ESTUDIO DE LA EFICIENCIA Y EFICACIA DE LAS METODOLOGÍAS HARDENING EN LA REDUCCIÓN DE VULNERABILIDADES EN LAS EMPRESAS COLOMBIANAS

ÁLVARO AUGUSTO FUENTES FORERO

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SAN VICENTE DEL CAGUÁN

2020

ESTUDIO DE LA EFICIENCIA Y EFICACIA DE LAS METODOLOGÍAS HARDENING EN LA REDUCCIÓN DE VULNERABILIDADES EN LAS EMPRESAS COLOMBIANAS

ÁLVARO AUGUSTO FUENTES FORERO

Monografía como requisito para optar al título de:

Especialista en Seguridad Informática

Tutor:

Msc. Katerine Márceles Villalba

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SAN VICENTE DEL CAGUÁN

2020

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

San Vicente del Caguán, julio de 2020

RESUMEN

En la presente monografía denominada “El estudio de la eficiencia y eficacia de las metodologías hardening en la reducción de vulnerabilidades en las empresas colombianas”, busca en un principio conocer el estado en ciberseguridad en que se encuentra este gran segmento del mercado y plantea señalar el conjunto de medidas básicas que permitirán mejorar la seguridad y reducir los incidentes en los equipos de cómputo con sistemas operativos Windows en empresas de ese país.

La monografía cuenta con tres objetivos específicos los cuales servirán de guía a las PYMEs colombianas que buscan alcanzar el aseguramiento de sus sistemas informáticos, para lo cual requirieran reducir las posibilidades de ser afectados por ataques recurrentes y minimizar el número de vulnerabilidades al implementar las medidas expuestas en el documento, las cuales van desde el cambio de contraseñas, desinstalar software no seguro, eliminar las credenciales de usuarios, deshabilitar servicios que no serán usados y fortalecer las configuraciones de aquellos que estarán en uso.

A pesar de que este documento este enfocado en las PYME, también servirá de guía para que otro tipo de entidades de carácter público y privado e incluso particulares que busquen mejoras de seguridad informática.

PALABRAS CLAVE: Endurecimiento, Sistema Operativo, Seguridad Informática, Sistemas Endurecidos, Pequeña Y Mediana Empresa (Pyme), Ransomware, Copia De Seguridad, Phishing, Malware, Vulneración De Correo Electrónico De Empresas (Bec), Defensa En Profundidad.

ABSTRACT

In this monograph called "the study of the efficiency and effectiveness of hardening methodologies in reducing vulnerabilities in Colombian companies" seeks initially to know the state of cybersecurity in which this large segment of the market is located and suggests pointing out the whole of basic measures that will improve security and reduce computer equipment incidents with Windows operating systems in SME in that country.

The monograph has three specific objectives which will serve as a guide for Colombian SMEs that seek to achieve the assurance of their systems, reduce the possibility of being affected by recurrent attacks and their number of vulnerabilities when implementing the measures set forth in the document. which range from changing passwords, uninstalling unsecured software, removing user credentials, disabling services that will not be used and strengthening the settings of those that will be in use.

Although this document is focused on small and medium enterprises, it will also be useful for other types of public and private entities and even individuals that have a similar situation and set the goal of achieving the same objective.

KEYWORDS: Hardening, Operating System, Informatic Security, System Hardening, Small Medium Enterprise (Sme), Ransomware, Backup, Phishing, Malware, Business Email Compromise, Defense In Depth.

CONTENIDO

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pag.

GLOSARIO

Activos: Es un bien que posee una empresa.

Copia de Respaldo: es el procedimiento disponible que se tiene para restaurar la información en el evento que los archivos originales se presente alguna perdida o daño.

Fortalecer la seguridad del sistema: Es un proceso que elimina la mayor cantidad de riesgos que puedan afectar la seguridad, a través de la desinstalación de programas, protocolos, servicios y utilidades del sistema que sean innecesarios.

Información: Conjunto organizado de datos procesados, que resultan significativos para la empresa.

Phishing: Es un ataque que busca a través de estrategias como la ingeniería social de convencer al atacado a través de la suplantación de identidad.

PyME: Pequeña y mediana empresa.

Reforzado: Configurar un computador u otro dispositivo de red para resistir ataques.

Sistema Operativo (SO): Es el primer programa instalado en un equipo, es un programa maestro sobre el cual corren las aplicaciones, es el encargado del manejo de los recursos del sistema.

Cifrado EFS: Los sistemas operativos Windows desde el año 2000 cuentan con un sistema de cifrado por defecto denominado EFS (Encrypting File System), el cual se usa para proteger los datos individualmente vinculados a un usuario específico.

INTRODUCCIÓN

Gran parte del desarrollo económico de un país está ligado directamente a las pequeñas y medianas empresas, estas han venido incursionando con sus productos y servicios a nivel mundial a través de la internet, llevándolas a asumir nuevos retos que en el campo de la seguridad informática se les exige contar con una línea de defensa que le permita proteger su apartado productivo y sus activos de información.

El proceso de hardening o endurecimiento de sistemas, se presenta como una excelente alternativa para solventar estas necesidades, teniendo en cuenta que genera grandes beneficios desde el primer momento de su implementación y gracias a su flexibilidad, se adapta fácilmente a el presupuesto que suelen destinar las PyMES para el apartado de la seguridad informática.

El proceso de hardening en los sistemas operativos Windows, crea nuevas “capas” de seguridad o barreras que aseguran los navegadores, los documentos y los programas que corren en la máquina asegurada, dificultando que estos sean comprometidos en ataques por delincuentes informáticos.

Entre los pasos que se realizan en el hardening está actualizar y aplicar los parches de seguridad vigentes, monitorear las actividades sospechosas que se ejecuten en segundo plano y estar actualizados sobre el panorama de amenazas que se ciñen sobre estos sistemas con el fin de brindar una respuesta oportuna frente a nuevas amenazas.

Se selecciona este tema, considerando que a pesar de los potenciales beneficios que ofrece, no ha tenido un gran despliegue en las pequeñas y medianas empresas de Colombia. Por lo anterior, este documento contiene un problema; una justificación; un objetivo general y tres objetivos específicos; un marco referencial que contiene marco conceptual y marco legal; el desarrollo de estos pasos permitirá entender las buenas practicas que necesarias para endurecer los equipos con sistemas operativos Windows.

1. PLANTEAMIENTO DEL PROBLEMA

Las empresas colombianas hoy en día si aún no han migrado al mundo digital, planean hacerlo a corto plazo, debido al potencial que encuentran en la red de redes para brindar sus servicios, desde una plataforma donde puedan permanecer conectados las 24 horas con sus potenciales clientes. Esto puede llegar a generar el riesgo de ser atacados física y virtualmente por personas inescrupulosas, ya sea con fines de espionaje corporativo, razones políticas o personales, extorsiones, o como plataforma para atacar a una entidad aún más grande. Según artículo del diario el país (España) el 53% de las pequeñas y medianas empresas reconocieron haber sufrido ciberataques durante el 2017, una cifra alarmante que alcanzó tal punto debido a que estas entidades no cuentan con una infraestructura mínima requerida (personal calificado y equipos).

Las organizaciones efectivas deberían tener una línea base de seguridad en sus equipos, que garanticen un nivel mínimo satisfactorio de seguridad, pero las PYMEs no suelen prestar atención a los problemas que conlleva no contar con los hardware y software apropiados que garanticen su seguridad informática. Esto se debe generalmente al poco nivel de formación y de información con la que cuentan a la hora de tomar decisiones en ese campo.

Los emprendedores y gerentes suelen capacitarse en temas como mercadeo, publicidad y ventas; sin embargo, no se forman en los conceptos básicos de seguridad y del tratamiento adecuado de debe recibir la información, a pesar de que no se esperaría un conocimiento técnico altamente especializado, los directivos deberían tener niveles aceptables de conocimiento en los campo básicos de la seguridad informática que le permitan entender la importancia del cifrado de la información, políticas de seguridad y protección de datos, acuerdos de confidencialidad, manejo de incidentes, etc.

El hardening permite realizar un análisis de vulnerabilidades enfocado en encontrar fallas de seguridad y medir el impacto que estas tienen sobre los activos de la entidad, identificando estas falencias se establece un plan con los pasos necesarios para fortalecer y soportar ataques a los que los sistemas estarían siendo expuestos.

1.1 FORMULACIÓN DEL PROBLEMA

¿Qué tipos de acciones de hardening se pueden implementar en las PyMES Colombianas para reducir las vulnerabilidades de los sistemas que soportan los servicios críticos de esas organizaciones?

2. JUSTIFICACIÓN

El hardening o endurecimiento es un método que busca implementar estrategias que mejoren la seguridad de los sistemas, es un tema amplio que cuenta con bastante relevancia, de acuerdo al aumento que están teniendo los delitos informáticos a nivel mundial, donde los atacantes han enfocado sus esfuerzos a realizar ataques dirigidos a empresas[1], porque ahí consiguen una mayor rentabilidad, contrario a lo que sucedía al atacar a las personas del común, considerando que este tipo de organizaciones por su naturaleza manejan mayores recursos económicos.

El enfoque que se le da al documento en el de los sistemas Windows, contando con un campo de aplicación grande, esto genera una respuesta válida en la resolución de incidentes relacionados con la seguridad informática, debido a la popularidad de ese sistema operativo[2], el cual está presente en la mayoría de estaciones de trabajo y servidores que usan las PYMEs en Colombia, es otro factor determinante por parte de los delincuentes informáticos, los cuales priorizan las afectaciones a equipos de ese ecosistema.

El hardening es versátil, ofrece es la flexibilidad en su implementación, funciona correctamente en cualquier tamaño de la organización, se adapta a todo tipo de presupuestos y ofrece resultados positivos desde el primer momento de su implementación.

Llama la atención la poca implementación del hardening, evidenciándose en los últimos un aumento en los incidentes de seguridad reportados, deduciendo que no se han presentado cambios importantes en la inversión que realizan las PYMEs para minimizar su afectación[3], este estudio se presenta como una guía para mejorar esa situación a partir de recursos que tienen a su disposición.

[1] Ataques dirigidos. En: Kaspersky [en línea]. 16 de febrero de 2017. [Consultado: Mayo 3 de 2019]. Disponible en: https://latam.kaspersky.com/resource-center/threats/targeted-virus-attacks.

[2] CRUZ, Claudia. Windows 10 es el sistema operativo más usado del mundo En: CNET [en línea]. Enero 2 de 2019. [Consultado: 3 mayo de 2019] Disponible en:https://www.cnet.com/es/noticias/windows-10-es-el-sistema-operativo-mas-usado-en-las-computadoras-del-mundo/)

[3] ALVAREZ, Wendy. ¿Es la innovación en las pymes colombianas una estrategia para el comercio internacional?, Bogotá, 2014, 23 p, Ensayo. Universidad Militar Nueva Granada.

3. OBJETIVO GENERAL

Estudiar la metodología Hardening y el impacto que esta tendría en las pequeñas y medianas empresas de Colombia al reducir sus vulnerabilidades a ciberataques, a través de la recopilación y análisis de la bibliografía sobre esta temática, para lo cual se referenciarán herramientas de análisis y protección con el fin de evidenciar su eficiencia y eficacia.

3.1 OBJETIVOS ESPECIFICOS

- Realizar un diagnóstico de la situación del estado actual de la seguridad informática en las PYMES colombianas.

- Analizar las implicaciones que tendrían los equipos de cómputo con sistema operativo Windows al implementarse el hardening.

- Identificar las ventajas que tienen las herramientas como el Antivirus, sistema de detección de Intrusos, contraseñas y criptografía para mejorar la seguridad informática de los equipos de cómputo de las empresas.

4. MARCO REFERENCIAL

A continuación, mediante los diferentes ítems que componen el marco referencial se desglosarán los conceptos y antecedentes de la temática a profundizar.

4.1 MARCO CONCEPTUAL

Gracias a la globalización, la acelerada transformación tecnológica y la evolución que ofrecen las ventas en línea, ha llevado a las empresas colombianas a buscar llevar sus negocios a un nuevo nivel, donde sus productos y servicios se encuentren permanente disponibles y al alcance de cualquier potencial cliente, sin importar su ubicación, solo que este cuente con una conexión a internet.

La disponibilidad online conlleva a enfrentar retos y amenazas en materia de seguridad informática inéditos, con las que antes los empresarios no solían tratar, en especial como lo menciona un artículo de la revista Dinero[4] las PYMES colombianas no están acostumbradas a realizar inversiones significativas para prevenir ciberataques, teniendo pocas medidas de protección o nulas u obsoletas.

Mientras tanto la cibercriminalidad constantemente innova en su actuar criminal aprovechando las falencias y fisuras que encuentran disponibles, en especial en los mercados emergentes como son los países latinoamericanos, donde existe una pobre cultura en materia de ciberseguridad.

Para entender las implicaciones y bondades del hardening en primer lugar se debe entender la importancia de algunos términos, el primero de ellos es Vulnerabilidad, de acuerdo al Instituto Nacional de Ciberseguridad, esta se representa como "una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma"[5], estos fallos suelen venir de sistemas con problemas de diseño, equipos u software mal configurado, o falta de la implementación de procedimientos estandarizados, las vulnerabilidades deben ser identificadas y generar acciones que las eliminen.

---

[4] Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad. En: Revista Dinero. [en línea]. [Citada: 16 oct. 2019] https://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201

[5] Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? En: Instituto nacional de ciberseguridad. [en línea]. [Citada: 25 nov. 2019]. https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

Por otro lado, se tiene a las Amenazas, las cuales de acuerdo al mismo autor en el mismo artículo son "toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información" en otras palabras estas buscan afectar a los activos informáticos, generalmente son materializadas a través de ataques (robo, fraudes o malware), fenómenos naturales (inundaciones, incendios, o sobrecargas eléctricas) o desidia corporativa (mala implementación de protección de credenciales de acceso, no usar cifrado para proteger información sensible).

Siempre que exista una vulnerabilidad, habrá quien busque explotarla y obtener beneficios con esa acción, esto introduce otro de los términos de igual importancia conocido como el riesgo, el cual se define como "la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños."[6]

El hardening es una medida de seguridad que se aplica a las organizaciones con el fin de eliminar algunas de las causas más probables de generación del riesgo, al adoptar controles que mitiguen la posibilidad de su materialización.

Previa a la implementación del hardening es importante conocer el entorno a proteger, según el autor Marino del Río "No hay retorno de inversión más real que conocer el entorno que intentamos proteger, su comportamiento y particularidades"[7] por lo tanto el aseguramiento consiste en primer lugar en conocer detalladamente todo el funcionamiento de la empresa y todos los activos que se deben proteger.

4.2. MARCO LEGAL

4.2.1. Ley 527 de 1999[8]

Mediante esta ley se reglamentó el uso de la figura conocida como mensajes de datos, de las firmas digitales y su implementación en las transacciones comerciales, el objetivo principal es el de generar seguridad con el intercambio y manejo de la información de los establecimientos comerciales y de las entidades del estado.

---

[6] Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?. [en línea]. En: Instituto Nacional de Ciberseguridad. Mayo 3 de 2019 [Consultado: 25 noviembre de 2019] disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

[7] DEL RIO, Mariano M. La importancia de conocer el entorno a proteger [en línea]. En: Instituto Nacional de Ciberseguridad. Mayo 8 de 2019 [Consultado: 25 noviembre de 2019]. Disponible en: https://www.incibe-cert.es/blog/la-importancia-de-conocer-el-entorno-a-proteger.

[8] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1999

Se establece que una firma digital es válida solo cuando esta es personal e intransferible y está ligada a la información del mensaje, por otro lado se fija la normatividad de las entidades certificadoras, las cuales regulan y avalan que las firmas digitales tengan validez.

4.2.2. Ley 1266 de 2008[9]

Mediante esta legislación se reguló la administración de la información de bases de datos personales, especialmente en los sectores bancario, comercial y de servicios, esta ley se suele denominar como Habeas Data.

Para la realización de este documento se considera como un insumo importante teniendo en cuenta que las PYMEs realizan recolección y tratamiento de datos personales por lo ese tipo de información es uno de los activos críticos a proteger.

4.2.3. Ley 1273 de 2009[10]

En esta ley se incluyó en el Código Penal Colombiano, un nuevo bien jurídico que se denominó "de la protección de la información y de los datos", con la intención de proteger integralmente los sistemas de información y los datos, bajo esta norma se designan algunas conductas como delitos informáticos, entre las cuales se encuentra el Acceso abusivo a un sistema informático, Daño Informático, Uso de software malicioso, Suplantación de sitios web, entre otros.

4.2.4. Ley 1581 de 2012[11]

Esta norma genera las pautas sobre el manejo de la información personal, ordenando que se garantice la protección, almacenamiento y el correcto uso de ese tipo de datos, en ella se facultó para que la Súper Intendencia de Industria y Comercio ordenara la inscripción de todas las bases de datos personales que administras los establecimientos comerciales en el Registro Nacional de Bases de Datos (RNBD).

---

[9] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008

[10] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 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. Diario Oficial. Bogotá, D.C., 2009

[11] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012

Los establecimientos que realicen las siguientes actividades se verán cobijados por esta normatividad: recolección de datos personales de clientes, proveedores, contratistas y/o empleados; almacena, usa o circula datos personales de forma física o digital; No cuenta con un manual de políticas y procedimientos de protección de datos personales.

4.2.5 Reglamento General de la Protección de Datos GDPR[12]

Es una normatividad enfocada al tratamiento y protección de datos personales, afecta a todas las empresas con base en la Unión Europea, que tengan sedes en ella, que recopilen datos de personas residentes o que elaboren proyectos con empresarios radicados en esa jurisdicción.

De acuerdo a este reglamento los datos personales especialmente protegidos son los de origen personal, genético, biométrico, médico, entre otros, a los cuales se les debe garantizar un tratamiento y niveles de seguridad especiales.

La norma tiene una serie de principios relativos al tratamiento de los datos, algunos de ellos se pueden encasillar de la siguiente forma: legalidad, lealtad y transparencia; con fines determinados, explícitos y legítimos, sin que se le pueda dar otro uso distinto; adecuados, pertinentes y limitados a lo estrictamente necesario; exactos y actualizables, cuando se comprueben que no lo son.

5. DIAGNOSTICO DE LA SITUACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LAS PYMES COLOMBIANAS

En Colombia de acuerdo al marco jurídico[13] una PYME es una empresa donde los activos se encuentran entre 501 S.M.L.V (Salarios mínimos legales vigentes) y 15.000 S.M.L.V.

De acuerdo a un artículo publicado el 09/02/2015 en la revista Dinero[14]: “Las pymes representan el 99,9% del total de las empresas en Colombia, cerca de 1,6 millones de unidades empresariales[2].” En esta misma publicación se evidencia que estas empresas representan un segmento importante para la economía, teniendo en

[12]UNIÓN EUROPEA. PARLAMENTO EUROPEO. Reglamento general de protección de datos (27, abril, 2016). Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. EUR-Lex. Bruselas. 2016

[13] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 590. (10, julio, 2000). Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa. Diario Oficial. Bogotá, D.C., 2000

[14] Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad. En: Revista Dinero. [en línea]. [Citada: 16 oct. 2019] https://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201

cuenta que aportan el 38% del PIB Total de la nación, pero al encontrarse con dificultades del mercado solo el 50% de las PYMEs sobreviven al primer año y el 20% al tercero.

Es importante resaltar que en Colombia el 95% de las PYMEs son familiares[15], esto genera que no exista una diferenciación en la administración empresarial con la familiar, causando que en la mayoría de las situaciones se mezclen esos presupuestos, limitando claramente la inversión en desarrollo de nuevos productos y asimismo en seguridad informática.

A pesar de que esta situación es evidente entre los emprendedores, estos dudan en invertir en investigación y desarrollo, teniendo en cuenta que suelen depender de sus negocios de forma temprana y se enfocan en generar rentabilidad en el corto plazo[16].

Una de las principales causas de esta situación es la falta de interés que se le da a la hora de invertir en los segmentos importantes como son la innovación y el conocimiento[17], por lo cual se reduce su competitividad ante sus homologas que se encuentran en los países desarrollados.

Puntualmente esta situación se evidencia de acuerdo a una encuesta realizado por una empresa de consultoría de seguridad informática: “En Colombia más del 50% de las empresas mantuvieron o disminuyeron los recursos asignados a evitar ataques informáticos en el 2016”[18]. En la Encuesta Anual de Seguridad de la información[19], realizado por la empresa EY, se informa que en Colombia el 78% de las PYMEs en conjunto invierten menos de US$ 1 millón, para evitar los ataques informáticos.

5.1. PANORAMA DE INCIDENTES RELACIONADOS CON LA SEGURIDAD INFORMÁTICA

Hace una década fueron reemplazadas las personas que creaban los primeros archivos con malware por ocio y diversión (mal denominados Hackers), por organizaciones de crimen organizado internacional, los primeros mencionados

[15] Ibídem

[16] MENDEZ, Javier. 10 errores de seguridad que su pyme NO debe cometer. [en línea]. En: Revista Enter. Abril 24 de 2019. [Consultado 3 mayo de 2019] Disponible en: https://www.enter.co/especiales/empresas/10-errores-de-seguridad-que-su-pyme-no-debe-cometer/

[17] Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad. En: Revista Dinero. [en línea]. [Citada: 16 oct. 2019] https://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201

[18] Ibídem

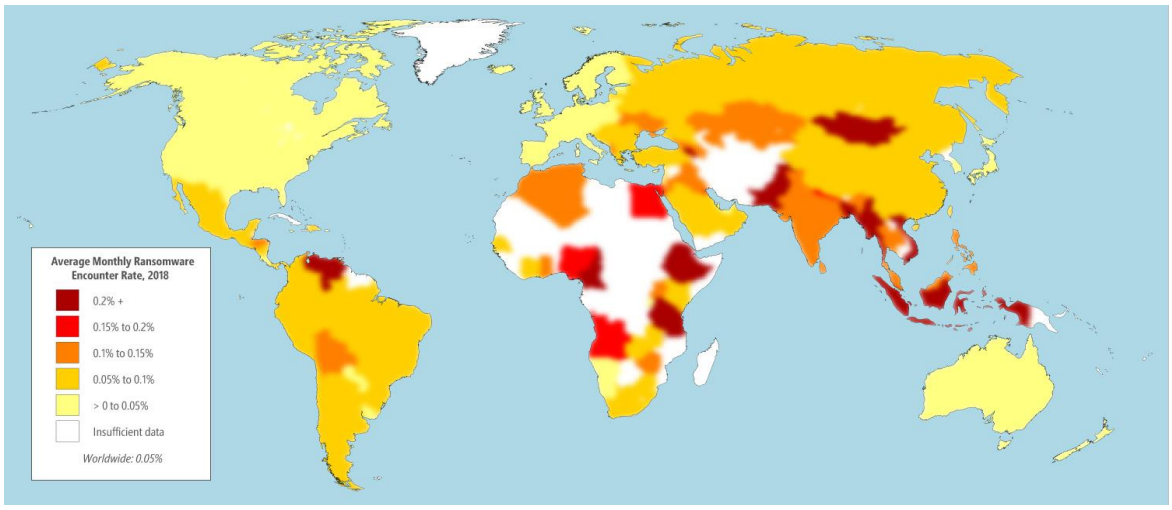
[19] EY, Encuesta Global de Seguridad de la Información 2018-19. Bogotá: EY, 2019. p. 37.

realizaban ataques que resultaban muy evidentes para sus víctimas y estos últimos optaron por generar ataques silenciosos que les permitían permanecer durante más tiempo realizando actividades maliciosas.

Los ataques a sistemas informáticos que generaron mayor preocupación a nivel mundial durante el año 2017 fueron los relacionados con ransomware (código malicioso que cifra los archivos de los sistemas y pide un rescate a modo de extorsión), donde se destacaron los denominados WannaCrypt y Petya, esto género que las organizaciones tomaran conciencia en las falencias que lo facilitaban y a pesar de que se esperaba un aumento paulatino de esta modalidad, en el 2018 se redujo.

Según el informe de inteligencia de seguridad de Microsoft # 24[20] Durante el año 2018 el país latinoamericano mayormente afectado por el código malicioso ramsonware fue Venezuela, con una tasa promedio mensual de 0.31 incidentes, seguido de Bolivia que se encuentra en el rango del (0,10% al 0,150%), Colombia se encuentra junto a la mayoría de los países vecinos situados entre el rango (0,05% al 0,10%) de incidentes mensuales como se puede apreciar en la ilustración 1.

Ilustración 1. Tasas de encuentros de ransomware 2018.



Fuente: Informe de inteligencia de seguridad de Microsoft volumen 24 enero a diciembre de 2018. Disponible en info.microsoft.com

Según el informe de inteligencia de seguridad de Microsoft # 24[21], donde se analizó el comportamiento de los ataques cibernéticos: “En 2018, los atacantes utilizaron

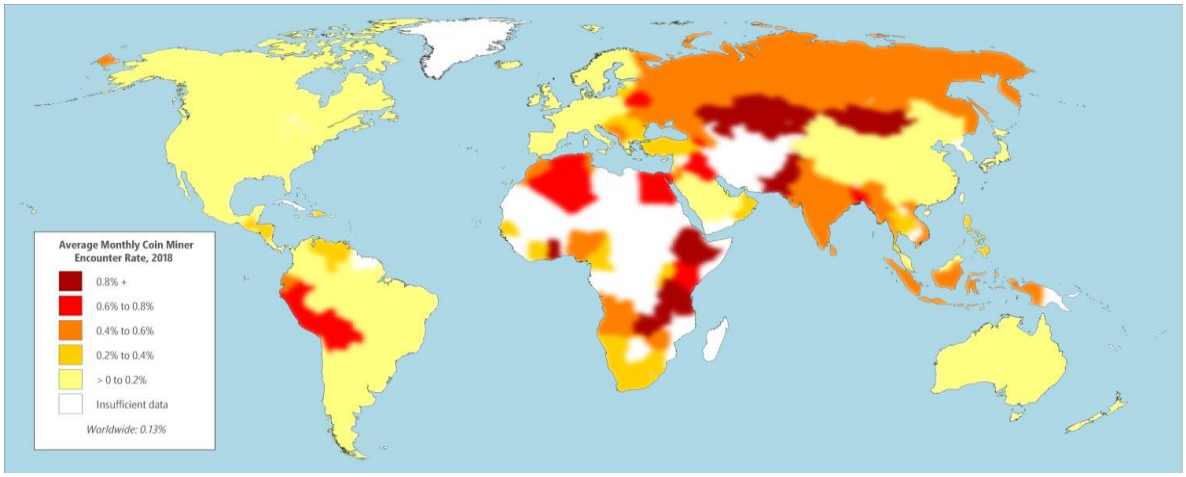
[20] MICROSOFT, Informe de Inteligencia de Seguridad de Microsoft. Redmond: SIRT, 2019. p. 9.
[21] Ibídem, p. 10.

diferentes artimañas, tanto nuevas (minería de moneda o coin-mining) como antiguas (suplantación de identidad o phishing)"[22], en su búsqueda continua de robar datos y recursos a clientes y organizaciones.

Actualmente los cibercriminales estarían dejando a un lado el ransomware y enfocando sus esfuerzos en realizar ataques donde pueden acceder y "robar" los recursos de los equipos de sus víctimas para generar el minado de criptodivisas, lo que se permite demostrar que estas personas son oportunistas sin escrúpulos buscando la forma más sencilla de adquirir rentas criminales.

Revisando el panorama regional[23] en este aspecto durante el 2018, los países mayormente afectados por esta modalidad son Bolivia y Perú, los cuales se encuentran en un rango de 0,60% a 0,80% incidentes por mes, seguidos de Venezuela y Ecuador los cuales se encuentran en un rango de 0,40% a 0,60% incidentes mensuales, Colombia se encuentra junto a la mayoría de los países del cono sur entre el rango de 0 a 0,20%, como se puede apreciar en la ilustración 2.

Ilustración 2. Tasas de encuentros de minería de moneda 2018.



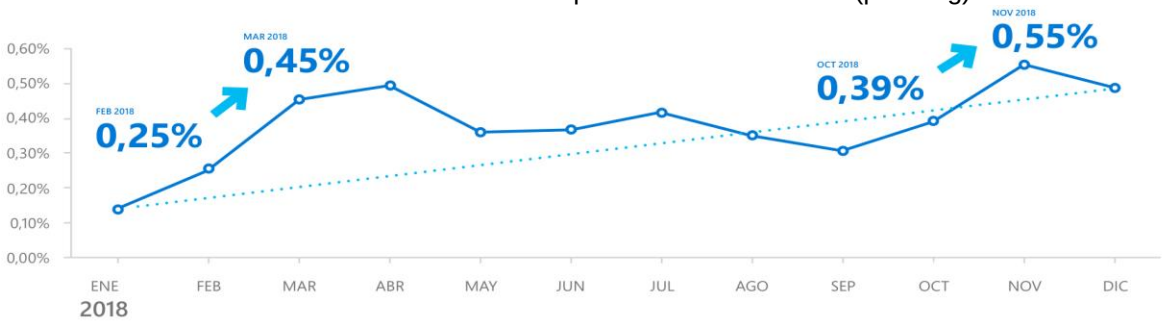
Fuente: Informe de inteligencia de seguridad de Microsoft volumen 24 enero a diciembre de 2018. Disponible en info.microsoft.com

En la ilustración 3 se evidencia un aumento en los clics que se dan a los enlaces relacionados con la suplantación de identidad (phishing), convirtiéndose en el tipo de ataque predilecto por los atacantes, los cuales son facilitados por la interacción humana de los usuarios, de acuerdo al análisis realizado por Microsoft[24], sobre la proporción de correos electrónicos entrantes se detectó: "un aumento del 250 por ciento entre enero y diciembre de 2018 de mensajes de suplantación de identidad

[22] Ibídem, p. 11.
[23] Ibídem, p. 9.
[24] Ibídem, p. 11.

(phishing)" pero a su vez se produjo una mitigación de daños con la implementación de nuevos modelos de machine learning que capturan estos fenómenos.

Ilustración 3. Correos electrónicos de suplantación de identidad (phishing) en 2018.



Fuente: Informe de inteligencia de seguridad de Microsoft volumen 24 enero a diciembre de 2018. Disponible en info.microsoft.com

El malware genera grandes retos para las PYMEs y la población en general, pues esta práctica causa perdida de información, reducción de la usabilidad, afectaciones a la propiedad intelectual, entre otras cosas[25], de acuerdo al análisis realizado por Microsoft[26]: "Las tasas de encuentros de malware oscilaron entre alrededor del 5 por ciento y más del 7 por ciento en 2017, a principios de 2018 se elevaron antes de disminuir durante la mayor parte del año a poco más del 4 por ciento"[27], esta empresa señala que la probable causa de esta disminución se deba a la aceptación masiva que están teniendo las personas y empresas al migrar al sistema operativo Windows 10, el cual cuenta por defecto con la herramienta de protección Windows Defender que ha tenido un buen comportamiento en la detección de malware, generando beneficios tangibles en la comunidad que lo adoptó.

No obstante, durante el año 2018, los países mayormente afectados por los diferentes tipos de malware fueron[28]: Venezuela y Bolivia con una tasa de encuentros mensuales del 12,00% al 16,00%, seguidos en la lista por Ecuador, Brasil y Perú, los cuales se encuentran entre un rango del 8,00% al 12,00% de encuentros por mes, y finalmente Colombia, Paraguay, Uruguay y Argentina, los

[25] MARTINELLI, Carlos. Cuáles son los problemas más frecuentes de Seguridad Informática [video]. YouTube, TECHcetera (6 de diciembre de 2016). 5:55 minutos. [Consultado: 12 de octubre de 2019]. Disponible en https://www.youtube.com/watch?v=cNIoTyKldj4

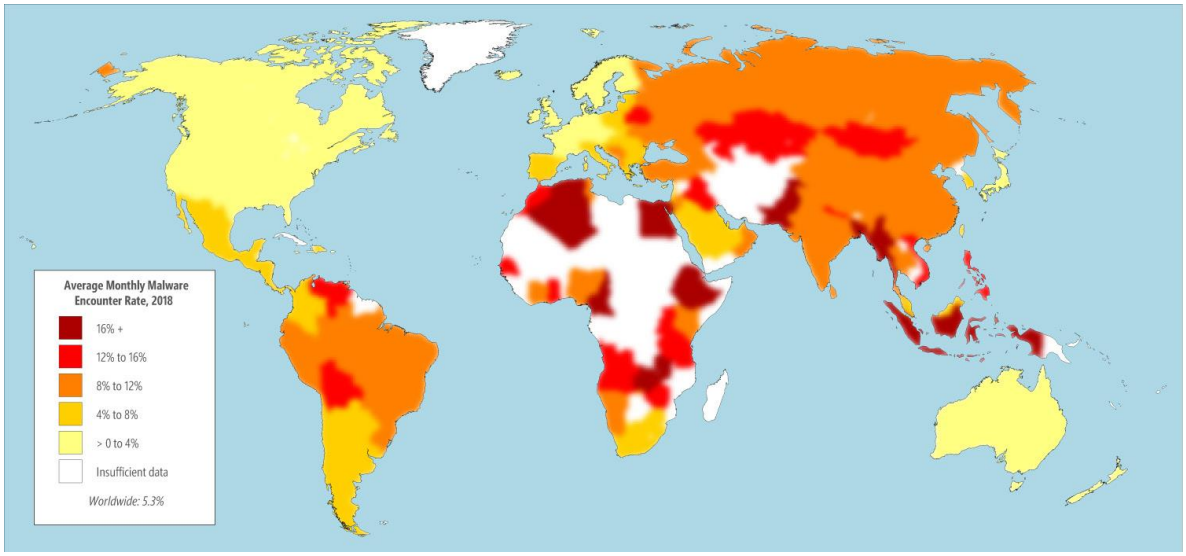
[26] MICROSOFT, Informe de Inteligencia de Seguridad de Microsoft. Redmond: SIRT, 2019. p. 9.

[27] Ibídem p. 25.

[28] Ibídem p. 25.

cuales se encuentran en la parte más baja de la tabla entre un rango del 4,00% al 8,00% en encuentros mensuales como se puede apreciar en la ilustración 4.

Ilustración 4. Media mensual de tasas de encuentros de malware en 2018.



Fuente: Informe de inteligencia de seguridad de Microsoft volumen 24 enero a diciembre de 2018. Disponible en info.microsoft.com

5.1.1. Panorama de incidentes relacionados con la seguridad informática en Colombia

De acuerdo a boletín difundido por el CAI Virtual en Colombia[29], el cibercrimen presenta un aumento exponencial en el país, teniendo en cuenta que en el 2017 aumentó un 28.3%, se señala que "La principal modalidad que afecta a los ciudadanos y empresas en el país son las estafas, bien sea a través de un correo electrónico, un mensaje de texto, una llamada, una falsa oferta de empleo o una estafa de compra online."

De acuerdo a la Encuesta Global de Seguridad de la Información 2018-19[30], los ataques informáticos están concentrados en las principales ciudades del país (Bogotá, Cali, Medellín, Barranquilla, Cartagena y Bucaramanga), teniendo en cuenta que es ahí donde se concentran la mayor cantidad de empresas y ciudadanos con acceso a internet.

Usando el carding (comercialización de datos de tarjetas de débito y crédito) los cibercriminales generaron perdidas en el país por aproximadamente 60.000

[29] POLICIA NACIONAL DE COLOMBIA. Informe: Balance Cibercrimen en Colombia 2017. Bogotá: Centro Cibernético Policía Nacional, 2017. p. 1.
[30] EY, Encuesta Global de Seguridad de la Información 2018-19. Bogotá: EY, 2019. p. 37.

millones de pesos; asimismo mediante la suplantación de correo corporativo los atacantes generaron perdidas en promedio de 380 millones en cada caso.

El ramsonware afectó en el país al segmento conformado por las PYMEs, generando durante el año 2017[31], se atendieran el CAI virtual a 52 víctimas, que denunciaron ser afectados por este programa malicioso, previamente se habían presentado 14 casos en el 2015 y 84 en el 2016, en la mayoría de casos se evidenció que la infección surgió a través de dar clic a archivos anexos en correos spam.

A nivel local, es importante resaltar que es uno de los ataques que más afectan a las empresas del país, según datos del Centro Cibernético Policial: "la suplantación de correo corporativo (tipo BEC)[32], que puede dejar una pérdida de 380 millones de pesos en cada ataque"[33], un ejemplo de ello se muestra en la ilustración 5.

Ilustración 5. Ejemplo de phishing simulando a Davivienda

Fuente: Phishing al Banco Davivienda. Disponible en Segu-Info.com

[31] POLICIA NACIONAL DE COLOMBIA. Informe: Balance Cibercrimen en Colombia 2017. Bogotá: Centro Cibernético Policía Nacional, 2017. p. 3.

[32] Las estafas en las que se utiliza el email corporativo crecerán un 69%. En: IT Digital Security [en línea]. 25 de enero de 2018. [Consultado 8 mayo de 2019]. disponible en: https://www.itdigitalsecurity.es/vulnerabilidades/2018/01/las-estafas-en-las-que-se-utiliza-el-email-corporativo-creceran-un-69

[33] El secuestro de información desangra a las empresas del país. Bogotá, Periódico Portafolio (enero 29 de 2019).

5.1.2. ¿Por qué deben invertir en Seguridad Informática las PYME?

Hoy en día la información se considera uno de los activos más importantes de las compañías, a pesar de ser un bien intangible, este genera ventajas competitivas importantes para quien lo posee, incluso si estas ideas se encuentran en periodo de investigación y aún no se han puesto en práctica.

Un nuevo producto contiene formulas, propiedades, costos, campañas de mercado, en fin, reflejan una inversión monetaria importante, realizada por la entidad que necesitan ser protegidos desde su procesamiento, almacenamiento, transmisión y modificación, la seguridad informática en este aspecto cobra vital relevancia porque todos estos procesos transcurren en equipos de cómputo.

5.1.3 Principales errores en seguridad informática cometidos por las Pymes Colombianas

Las empresas colombianas son vulnerables a ataques informáticos, debido principalmente a la falta de previsión, al no tomar en cuenta las medidas mínimas de seguridad y a errores humanos cometidos por los usuarios, los cuales son aprovechados por los atacantes, entre esos se tienen:

5.1.3.1 Negar que existen riesgos:

Actualmente sin importar el tamaño de la empresa, existe un interés por parte de los cibercriminales de generar ataques que les pueda representar adquirir dividendos ilegales.

Las empresas pequeñas suelen obviar las medidas de seguridad porque consideran que por su tamaño no serán objeto de interés para la cibercriminalidad, pero para estos sujetos el solo hecho de que una entidad recopile información personal de los clientes (algo que toda PyME realiza) generaría un beneficio.

5.1.3.2 No invertir en seguridad informática.

Los equipos y personal requeridos para proteger a la empresa de ataques informáticos podrían parecer demasiado costosos para los empresarios, teniendo en cuenta que no ven claramente redituable su inversión, como podría suceder con un gasto similar en otros campos de la organización, pero es importante darle a

conocer a los decisores que sin lugar a duda un incidente en seguridad podría causar un impacto enorme en la estabilidad de la entidad.

5.1.3.3 No contar con los sistemas actualizados

Mantener los sistemas actualizados es una de las practicas más importantes en materia de seguridad que puede realizar una organización, teniendo en cuenta que la gran mayoría de los ataques masivos se pueden prevenir simplemente realizando esta actividad.

5.1.3.4 El eslabón más débil es el humano

Analizando a la mayoría de ataques se encuentra como factor común, la implementación de estrategias relacionadas con ingeniería social, porque a pesar de que se realicen grandes inversiones en equipos o se mantenga actualizado los sistemas es difícil educar al ser humano para que evite ser víctima de uno de ellos.

5.1.3.5 Falta de capacitación en seguridad

En el país muy pocas empresas invierten en capacitación de su personal en temas relacionados con la seguridad informática, la cual es vital para protegerse al identificar de forma anticipada los vectores de ataque dirigidos a afectar al componente humano, de estos se puede mencionar la ingeniería social y correos tipo phishing.

5.1.3.6 No monitorear las actividades y equipos usados por los empleados

Teniendo en cuenta que cada vez es más común que los empleados ingresen a sus sitios de trabajo con dispositivos inteligentes equipados con cámaras e internet (lo cual en principio no se considera negativo, porque esos equipos son una herramienta que mejoran su desempeño con una inversión nula por parte de la compañía), es importante monitorear que información estarían recopilando y que vulnerabilidad existe con esa actividad, para esto se debe generar un protocolo que establezca que información puede guardar y bajo que principios.

6. IMPLICACIONES QUE HACEN NECESARIA LA IMPLEMENTACIÓN DEL HARDENING EN LAS PYMES COLOMBIANAS

De acuerdo a los errores antes mencionados, es conveniente realizar un diagnóstico en materia de ciberseguridad conociendo los principales ataques que pueden afectar a las Pequeñas y medianas empresas colombianas:

6.1 RANSOMWARE

Es un tipo de programa malicioso que impide ingresar a los sistemas operativos y archivos[34], con el ofrecimiento de revertir este proceso, se chantajea a la víctima, solicitando que realice un pago que puede variar desde criptodivisas, tarjetas de crédito, hasta el envío de fotos intimas entre otro tipo de peticiones, a la fecha se han identificado distribuciones en equipos con sistemas operativos Windows, Mac y Android[35].

La infección suele producirse a través de la distribución de correos electrónicos spam que suelen venir con archivos anexos o enlaces que parecerían legítimos, pero con artimañas que usadas en conjunto con la ingeniería social, logran que los usuarios accedan a ellos, materializando el ataque[36].

En un principio los ataques se enviaban de forma aleatoria, pero con el tiempo los atacantes al ver el potencial que tenía este método para la consecución de dinero, se enfocaron en afectar a empresas en las economías más grandes de latinoamerica, por este motivo durante el año 2018 de acuerdo a la empresa de seguridad informática ESET: "Los países de la región que cerraron el pasado año con más detecciones fueron Colombia (30%), Perú (16%) y México (14%)"[37] esto se visualiza en la ilustración 6.

Ilustración 6. Detecciones de FileCoder en Latinoamérica durante 2018.

Fuente::welivesecurity.com

[34] PAUS, Lucas. Ransomware: 10 formas en las que puede comportarse al infectar un sistema. En: WeLiveSecurity [en línea]. 29 de mayo de 2018. [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2018/05/29/formas-ransomware-puede-comportar-al-infectar-sistema/.

[35] Ransomware. En: Malwarebytes [en línea]. [Consultado 3 mayo de 2019] disponible en: https://es.malwarebytes.com/ransomware/.

[36] COBB, Stephen. El ransomware continúa siendo una amenaza peligrosa para las empresas. En: WeLiveSecurity [en línea]. Noviembre 7 de 2018 [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2018/11/07/ransomware-continua-amenaza-peligrosa-empresas/

[37] GIUSTO, Denise. Países más afectados por el ransomware en Latinoamérica durante 2018.

De acuerdo al blog malwarebytes[38] se considera que existen tres tipos de ransomware, Scareware, bloqueadores de pantalla y ransomware del cifrado, como se observa en la Tabla 1:

Tabla 1. Clasificación de Ransomware

Tipo	Observaciones
Scareware:	Son mensajes emergentes que aparecen haciéndole creer a la víctima que sus archivos están en peligro y que debe acceder ante las pretensiones del atacante, cuando realmente su información se encuentra a salvo. Teniendo en cuenta que es un programa que está diseñado para solo mostrar los mensajes, sucederá que, aún realizando el pago extorsivo, continuará el algoritmo advirtiendo sobre la presencia del supuesto malware **(nivel de amenaza baja).**
Bloqueadores de pantalla:	En este nivel el atacante logra generar un bloqueo de la pantalla del equipo de cómputo, generalmente aparecerá un mensaje de un ente gubernamental como CIA o FBI, informando que esta almacenando archivos que lo involucran con delitos como pornografía infantil, descarga de software, solicitando un pago para poder acceder a ellos, a pesar de esto los archivos no se encuentran cifrados **(nivel de amenaza media).**
Ransomware del cifrado:	Es en este nivel donde genera una afectación grave a la disponibilidad e integralidad de la información, teniendo en cuenta que se encuentra cifrada por el atacante y es casi imposible que un profesional logré restablecerla, generando que la solución sea que pague, sin tener ninguna garantía que recuperará los datos **(nivel de amenaza alta)[39].**

Fuente: Malwarebytes - Todo acerca del ransomware.

6.1.1 Evolución histórica

Históricamente el primer registro de esta práctica ilegal, se conoció en los años 80 cuando apareció el ransomware conocido como PC Cyborg o AIDS, el cual una vez alcanzaba el equipo de la víctima, cifraba los ficheros contenidos en la partición C: del equipo, posteriormente a esto generaba que el equipo se reiniciara unas 90 veces, para luego avisar que debía enviar a una dirección postal una cantidad de dinero para renovar una supuesta licencia.

[38] Malwarebytes - Todo acerca del ransomware.

[39] MENDOZA, Miguel. El impacto del ransomware en Latinoamérica durante 2017. En: WeLiveSecurity [en línea]. Marzo 1 de 2018. [Consultado 3 mayo de 2019] [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/

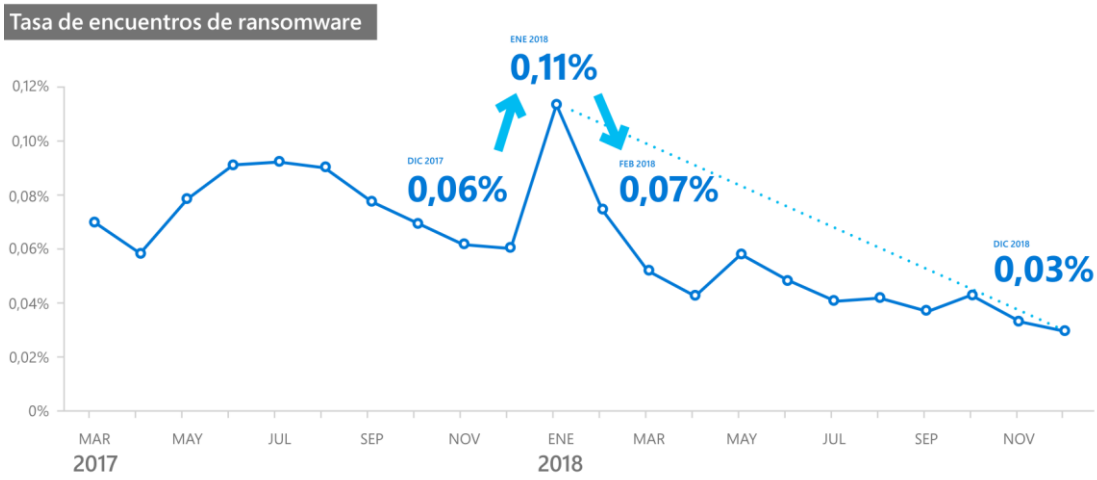
Posteriormente en el año 2004 apareció el ransomware llamado GpCode con un cifrado leve que pedía un rescate para recuperar los archivos, en el año 2007 se lanzó WinLock que se caracterizó por no cifrar archivos, sino que estuvo enfocado en bloquear las pantallas, mostrando imágenes pornográficas, exigiendo el envío de un SMS de pago para recuperar el control.

En el 2012 surgió un nuevo ransomware que fungía ser un aviso de advertencia de los organismos de seguridad (Policía local, Interpol y FBI), en este caso los agresores usaban la ingeniería social para hacerles creer a sus víctimas que el equipo se encontraba bajo investigación, manifestando que el usuario descargó información que lo implicaba en delitos como la pornografía infantil, los pagos se generaron con tarjetas prepagos para internet.

El capítulo más representativo en la historia de este malware, tuvo su desarrolló en el año 2013 cuando apareció CryptoLocker, el cual incluía un cifrado de nivel militar y almacenaba la llave para descifrarlo en un servidor remoto, haciendo casi imposible la recuperación de los archivos a través de herramientas externas, generando que las victimas realizaran una cantidad considerable de pagos.

Teniendo en cuenta que las organizaciones están siendo más conscientes del peligro que significa para ellas este tipo de ataques, han generado cambios en la plataforma de seguridad informática y estos se han ido reduciendo durante el año 2018, como se puede apreciar en la ilustración 7.

Ilustración 7. Tasa de encuentros de ransomware.



Fuente: Informe de inteligencia de seguridad de Microsoft volumen 24 enero a diciembre de 2018. Disponible en info.microsoft.com

6.1.2 Como defenderse

En primer lugar, no se deben realizar pagos a los extorsionistas, evitando con esto que haya mayor interés por esta modalidad y que estos ataques no

aumenten exponencialmente a futuro, asimismo evitar que se presenten nuevos ataques en contra de la misma víctima[40].

- Contactar a un experto en seguridad informática que busque la mejor solución a este problema desde un principio.

- Evitar la infección a través de la instalación y correcta configuración de un programa de antivirus y protección contra malware de este tipo[41].

- Crear periódicamente copias de seguridad de la información, incluso en diferentes dispositivos y ciclos de copiado (backup diario y semanal), es importante resaltar que debe realizarse en un dispositivo externo o en la nube (con su respectivo cifrado), los dispositivos usados para guardar las copias deben permanecer desconectados en el tiempo de desuso.

- Mantener los sistemas operativos y demás software siempre actualizados, teniendo en cuenta que los atacantes aprovechan las vulnerabilidades que son dadas a conocer por la comunidad de desarrolladores, por lo cual se recomienda automatizar este proceso.

- Implementar un Sistema de Gestión de Seguridad de la Información que establezca puntos de control a las medidas enunciadas anteriormente y que genere conocimiento y doctrina entre los usuarios para evitar que caigan en las estratagemas de la ingeniería social.

- Se debe desconfiar de cualquier tipo de enlace recibido a través de correo electrónico, redes sociales, mensajería instantánea o incluso juegos online, especialmente cuando son enviados por contactos desconocidos.

- Instalar un software antivirus que cuente con detección mediante heurísticas, la cual permite detectar este tipo de ataques en forma temprana.

- Mostrar siempre las extensiones de los archivos en los equipos de cómputo con sistema operativo Windows, manteniendo un cuidado especial con

[40] Consejos de prevención ransomware. En: nomoreransom [en línea]. [Consultado 3 mayo de 2019] disponible en: https://www.nomoreransom.org/es/prevention-advice.html

[41] CATOIRA, Fernando. 5 consejos para controlar una infección por malware. En: WeLiveSecurity [en línea]. Marzo 13 de 2012 [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2012/03/13/consejos-controlar-infeccion-malware/

extensiones de ejecutables como .exe, .vbs y .scr. teniendo en cuenta que pueden usar señueles como imágenes y videos con esas extensiones.

6.2 AMENAZAS DIRIGIDAS A EMPRESAS:

En un principio los atacantes realizaban ataques masivos con el fin de abarcar la mayor cantidad de equipos posibles, pero actualmente han encontrado mucho más rentable enfocar sus acciones ofensivas hacia un segmento de mercado, incluso hacia una empresa especifica.

A veces solo buscan un segmento de mercado (bancos, e-commerce, empresas de servicios públicos, etc), o incluso llegan a desarrollar un malware específico para una empresa u organización, como un troyano diseñado a afectar un servidor concreto.

Teniendo en cuenta que los tipos de empresas mencionadas anteriormente cuentan con una infraestructura robusta para protegerse de este tipo de ataques, los cibercriminales se valen de algunas estrategias para recopilar información o acceder a lugares críticos para la organización, dos de las más importantes son:

6.2.1 Suplantación correo corporativo (phishing):

Cuando se habla de phishing se suele entender la mecánica tradicional que ha tenido este ataque, el cual es difundido a través de correos, que suelen simular a entidades reales, como empresas de envío (UPS, Servientrega, 472, etc), entidades bancarias o simplemente organismos gubernamentales, donde solicitan de una forma convincente que actualice información personal dando clic sobre un enlace, redirigiendo a la víctima a un sitio web falso[42].

Teniendo en cuenta esto hay un consenso sobre el phishing, denominando que es una técnica usada por los atacantes para apropiarse de información privilegiada, la cual suele ser usada como insumo y preámbulo para realizar ataques más elaborados[43], o simplemente los criminales buscan obtener datos personales como cuentas bancarias, tarjetas de crédito y usuarios y contraseñas de servicios para realizar el hurto de valores.

---

[42] Phishing, En: Avast [en línea]. [Consultado 8 mayo de 2019] disponible en: https://www.avast.com/es-es/c-phishing

[43] El 'phishing' se disfraza de correo. En: ComputerWorld [en línea]. 3 de Agosto de 2018 [Consultado 8 mayo de 2019] disponible en: https://cso.computerworld.es/proteccion-de-datos/el-phishing-se-disfraza-de-correo

Pero cuando los ataques son enfocados hacia las empresas se denominan Business Email Compromise o BEC o también conocidos como “el fraude CEO”, es un delito que va en aumento, situación que es reconocida en el informe y plan de acción federal para la determinación de riesgos en ciberseguridad de 2018, donde se menciona la preocupación por este tipo de ataques y sus otras logradas a través de SMS o VoIP. Estos ataques están enfocados principalmente en dos técnicas: la captura de credenciales y la suplantación de identidad, esta última mediante el envío de correos electrónicos que buscan engañar a personal de la compañía ubicados en otros departamentos (por ejemplo, mediante el correo se simula ser un funcionario con un alto cargo, donde se ordena al departamento de finanzas que realice un pago a una cuenta de ahorros que claramente no está autorizado por el funcionario que dice ser), debido a la simplicidad de esta técnica, esta modalidad es una de las más populares.

Teniendo en cuenta que los BEC están claramente enfocados en el sector corporativo, ha generado que sean uno de los objetivos más rentables en explotar[44], tanto así que de acuerdo a Trend Micro: “se proyecta que superen los 9.000 millones de dólares en 2018, lo que significa un incremento del 69% respecto a 2017”[45], esto ha generado que se cree un mercado clandestino donde se comercien las herramientas necesarias para ejecutar estos ataques, facilitando que incluso atacantes inexpertos puedan ejecutarlos.

6.2.1.1 Evolución de los métodos de ataque de suplantación de identidad:

Teniendo en cuenta que se han desarrollado nuevas herramientas para la prevención de esta modalidad de fraude, los atacantes han ido renovando sus estrategias para adaptarse a ellas, pasando a tener ataques cada vez más polimórficos, ya no se conforman con utilizar solo una dirección URL, dominio o dirección IP, desde donde lanzan sus ataques, sino que montan una infraestructura robusta que les ofrece múltiples puntos de ataque.

Asimismo, la naturaleza de los ataques ha mutado, ahora pueden enfocarse en ejecutar ataques de suplantación de identidad cortos de unos pocos minutos a

[44] Aprendiendo a identificar los 10 phishing más utilizados por ciberdelincuentes. En: OSI. [en línea]. [Consultado 8 mayo de 2019] disponible en: https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen

[45] Las estafas en las que se utiliza el email corporativo crecerán un 69%. En: IT Digital Security [en línea]. 25 de enero de 2018. [Consultado 8 mayo de 2019]. disponible en: https://www.itdigitalsecurity.es/vulnerabilidades/2018/01/las-estafas-en-las-que-se-utiliza-el-email-corporativo-creceran-un-69

modalidad de ataque en serie, que saturan a la víctima con múltiples correos en un periodo corto de tiempo (generalmente días).

Se ha observado que los atacantes actualmente buscan alojar sus enlaces fraudulentos en infraestructura hospedada (adquieren dominios de sitios con apariencia inofensiva) y en los servicios de nube públicos, dificultando su detección.

6.2.1.2 Estrategias de protección en contra del phishing:

- La mejor protección consiste en que el usuario conozca esta modalidad de engaño y lo identifique, lo cual no es una tarea complicada teniendo en cuenta que en general suelen ser mensajes solicitando datos personales.

- Los usuarios no deben responder a mensajes no solicitados por correo electrónico, redes sociales o programas de mensajería instantánea.

- En especial se debe hacer énfasis en no abrir archivos anexos de correos o mensajes sospechosos.

- Los empleados deben mantener una actitud siempre a la defensiva al recibir llamadas telefónicas, o al entrevistarse con personas desconocidas, obviando entregar información personal o sensible de la empresa.

- Siempre revisar que las URL correspondan a las reales antes de ingresar usuarios y contraseñas.

- Se debe mantener el software y sistemas operativos actualizados a la versión más reciente.

6.2.2 Malware:

El origen de la palabra malware está relacionada con el software malintencionado, es un programa diseñado para dañar, alterar o interrumpir las operaciones normales, también es utilizado para robar datos y su motivación puede variar entre las travesuras, el vandalismo o en su mayoría de ocasiones su intención gira alrededor del crimen.

Tabla 2. Clasificación de Malware

Tipo	Observaciones
Virus:	Es un malware adjunto a un programa huésped (host o anfitrión)**,**el virus siempre debe ir unido a otro archivo el cual

	permite que este pueda propagarse, para esto requiere de la interacción humana, por ejemplo el reenvío de información a través de un correo spam infectado.
Gusanos	Son similares a los virus, pero a diferencia de él, es un programa autónomo que no requiere de un programa huésped, ni requiere de intervención humana para propagarse, este proceso lo hace a través de la explotación de una vulnerabilidad del sistema operativo.
Troyanos	Reciben su nombre de la estrategia usada por los griegos para infiltrarse en la ciudad de Troya (relatada en la Odisea), es un programa que en apariencia y en su funcionalidad aparenta ser legítimo y útil, pero en segundo plano puede estar robando información privilegiada o infectando a los mensajes de correo electrónico enviado.
Bots	Es una aféresis de la palabra robot, realiza acciones cotidianas realizadas por las personas, como por ejemplo enviar correos electrónicos, abrir sesiones de chat, navegar por internet, en su origen podría ser inofensivo, pero si se combina con un virus puede convertirse en algo peligroso, debido a que aprovechará la automatización que realiza el programa.
Keyloggers	Es un software malicioso que una vez instalado en el equipo de la víctima recopila toda la información ingresada a través de los dispositivos de entrada (teclado, mouse) y los difunde a una cuenta establecida por el atacante.
Ransomware	Es un tipo de programa malicioso que al instalarse cifra la información, impidiendo acceder al sistema operativo y archivos, los atacantes con el ofrecimiento de revertir este proceso chantajean a la víctima generalmente exigiendo criptodivisas.
Hoax	Es un tipo de mensaje diseñado por un atacante con el fin de generar miedo y alarma entre los usuarios, como característica especial, estos se diseñan con el fin de generar que sus víctimas los reenvíen a sus contactos, generando una cadena de desinformación.

Fuente: el autor.

Debido a la amplia variedad de malware observado en la tabla 2, es recomendable invertir en herramientas de detección que estén dentro de la compañía, se debe realizar un trabajo de análisis que permita prever cómo evolucionarán a futuros los nuevos ataques y desde el presente prepararse para evitarlos.

6.2.2.1 Estrategias de protección en contra del malware:

En primer lugar, para establecer si el equipo o sistemas están infectados, se generan sospechas de malware, cuando se evidencie alguno o varios de los siguientes síntomas:

- Aparecen ventanas o imágenes emergentes del tipo pop-ups sin ninguna explicación aparente.
- El firewall emite alertas donde da a conocer que algunos servicios pretenden conectarse a internet sin permiso del usuario.
- Algunos contactos de correo electrónico o redes sociales, dan a conocer que están recibiendo email sin que el usuario haya enviado.
- Existen demoras al iniciar el sistema operativo o al abrir un programa.

6.2.2.2 Medidas para desinfectar malware

- Una vez existan las sospechas es recomendable que se desconecte de internet.
- Es importante que los equipos cuenten con un software antivirus activo y actualizado[46].
- Con esta herramienta se debe realizar un análisis exhaustivo al sistema.
- Si se sospecha de un posible robo de credenciales es recomendable cambiarlas en todos los servicios.

6.3 Ataques emergentes que podrían afectar a las empresas:

[46] VAZQUEZ, Lucia. La importancia de los antivirus y la seguridad en las empresas. En: Empresa y Economía [en línea]. 12 de marzo de 2012 [Consultado 16 octubre de 2019] disponible en: http://empresayeconomia.republica.com/aplicaciones-para-empresas/la-importancia-de-los-antivirus-y-la-seguridad-en-las-empresas.html

6.3.1 Criptojacking:

Es un ataque en donde se usa los recursos informáticos de la víctima para minar criptomonedas de forma engañosa, en la mayoría de casos sin notarlo, el malware suele posesionarse del navegador web por lo que afecta tanto a estaciones de trabajo como a dispositivos móviles.

Teniendo en cuenta que la minería de criptodivisas cada vez requiere instalaciones y recursos energéticos más exigentes, los atacantes buscan apoderarse de la mayor cantidad de equipos para minar la mayor cantidad de nuevas monedas, generando que la víctima sufra ralentizaciones en las labores que realiza normalmente, el desgaste de sus recursos y cobros excesivos del servicio de energía eléctrica.

6.3.2 Supply Chain:

También conocidos como ataques a la cadena de suministros, son bastante complejos de detectar para el usuario final, en este el atacante busca afectar directamente al desarrollador de software, buscando aprovechar las vulnerabilidades que tiene en su infraestructura para colarse e instalar malware oculto en los procesos de compilación y actualización de aplicaciones legitimas.

Teniendo en cuenta que este software es identificado como seguro y confiable por el sistema operativo y software de antivirus, el atacante ejecuta fácilmente su código malicioso.

7. VENTAJAS QUE OFRECE EL ASEGURAMIENTO DE EQUIPOS CON SISTEMA OPERATIVO WINDOWS.

Como se puede observar en la tabla 3, actualmente cuando se habla de sistemas operativos para equipos de escritorio, Microsoft domina el mercado, de acuerdo al portal netmarketshare[47] se estima que Windows 10 cuenta con el 39% de la cuota de mercado mundial, seguido de Windows 7 con un 37%, su gran popularidad juega en contra, porque esto lo convierte en el mayor objetivo por parte de los cibercriminales.

[47] Operating System Share by Version. Netmarketshare

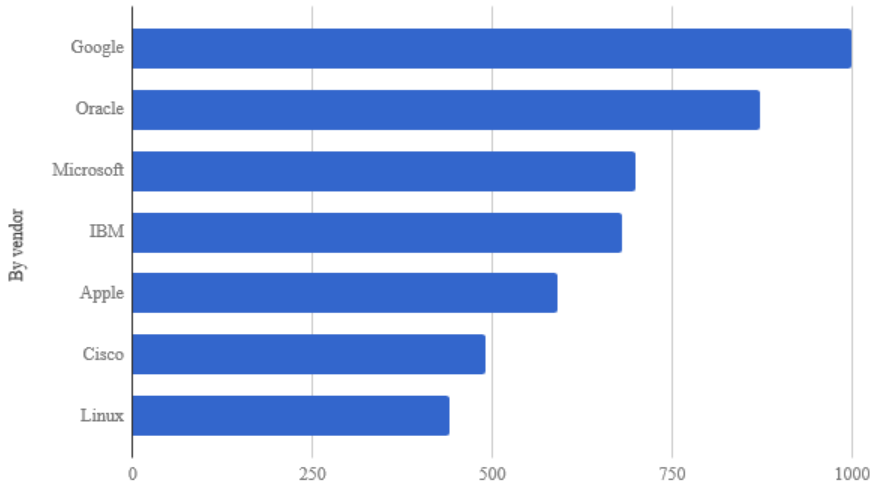
Tabla 3. Distribución de los sistemas operativos para escritorio

Posición	Sistema Operativo	Cuota de mercado
1	Windows 10	39.22%
2	Windows 7	36.9%
4	Windows XP	4.54%
5	Windows 8.1	4.45%

Fuente: Netmarketshare - Sistemas operativos por versión.

De acuerdo a un artículo publicado por la empresa GFI Software en el año 2018[48], en el cual realiza un análisis de vulnerabilidades de los principales sistemas operativos y aplicaciones, reconoció que los sistemas con Windows es uno de los tres de la lista con mayor cantidad de ellas, (ver ilustración 8).

Ilustración 8. Vulnerabilidades detectadas por fabricante



Fuente: The most vulnerable players of 2017. Disponible en GFILabsTeam.com

Esta misma situación ocurre en Colombia, donde su popularidad está extendida de forma similar, debido a la gran popularidad de los sistemas Windows en los equipos adquiridos por las empresas locales, de ahí la importancia por implementar la

[48] The most vulnerable players of 2017. En: TechTalk [en línea]. Marzo 29 de 2018 [Consultado 8 mayo de 2019] disponible en: https://techtalk.gfi.com/the-most-vulnerable-players-of-2017/

estrategia hardening para disminuir la probabilidad de materialización de ataques a esos sistemas.

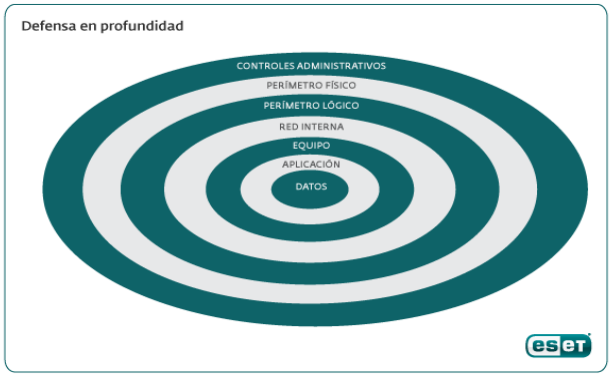
7.1 DEFENSA EN PROFUNDIDAD (DEFENSE IN DEPTH):

Es un modelo que a través de diferentes capas busca aplicar los controles necesarios para proteger los datos, partiendo de la premisa: "si es posible proteger a un activo de la organización con más de una medida de seguridad, hágalo, el objetivo del modelo también es claro: para que un atacante llegue a un dato o información, debe poder vulnerar más de una medida de seguridad"[49].

En la práctica se podría aplicar en una política del sistema de gestión de seguridad de la empresa, en donde a pesar que los equipos y servidores están protegidos al iniciar con usuario y contraseña, también se incluirá otro sistema de autenticación dentro en una aplicación o servicio donde se maneja información sensible, asimismo para ingresar físicamente a esa máquina, se debe atravesar la seguridad física perimetral, obligando a usar una llave para acceder a la habitación donde se encuentra.

Es importante realizar una evaluación de la cantidad de capas a aplicar[50], considerando que a mayor defensa (capas) aumenta exponencialmente su costo, llevando a los responsables a crear una estrategia de seguridad, como se puede apreciar en la ilustración 9.

Ilustración 9. Defensa en Profundidad.



Fuente: Defensa en profundidad. Disponible en welivesecurity.com

[49] BORTNIK, Sebastián. Defensa en profundidad. En: WeliveSecurity [en línea]. 24 de mayo de 2010. [Consultado 8 mayo de 2019] disponible en: (https://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/

[50] ISO 27001: Componentes de la defensa en profundidad. En: SGSI [en línea]. 14 de enero de 2015. [Consultado 8 mayo de 2019] disponible en: https://www.pmg-ssi.com/2015/01/iso-27001-componentes-de-la-defensa-en-profundidad

7.1.1 Niveles que componen la seguridad lógica:

De acuerdo a la ISO27001 esta estrategia debe ser coordinada y plasmada en el Sistema de Gestión de Seguridad de la Información, asimismo los datos recolectados con ella deben estar a disposición para la toma de decisiones.
Existen varios niveles de la seguridad lógica, los mas comunes son los siguientes:

7.1.2 Seguridad en el perímetro:

Hace referencia a las medidas de seguridad necesarios para asegurar los límites físicos de la empresa, para esto se recomienda:

- Definir los accesos y salidas con los que se cuentan y proveer su seguridad.
- Se debe llevar un registro detallado de los accesos que se permitan.
- En esos accesos se debe generar un filtro que revise la información que entre y salga.

7.2 TECNOLOGÍA CORTAFUEGOS

Esta tecnología permite controlar la transmisión de información a los distintos niveles y filtros con los que se cuenta, proporcionando una protección en contra de los ataques que se presenten (internos/externos).

Es un recurso muy importante, teniendo en cuenta que cuanta con varios niveles de protección que se adaptan a los requerimientos de la empresa, teniendo en cuenta que parte de la seguridad informática de la empresa depende de este dispositivo, es importante adquirir uno de un fabricante con buena reputación y soporte.

7.3 CENTROS DE RESPALDO

La información es uno de los activos más importantes con los que cuenta una empresa, de ahí la importancia de su protección, se debe contar con un sistema y proceso que garantice la continuidad del negocio en caso de se presente una eventualidad (ataque o siniestro) que la afecte.

Los centros de respaldo se consideran una excelente inversión, teniendo en cuenta que garantizan la disponibilidad del servicio de forma temporal mientras se resuelve la contingencia.

7.4 CRIPTOGRAFÍA:

Son técnicas que buscan alterar los mensajes con el fin de evitar que sean leídos por los receptores no autorizados, es uno de los mecanismos más usados en la seguridad digital, prácticamente todos los sistemas actuales la han adoptado para garantizar la integridad y la confidencialidad.

Para entender un poco más sobre ella, es importante revisar el etimológico de ese término, el cual proviene del griego Kriptos, que significa ocultar, y de la palabra Graphos, del mismo origen que hace referencia a escritura, en resumen “ocultar la escritura” a través de la aplicación de técnicas que permitan hacer ininteligible un mensaje.

En la práctica esta ciencia diseña dispositivos o aplicaciones que son capaces de transformar mensajes claros a mensajes cifrados, esta transformación se denomina cifrar y el proceso inverso descifrar, es importante resaltar que este procedimiento sólo es factible con el conocimiento de una o más llaves de cifrado.

El cifrado de la información sensible es una práctica importante que es recomendado en las PYMEs, porque garantiza la continuidad del negocio, escoger la mejor opción requiere de un importante análisis de costo versus beneficio, el cual debe realizarse en conjunto con la alta gerencia, teniendo en cuenta que esta selección impactará notablemente con las actividades que se realizan al interior de la organización.

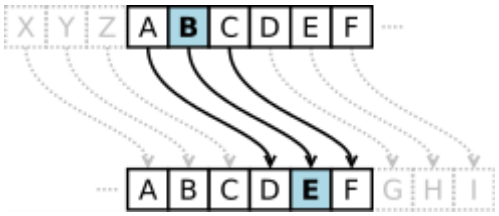
Es recomendable desarrollar políticas de seguridad que garanticen desde la alta gerencia medidas que impacten en todos los niveles de la empresa, teniendo en cuenta que en la era de la información, su protección es uno de los activos más importantes a proteger.

7.4.1 Desarrollo histórico de la Criptografía:

7.4.1.1 Cifrado por desplazamiento

El cifrado por desplazamiento o cifrado César es uno de los cifrados más sencillos, es usado desde la época del imperio romano, en esa época el emperador enviaba mensajes a sus generales, moviendo algunas letras un número de posiciones determinadas siguiendo el orden alfabético, la llave de cifrado corresponde a K y corresponde a un número entero, ubicado entre 0 y 26 (27 dígitos componen el alfabeto castellano), en el siguiente ejemplo se aprecia lo enunciado, se usa un desplazamiento de tres espacios, así que una B en el texto original se convierte en una E en el texto codificado (ver ilustración 10):

Ilustración 10. Cifrado por desplazamiento



Fuente: Cifrado César. Disponible en Wikipedia

Para cifrar se suele usar aritmética modular de acuerdo a los siguientes pasos:

1. Se convierten las letras del alfabeto en el número que le corresponda, iniciando desde el 0, (A=0, B=1, C=3, etc.), este número se denomina X.

2. Se realiza la siguiente ecuación Y=(X+K) mod 27 (El modulo es 26 cuando se cifra texto en el alfabeto anglosajón)

3. El resultado Y del número tomado en la ecuación, corresponde a la letra con ese lugar en el alfabeto.

Tabla 4. Posición Numérica del Alfabeto Español

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z

EJEMPLO: cifrado por desplazamiento con la llave K=12

	U	N	A	D	MENSAJE ORIGINAL
	21	13	0	3	
+	12	12	12	12	
(	33	25	12	15	)mod 27
	6	25	12	15	
	G	Y	M	O	MENSAJE CIFRADO

Pasos para descifrar el mensaje:

	G	Y	M	O	MENSAJE CIFRADO
	6	25	12	15	
-	12	12	12	12	
(	-6	13	0	3	)mod 27
	21	13	0	3	
	U	N	A	D	MENSAJE ORIGINAL

Observaciones:

- Es un método de cifrado inseguro porque un buen método de cifrado debe prevenir que un atacante que obtenga el mensaje, pero no cuente con la llave, pueda descubrir su contenido, teniendo en cuenta que el alfabeto castellano cuenta con tan solo 27 dígitos, este puede ser resuelto en máximo 27 intentos por el atacante (ataque de fuerza bruta).

7.4.1.2 Cifrado Afín

Se denomina cifradores por sustitución genéricos, monogramicos y monoalfabeticos, los sistemas de cifra clásica que obtienen el alfabeto de cifrado a partir de la ecuación C=a*m + b mod n.

Esta operación se suele denominar como decimación, si la constante de desplazamiento b=0, se habla de decimación pura, si la constante de multiplicación a=1, se habla de desplazamiento puro, y si no se dan están condiciones (a$\neq 1, b \neq 0$) se habla de una cifra afín.

Si se aplica una decimación de a=2 ahora las letras se distribuyen en dos espacios y posteriormente a este, se le añade un desplazamiento de D=4

Tabla 5. Desplazamiento numérico del Alfabeto

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	G	I	K	M	Ñ	P	R	T	V	X	Z	B	D	F	H	J	L	N	O	Q	S	U	W	Y	A	C

Obteniendo el alfabeto final para la ecuación de cifra c=2*m + 4 mod 27

EJEMPLO:

Se cifra la abreviatura UNAD con la cifra afín c=11*m-3 mod 27

U	21*11-3 = 228 mod 27 = 12	M
N	13*11-3 = 140 mod 27 = 5	F
A	0*11-3 = -3 mod 27 = -3	X
D	3*11-3 = 30 mod 27 =3	D

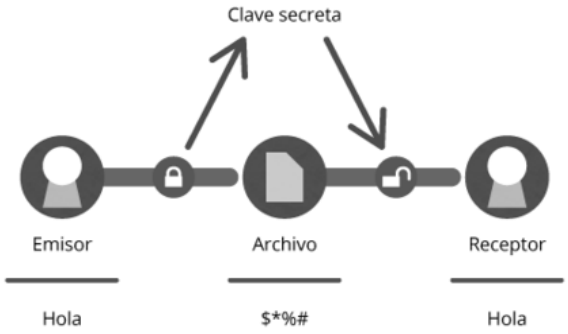
La operación se realizará con la formula m=(c-b)*inv(a,n) mod n, a partir del ejemplo anterior el inverso de (11,27) = 5, se procede a hallar:

M	[12-(-3)]*5 = 75 mod 27 = 21	U
F	[5-(-3)]*5 = 40 mod 27 = 13	N
X	[-3-(-3)]*5 = 0 mod 27 = 0	A
D	[3-(-3)]*5 = 30 mod 27 = 3	D

7.4.1.3 Criptografía Simétrica

Solo utiliza una llave para cifrar y descifrar, la cual deben conocer los emisores y receptores del mensaje, esta característica es su principal debilidad, teniendo en cuenta que al ser interceptado el mensaje se puede obtener la llave, como se puede apreciar en la ilustración 11.

Ilustración 11. Cifrado Simétrico.



Fuente: Tipos de criptografía: simétrica, asimétrica e hibrida. Disponible en: Portal Genbeta

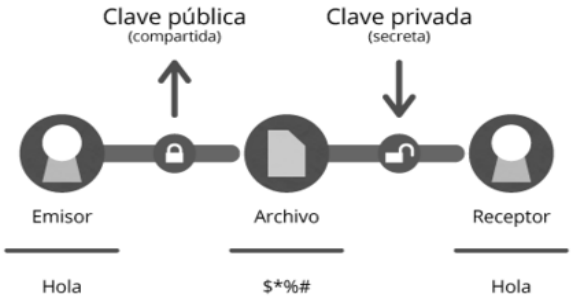
Ventajas: El proceso de cifrar y descifrar toma menos tiempo.

Desventajas: Es más insegura porque difunde la clave en los envíos.

7.4.1.4 Criptografía Asimétrica

En este tipo de cifrado, se usa dos llaves, una pública que puede difundirse sin inconvenientes y la otra privada que debe ser preservada con seguridad, es difícil que a partir de la interceptación de la llave publica un atacante pueda descifrar la llave privada, teniendo en cuenta que estas llaves pueden tener un tamaño de 2048 bits, con los equipos informáticos actuales le tomaría años resolver con ataques de fuerza bruta, como se puede apreciar en la ilustración 12.

Ilustración 12. Cifrado Asimétrico.



Fuente: Tipos de criptografía: simétrica, asimétrica e hibrida. Disponible en: Portal Genbeta

7.4.1.5 Criptografía Hibrida:

Combina las ventajas de los dos tipos antes mencionados y los integra en un nuevo sistema de cifrado, con las siguientes características:

- El receptor crea una llave privada y otra pública.
- Cifra la información en tiempo real.
- El receptor envía la llave pública.
- Se realiza el cifrado de la información usando la llave publica del receptor.
- Se envía el archivo cifrado en tiempo real y la clave del archivo en forma asíncrona (solo tiene acceso a ella el receptor).

7.4.1.6 Algoritmo Advanced Encryption Standard – AES

Teniendo en cuenta las características y los requerimientos de seguridad que tienen las PYMEs colombianas para proteger la información sensible se recomienda el algoritmo de cifrado AES, puesto que es uno de los más seguros actualmente fue diseñado para reemplazar los anteriores estándares DES y 3-DES y actualmente es uno de los criptosistemas más usados en el mundo.

El AES se considera ideal en el manejo de la información sensible, distinción dada por parte de la Agencia Nacional de Seguridad (NSA) de los Estados Unidos, esto

ha garantizado que sea el cifrado predilecto por las organizaciones gubernamentales e incluso destinado para su uso en el sector bancario, de acuerdo a que no se ha descubierto una vulnerabilidad que pueda permitir un ataque efectivo contra este método[51].

7.4.1.6.1 Descripción del método de cifrado AES

En este tipo de cifrado se parte de un mensaje original en texto plano:

Hola Fernando estos son los datos financieros del último trimestre, recuerda que debes presentarlos a la junta directiva del banco y no compartirlos con personas que no cuenten con la autorización

Se inicia convirtiendo el texto plano a hexadecimal, esto se realiza porque este sistema tiene como base 16 y en él dos dígitos hexadecimales equivalen a un byte, facilitando su división en bloques:

75 72 20 61 64 69 70 69 73 63 69 6e 67 20 65 6c 69 74 2c 20 73 65 64 20 64 6f 20 65 69 75 73 6d 6f 64 20 74 65 6d 70 6f 72 20 69 6e 63 69 64 69 64 75 6e 74 20 75 74 20 6c 61 62 6f 72 65 20 65 74 20 64 6f 6c 6f 72 65 20 6d 61 67 6e 61 20 61 6c 69 71 75 61 2e 20 55 74 20 65 6e 69 6d 20 61 64 20 6d 69 6e 69 6d 20 76 65 6e 69 61 6d 2c 20 71 75 69 73 20 6e 6f 73 74 72 75 64 20 65 78 65 72 63

Luego se separa el texto en plano que se desea cifrar en bloques de columnas de 4 por 4, esto es debido a que el cifrado AES es al menos de 128 bits, como se representa más adelante, así se verían los primeros bloques:

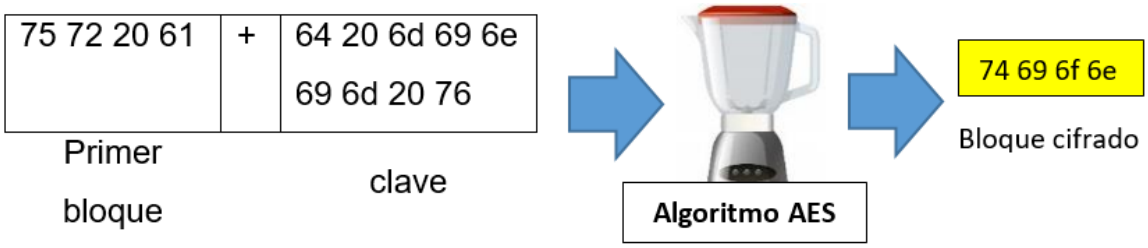
75 72 20 61	64 69 70 69	73 63 69 6e	67 20 65 6c	69 74 2c 20	64 6f 20 65

En la ilustración 13, se observa que luego a cada bloque se le suma el código hexadecimal de la clave seleccionada, la cual solo debe ser de conocimiento del

[51] How does AES encryption work? Advanced Encryption Standard. [video]. YouTube, Shad Sluiter (23 de Agosto de 2019). 12:49 minutos. [consultado: 3 noviembre 2019]. Disponible en: https://www.youtube.com/watch?v=lnKPoWZnNNM

emisor y receptor, estos bloques se mezclan usando el algoritmo AES dando como resultado un bloque cifrado:

Ilustración 13. Funcionamiento del Algoritmo AES



Fuente: El autor.

Este proceso se repite con cada uno de los bloques del mensaje hasta que se genere el texto cifrado, el cual es el que se envía a través de los canales de comunicación autorizados por las entidades.

AES cuenta con tres opciones distintas que garantizan mayor robustez del cifrado, AES-128, AES-192, AES-256 bits, de acuerdo a esta elección se genera el tamaño de los bloques, como se puede observar en el siguiente ejemplo:

Tabla 6. Representación robustez del cifrado

Clave de 128 bits	64 20 6d 69 6e 69 6d 20 76
Clave de 192 bits	64 20 6d 69 6e 69 6d 20 64 20 6d 69 6e 20 64 20 6d 69 6e 69 6d 6d 20 64 20 6d 69 69 64 20 6d 69 6e 69 6e 69 6d 20
Clave de 256 bits	64 20 6d 69 6e 69 6d 20 64 20 6d 39 6e 22 64 20 6d 6d 69 6e 69 6d 20 64 20 6d 69 64 6d 69 6c 2f 69 6e 19 20 6d e9 6e 69 6e 29 6d 20

7.4.1.6.2 Observaciones del método de cifrado AES:

- Luego de ejecutarse el algoritmo se genera un bloque con información que a simple vista parecería aleatoria, generando que al atacante le sea imposible de entender.

- Se podría pensar que una buena práctica es seleccionar siempre el cifrado más robusto posible (en este caso 256 bits), pero en la práctica esto estaría representado por más tiempo en el proceso de cifrado y mayor consumo de recursos informáticos.

- Actualmente los 128 bits de longitud se consideran seguros, teniendo en cuenta que no existe registro documental que indique que este cifrado haya sido roto.

7.4.1.7 Algoritmo de intercambio de claves Diffie-Hellman

Este algoritmo permite a dos entidades el envío de información privada a través de un medio inseguro, enfocan su seguridad en ocultar la clave que se usa para cifrar la información, es importante que el emisor y receptor no compartan públicamente la clave, es por este motivo que deben ponerse de acuerdo previamente[52].

En la práctica este método funciona cuando dos participantes acuerdan usar una contraseña privada enviada por un canal inseguro, para este propósito los dos acuerdan usar un par de números, un primo grande *p* y un generador *g.*

$$\text{Emisor} = g^{\alpha} \bmod p. \quad \text{Receptor} = g^{\beta} \bmod p.$$

Debido a que en ejercicios normales se usa números grandes como potencias y que no se comparte el código secreto, descifrarlo con ataques de fuerza bruta es una tarea que consumirá recursos en exceso, disuadiendo de esta acción a los atacantes.

Ejemplo de aplicación:

En un principio el emisor y receptor acuerdan sobre qué número usaran como módulo primario y generador, luego cada uno de ellos escoge un número aleatorio,

[52] Intercambio de llaves Diffie-Hellman. [video]. YouTube, Khan Academy. 2:18 minutos [consultado: 3 noviembre 2019]. Disponible en: https://es.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-2

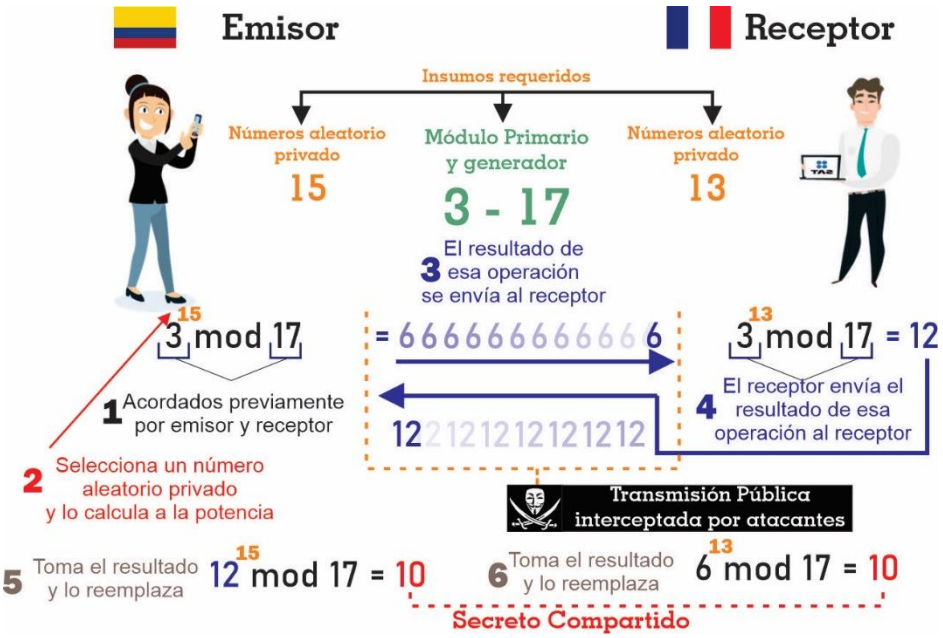
el emisor comienza calculando la potencia del módulo (usando su número aleatorio privado), una vez hallado el resultado se envía públicamente al receptor.

Ahora el receptor con su número aleatorio privado realiza la misma fórmula que hizo el emisor (elevando a la potencia el modulo primario), de la misma forma envía el resultado obtenido por un canal público.

Ahora sigue el paso más importante el emisor toma el resultado de la operación del receptor y lo reemplaza por el modulo primario original, al resolver esta operación se obtiene el secreto que se ha compartido, el receptor realiza lo mismo, obteniendo la misma información.

En la ilustración 14 se observa cómo se utilizan números relativamente pequeños, pero en la práctica se sugiere escoger números lo suficientemente grandes, generando que sea imposible de descifrar el método de intercambio de claves.

Ilustración 14. Funcionamiento intercambio de claves Diffie-Hellman



Fuente: El Autor

8. BUENAS PRÁCTICAS EN LA IMPLEMENTACIÓN DE HARDENING EN EQUIPOS WINDOWS:

- Crear una directiva que obligue a los usuarios a generar contraseñar robustas (que incluyan caracteres alfanuméricos, números y símbolos), tener contraseñas débiles facilita que se generen ataques.

- Todos los sistemas deben contar con perfiles con altos privilegios o permisos administrativos, el usuario promedio no debe contar con permisos para instalación de software.

- Por defecto los sistemas operativos de la empresa deben bloquear la ejecución automática de dispositivos USB, teniendo en cuenta que es una vulnerabilidad ampliamente utilizada por los atacantes.

- Es importante migrar a sistemas operativos vigentes en caso de contar con ese tipo de sistemas antiguos como Windows XP o 7, los cuales ya no cuentan con actualizaciones oficiales del fabricante.

- Contar con una herramienta que automatice el proceso de descarga e instalación de actualizaciones a los sistemas operativos y software.

- Permitir la visualización de archivos ocultos y extensiones de los archivos, teniendo en cuenta que esto facilita la detección de malware y/o vectores de ataque.

8.1 CONSEJOS PARA IMPLEMENTAR EFECTIVAMENTE EL ASEGURAMIENTO EN EQUIPOS CON SISTEMAS OPERATIVOS WINDOWS EN LAS PYME:

De acuerdo a los datos analizados previamente las PYMES en Colombia no hacen lo necesario para asegurar esos sistemas operativos, a pesar de que se tiene el conocimiento suficiente para hacerlo (en el imaginario colectivo se suele asumir que algunas prácticas como la instalación de una herramienta de antivirus y actualizar el Sistema operativo es una actividad necesaria para fortalecer la seguridad).

Es importante involucrar a la gerencia de las entidades donde se busca implementar el proceso de aseguramiento de los sistemas, para que la seguridad informática se convierta en una política empresarial, en caso de no contar con el apoyo de la cabeza empresarial, esto dificultaría llevar a un buen término este tipo de procesos.

Teniendo en cuenta lo anterior, para mejorar la seguridad el hardening en equipos de cómputo con sistema operativo Windows, se requiere de una serie de pasos que pueden denominarse capas de protección, de acuerdo a la autora Roberta Bragg, en su libro Hardening Windows Systems, hay 10 recomendaciones esenciales para el endurecimiento de este SO[53]:

8.2 FORTALECER LA POLÍTICA DE CONTRASEÑAS[54]

El uso de contraseñas débiles facilita que terceros puedan adivinarlas o descifrarlas, saltándose con esto uno de los controles informáticos más importantes con los que cuentan las empresas para resguardan sus activos informáticos.

Para que se considere que se cuenta con una política de contraseñas robusta en las empresas se requiere la implementación de algunas políticas de seguridad en ese ámbito:

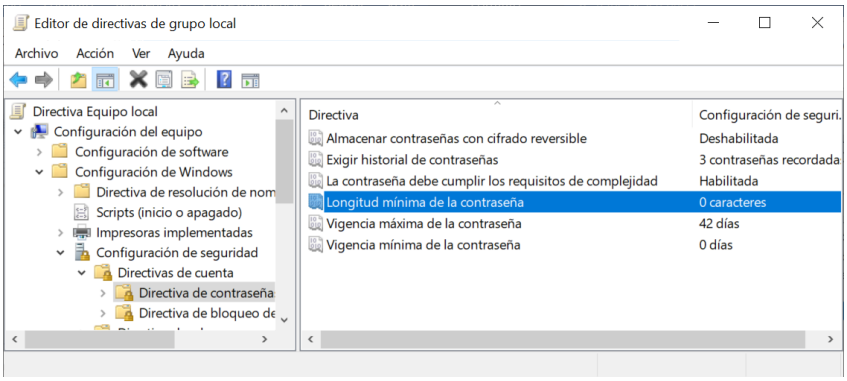
- Forzar a que periódicamente se solicite el cambio de contraseña.
- Las contraseñas deben ser largas e incluir letras en mayúscula, minúscula, símbolos y números.
- No permitir que estén compuestas solo por espacios en blanco.
- Verificar que no se puedan repetir contraseñas usadas previamente por el usuario.
- Evitar el uso del mismo usuario como contraseña.

Es importante aclarar que estos parámetros se pueden configurar desde las políticas de la consola EPO de Windows Server y lanzarse a todas las estaciones de trabajo que conforman el Directorio activo, en caso de no contar con este servicio se procede editando las directivas localmente en cada estación de trabajo, como se evidencia en la ilustración 15.

[53] BRAGG, Roberta, Roberta Bragg's 10 Windows hardening tips in 10 minutes. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019]. disponible en: https://searchsecurity.techtarget.com/tip/Roberta-Braggs-10-Windows-hardening-tips-in-10-minutes?

[54] BRAGG, Roberta, Strengthen the password policy. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchenterprisedesktop.techtarget.com/feature/Strengthen-the-password-policy?_SS

Ilustración 15. Editor de directivas de grupo local.



Fuente: El autor

La persona encargada de administrar los recursos y la seguridad debe asignar usuarios únicamente con los roles y permisos mínimos requeridos para el cumplimiento de sus funciones en la compañía, si por necesidades laborales estos cambian con el tiempo, se debe realizar una constante actualización de ellos, asimismo se debe eliminar los usuarios asignados a empleados que ya no laboren en la PYME.

Observación: Se considera una buena práctica de seguridad, que los usuarios designados con el rol de administrador no sean los mismos con los que se realiza el trabajo cotidiano en las estaciones de trabajo.

8.3 BLOQUEAR LA ADMINISTRACIÓN DEL TERMINAL EN FORMA REMOTA[55]

Como se mencionó en el punto anterior, si la empresa cuenta con pocos equipos de cómputo puede optar por administrarlos uno a uno desde la configuración local, pero si se trata de una entidad con una cantidad considerable de equipos (como suele ser el caso de la mayoría de PYMES) es recomendable optar por administrarlos con Active Directory, el cual es un servicio que comparte información (creación de grupos y gestión de archivos) y organiza recursos (red local y periféricos), desde el sistema operativo Windows Server.

Para esto se recomienda habilitar solo la opción de administración con ese servicio y deshabilitar la administración remota para todo lo demás; por otro lado, siempre que se pueda es recomendable bloquear el acceso a los puertos de los servicios

[55] BRAGG, Roberta, Lock down administrative workstations. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/feature/Lock-down-administrative-workstations?_SS

administrativos, en este punto es importante aclarar que este bloqueo se puede enfocar en limitar cierta cantidad de accesos a esos puertos.

Se debe realizar un análisis de estos casos, por ejemplo, solo algunas cuentas requieren acceso a un computador especifico, se deben bloquear todos los demás, la correcta administración de estos recursos puede brindar grandes beneficios como permitir que se preste correctamente el soporte técnico de mesa de ayuda de forma remota y en el caso contrario puede permitir el fácil acceso por parte de atacantes a la compañía.

8.4 BLOQUEAR LAS ESTACIONES DE TRABAJO DE USO ADMINISTRATIVO[56]

Es común que se suela designar algunas estaciones de trabajo como administrativas, desde donde solo se acceda para realizar la administración de la red, archivos y demás recursos de la entidad, es muy importante destinar una buena cantidad de recursos disponibles en el correcto aseguramiento de estos equipos, para lo cual es importante mencionar algunas recomendaciones.

- No se debe escatimar en la instalación y automatización de actualizaciones y parches de seguridad.

- Se recomienda instalar un firewall que controle el acceso y salida de los paquetes de información.

- Las estaciones de trabajo administrativas no deben ser destinadas para el trabajo cotidiano que realizan los empleados, es por ese motivo que solo se debe instalar el software estrictamente necesario para el propósito designado.

- No solo se trata de garantizar la seguridad de los sistemas, sino que se debe asegurar físicamente estos equipos, usando las barreras físicas necesarias para evitar que terceros sin autorización accedan a esos recursos.

[56] Ibidem

8.5 ASEGURAR FÍSICAMENTE TODOS LOS SISTEMAS[57]

Para esto se debe realizar un análisis de los requerimientos que se tiene en cada caso en particular, si se busca el aseguramiento de los equipos de cómputo portátiles, se debe verificar si en el puesto de trabajo donde suele usarse se cuenta con un cable de seguridad que dificulte su robo, si el equipo suele moverse a sitios ya establecidos se debe contar con un el mismo sistema para esos puntos.

En ese mismo caso se debe analizar si a pesar de encontrarse el portátil asegurado físicamente, se facilita extraer el disco duro, en este evento se debe analizar y estimar el valor de la información que tiene guardada, en muchas ocasiones la pérdida o fuga de la información almacenada, supera el valor del equipo, en este último caso debería llevarse siempre a la mano el disco duro de esa información u optar por el cifrado de discos.

En un caso similar se debe analizar qué hacer con la información sensible almacenada en los teléfonos celulares empresariales, analizar qué pasaría con los activos de información si el dispositivo se pierde o se estropea, ¿un tercero podría acceder fácilmente a la información? Y a partir de ese proceso implementar políticas de seguridad.

Por ultimo otra recomendación en el aseguramiento físico es el bloqueo a los puertos USB, unidades ópticas en las estaciones de trabajo, evitando la salida de información de la empresa, esto se alcanza a través de la implementación de listas blancas de dispositivos externos autorizados.

8.6 DESACTIVE EL SISTEMA DE ENCRIPTADO DE ARCHIVOS EFS[58]

Si la entidad no cuenta con una política claramente establecida para la administración del cifrado EFS en los sistemas operativos Windows, que contemple procedimientos de copia de seguridad de llaves y backup de las mismas, se recomienda deshabilitar esa opción, la cual suele estar activa por defecto, permitiendo que cualquier usuario con un poco de curiosidad la pueda activar, generando pérdidas de información importantes si se realiza sin los protocolos adecuados.

Se puede desactivar en todos los equipos desde las directivas de grupo GPO si se cuenta con un servidor o realizar el procedimiento uno a uno en las estaciones de trabajo.

---

[57] BRAGG, Roberta, Physically secure all systems. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999836/Physically-secure-all-systems?_SS

[58] BRAGG, Roberta, Disable EFS. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en:https://searchwindowsserver.techtarget.com/news/999853/Disable-EFS)

8.7 PROHÍBA LAS REDES INALÁMBRICAS QUE NO CUMPLAN CON LOS REQUERIMIENTOS DE SEGURIDAD DE LA ENTIDAD[59]

Las redes inalámbricas son muy atractivas para los usuarios, teniendo en cuenta su bajo costo de implementación (con unos pocos parámetros se tiene un rápido acceso), desafortunadamente este tipo de redes cuentan con dispositivos que suelen mantener la configuración que traen por defecto, permitiendo que fácilmente un atacante acceda a los activos informáticos a través de ellas, en especial al imposibilitarse controlar la cobertura que tiene la red.

La política más eficaz para el manejo de estas redes es su bloqueo a menos que cumplan con las políticas de seguridad necesarias para evitar ataques, en particular estas redes deben requerir cifrado y autenticación como lo ofrece el protocolo WPA2, el cual está pensado para ser usado en forma segura por las empresas.

8.8 PROHIBIR QUE EQUIPOS DE CÓMPUTO EXTERNOS SE CONECTEN A LA RED DE LA EMPRESA[60]

Una vez implementado en los equipos de la empresa un protocolo de seguridad de la información eficaz, en donde se cuente con software parchado y actualizado, contraseñas robustas y difíciles de adivinar usando ataques de fuerza bruta, se debe evitar a toda costa que se conecten a esas redes equipos externos, porque estos pueden tener una o varias vulnerabilidades.

En lugar de autorizar estas conexiones se deben establecer políticas de seguridad que obliguen a realizar una inspección y actualización obligatoria antes de regresarlo, teniendo en cuenta lo difícil de realizar se pueden seguir las siguientes recomendaciones:

- Los equipos de red deben requerir autenticación de usuario para permitir el acceso a la red, esto es importante cuando usuarios externos se sienten tentados a usar las redes LAN o inalámbricas que encuentre a su disposición.

---

[59] BRAGG, Roberta, Ban wireless networks that don't meet tough security policy requirements. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en:https://searchwindowsserver.techtarget.com/news/999855/Ban-wireless-networks-that-dont-meet-tough-security-policy-requirements)

[60] BRAGG, Roberta, Don't allow unprotected laptops and desktops to connect to the LAN. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999861/Dont-allow-unprotected-laptops-and-desktops-to-connect-to-the-LAN

- Use el filtrado de conexiones inalámbricas por dirección MAC, en el caso de que una persona externa llegue a obtener la contraseña de la red wifi se imposibilite su acceso a menos que el administrador del recurso lo autorice.

- Cree segmentos de red destinados exclusivamente a ser usados por dispositivos externos a la entidad, sin permitir el acceso a información sensible de la empresa.

- No permita el acceso a equipos externos que no estén al día con las actualizaciones y parches de seguridad.

8.9 NO PERMITIR EL USO DE CUENTAS CON PRIVILEGIOS DE ADMINISTRADOR PARA EL USO COTIDIANO[61]

Al existir cuentas con permisos elevados: cuentas de administrador o cuentas de usuario con permisos que cuenten con acceso a múltiples sistemas, se recomienda establecer en una política de seguridad que los usuarios que cuenten con ese nivel de acceso estén obligados a usar cuentas alternas para realizas las actividades cotidianas laborales (uso de herramientas ofimáticas, acceso a correo eléctrico, etc.).

Puesto que algunos virus se propagan con acciones sencillas como abrir un simple archivo anexo de un correo electrónico, si se cuenta con un sistema operativo endurecido y el usuario no cuenta con permisos elevados se puede mitigar el daño causado.

8.10 GUARDAR LOS SECRETOS[62]

La ingeniería social se aprovecha del afán inherente que tienen los seres humanos por ayudar al prójimo, incluso al interactuar con desconocidos suele mostrarse afable, un atacante tiene una ventaja mayor cuando simula envestirse con un cargo jerárquico superior al de la víctima.

Las PYME deben evitar que sus empleados fuguen información de forma culposa, para este propósito deben implementar un programa de capacitación constante,

[61] BRAGG, Roberta, Use Runas or Su. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/feature/Use-Runas-or-Su

[62] BRAGG, Roberta, Keep secrets. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019]disponible en: https://searchenterprisedesktop.techtarget.com/news/999842/Keep-secrets?_SS

donde se socialice un manual de buenas prácticas en seguridad de la información, asimismo se deben realizar pruebas simuladas de vulnerabilidad para establecer el nivel de respuesta de cada uno de los funcionarios.

8.11 DESACTIVAR LAS CONEXIONES BLUETOOTH[63]

Cada día un mayor número de dispositivos cuentan con este tipo de conexiones, en el ambiente empresarial se pueden encontrar principalmente en los teléfonos móviles y la transferencia de información hacia los equipos de cómputo y en menor medida en televisores inteligentes, tabletas, altavoces, etc.

En vista de esta nueva adopción los atacantes han puesto su mirada en esta tecnología buscando formas de cometer intrusiones, por lo tanto, la mejor practica es desactivar por defecto estas conexiones y adquirir estaciones de trabajo que no cuenten con esta característica.

8.12 IMPORTANCIA DE LA IMPLEMENTACIÓN DE UNA SOLUCIÓN DE ANTIVIRUS EN EL ENTORNO EMPRESARIAL:

De acuerdo a un reporte realizado por la empresa ESET el número de detecciones de malware van en aumento, “en promedio se procesaban alrededor de 200.000 muestras diferentes cada día; finalizando 2016 este número se acercaba a las 300.000”[64].

De acuerdo al informe #14 de inteligencia de seguridad de Microsoft[65]: “el 24% de los ordenadores no poseen protección anti-virus” esto genera que sean vulnerables a ataques o que peligren los datos personales o empresariales.

Es evidente que debido a la buena rentabilidad criminal que genera los ciberdelitos, diariamente aparezcan nuevas amenazas informáticas, por esto es importante contar con una herramienta que logre identificar estas amenazas antes de que cumplan su cometido, para este propósito se cuenta con herramientas de antivirus

[63] BRAGG, Roberta, Disable infrared file transfer. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999910/Disable-infrared-file-transfer

[64] GUTIERREZ, Camilo. 7 motivos por los que necesitas tener un antivirus. En: WeLiveSecurity [en línea]. 6 de enero de 2017 [Consultado 16 octubre de 2019] disponible en: https://www.welivesecurity.com/la-es/2017/01/06/motivos-tener-un-antivirus/

[65] MICROSOFT, Informe de Inteligencia de Seguridad de Microsoft. Redmond: SIRT, 2019. p. 9.

las cuales han ido mutando para convertirse en soluciones de seguridad integrales, las cuales cuentan actualmente como mínimo con soluciones de antispam, antipishing y escaneo de memoria.

Por eso en la carrera de la ciberseguridad es importante contar con una herramienta de antivirus que se adapte a los retos actuales y futuros:

- Existe una difusión constante de malware a través de diferentes canales, correo electrónico, redes sociales, aplicaciones de mensajería instantánea, etc.

- Evite ataques en los que el usuario no tiene una interacción directa, como pueden ser los ataques de inyección en sitios web, donde sin percatarse se puede estar ejecutando código malicioso.

- Debido a la gran competitividad empresarial, han surgido nuevas tecnologías que son implementadas rápidamente en esos entornos, estas las cuales traen consigo nuevas amenazas.

- A pesar de que se consideró en el imaginario colectivo que otros sistemas operativos como Linux y MacOS eran invulnerables al malware, hoy en día se ve un mayor interés por afectarlos, asimismo por llegar a los sistemas operativos de los teléfonos móviles más populares (iOS y Android).

8.13 SISTEMA DE DETECCIÓN DE INTRUSOS:

Dentro de las herramientas que componen la seguridad de las PYMEs, es importante tener en cuenta los IDS (Intrusión Detection Systems), el cual puede ser un dispositivo o aplicación que detecta en forma temprana actividades anómalas que ocurren en los sistemas[66], activando alarmas en el momento de evidenciarse y permitiendo detener el incidente y facilitando la identificación del intruso.

Parte de su funcionamiento consiste en identificar el comportamiento que tiene un usuario normal y alertar cuando se sospeche de una actividad intrusiva.

Beneficios que otorga:

[66] Detección de Intrusos en Tiempo Real. En: segu-info [en línea]. [Consultado 16 octubre de 2019] disponible en: https://www.segu-info.com.ar/proteccion/deteccion.htm

- Genera un reporte con información de comportamientos maliciosos, sirviendo de insumo para la toma de decisiones.
- Permite reaccionar antes de que ocurran daños.
- Permite identificar desde que lugar se generan los ataques a la entidad.
- Funciona como una analogía de una cámara de seguridad y sistema de alarma.
- Detecta ataques donde se abusa de privilegios otorgados a los usuarios.
- Genera dificultades de ocultamiento de la evidencia de los atacantes.

Problemas que podrían generar:

- Se pueden producir algunos falsos positivos.
- No reemplaza a sistemas importantes como lo es el firewall.
- Ante nuevas modalidades usadas por los atacantes el IDS requerirá una reconfiguración de sus perfiles de monitoreo.

CONCLUSIONES

Los emprendedores deben reconocer que al llevar sus productos al mercado mundial a través de la internet no solo amplían el rango comercial, sino que en ese contexto se pueden llegar a generar nuevos desafíos y amenazas que puedan afectar radicalmente la continuidad del negocio; con el fin de resolver esta situación se debe pensar en la implementación de seguridad informática como una inversión y en ese campo el hardening aporta un retorno a la inversión positivo, esto lo hace valido para ser tenido en cuenta al realizar implementaciones de seguridad en ese ámbito.

No obstante, se evidencio la importancia de verificar la correcta configuración de los elementos de seguridad del sistema operativo, dado que es la parte principal del aseguramiento, al aplicar los cambios requeridos y mantener constantemente una configuración optima, así mismo se puede llegar a un nivel de confianza alto que genere que los sistemas funcionen correctamente y que la empresa pueda enfocarse en su crecimiento.

Por otra parte, se detectó que no basta solo con realizar una inversión en equipos y software, dado que toda la implementación con relación a la seguridad debe estar acompañada por una buena capacitación a la totalidad de usuarios y la incorporación de protocolos y políticas de seguridad que refuercen esas herramientas.

RECOMENDACIONES

Los administradores y dueños de las PYMEs deben concientizarse sobre la necesidad de implementar un Sistema de Gestión de seguridad de la información que facilite el aseguramiento de los sistemas.

Es importante fortalecer las políticas de seguridad informática en ese tipo de empresas, en caso de no contar con ellas se deben crear de acuerdo a sus requerimientos específicos.

El aseguramiento de los sistemas debe funcionar de manera permanente, mínimo se debe contar con herramientas de monitoreo en tiempo real y la instalación automática de actualizaciones críticas.

Es ideal que se contemple dentro de los manuales de cargos y funciones, los roles y/o cargos concernientes a la seguridad informática, si el tamaño de la empresa lo permite, se debería destinar en lo posible, personal con exclusividad para esa misión.

BIBLIOGRAFÍA

Ataques dirigidos. En: Kaspersky [en línea]. 16 de febrero de 2017. [Consultado: Mayo 3 de 2019]. Disponible en: https://latam.kaspersky.com/resource-center/threats/targeted-virus-attacks.

Ransomware. En: Malwarebytes [en línea]. [Consultado 3 mayo de 2019] disponible en: https://es.malwarebytes.com/ransomware/.

CATOIRA, Fernando. 5 consejos para controlar una infección por malware. En: WeLiveSecurity [en línea]. Marzo 13 de 2012 [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2012/03/13/consejos-controlar-infeccion-malware/

ALVAREZ, Wendy. ¿Es la innovación en las pymes colombianas una estrategia para el comercio internacional?, Bogotá, 2014, 23 p, Ensayo. Universidad Militar Nueva Granada.

GIUSTO, Denise. Países más afectados por el ransomware en Latinoamérica durante 2018.

COBB, Stephen. El ransomware continúa siendo una amenaza peligrosa para las empresas. En: WeLiveSecurity [en línea]. Noviembre 7 de 2018 [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2018/11/07/ransomware-continua-amenaza-peligrosa-empresas/

PAUS, Lucas. Ransomware: 10 formas en las que puede comportarse al infectar un sistema. En: WeLiveSecurity [en línea]. 29 de mayo de 2018. [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2018/05/29/formas-ransomware-puede-comportar-al-infectar-sistema/.

MENDOZA, Miguel. El impacto del ransomware en Latinoamérica durante 2017. En: WeLiveSecurity [en línea]. Marzo 1 de 2018. [Consultado 3 mayo de 2019]

[Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/

MENDEZ, Javier. 10 errores de seguridad que su pyme NO debe cometer. [en línea]. En: Revista Enter. Abril 24 de 2019. [Consultado 3 mayo de 2019] Disponible en: https://www.enter.co/especiales/empresas/10-errores-de-seguridad-que-su-pyme-no-debe-cometer/

CRUZ, Claudia. Windows 10 es el sistema operativo más usado del mundo En: CNET [en línea]. Enero 2 de 2019. [Consultado: 3 mayo de 2019] Disponible en: https://www.cnet.com/es/noticias/windows-10-es-el-sistema-operativo-mas-usado-en-las-computadoras-del-mundo/

Phishing, En: Avast [en línea]. [Consultado 8 mayo de 2019] disponible en: https://www.avast.com/es-es/c-phishing

El 'phishing' se disfraza de correo. En: ComputerWorld [en línea]. 3 de Agosto de 2018 [Consultado 8 mayo de 2019] disponible en: https://cso.computerworld.es/proteccion-de-datos/el-phishing-se-disfraza-de-correo

Las estafas en las que se utiliza el email corporativo crecerán un 69%. En: IT Digital Security [en línea]. 25 de enero de 2018. [Consultado 8 mayo de 2019]. disponible en: https://www.itdigitalsecurity.es/vulnerabilidades/2018/01/las-estafas-en-las-que-se-utiliza-el-email-corporativo-creceran-un-69

The most vulnerable players of 2017. En: TechTalk [en línea]. Marzo 29 de 2018 [Consultado 8 mayo de 2019] disponible en: https://techtalk.gfi.com/the-most-vulnerable-players-of-2017/

Aprendiendo a identificar los 10 phishing más utilizados por ciberdelincuentes. En: OSI. [en línea]. [Consultado 8 mayo de 2019] disponible en: https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen

BORTNIK, Sebastián. Defensa en profundidad. En: WeliveSecurity [en línea]. 24 de mayo de 2010. [Consultado 8 mayo de 2019] disponible en: (https://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/

ISO 27001: Componentes de la defensa en profundidad. En: SGSI [en línea]. 14 de enero de 2015. [Consultado 8 mayo de 2019] disponible en: https://www.pmg-ssi.com/2015/01/iso-27001-componentes-de-la-defensa-en-profundidad

BRAGG, Roberta, Roberta Bragg's 10 Windows hardening tips in 10 minutes. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019]. disponible en: https://searchsecurity.techtarget.com/tip/Roberta-Braggs-10-Windows-hardening-tips-in-10-minutes?

BRAGG, Roberta, Strengthen the password policy. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchenterprisedesktop.techtarget.com/feature/Strengthen-the-password-policy?_SS

BRAGG, Roberta, Lock down administrative workstations. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/feature/Lock-down-administrative-workstations?_SS

BRAGG, Roberta, Physically secure all systems. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999836/Physically-secure-all-systems?_SS

BRAGG, Roberta, Disable EFS. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999853/Disable-EFS

BRAGG, Roberta, Ban wireless networks that don't meet tough security policy requirements. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999855/Ban-wireless-networks-that-dont-meet-tough-security-policy-requirements

BRAGG, Roberta, Don't allow unprotected laptops and desktops to connect to the LAN. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999861/Dont-allow-unprotected-laptops-and-desktops-to-connect-to-the-LAN

BRAGG, Roberta, Use Runas or Su. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/feature/Use-Runas-or-Su

BRAGG, Roberta, Keep secrets. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019]disponible en: https://searchenterprisedesktop.techtarget.com/news/999842/Keep-secrets?_SS

BRAGG, Roberta, Disable infrared file transfer. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999910/Disable-infrared-file-transfer

GUTIERREZ, Camilo. 7 motivos por los que necesitas tener un antivirus. En: WeLiveSecurity [en línea]. 6 de enero de 2017 [Consultado 16 octubre de 2019] disponible en: https://www.welivesecurity.com/la-es/2017/01/06/motivos-tener-un-antivirus/

VAZQUEZ, Lucia. La importancia de los antivirus y la seguridad en las empresas. En: Empresa y Economía [en línea]. 12 de marzo de 2012 [Consultado 16 octubre de 2019] disponible en: http://empresayeconomia.republica.com/aplicaciones-para-empresas/la-importancia-de-los-antivirus-y-la-seguridad-en-las-empresas.html

Detección de Intrusos en Tiempo Real. En: segu-info [en línea]. [Consultado 16 octubre de 2019] disponible en: https://www.segu-info.com.ar/proteccion/deteccion.htm

¿Por qué fracasan las pymes en Colombia?. En: Revista Dinero [en línea]. Febrero 9 de 2015 [Consultado 8 mayo de 2019] disponible en: https://www.dinero.com/economia/articulo/pymes-colombia/212958

GUTIERREZ, Pedro. Tipos de criptografía: simétrica, asimétrica e hibrida. . En: GenBeta [en línea]. 25 de agosto de 2017 [Consultado 16 octubre de 2019] disponible en: https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Cryptojacking. En: Malwarebytes [en línea]. [Consultado 3 mayo de 2019] Disponible en: https://es.malwarebytes.com/cryptojacking/

Ataques de cadena de suministro. [en línea]. Marzo 6 de 2019 [Consultado 3 mayo de 2019] disponible en: https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/supply-chain-malware

POLICIA NACIONAL DE COLOMBIA. Informe: Balance Cibercrimen en Colombia 2017. Bogotá: Centro Cibernético Policía Nacional, 2017. p. 1 y 7.

EY, Encuesta Global de Seguridad de la Información 2018-19. Bogotá: EY, 2019. p. 37.

Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad. En: Revista Dinero. [en línea]. [Citada: 16 oct. 2019] https://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos,

del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1999

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 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. Diario Oficial. Bogotá, D.C., 2009

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012

UNIÓN EUROPEA. PARLAMENTO EUROPEO. Reglamento general de protección de datos (27, abril, 2016). Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. EUR-Lex. Bruselas. 2016

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 590. (10, julio, 2000). Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa. Diario Oficial. Bogotá, D.C., 2000

How does AES encryption work? Advanced Encryption Standard. [video]. YouTube, Shad Sluiter (23 de Agosto de 2019). 12:49 minutos. [consultado: 3 noviembre 2019]. Disponible en: https://www.youtube.com/watch?v=lnKPoWZnNNM

Intercambio de llaves Diffie-Hellman. [video]. YouTube, Khan Academy. 2:18 minutos [consultado: 3 noviembre 2019]. Disponible en:

https://es.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-2

MICROSOFT, Informe de Inteligencia de Seguridad de Microsoft. Redmond: SIRT, 2019. p. 9-11, 25.

Formato Resumen Analítico especializado (RAE)

Tema:	Eficiencia y eficacia de las metodologías hardening en la reducción de vulnerabilidades de las PYME en Colombia
Título:	ESTUDIO DE LA EFICIENCIA Y EFICACIA DE LAS METODOLOGÍAS HARDENING EN LA REDUCCIÓN DE VULNERABILIDADES EN LAS EMPRESAS COLOMBIANAS
Autor:	ÁLVARO AUGUSTO FUENTES FORERO
Fuente Bibliográfica:	Ataques dirigidos. En: Kaspersky [en línea]. 16 de febrero de 2017. [Consultado: Mayo 3 de 2019]. Disponible en: https://latam.kaspersky.com/resource-center/threats/targeted-virus-attacks. Ransomware. En: Malwarebytes [en línea]. [Consultado 3 mayo de 2019] disponible en: https://es.malwarebytes.com/ransomware/. CATOIRA, Fernando. 5 consejos para controlar una infección por malware. En: WeLiveSecurity [en línea]. Marzo 13 de 2012 [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2012/03/13/consejos-controlar-infeccion-malware/ ALVAREZ, Wendy. ¿Es la innovación en las pymes colombianas una estrategia para el comercio internacional?, Bogotá, 2014, 23 p, Ensayo. Universidad Militar Nueva Granada. GIUSTO, Denise. Países más afectados por el ransomware en Latinoamérica durante 2018. COBB, Stephen. El ransomware continúa siendo una amenaza peligrosa para las empresas. En: WeLiveSecurity [en línea]. Noviembre 7 de 2018 [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2018/11/07/ransomware-continua-amenaza-peligrosa-empresas/ PAUS, Lucas. Ransomware: 10 formas en las que puede comportarse al infectar un sistema. En: WeLiveSecurity [en línea]. 29 de mayo de 2018. [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2018/05/29/formas-ransomware-puede-comportar-al-infectar-sistema/. MENDOZA, Miguel. El impacto del ransomware en Latinoamérica durante 2017. En: WeLiveSecurity [en línea]. Marzo 1 de 2018. [Consultado 3 mayo de 2019] [Consultado 3 mayo de 2019] disponible en https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/ MENDEZ, Javier. 10 errores de seguridad que su pyme NO debe cometer. [en línea]. En: Revista Enter. Abril 24 de 2019. [Consultado 3 mayo de 2019] Disponible en: https://www.enter.co/especiales/empresas/10-errores-de-seguridad-que-su-pyme-no-debe-cometer/ CRUZ, Claudia. Windows 10 es el sistema operativo más usado del mundo En: CNET [en línea]. Enero 2 de 2019. [Consultado: 3 mayo de 2019] Disponible en: https://www.cnet.com/es/noticias/windows-10-es-el-sistema-operativo-mas-usado-en-las-computadoras-del-mundo/ Phishing, En: Avast [en línea]. [Consultado 8 mayo de 2019] disponible en: https://www.avast.com/es-es/c-phishing El 'phishing' se disfraza de correo. En: ComputerWorld [en línea]. 3 de Agosto de 2018 [Consultado 8 mayo de 2019] disponible en: https://cso.computerworld.es/proteccion-de-datos/el-phishing-se-disfraza-de-correo Las estafas en las que se utiliza el email corporativo crecerán un 69%. En: IT Digital Security [en línea]. 25 de enero de 2018. [Consultado 8 mayo de 2019]. disponible en: https://www.itdigitalsecurity.es/vulnerabilidades/2018/01/las-estafas-en-las-que-se-utiliza-el-email-corporativo-creceran-un-69 The most vulnerable players of 2017. En: TechTalk [en línea]. Marzo 29 de 2018 [Consultado 8 mayo de 2019] disponible en: https://techtalk.gfi.com/the-most-vulnerable-players-of-2017/ Aprendiendo a identificar los 10 phishing más utilizados por ciberdelincuentes. En: OSI. [en línea]. [Consultado 8 mayo de 2019] disponible en: https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen

BORTNIK, Sebastián. Defensa en profundidad. En: WeliveSecurity [en línea]. 24 de mayo de 2010. [Consultado 8 mayo de 2019] disponible en: (https://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/

ISO 27001: Componentes de la defensa en profundidad. En: SGSI [en línea]. 14 de enero de 2015. [Consultado 8 mayo de 2019] disponible en: https://www.pmg-ssi.com/2015/01/iso-27001-componentes-de-la-defensa-en-profundidad

BRAGG, Roberta, Roberta Bragg's 10 Windows hardening tips in 10 minutes. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019]. disponible en: https://searchsecurity.techtarget.com/tip/Roberta-Braggs-10-Windows-hardening-tips-in-10-minutes?

BRAGG, Roberta, Strengthen the password policy. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchenterprisedesktop.techtarget.com/feature/Strengthen-the-password-policy?_SS

BRAGG, Roberta, Lock down administrative workstations. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/feature/Lock-down-administrative-workstations?_SS

BRAGG, Roberta, Physically secure all systems. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999836/Physically-secure-all-systems?_SS

BRAGG, Roberta, Disable EFS. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999853/Disable-EFS

BRAGG, Roberta, Ban wireless networks that don't meet tough security policy requirements. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999855/Ban-wireless-networks-that-dont-meet-tough-security-policy-requirements

BRAGG, Roberta, Don't allow unprotected laptops and desktops to connect to the LAN. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999861/Dont-allow-unprotected-laptops-and-desktops-to-connect-to-the-LAN

BRAGG, Roberta, Use Runas or Su. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/feature/Use-Runas-or-Su

BRAGG, Roberta, Keep secrets. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019]disponible en: https://searchenterprisedesktop.techtarget.com/news/999842/Keep-secrets?_SS

BRAGG, Roberta, Disable infrared file transfer. En: Search Enterprise [en línea]. [Consultado 12 octubre de 2019] disponible en: https://searchwindowsserver.techtarget.com/news/999910/Disable-infrared-file-transfer

GUTIERREZ, Camilo. 7 motivos por los que necesitas tener un antivirus. En: WeLiveSecurity [en línea]. 6 de enero de 2017 [Consultado 16 octubre de 2019] disponible en: https://www.welivesecurity.com/la-es/2017/01/06/motivos-tener-un-antivirus/

VAZQUEZ, Lucia. La importancia de los antivirus y la seguridad en las empresas. En: Empresa y Economía [en línea]. 12 de marzo de 2012 [Consultado 16 octubre de 2019] disponible en: http://empresayeconomia.republica.com/aplicaciones-para-empresas/la-importancia-de-los-antivirus-y-la-seguridad-en-las-empresas.html

Detección de Intrusos en Tiempo Real. En: segu-info [en línea]. [Consultado 16 octubre de 2019] disponible en: https://www.segu-info.com.ar/proteccion/deteccion.htm

¿Por qué fracasan las pymes en Colombia?. En: Revista Dinero [en línea]. Febrero 9 de 2015 [Consultado 8 mayo de 2019] disponible en: https://www.dinero.com/economia/articulo/pymes-colombia/212958

	GUTIERREZ, Pedro. Tipos de criptografía: simétrica, asimétrica e hibrida. . En: GenBeta [en línea]. 25 de agosto de 2017 [Consultado 16 octubre de 2019] disponible en: https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida Cryptojacking. En: Malwarebytes [en línea]. [Consultado 3 mayo de 2019] Disponible en: https://es.malwarebytes.com/cryptojacking/ Ataques de cadena de suministro. [en línea]. Marzo 6 de 2019 [Consultado 3 mayo de 2019] disponible en: https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/supply-chain-malware POLICIA NACIONAL DE COLOMBIA. Informe: Balance Cibercrimen en Colombia 2017. Bogotá: Centro Cibernético Policía Nacional, 2017. p. 1 y 7. EY, Encuesta Global de Seguridad de la Información 2018-19. Bogotá: EY, 2019. p. 37. Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad. En: Revista Dinero. [en línea]. [Citada: 16 oct. 2019] https://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1999 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 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. Diario Oficial. Bogotá, D.C., 2009 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012 UNIÓN EUROPEA. PARLAMENTO EUROPEO. Reglamento general de protección de datos (27, abril, 2016). Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. EUR-Lex. Bruselas. 2016 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 590. (10, julio, 2000). Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa. Diario Oficial. Bogotá, D.C., 2000 How does AES encryption work? Advanced Encryption Standard. [video]. YouTube, Shad Sluiter (23 de Agosto de 2019). 12:49 minutos. [consultado: 3 noviembre 2019]. Disponible en: https://www.youtube.com/watch?v=lnKPoWZnNNM Intercambio de llaves Diffie-Hellman. [video]. YouTube, Khan Academy. 2:18 minutos [consultado: 3 noviembre 2019]. Disponible en: https://es.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-2 MICROSOFT, Informe de Inteligencia de Seguridad de Microsoft. Redmond: SIRT, 2019. p. 9-11, 25.
Año:	2020
Resumen:	En la presente monografía denominada “El estudio de la eficiencia y eficacia de las metodologías hardening en la reducción de vulnerabilidades en las empresas colombianas”, busca en un principio conocer el estado en ciberseguridad en que se encuentra este gran segmento del mercado y plantea señalar el conjunto de medidas básicas que permitirán mejorar la seguridad y reducir los incidentes en los equipos de cómputo con sistemas operativos Windows en empresas de ese país.

	La monografía cuenta con tres objetivos específicos los cuales servirán de guía a las PYMEs colombianas que buscan alcanzar el aseguramiento de sus sistemas informáticos, para lo cual requirieran reducir las posibilidades de ser afectados por ataques recurrentes y minimizar el número de vulnerabilidades al implementar las medidas expuestas en el documento, las cuales van desde el cambio de contraseñas, desinstalar software no seguro, eliminar las credenciales de usuarios, deshabilitar servicios que no serán usados y fortalecer las configuraciones de aquellos que estarán en uso. A pesar de que este documento este enfocado en las PYME, también servirá de guía para que otro tipo de entidades de carácter público y privado e incluso particulares que busquen mejoras de seguridad informática.
Palabras Claves:	Endurecimiento, Sistema Operativo, Seguridad Informática, Sistemas Endurecidos, Pequeña Y Mediana Empresa (Pyme), Ransomware, Copia De Seguridad, Phishing, Malware, Vulneración De Correo Electrónico De Empresas (Bec), Defensa En Profundidad.
Contenidos:	PLANTEAMIENTO DEL PROBLEMA FORMULACIÓN DEL PROBLEMA JUSTIFICACIÓN OBJETIVO GENERAL OBJETIVOS ESPECIFICOS MARCO REFERENCIAL MARCO CONCEPTUAL MARCO LEGAL DIAGNOSTICO DE LA SITUACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LAS PYMES COLOMBIANAS IMPLICACIONES QUE HACEN NECESARIA LA IMPLEMENTACIÓN DEL HARDENING EN LAS PYMES COLOMBIANAS VENTAJAS QUE OFRECE EL ASEGURAMIENTO DE EQUIPOS CON SISTEMA OPERATIVO WINDOWS. BUENAS PRÁCTICAS EN LA IMPLEMENTACIÓN DE HARDENING CONCLUSIONES RECOMENDACIONES
Descripción del problema de investigación:	Las empresas colombianas hoy en día si aún no han migrado al mundo digital, planean hacerlo a corto plazo, debido al potencial que encuentran en la red de redes para brindar sus servicios, desde una plataforma donde puedan permanecer conectados las 24 horas con sus potenciales clientes. Esto puede llegar a generar el riesgo de ser atacados física y virtualmente por personas inescrupulosas, ya sea con fines de espionaje corporativo, razones políticas o personales, extorsiones, o como plataforma para atacar a una entidad aún más grande. Según artículo del diario el país (España) el 53% de las pequeñas y medianas empresas reconocieron haber sufrido ciberataques durante el 2017, una cifra alarmante que alcanzó tal punto debido a que estas entidades no cuentan con una infraestructura mínima requerida (personal calificado y equipos). Las organizaciones efectivas deberían tener una línea base de seguridad en sus equipos, que garanticen un nivel mínimo satisfactorio de seguridad, pero las PYMEs no suelen prestar atención a los problemas que conlleva no contar con los hardware y software apropiados que garanticen su seguridad informática. Esto se debe generalmente al poco nivel de formación y de información con la que cuentan a la hora de tomar decisiones en ese campo. Los emprendedores y gerentes suelen capacitarse en temas como mercadeo, publicidad y ventas; sin embargo, no se forman en los conceptos básicos de seguridad y del tratamiento adecuado de debe recibir la información, a pesar de que no se esperaría un conocimiento técnico altamente especializado, los directivos deberían tener niveles aceptables de conocimiento en los campo básicos de la seguridad informática que le permitan entender la importancia del cifrado de la información, políticas de seguridad y protección de datos, acuerdos de confidencialidad, manejo de incidentes, etc. El hardening permite realizar un análisis de vulnerabilidades enfocado en encontrar fallas de seguridad y medir el impacto que estas tienen sobre los activos de la entidad, identificando estas falencias se establece un plan con los pasos necesarios para fortalecer y soportar ataques a los que los sistemas estarían siendo expuestos.
Objetivo General:	Estudiar la metodología Hardening y el impacto que esta tendría en las pequeñas y medianas empresas de Colombia al reducir sus vulnerabilidades a ciberataques, a través de la recopilación y análisis de la bibliografía sobre esta temática, para lo cual se referenciarán herramientas de análisis y protección con el fin de evidenciar su eficiencia y eficacia.
Objetivos Específicos:	Realizar un diagnóstico de la situación del estado actual de la seguridad informática en las PYMES colombianas.

	Analizar las implicaciones que tendrían los equipos de cómputo con sistema operativo Windows al implementarse el hardening. Identificar las ventajas que tienen las herramientas como el Antivirus, sistema de detección de Intrusos, contraseñas y criptografía para mejorar la seguridad informática de los equipos de cómputo de las empresas.
Metodología:	Se llevó a cabo a través de una metodología descriptiva y documental, siguiendo el desarrollo de cada uno de los objetivos, primeramente, se hizo una búsqueda y recopilación de información, generando el diagnóstico de la situación del estado actual de la seguridad informática en las pymes colombianas y las implicaciones por las que se hace necesaria la implementación del hardening en ellas, posteriormente se realizó un análisis llegando a conocer las ventajas que ofrece el aseguramiento de equipos con sistema operativo Windows y se estableció un listado de buenas prácticas en la implementación de hardening, finalizando con unas conclusiones y recomendaciones.
Principales referentes teóricos y conceptuales:	Se tomó como referentes principales para la creación del documento el Informe de Inteligencia de Seguridad de Microsoft, en donde se pudo evidenciar las afectaciones presentadas en Latinoamérica en la distribución de código malicioso, ramnsonware, señalando que Colombia se encuentra junto a la mayoría de los países vecinos situados entre el rango (0,05% al 0,10%) de incidentes mensuales. Por otro lado se estableció que durante el 2018, los atacantes utilizaron diferentes artimañas, tanto nuevas (minería de moneda o coin-mining) como antiguas (suplantación de identidad o phishing)", en su búsqueda continua de robar datos y recursos a clientes y organizaciones, de nuevo Colombia se encuentra junto a la mayoría de los países del cono sur entre el rango de 0 a 0,20% de incidentes reportados por mes. En este mismo informe se alerta por un aumento en los clics que se dan a los enlaces relacionados con la suplantación de identidad (phishing), convirtiéndose en el tipo de ataque predilecto por los atacantes, de acuerdo al mismo análisis se detectó: un aumento del 250 por ciento entre enero y diciembre de 2018 de mensajes de suplantación de identidad (phishing). Por otro lado, se tuvieron en cuenta como referente los informes difundidos por el CAI Virtual de la Policía Nacional, en el Informe Balance del Cibercrimen en Colombia 2017, se contextualizó sobre el aumento exponencial que tendría el el cibercrimen en el país, teniendo en cuenta que en el 2017 aumentó un 28.3%, se señala que "La principal modalidad que afecta a los ciudadanos y empresas en el país son las estafas, bien sea a través de un correo electrónico, un mensaje de texto, una llamada, una falsa oferta de empleo o una estafa de compra online." En el informe difundido por la misma entidad denominado Costos del Cibercrimen en Colombia 2016 – 2017, se alerta por la afectación que tuvo el ramsonware en el país, específicamente en el segmento conformado por las PYMEs, donde se señala que se atendieran a 52 víctimas, que denunciaron ser afectados por este programa malicioso.
Resultados	Concientización a los administradores y dueños de las PYMEs sobre la necesidad de implementar un Sistema de Gestión de seguridad de la información que facilite el aseguramiento de los sistemas. Se demostró la necesidad de crear y fortalecer las políticas de seguridad en ese tipo de empresas. Se evidenció que los sistemas requieren para su aseguramiento de permanente monitoreo y la instalación de actualizaciones críticas. Se definió la necesidad de crear dentro del talento humano de las entidades roles y/o cargos concernientes a la seguridad informática. Se propuso controles para los riesgos evidenciados

Conclusiones	Los emprendedores deben reconocer que al llevar sus productos al mercado mundial a través de la internet no solo amplían el rango comercial de maniobra, sino que en ese contexto se generan nuevos desafíos y amenazas que pueden afectar radicalmente la continuidad del negocio, con el fin de resolver esta situación se debe pensar en la seguridad informática como una inversión y en ese campo el hardening aporta un retorno a la inversión positivo, esto lo hace valido para ser tenido en cuenta al realizar implementaciones de seguridad en ese ámbito. Verificar la correcta configuración de los elementos de seguridad del sistema operativo es la parte principal del aseguramiento, al aplicar los cambios requeridos y mantener contantemente una configuración optima, se puede llegar a un nivel de confianza alto que genere que los sistemas funcionen correctamente y que la empresa pueda enfocarse en su crecimiento. Para alcanzar el éxito en la carrera de la seguridad informática, no basta solo con realizar una inversión en equipos y software, toda implementación hecha debe estar acompañada por una buena capacitación a la totalidad de usuarios y la incorporación de protocolos y políticas de seguridad que refuercen esas herramientas.
AUTOR	ÁLVARO AUGUSTO FUENTES FORERO