que reconozca las mejores prácticas internacionales para abordar los riesgos en el ciberespacio.[67]

El Informe de Ciberseguridad para América Latina y el Caribe 2016, escrito por el Observatorio de Ciberseguridad y la OEA, pregunta si la región está lista o no. El informe indica que la región de ALC está acelerando su desarrollo en materia de ciberseguridad y agrega que los principales países como México, Brasil, Argentina, Chile y Colombia han alcanzado un nivel intermedio de preparación para la ciberseguridad, aunque sus capacidades aún son limitadas debido a La falta de avances regionales, en comparación con sus homólogos europeos.[68]

9. PANORAMA DE MEDIDAS Y MERCADO DE SEGURIDAD CIBERNÉTICA DE AMÉRICA DEL SUR

El aumento de los ataques cibernéticos en América del Sur ha impulsado al gobierno a formular y adoptar marcos regulatorios integrados, vinculando todos los aspectos de las amenazas cibernéticas, principalmente la privacidad de los datos. La adopción de estos marcos regulatorios integrados, a su vez, ha creado una gran oportunidad para los actores del mercado, como IBM Corporation, Cisco Systems Inc. y Symantec Corporation. Entre otras compañías también se ha involucrado el mercado de seguridad en la nube.

Las empresas están pasando de la arquitectura de red tradicional a los sistemas de seguridad cibernética basados en la nube. La seguridad cibernética basada en

[67] Redacción Judicial. (2018, 6 octubre). Centro de Capacidades para la Ciberseguridad de Colombia 'C4'. Recuperado de https://www.elespectador.com/noticias/judicial/asi-trabajara-el-nuevo-centro-de-ciberseguridad-de-la-policia-nacional-articulo-804618b

[68] OBSERVATORY CYBERSECURITY IN LATIN AMERICA AND THE CARIBBEAN. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Recuperado de https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

la nube está ganando protagonismo, ya que la nube es una opción rentable y asequible tanto para pymes como para grandes empresas. Las soluciones de seguridad cibernética basadas en la nube permiten la recopilación inteligente de datos y el modelado de amenazas, la colaboración fácil de los datos y la identificación y el bloqueo de los ataques, con un retraso mínimo entre la detección y la remediación, lo que, a su vez, da como resultado una comunicación segura.[69]

En la siguiente tabla 3 se presenta un resumen de los países de América Latina y el Caribe por orden de clasificación según el índice creado por el Global Cybersecurity Índex 2017 publicado por ITU y ABI-research.

Tabla 3 Informes de Ciberseguridad

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURES	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURES	Standardization bodies	Cybersecurity good practice	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Inter-agency partnerships	COOPERATION	GCI
Antigua and Barbuda																														
Argentina																														
Bahamas																														
Barbados																														
Belize																														
Bolivia																														
Brazil																														
Canada																														
Chile																														
Colombia																														
Costa Rica																														
Cuba																														
Dominica																														
Dominican Republic																														
Ecuador																														
El Salvador																														
Grenada																														
Guatemala																														
Guyana																														
Haiti																														
Honduras																														
Jamaica																														
Mexico																														
Nicaragua																														
Panama																														
Paraguay																														
Peru																														
Saint Kitts and Nevis																														
Saint Lucia																														
Saint Vincent and the Grenadines																														
Suriname																														
Trinidad and Tobago																														
United States of America																														
Uruguay																														
Venezuela																														

Fuente:

Cisco realizó un Informe de seguridad cibernética para Pymes en 2018 y estudia los datos de 1,816 encuestados de Pymes en 26 países en los que incluye a Colombia. Este informe ofrece un análisis del panorama que enfrentan las organizaciones más pequeñas en el tema de seguridad, y qué recomendaciones o acciones deben seguir estas organizaciones para atenderlo de una manera más efectiva. Si hubiera recursos de personal disponibles, sería más probable que las empresas medianas invirtieran en:

• Actualización de la seguridad en el punto final a una protección contra malware avanzado más sofisticado/EDR: La respuesta más común con un 19%.

• Mejor seguridad de las aplicaciones web contra ataques web (18%).

[69]TECNÓSFERA EL TIEMPO. (2018, 4 abril). Recomendaciones para proteger la información que sube a la nube. Recuperado dehttps://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-proteger-la-informacion-en-la-nube-201230

• Implementar la prevención de intrusiones, que aún se considera una tecnología vital para detener los ataques a la red y explotar los intentos (17%).[71]

Los programas gubernamentales destinados a apoyar a las PYME ya existen y han demostrado ser valiosos para apoyar un ecosistema favorable para las PYME. Una evaluación de los programas de apoyo a las PYME en cuatro países latinoamericanos (Chile, Colombia, México y Perú) encontró impactos positivos estadísticamente significativos de dichos programas, especialmente con respecto a las ventas y el desempeño empresarial. Por ejemplo, la participación en programas dirigidos a las PYME en Chile, como programas de redes empresariales y programas de promoción de exportaciones, se asoció con mejoras positivas en corto y mediano plazo y en Colombia, las PYME que se beneficiaron de un fondo gubernamental fueron impactadas positivamente en cuanto a exportaciones e inversión en I+D.[72]

10. COLOMBIA APROBÓ COMO PRIMERA MEDIDA UNA POLÍTICA DE SEGURIDAD Y DEFENSA CIBERNÉTICA EN 2011, CONVIRTIÉNDOSE EN EL PRIMER PAÍS DE AMÉRICA LATINA EN ADOPTAR UNA ESTRATEGIA NACIONAL PARA ENFRENTAR EL DELITO CIBERNÉTICO

El Fondo Colombiano para la Modernización y el Desarrollo Tecnológico de las Micro, Pequeñas y Medianas Empresas (FOMIPYME) es la principal iniciativa pública para apoyar a las PYME en Colombia. Mientras que otros programas públicos y actividades se enfocan en temas específicos, este programa intenta tener una intervención más integral. FOMIPYME financia proyectos, programas y actividades para el desarrollo tecnológico de las PYMES y la aplicación de mecanismos no financieros destinados a su desarrollo. Este propósito inicial ha ido cambiando, debido en parte a la incorporación de recursos de las regiones a través de acuerdos, y también debido a la introducción de proyectos dirigidos a los desplazados internos y la población vulnerable.

En términos de cooperación e intercambio de información entre el sector privado y las autoridades gubernamentales, las normas específicas se describen en el Decreto 1704 (2012), que establece disposiciones que deben cumplir los proveedores de redes y servicios de telecomunicaciones para respaldar de manera eficaz y oportuna el trabajo. De las autoridades nacionales. Además, las autoridades nacionales han tratado de desarrollar relaciones con entidades clave

[71] CISCO. (2017). INFORME ESPECIAL DE CIBERSEGURIDAD DE CISCO. Recuperado de https://www.cisco.com/c/dam/global/es_mx/products/pdfs/cisco-2018-smb-report-spa.pdf?CCID=cc000159&DTID=&OID=rptsc011890

[72] [57] OEA. (2013). OPORTUNIDADES Y DESAFÍOS PARA LAS PYMES EN EL CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TIC. Recuperado de http://www.oas.org/es/sms/cicte/docs/white-papers/ESP_Digital_-_white_paper_3.pdf

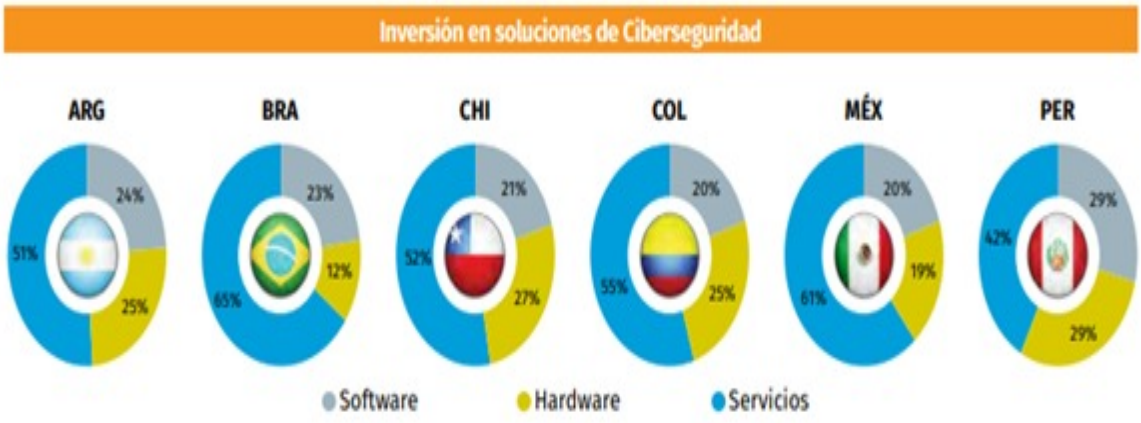
del sector privado para aumentar aún más la cooperación y el intercambio de información.
La cooperación internacional ha sido sólida, ya que las autoridades nacionales han colaborado directamente con agencias de contraparte en otros países de la región para responder a los ataques cibernéticos o actos de ciberdelito.[73]

Colombia registró menos incidentes cibernéticos en 2012 que en 2011, emparejándose con Chile como uno de los pocos países latinoamericanos con esa distinción[74]. El sistema de Colombia con respecto a la transmisión de datos utiliza más medidas de seguridad en la medida en que "requiere un consentimiento previo, expreso e informado", pero es muy estricto sobre cómo se procesa electrónicamente la información personal; La ley colombiana establece que "los datos personales, a excepción de la información pública, no estará disponible en Internet[75]. El inconveniente de esta estipulación es que no tiene en cuenta que los servicios prestados en Internet a veces requieren que la información personal sea registrada y, por lo tanto, solo trata a Internet como una herramienta de comunicación.

Producto del desarrollo tecnológico las leyes han tenido que adaptarse a los nuevos mecanismos de delitos en el ciberespacio, Latinoamérica ha venido avanzando en proporción a los delitos que se vienen presentando en la región, así mismo países como Colombia y Uruguay han sido enfáticos en un tratamiento de datos más estricto aun así muchas veces la legislación local no alcanza a cubrir la totalidad de posibles de delitos que pueden aparecer a diferencia de la Unión Europea o Norte América donde se adelanta proyectos de ley que regulen los posibles usos de la inteligencia artificial. Latinoamérica es distante aun de este tipo de medidas, pero no dista de los posibles ataques, la economía Latinoamericana es potencial victima debido aun a su desventaja de recursos, leyes, mecanismos y compromiso en cuanto a ciberseguridad refiere.
Brasil, Chile y México han mostrado una inversión mayoritaria en servicios de ciberseguridad este tipo de inversiones también ha creado una demanda en la región donde otros países han decidió tomar parte de dicha inversión como Colombia, Argentina y Perú en la figura 20 se observa el porcentaje de capital invertido respecto a las soluciones adquiridas

Figura 20 Inversión de Ciberseguridad

[73] AMERIPOL. (2016). FASCÍCULO DOCTRINAL No. 13. Recuperado de http://www.ameripol.org/portalAmeripol/ShowBinary?nodeId=/WLP%20Repository/72002//archivo
[74]OAS & Trend Micro (2013). Tendencias de ciberseguridad en América Latina y el Caribe y respuestas gubernamentales. Obtenido de http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf
[75] 60] Cruz, X. (2012). Protección de datos y problemas de privacidad en América Latina. Tiempos de nubes. Obtenido de http://cloudtimes.org/2012/11/21/data-protection-privacy-issues-latin-america/



Fuente:

En este contexto, el total de la inversión en seguridad de la información en Latinoamérica en 2017 fue de 2.700 millones de dólares y se espera un crecimiento anual compuesto de 11,5% en el período 2017- 2021. Las empresas de la región invierten un promedio del 16,5% del total del presupuesto de TI para la protección de infraestructura, sistemas y datos. Es notable que las empresas de tamaño medio, de entre 100 a 250 empleados, asignen un porcentaje significativamente mayor (24%) de su inversión de TI a ciberseguridad.[76]

11. APORTAR UN ANÁLISIS SOBRE LAS MEDIDAS QUE SE ESTÁN TOMANDO PARA PREVENIR CIBERATAQUES EN LAS PYMES DE COLOMBIA

11.1 PRACTICAS DE SEGURIDAD DIGITAL EN LAS EMPRESAS

A continuación, se relacionan algunas medidas o mejores prácticas para comprender mejor los factores referentes a ciberseguridad que se estudiaron en la Pymes colombianas en sector privado y público:

[76] MICROSOFT. (2018, marzo). Fortinet presenta estudio sobre inversiones en ciberseguridad en Colombia. Recuperado de http://acis.org.co/portal/content/NoticiaDelSector/fortinet-presenta-estudio-sobre-inversiones-en-ciberseguridad-en-colombia

- A nivel organizacional se estudia que tan preparadas están las áreas y jefe seguridad información, seguridad digital, entre otras áreas aplicables al entorno de la seguridad.

- Políticas referentes a controles de acceso y roles en los empleados, que tipos políticas de actualización de contraseñas y que tan cercano es el concepto seguridad de la información dentro de la compañía en general.

- Que tan frecuente se realizan pruebas de penetración y seguridad de la información en las organizaciones.

- Tipos de soluciones que gestionan la infraestructura en general y metodología de uso.

11.2 NIVEL DE PREPARACIÓN PARA HACER FRENTE A UN INCIDENTE DIGITAL (TAMAÑO DE LA EMPRESA A NIVEL PRIVADO)

Con el fin de evaluar el impacto que puede tener un incidente digital y los tipos de prácticas que lo conllevan se analiza la encuesta realizada por el Mintic. El 37% de las empresas encuestadas en la empresa encuestadas en el sector de industrias y comercio consideran que están preparadas para manejar un incidente de tipo cibernético, otro 30 % que no tienen las suficientes medidas para enfrentar un incidente.

En cuanto al tamaño de las empresas el 70% las grandes empresas indican que cuentas con las mejores prácticas frente a los incidentes, el 45% de las medianas pymes indica que cuentas con buenas prácticas; solo el 22% no está de acuerdo ni desacuerdo.

Cuáles son los estándares a nivel internacional de ISOS 27000 en todas sus versiones entre otros estándares internacionales de acuerdo a al conocimiento de estos estándares surgieron preguntas como, por ejemplo: ¿Qué tipo de prácticas de seguridad digital son implementadas en las compañías? A lo cual el 55% del sector comercio, el 70% del sector industrial, 59% sector de servicios indico tomar medidas de tipo normativo.

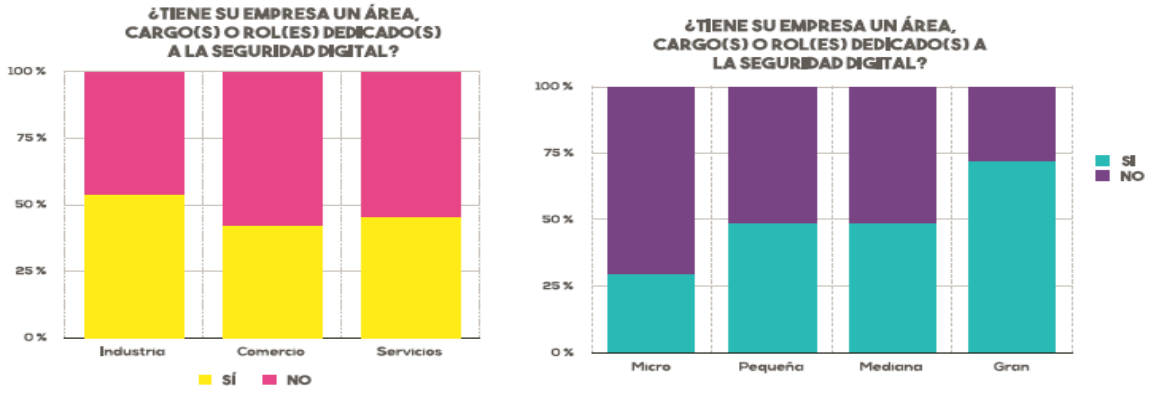
El Sector comercio el 43%, Industria 63% y el 43% a nivel servicios indicaron que toman medidas implementando normas o estándares técnicos como IS0 27001.

11.2.1¿TIENE SU ENTIDAD/EMPRESA UN ÁREA, CARGO (S) O ROL(ES) DEDICADO (S) A LA SEGURIDAD DIGITAL (SEGURIDAD DIGITAL Y/O DE SEGURIDAD DE LA INFORMACIÓN)?

En la figura 21 se puede observar las áreas y profesionales dedicados a la seguridad según perfil el perfil y tamaño de las compañías, según estadísticas el 37% de las microempresas, el 58% de pequeñas, 64% medianas, 58% de las empresas Grandes, indicaron que gestiona la seguridad bajo el departamento de TI.

El 18% de las pequeñas, el 22% de las microempresas, el 7% de las medianas y el 7% de empresas grandes indicaron que su seguridad es basada en un área de Seguridad digital. A nivel de sectores comerciales se indicó comercio 83%, 55% a nivel Industrial y el 47 a nivel de Servicios, dejaron a cargo el tema de seguridad bajo el esquema de área departamento de TI.

Figura 21 Tiene su entidad/empresa un área, cargo

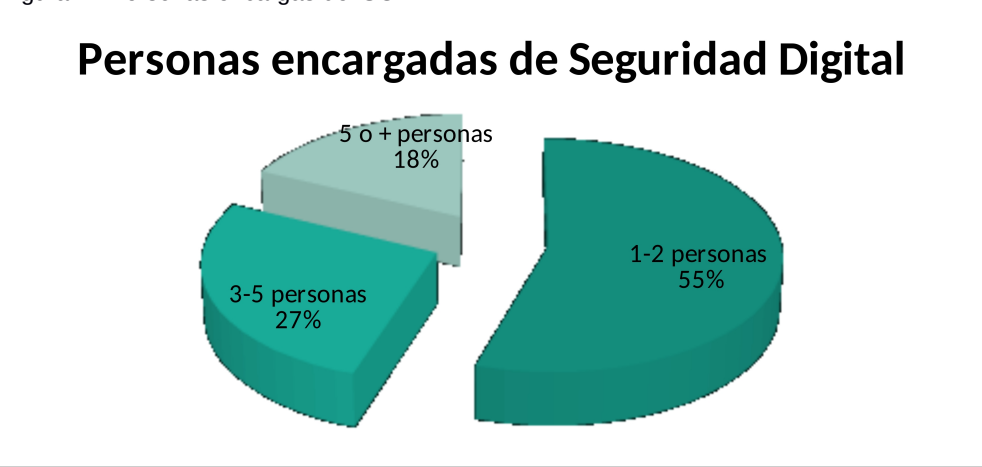


Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

Las compañías pueden incluir una persona que maneje la seguridad informática, pero esto no les garantiza estar a salvo de tener incidencias de seguridad por lo que es necesario capacitar a más personal en el área de TI en el manejo de estos incidentes y procedimientos a seguir en caso de presentarse.

La seguridad informática se ubica como área transversal que cubre todas las áreas de TI (desarrollo, redes eh infraestructura, mesa de servicio, integración Devops) es por eso que el área de seguridad se debe fortalecer, en la siguiente figura 22 se puede apreciar la cantidad de personas a cargo de la seguridad dentro de las compañías actualmente.

Figura 22 Personas encargas del SG



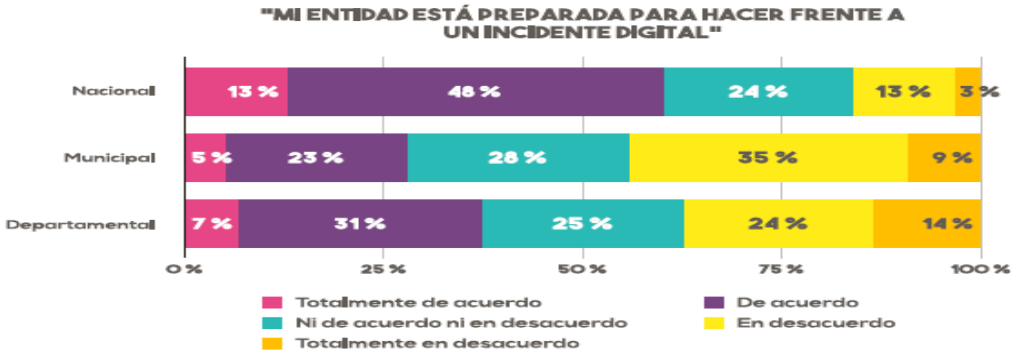
Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

A pesar de las campañas, normativas, casos actuales y demás mecanismos que exponen la necesidad de tener un área tan importante como la seguridad de la información en las organizaciones aun así no se destina ni los recursos suficientes ni el interés que esta área demanda.

11.3 NIVEL DE PREPARACIÓN PARA HACER FRENTE A UN INCIDENTE DIGITAL (TAMAÑO DE LA EMPRESA)

Teniendo en cuenta hoy en día la tercerización de recursos como por ejemplo IaaS, SaaS, PaaS que les aportan una capa de seguridad a las compañías aun así no es la solución total para la gestión de la seguridad en las pymes y organizaciones estatales hay brechas importantes en los sectores más retirados geográficamente como son los municipios en la figura 23 se puede observar los resultados de la encuesta del Mintic sobre si están preparadas las entidades para manejar los incidentes digitales. Según las empresas analizadas se indica que el 48% y el 13% a nivel nacional implementan prácticas frente a incidentes digitales comparado a nivel municipal y departamental solo con el 23% y el 31%.

Figura 23 Incidente Digital

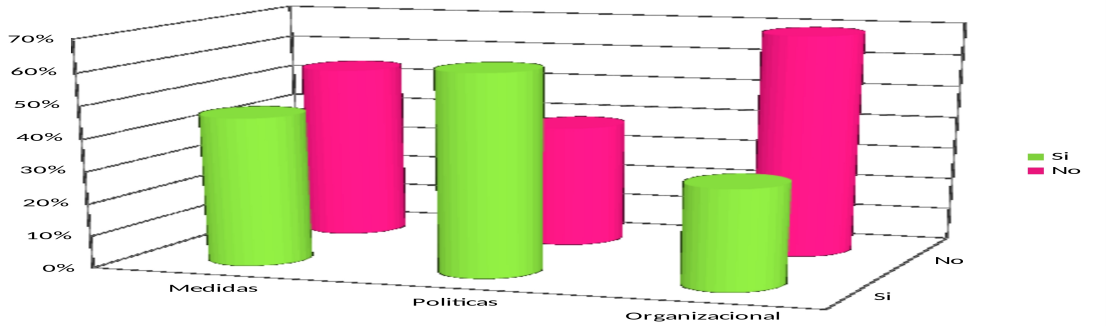


Fuente:

De acuerdo al análisis anterior se pueden plantear interrogantes en las pymes más específicamente en el sector privado, un interrogante puede ser: ¿Qué medidas se toman en el sector público y que puedan ser replicadas en el sector privado en pro de la seguridad digital? También, ¿Qué recursos normativos y recursos tecnológicos referentes a ciberseguridad se pueden implementar en el sector público y privado?

Continuando con los datos de la encuesta del Mintic se ven resultados de porcentaje en cuanto a medidas de seguridad digital tomadas en las pymes y las que no toman ninguna medida, 62% asegura la información por medio de políticas organizacionales, el 46% usan medidas técnicas para asegurar la información digital, solo el 31% indica que realizan medidas organizativas para combatir el tema, como se refleja en la figura 24.

Figura 24 Prácticas implementadas en las pymes



Fuente: https://publications.iadb.org/handle/11319/8552?locale-attribute=es

12. ¿ACTUALMENTE LAS EMPRESAS ESTAN PREPARADAS ANTE UN CIBERATAQUE?

Los ataques cibernéticos en los últimos años han impactado a nivel mundial las empresas; ataques como el ransomware o malware de cifrado de archivos, alertan a los países sobre qué tan preparadas están en las organizaciones para prevenirlos.
La OEA y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) junto con el Banco Interamericano de Desarrollo indicaron que el 65% de las empresas entrevistadas el 81% cuenta con internet en el sector público.

El 81% de los empleados de las pymes Colombianas tiene acceso a internet, el problema es que solo el 1% del presupuesto es destinado a la ciberseguridad, la demanda de soluciones de seguridad ha venido aumentando considerablemente debido a sus costos muchas veces las pymes prefieren invertir en pasivamente y dejar la seguridad en segundo plano o ni se tiene en cuenta como recurso indispensable para el aseguramiento de sus activos.

Si continúan las pymes como motor principal de la económica nacional entonces deben mejorar la inversión digital integral donde haya sinergia en los mecanismos que interactúan; soportados por la seguridad, disponibilidad, integridad de los servicios. Pero no solo el compromiso del sector empresarial sino apoyo del gobierno nacional ya que la inversión se inclina siempre al sector público.

Este estudio del Mintic y la OEA también muestra un análisis donde se comprenden los impactos de los incidentes y la seguridad digital en Colombia y como empiezan a tomarse en cuenta, más cuando las áreas de TI empiezan a tomar fuerza y tener prioridad en los procesos internos de las organizaciones, aún queda camino que recorrer en el campo de seguridad digital pero ya se comprende su necesidad inicial.

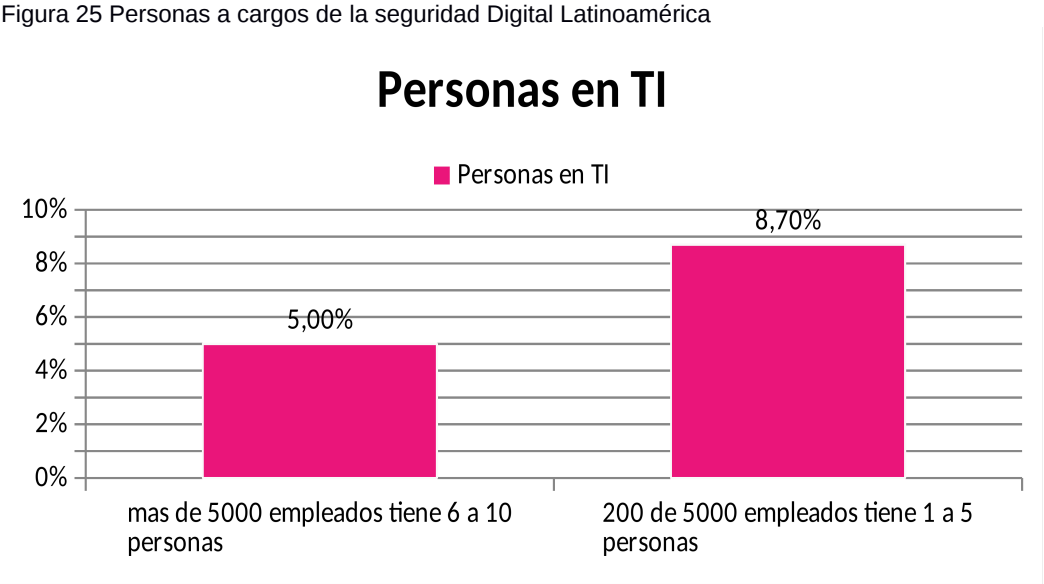
12.1 PRESUPUESTO ASIGNADO PARA LAS PYMES

El 14,2% en Latinoamérica tiene perfil de directores de seguridad informática en su organigrama, es decir que empiezan los empresarios a tomar conciencia de la importancia que tiene las áreas de tecnología y seguridad informática en sus empresas y que tanto dependen de ellas.

A continuación, se evidencia en la figura 25 a nivel general de Latinoamérica en las empresas según su tamaño que tantas personas se encuentran contratadas en los departamentos de tecnología[77]

[77] ¿Están preparadas las empresas ante un ciberataque?, ED. El tiempo, 28, Nov, 2017, Disponible en: https://www.eltiempo.com/economia/empresas/estan-preparadas-las-empresas-ante-un-ciberataque-156308

Figura 25 Personas a cargos de la seguridad Digital Latinoamérica



Fuente: https://www.eltiempo.com/economia/empresas/estan-preparadas-las-empresas-ante-un-ciberataque-156308

En cuestión de presupuesto el 2,8% destina recursos al sector financiero, la banca 3% y el 5% de presupuesto general para el tema de seguridad. El 1,7 % de las empresas que prestan el servicio de consultoría destinan hasta el 10% que se tuvo proyectado para 2017. En conclusiones generales se pasó de 55% de presupuesto basado en el 2016 se aumentó a un 71% en el transcurso del año 2017 lo cual muestra un notable avance.

13. INCIDENTES IDENTIFICADOS Y RIESGOS EN LAS PYMES

Según el análisis de los incidentes que se identifican y notifican se aprecia en orden descendente los sectores con más incidentes reportados; como es el caso de servicios financieros con 18,3% educación 15%, gobierno y consultoría 10.2% resaltando como principales motivos los caballos de Troya con un 14,4%, instalación de software no autorizado 13,8%, phishing 11,2%, ransomware 7,5% eh ingeniería social 6,1%.

El 42,61% de los encuestados en las compañías manifestó tener contactos que los asisten en caso de incidentes de ciberseguridad, un 57,39% son conscientes de las medidas de mitigación, el 17,05% tiene una estrategia de manejo del ciberespacio, finalmente el 21,59% cuenta con un procedimiento o metodología que administre los recursos digitales y evidencias.

Las empresas participantes no ven la seguridad informática como un riesgo palpable en el que se deba invertir; el 33% el cual los asocia a riesgos de operación, así el 17,9% a riesgos legales, de igual manera 17,9% riesgos económicos, 17,1% son riesgos de imagen corporativa y 11,9 riesgos transversales y colaterales.

Los datos presentados dependen de la frecuencia de los análisis de riesgos, empresas que son más dedicadas son las de consultoría por otro lado el 7,39% son de servicios financieros y banca que hacen análisis de 2 a 4 veces anualmente, los demás sectores mínimamente uno al año.

Se puede inferir que en la actualidad que el conocimiento de flujos y procesos es contraproducente con la escasez de habilidades directivas, aunque haya mayor asignación de presupuesto no se cubre por completo ni se usa correctamente generando el tipo de inestabilidad que se expone.[78]

14. MEDIDAS ACTIVAS QUE LAS PYMES PUEDEN ADOPTAR PARA REFORZAR LA SEGURIDAD DIGITAL

En el 2018 los desafíos aún son latentes en las organizaciones con respecto a cómo tomar medidas para reforzar la seguridad cibernética en las PYMES, a continuación, se presentan algunas medidas a tener en cuenta.

•Elegir el personal adecuado y establecer tareas a un empleado especifico que trabaje en el área de seguridad cibernética, permite que el compromiso con el rol se enfoque en lo que realmente importa, en caso no tener presupuesto para dedicar personal de tiempo completo al menos que este alguien un tiempo parcial en la compañía dedicado a realizar estas tareas, para ello también es de destacar que el empleado elegido deber contar con el perfil profesional en esta área.

• Crear conciencia sobre el tema de seguridad en su empresa, use las políticas internas de la compañía como un tema de sensibilización y realice cursos de capacitaciones para concientizar y que también adquieran conocimiento en estas áreas, así ayudaran a que su pyme sea más segura.

• Diseñe productos y servicios de manera que ambos sean integrados, cuyo fin sea proteger los datos de la empresa y personales que sean confidenciales, esto ayudara a generar responsabilidad de manipulación de información.

[78] ¿Están preparadas las empresas ante un ciberataque?, ED. El tiempo, 28, Nov, 2017, Disponible en: https://www.eltiempo.com/economia/empresas/estan-preparadas-las-empresas-ante-un-ciberataque-156308

• Busque recursos, indague, pregunte y mantenga contacto directo con las gestiones gubernamentales y la policía en busca de seguridad digital/o información para su PYME con el fin de mantener conocimiento actualizado y las nuevas herramientas y habilidades existente para contraatacar los ciberataques.

• Implemente y audite las normas oficiales en su empresa referente con la seguridad cibernética y protección de datos, con el fin de que tanto usted como empresario y el gobierno mantengan una línea clara, con el fin de tener un ecosistema empresarial confiable y seguro.[79]

.

[79]OPORTUNIDADES Y DESAFÍOS PARA LAS PYMES EN EL CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TIC, aws, 2018, Disponible en: http://www.oas.org/es/sms/cicte/docs/white-papers/ESP_Digital_-_white_paper_3.pdf

15. CONCLUSIONES

- Un mercado de la tecnología en pleno auge con los teléfonos inteligentes, dispositivos portátiles y un número creciente de usuarios de internet en Colombia, la adopción de nuevas tecnologías con la llamada economía naranja o revolución 4.0 trae excelentes avances para las personas y compañías pero también representa oportunidades a las organizaciones criminales, estafadores y oportunistas dando cabida a diversos tipos de ataques sofisticados, sin embargo, la forma más común que se ve en Colombia continua siendo el phishing, la suplantación de correo y las fugas de información, muchas veces dentro de una empresa la complicidad pasiva o activa de los empleados internos implica riesgos de consideración ya que sin importar cuantos recursos se empleen en la protección puede haber filtraciones a través de un interno, esto puede abarcar todas las áreas y perfiles de la empresa.

  De acuerdo a los análisis anteriores Colombia es de los principales países que más ha invertido en planes de ciberseguridad y ciberdefensa para el sector público, la otra cara de la moneda se refleja en la creciente formación de pymes que se ven desobligadas o desconocen la ciberseguridad como tema puntal en la base de sus negocios.

  Las nuevas entidades del gobierno como el C4 serán responsables de coordinar las estrategias públicas y privadas para combatir el delito cibernético, así como el fortalecimiento de los organismos de control dedicados a supervisar esta forma de actividad delictiva. Las oficinas de los fiscales especializados también se deben fortalecer en todos los aspectos para hacer frente a los delitos cibernéticos.

- A menudo es más difícil para las organizaciones más pequeñas asegurar sus activos debido a la falta de recursos o incluso a la falta de conciencia. No es sorprendente entonces que las pequeñas empresas se hayan convertido cada vez más en el objetivo principal de los delincuentes y que la tendencia a nivel mundial no sea muy diferente en Latinoamérica puntualmente en Colombia el phishing no pierde tendencia por la versatilidad de este ataque, así como forma de automatizarlo, la suplantación de correos afecta más a las empresas emergentes en Colombia, lo que muestra una tendencia como método predilecto y más efectivo junto con el fraude en el sector empresarial en Colombia, ahora el ransomware surge como punto de inflexión en las amenazas latentes y crecientes en la región.

Las medidas que se están tomando son por ejemplo el fortalecimiento de la legislación como la ley de la modernización en Colombia, los últimos años con los decretos y leyes establecidas del 2009 en adelante han contribuido al sector de la seguridad y han sido de las más completas después de Brasil, también la emergente adopción de software libre como solución de bajo costo esto, no quiere decir que no sea confiable o mala solución, también la conciencia de los clientes quienes prefieren contar con empresas que tengan normatividad establecida en cuanto a manejo de información. El panorama en Latinoamérica tampoco es favorable a pesar de que cada día haya organismos que supervisen las practicas digitales de los mercados como la OEA, Colombia sigue mejorando sus prácticas por encima de países como México, Perú Ecuador. Los planes de seguridad cibernética, los centros de defensa y las nuevas leyes contra los delitos cibernéticos abarcan algunas de las estrategias principales de los gobiernos, mientras que las empresas invierten en soluciones para proteger sus datos.

- En el análisis anterior se apreció los impactos operativos y financieros de los ataques cibernéticos y como se están volviendo más notorios en las pymes en Colombia, algunas aún están asumiendo estos riesgos con más responsabilidad adquiriendo pólizas de riesgos contra incidentes de seguridad también usando soluciones como; IaaS, SaaS, PaaS si bien las pequeñas empresas no representarían un gran botín para los ciberdelincuentes a menudo no están bien protegidas, dada la posibilidad de elegir entre "grandes y difíciles" y "pequeñas y fáciles", muchos ciberdelincuentes se sienten atraídos por esta última oportunidad. Los gobiernos y el sector privado en Latinoamérica buscan nuevas formas de protegerse contra la piratería y técnicas como el malware y el phishing. La ciberdelincuencia le cuesta a Latinoamérica grandes cifras eh impactos colaterales como daño de imagen y pérdida de credibilidad.

  Las pymes colombianas particularmente según los análisis expuestos siguen siendo vulnerables a los ataques cibernéticos porque carecen de recursos en general especialmente de profesionales de la seguridad informática para proteger sus activos. También hay pymes emergentes con soluciones de seguridad en el país gran parte en Antioquia, Risaralda y Bogotá también la demanda de profesionales de la seguridad ha hecho que varias universidades decidan ofrecer estas formaciones de manera presencial y virtual, la normatividad también ha tenido un papel importante en las políticas internas de la compañía ya que buscando posicionarse en el sector optan por certificarse en seguridad y buenas prácticas de manejo de información.

16. RECOMENDACIONES

- La preparación para la seguridad cibernética comienza con una comprensión completa de las vulnerabilidades internas y externas que pueden afectar a cualquier negocio, cómo los piratas informáticos pueden ingresar incluidos sus diferentes métodos y motivos, en este caso los más comunes y cómo identificar los puntos de debilidad.

- Colombia como se muestra en las estadísticas a nivel de Latinoamérica cuenta con una de las fuerzas más capacitadas y con más recursos para la ciberdefensa sin embargo estos recursos están destinados para el sector público y militar. Las pequeñas empresas quedan a la merced de sus propios recursos y capacidades si no se cuenta con grandes capacidades económicas para invertir en presupuestos ya que en principio no muestran ganancia o necesidad urgente para los directivos entonces queda tomar medidas o uso de buenas prácticas como por ejemplo educar a los empleados sobre el manejo de la información las prácticas seguras, seguimiento de políticas internas y mecanismos básicos de seguridad como contraseñas complejas y únicas, mantener un entorno de escritorio limpio donde la información personal y confidencial no esté expuesta

- El uso de herramientas open-source puede ayudar a mejorar la ciberseguridad de forma notoria hay todo tipo de soluciones open-source robustas, confiables y gestionables llámense firewalls, IDS, UTM, correlacionador de eventos.

- las organizaciones no solo deben asegurar la información de sus clientes, también articular niveles de protección o uso de pólizas para incidentes de ciberseguridad, mientras se capacitan sobre mejores prácticas de seguridad de la información por lo tanto las pymes emergentes y las que trascienden deben contemplar este tema como algo clave en el desarrollo de cada proyecto del que tomen parte, las estrategias de seguridad de digital deben estar estrechamente alineadas con la estrategia organizacional general y deben adherirse a los principios de confidencialidad, integridad y disponibilidad, transversalmente a los planes de preparación, protección, detección, respuesta y recuperación en incidentes de seguridad.

- Cifrar dispositivos que contengan información sensible. Esto asegura que, si un dispositivo se pierde o es robado, los datos que contiene pueden mantenerse inaccesibles al delincuente.

- La ciberdelincuencia también ha abierto mercado para empresas con soluciones inteligentes con el uso de machine learning darktrace. También las empresas aseguradoras y las aseguradoras en Latinoamérica han visto un notable mercado y por eso han desarrollado una variedad de coberturas para ayudar a las

empresas y mitigar este posible riesgo. Estas políticas generalmente cubren violaciones de datos que involucran datos financieros, de clientes, empleados, así como cualquier tipo de ataque cibernético que interrumpa las operaciones de una empresa.[80]

- La recomendación general que se realiza es proteger la infraestructura tecnológica, que todos los esfuerzos se encuentren enfocados en la protección no solo de la información y datos, sino la reputación de la compañía, se puede comenzar analizando las necesidades primarias a cubrir, el tamaño de la empresa, cantidad de usuarios, el valor de los activos con los que se va a trabajar y ver qué soluciones hay en el mercado desde un antivirus hasta hardware especializado y personal capaz de operar y gestionar infraestructuras según la demanda, la implementación de software o hardware deben ir de la mano de la capacitación al personal el cual va a interactuar con los activos de la compañía mediante acuerdos de confidencialidad y constante retroalimentación con el uso de buenas prácticas, implementar políticas de seguridad, realizar actualizaciones de los sistemas operativos constantemente con el fin de evitar vulnerabilidades día Zero.

- Muchas agencias gubernamentales y empresas privadas en Latinoamérica están tomando medidas concretas para combatir el delito cibernético. Las soluciones para proteger las redes de datos y los servidores continúan siendo cada vez más sofisticadas y difíciles de vulnerar. Se debe considerar aumentar los recursos en ciberseguridad; Contratar a especialistas en el área, adoptar tecnologías eficientes de respaldo de información, virtualización de datos, campañas de educación a los empleados.

- Las compañías que dependen en gran medida del uso de redes e internet deben identificar periódicamente sus vulnerabilidades y definir su tolerancia al riesgo cibernético. Las compañías deben considerar cómo podrían responder en caso de un ataque cibernético. Si bien la amenaza puede parecer inexistente hay que tener un plan de contingencia implementado, puede minimizar en gran medida los costos financieros y de reputación para la compañía.

[80]Darktrace presenta solución de seguridad basada en IA y Machine Learning, [en línea] mayo 31, 2019, Disponible en www.insitio.com/mx/darktrace-presenta-solucion-basada-en-ia-machine-learning

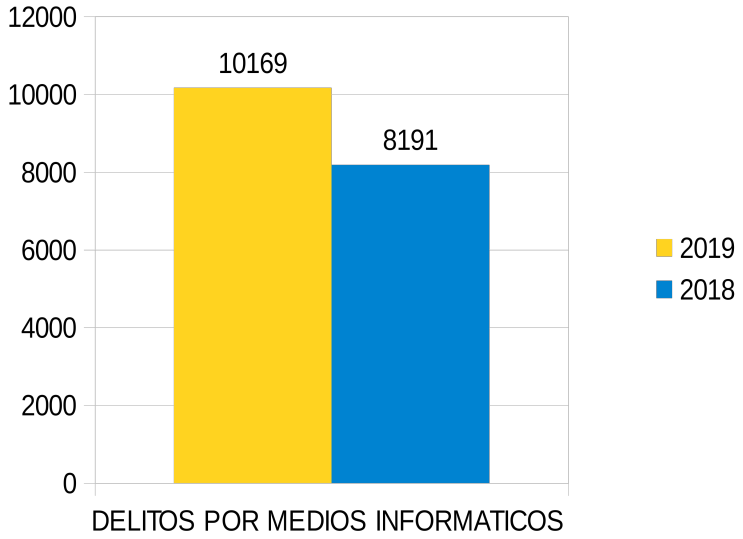
17. RESULTADOS ESPERADOS

Se busca generar un documento donde se contextualice el estado de la ciberseguridad en las pymes de Colombia, al obtener un estudio donde se muestren las técnicas más usadas del cibercrimen en este sector así como las técnicas más comunes o los métodos que se están empleando para la protección contra los ataques en el ciberespacio, se busca tener un alcance puntual y específico sobre la ciberseguridad en las pymes, un material que soporte datos y corresponda al escenario en el que se encuentra Colombia respecto a Latinoamérica no solo se generar un documento ilustrativo sino un soporte que permita ser referente de este tipo de monografías dando pie a futuros estudios en esta área. Es fundamental continuar con el estudio en el campo de las tecnologías de la información debido la demanda con que se vienen desarrollando nuevas soluciones, de igual manera se desarrollan amenazas y las variables de riesgo irán cambiando proporcionalmente al uso adecuado o inadecuado de la información, los datos de esta monografía serán datos que contribuyan a un soporte general sobre los modelos de estudio en esta área en concreto para Colombia.

Por lo tanto, se busca justificar la creación e implementación de estrategias de seguridad de la información a partir de la contextualización de todos los factores expuestos en esta monografía.

Ciertos delitos empiezan tener diferencias considerables en Colombia, los denuncios en el sector productivo también han incrementado así lo muestra la figura 26 de los dos últimos años.

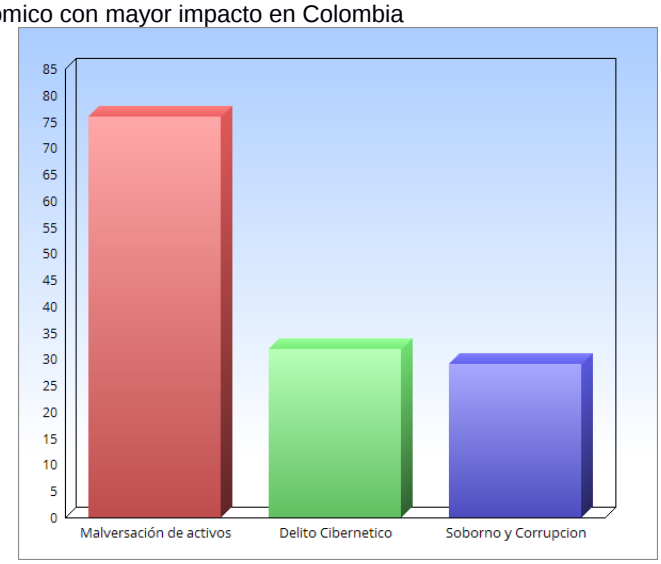
Figura 26 Delitos por medios informáticos en sectores productivos



Fuente: Lo autores

Durante 2016 según la encuesta delitos económicos se demostró como el ciberdelito en el escenario financiero y productivo ha tomado fuerza al llegar casi al nivel de la corrupción, esto ha sido producto también de muchos factores como el anonimato con que se ejecutan los ataques o los desconocimientos tecnológicos de la víctima, complicidad etc. Como se aprecia en la figura 27 ocupo el segundo lugar después de la malversación.[81]

Figura 27 Delitos económico con mayor impacto en Colombia



Fuente: Lo autores

[81] PWC; Hacia nueva técnica en los negocios, [en línea]COLOMBIA, 2016, Disponible en https://www.pwc.com/co/es/publicaciones/crime-survey-2016.pdf

Esta información permite entrever que las amenazas están lejos de disminuir para todos los sectores no solo para las pymes y es comprensible ya que la presión de la globalización demanda el uso de las tecnologías de la información y estas muchas veces se adoptan sin prever los riesgos, de igual manera los atacantes dependen de la tecnología empleada por la víctima para categorizar su ataque. Es por esto que si bien no se emplearía un malware del 2012 si se pudiera usar su heurística o su metodología de infección para adaptarlo y mejorarlo de acuerdo a la nueva víctima.

Este tipo de resultados esperados también busca que se permita identificar por qué las pymes son la presa predilecta de los atacantes, las pymes gran parte de sus recursos son empleados en su producción de activos, pero pocos de estos se destinan a la protección de los mismos, estos son algunos de los errores cometidos por las compañías la gran mayoría subestima el valor de los activos con los que cuenta o simplemente los ignora.

- No reconocer que hay riesgos
- No dedicar suficientes recursos
- No mantener actualizado el software
- No tener en cuenta los riesgos que generan sus empleados
- No capacitar a los empleados
- No tener software de seguridad
- No estar pendiente de los equipos de sus empleados
- No proteger bien los datos
- No manejar bien los backups
- No tener listo un plan de respuesta

Así como en contra medida las soluciones que se implementan deben reducir esas brechas al máximo ya que muchas de estas Pymes están en proceso de transición y muchos procesos dentro de la empresa pueden estar en proceso de maduración o gestación esto por supuesto acarrea vulnerabilidades en muchos aspectos, aparte de los virus o amenazas técnicas también está la humana, fugas de información o insiders algunas medidas que actualmente se están tomando son, por ejemplo:

- Personal especializado.
- Antivirus y antimalware.
- Backups.
- Uso de software legal.
- Formación de los trabajadores.
- Implementación soluciones en la nube.
- Aplicación de un SGSI.
- Hardware dedicado como firewall.

Estos últimos años el sector público de Colombia ha tenido un considerable aumento de presupuesto a la hora de proteger sus intereses por ejemplo la formación del C4 el complejo más grande de Latinoamérica para la ciberseguridad ,colcert, centro cibernético de la policía entre otros este tipo de entidades han recibido un aumento de presupuestos y alianzas estratégicas, para el sector privado no se puede decir lo mismo ya que los recursos de los que se deben valer son propios y gran parte del presupuesto se debe invertir en los activos o materia prima que son los que hacen que funcione la compañía, el respaldo económico o tecnológico del gobierno al sector de las pymes no ha sido contundente como se espera ya que como lo manifiesto el observatorio nacional de ciberseguridad el horizonte de amenazas es muy amplio y las pymes constituyen el 80% del empleo del país es por esto que las alianzas, capacitaciones, talleres, hackatones, meetups o cualquier tipo de actividad que constituya educación sobre este importante tema.

18. DOCUMENTO RAE

Anexo 1. RAE

TÍTULO

ESTUDIO MONOGRÁFICO SOBRE CASOS MÁS COMUNES DE CIBERCRIMEN EN LAS PYMES COLOMBIANAS

MONOGRAPHIC STUDY ON MORE COMMON CASES OF CYBERCRIME IN COLOMBIAN SMEs

Autores: Oscar Javier Carvajal

Ana Milena Marin

Estudiantes

UNAD

JAG

ECBIT

eskarvajal@gmail.com

compuyoyis_@hotmail.com

RESUMEN

El estado actual de la ciberseguridad en las Pymes Colombianas se debe estudiar más a fondo ya que sobre estas empresas se sostiene más del 80 % de la economía nacional, es por eso que este estudio monográfico aborda las metodologías, prácticas y técnicas con que se manipulan los datos y se gestiona la infraestructura en pro de la seguridad de la información y también las técnicas con que se cometen los delitos cibernéticos en Colombia esto se logra analizando encuestas del Ministerio de telecomunicaciones, OEA, Policía y demás entes que convergen en la protección de información en la república de Colombia.

Una vez se comprende el estado actual de la ciberseguridad en las Pymes Colombianas se puede establecer un comparativo a nivel regional con indicativos de empresas que ofrecen soluciones de seguridad en Latinoamérica y que a partir de estos datos actualizados se puede clasificar cada país de la región en lo que refiere a su gestión de ciberseguridad. Se obtiene resultados donde se aprecian metodologías o técnicas que convergen en un objetivo común, por ejemplo, el sector financiero y técnicas que resaltan en este sector como el phishing.

El comportamiento del cibercrimen en Colombia los últimos diez años ha venido trascendiendo según los datos reunidos en esta monografía, es decir los delitos cibernéticos se adaptan al crecimiento de las empresas, dejando que el ciudadano común sea el objetivo principal y pasando a elegir objetivos de mayor valor como las Pymes, más cuando estas no ven la inversión en ciberseguridad como una prioridad o ignoran la importancia de esta área tanto para sus procesos internos como externos y la relación con clientes, proveedores y demás áreas involucradas en el flujo de información.

Palabras Claves: Ciberseguridad- Opensource- Legislación- Ransomware- Amenaza.

ABSTRACT

The current state of cybersecurity in Colombian SMEs should be studied further since these companies support more than 80% of the national economy, which is why this monographic study addresses the methodologies, practices and techniques with which they are handled the data and the infrastructure for information security management and also the techniques with which cyber crimes are committed in Colombia is managed. This is achieved by analyzing surveys of the Ministry of telecommunications, OAS, Police and other entities that converge in the protection of information in the republic of Colombia.

Once the current state of cybersecurity in Colombian SMEs is understood, a comparison can be established at the regional level with indications of companies that offer security solutions in Latin America and that from this updated data each country in the region can be classified in Regarding your cybersecurity management. Results are obtained where methodologies or techniques that converge in a common objective are appreciated, for example, the financial sector and techniques that stand out in this sector such as phishing.

The behavior of cybercrime in Colombia for the last ten years has been transcending according to the data gathered in this monograph, that is, cybercrimes adapt to the growth of companies, leaving the common citizen to be the main objective and moving on to choose objectives of greater value as SMEs, especially when they do not see investment in cybersecurity as a priority or ignore the importance of this area for both their internal and external processes and the relationship with customers, suppliers and other areas involved in the flow of information.

Keywords: Cybersecurity- Opensource- Legislation- Ransomware- Threat.

DESARROLLO DE LA PONENCIA

INTRODUCCIÓN

El contexto de esta monografía pretende analizar las principales técnicas, herramientas y amenazas a las que se ven expuestas las pymes o empresas que no cuentan con infraestructuras de seguridad o malas prácticas en las mismas, el desarrollo tecnológico en las Pymes crece en proporción a su mercado, pero el uso responsable de estas tecnologías no es la prioridad de las organizaciones, el problema también radica en la cultura organizativa, en la forma como solo se invierte en materia prima o la forma de adquirir o ampliar mas negocios y mercados. Estos antecedentes sirven de base para entender que la metodología con que se interviene la infraestructura tecnológica en Colombia se basa solo en modelos funcionales, pero no se aborda la manera como estos modelos funcionan.

El objetivo general es contribuir con un estudio monográfico sobre las amenazas y riesgos cibernéticos que afectan a las Pymes en Colombia y busca que se adopte el tema con más compromiso dejando de verlo como un asunto externo y verlo como un engranaje importante en el funcionamiento de las compañías.

MATERIALES Y MÉTODOS

En esta monografía se adopta el modelo de compilación con forma discursiva-explicativa y con técnica de recopilación bibliográfica, documental y electrónica. Con fichas bibliográficas de resumen y análisis, también el bosquejo preliminar de ideas se implementó sobre el estado de la ciberseguridad en las pymes colombianas consultando documentos públicos del ministerio del telecomunicaciones, policía nacional, OEA , estudios de compañías como Cisco, ESET, Symantec y demás compañías enfocadas en soluciones de seguridad en la región.

RESULTADOS RELEVANTES

Se obtiene un estudio monográfico donde se muestran las técnicas más usadas del cibercrimen en este sector, así como las técnicas más comunes o los métodos que se están empleando para la protección contra los ataques en el ciberespacio. Se aporta un material que soporta datos y corresponde al escenario en el que se encuentra Colombia respecto a Latinoamérica.

Es fundamental continuar con la investigación en el campo de las tecnologías de la información debido la demanda con que se vienen desarrollando nuevas soluciones, de igual manera se desarrollan amenazas y las variables de riesgo irán cambiando proporcionalmente al uso adecuado o inadecuado de la información, los datos de esta monografía son datos que contribuyan a un soporte general sobre los modelos de estudio en esta área en concreto para Colombia.

“se puede observar los resultados de la encuesta del Mintic sobre si están preparadas las entidades para manejar los incidentes digitales. Según las empresas analizadas se indica que el 48% y el 13% 56 a nivel nacional implementan prácticas frente a incidentes digitales comparado a nivel municipal y departamental solo con el 23% y el 31%.”

“Este tipo de resultados esperados también busca que se permita identificar por qué las pymes son la presa predilecta de los atacantes, en las pymes gran parte de sus recursos son empleados en su producción de activos, pero pocos de estos se destinan a la protección de los mismos”

“Colombia como se muestra en las estadísticas a nivel de Latinoamérica cuenta con una de las fuerzas más capacitadas y con más recursos para la ciberdefensa sin embargo estos recursos están destinados para el sector público y militar.”

CONCLUSIONES

Las pymes colombianas particularmente según los análisis expuestos siguen siendo vulnerables a los ataques cibernéticos porque carecen de recursos en general especialmente de profesionales de la seguridad informática para proteger sus activos.

Las técnicas mas usadas y con mayor beneficio para los delincuentes en Colombia siguen siendo la gran mayoría BEC, spear phishing,malware. Independientemente de que estas técnicas prevalezcan lo que a cambiado es la metodología con que las emplean y las formas en que buscan llegar a los objetivos también como perfeccionan los ataques evadiendo antivirus y usando certificados legítimos.

La posibilidad de elegir entre "grandes y difíciles" y "pequeñas y fáciles", muchos ciberdelincuentes se sienten atraídos por esta última oportunidad en lo que respecta a delitos ciberneticos.

Las medidas que se están tomando son por ejemplo el fortalecimiento de la legislación como la ley de la modernización en Colombia, los últimos años con los decretos y leyes establecidas del 2009 en adelante han contribuido al sector de la seguridad y han sido de las más completas después de Brasil, también la emergente adopción de software libre como solución de bajo costo esto, no quiere decir que no sea confiable o mala solución, también la conciencia de los clientes quienes prefieren contar con empresas que tengan normatividad establecida en cuanto a manejo de información.

18. BIBLIOGRAFIA

- ARANGO, Rodrigo Alcides Patiño. Afectación del cibercrimen en las pymes. La corrupción en la contratación administrativa: el caso de Costa Rica. [EN LINEA], octubre, 2017., 8, p. 59. Disponible en

- Balance Cibercrimen Colombia 2017 [En línea]. Centro cibernético policial. Diciembre, 15,201., Disponible en

- BALANTA, Heidi, Legislación que Protege la Información en Colombia, [en línea], Junio, 2014., Disponible en:
- BOLAÑOS DIAZ, Andrés; NARVAEZ, Teresa de Jesús. Análisis Comparativo Sobre Delitos Informáticos En Colombia Con Relación A Seis Países De Latinoamérica. 2014. [En Línea]. 100p.Disponible en:

- Dos de cada 10 empresas, víctimas de robo de datos [En línea]. En: Periódico El tiempo. Abril, 2013., 1 p. Disponible en:

- El Centro Cibernético de la Policía Nacional y la CCIT presentaron el Primer Informe sobre el [38] Cibercrimen en Colombia. [EN LINEA], Cámara Colombiana de Informática y Telecomunicaciones. Marzo, 31, 2017., Disponible en:

- Estamos preparados en América Latina y el Caribe.2016, [En línea]. Banco Interamericano de Desarrollo, 193p.Disponible en:

- Este año, fraudes cibernéticos han costado US$ 500 millones,[en línea], Noviembre,2011., Disponible en:

- Los sectores económicos más impactados por el cibercrimen en Colombia [En línea]. En: Periódico Dinero. Septiembre, 9, 2017., 1 p. Disponible en

- Informe Amenazas del Cibercrimen en Colombia 2016 - 2017 Marzo, 2017,15p. Disponible en

- Perspectivas de la OCDE sobre la economía digital 2015 [EN LINEA], Microsoft, 2015., 326p. Disponible en:

- POLICY GUIDELINES ON CYBERSECURITY AND CYBERDEFENSE. [EN LINEA], Julio, 2011., 43, p. Disponible en:

- RENDÓN LÓPEZ, Diana María. La eficacia de la prueba digital en el proceso penal colombiano. [EN LINEA], 2012. Tesis de Licenciatura. Universidad de Medellín, 29p., Disponible en:

- VÁSQUEZ ZARATE, Katy Alejandra; CÁRDENAS RODRÍGUEZ, María Paula. Propuesta de buenas prácticas para fortalecer los controles de prevención y detección temprana del cibercrimen en las empresas colombianas. [EN LINEA], 2015. Tesis de Licenciatura. Facultad de Ciencias Económicas y Administrativas Disponible en:

- WIGHT, Andrew, Colombia seis tripling off economic impact of fraud, corruption, cyber crime, [en línea] En: Colombia Reports, Noviembre, 2013., Disponible en

- [48]WIRE, Andrean, Cibercrimen: un riesgo constante de las PYMES [En Línea]. Colombia. Diciembre, 1 ,2017., 1p. Disponible en http://colombiaempresarial.com.co/2017/12/01/cibercrimen-un-riesgo-constante-de-las-pymes/y_contable/links/5a143bf0aca27240e308f614/Segundo-Congreso-Internacional-Crimen-economico-y-fraude-financiero-y-contable.pdf#page=59

- NIÑO WILCHES, Yamith, IMPORTANCIA DE LA IMPLEMENTACIÓN DEL CONCEPTO DE CIBERSEGURIDAD ORGANIZACIONAL EN LAS ORGANIZACIONES TIPO PYMES. [EN LINEA], 2015. Maestría Gestión de Organizaciones. Universidad Militar Disponible en: