MASTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES (MISTIC)

Desarrollo de una guía de controles de ciberseguridad para la protección integral de la PYME

TRABAJO FINAL DE MÁSTER

ESTUDIANTE: GABRIELA RATTI BITTINGER

DIRECTOR: MARCO ANTONIO LOZANO MERINO

EMPRESA: Instituto Nacional de Ciberseguridad de España (INCIBE)

Diciembre 2017

Resumen

La ciberseguridad se ha posicionado, a lo largo de los últimos años, como una de las principales preocupaciones de las empresas de todo el mundo. Si bien, la dependencia tecnológica de un negocio varía enormemente de acuerdo a múltiples factores, es innegable que hoy en día la gran mayoría de las empresas ha ido incorporando la tecnología como una herramienta importantísima para la supervivencia del negocio. Esto ha generado una enorme cantidad de oportunidades y ha representado un avance con respecto a la manera antigua y tradicional de manejar la información y los procesos; sin embargo, también ha traído consigo muchos riesgos, entre ellos los ciberataques, que han ido evolucionando también a la par que las tecnologías, con un enorme abanico de amenazas, técnicas y objetivos de ataques. Entre las amenazas, podemos encontrar a cibercriminales, *hacktivistas*, gobiernos hostiles, amenazas internas como empleados infieles, entre muchos otros. Las técnicas para llevar a cabo un ciberataque también son muy diversas y han ido mutando a lo largo del tiempo, desde *malware* (software malicioso), phishing, denegación de servicio, explotación de vulnerabilidades de software, entre muchas otras. Los objetivos pueden variar desde la simple diversión de "*hackear*" hasta la obtención de importantes beneficios económicos o incluso la disrupción completa de un negocio determinado.

Las micro, pequeñas y medianas empresas están igualmente expuestas a estos riesgos. Muchas PYMEs son víctimas de ciberataques diversos, desde infecciones por malware, phishing, desfiguración de sitios web, fuga de información, entre muchos otros. Muchas veces una PYME es atacada para, a través de ella, hacer daños a terceros. Según el Instituto Nacional de Seguridad (INCIBE), en 2016 se detectaron más de 115.000 incidentes cibernéticos, de los cuales alrededor del 70% fueron contra PYMES. El coste económico promedio de un ciberdelito en España ronda entre 20.000 y 50.000 euros. Teniendo en cuenta, además, que las PYMES representan más del 90% de la economía de la mayoría de los países, el impacto que pueden generar los ciberataques a este sector es significativo. Una gran dificultad a la que se enfrentan las PYMEs es que, a diferencia de una empresa grande, muchas veces no cuentan con los recursos necesarios para protegerse de manera adecuada.

Esto nos obliga a aumentar los esfuerzos para fortalecer la seguridad de las PYMEs de una forma integral, efectiva y práctica. Este Trabajo Final de Master ha buscado diseñar una guía de controles de seguridad de fácil implementación en una PYME, no solo basado en las buenas prácticas y normas vigentes, sino teniendo también en cuenta la realidad de estas micro, pequeñas y medianas empresas, en cuanto a los riesgos más críticos y los controles más efectivas para estos riesgos, de acuerdo a los recursos de tiempo, dinero y conocimiento que una PYME puede realmente destinar para alcanzar un nivel de protección aceptable.

Summary

In recent years, cybersecurity has become one of the main concerns of companies around the world. Although, the technological dependence of a business varies enormously according to multiple factors, it is undeniable that nowadays the most companies have been incorporating technology as a very important tool for business survival. This has created many opportunities and represents an improvement over the old, traditional way to manage information and processes; however, it has also brought many risks, including cyber attacks, which have also evolved along with technologies, with a huge range of threats, techniques and goals. Among the threats, we can find cybercriminals, hacktivists, hostile governments, internal threats as disgruntled employees and many others. The techniques to carry out a cyber attack are also very diverse and have been mutating over time, from malware (malicious software), phishing, denial of service, exploitation of software vulnerabilities, among many others. The goals of an attack can vary from simple fun of "hacking", to obtaining significant economic benefits or even the complete disruption of a certain business.

Micro, small and medium enterprises (SME) are equally exposed to these risks. Many SMEs are victims of various cyber attacks, from malware infections, phishing, website disfigurement, information leakage, among many others. Often an SME is attacked to damage third parties through it. According to the National Security Institute (INCIBE), in 2016 more than 115,000 cyber incidents were detected, of which almost 70% were against SMEs. The average economic cost of a cybercrime in Spain is between 20,000 and 50,000 euros. Considering that SMEs represent more than 90% of the economy of most countries, the impact that cyber attacks on this sector can generate is significant. A great difficulty faced by SMEs is that, unlike a large company, they often do not have necessary resources to protect themselves.

Therefore, we need to increase efforts to strengthen the security of SMEs in a comprehensive, effective and practical way. This Master's Final Project has sought to design a security controls guide that is easy to implement in an SME, not only based on good practices and current standards, but also considering the reality of these micro, small and medium-sized companies, in terms of the most critical risks and the most effective controls for those risks, according to the resources of time, money and knowledge that an SME can use to achieve an acceptable level of protection.

Índice de contenidos

Capítulo 1: Introducción

Justificación

Las tecnologías de la información y comunicación han avanzado y revolucionado por completo el mundo, en todos sus aspectos, entre ellos, el manejo de información y los procesos de negocio. Prácticamente todas las empresas de todos los sectores y de todos tamaños, incluidas las PYMEs, han ido incorporando tecnología, en mayor o menor medida. En algunos casos, el negocio se basa de manera fundamental en la tecnología; en otros casos, se apoya en la tecnología como un instrumento. En ambos casos, la competitividad de una empresa está fuertemente ligada al aprovechamiento óptimo de la tecnología, siendo este factor un diferenciante importante de una empresa frente a su competencia.

Los riesgos relacionados a la tecnología también han ido evolucionando. Los ciberataques se han diversificado, son cada vez más frecuentes, más sofisticados y, al mismo tiempo, más fáciles de ser llevados a cabo. Sin embargo, los ciberataques no son el único riesgo. Existen riesgos relacionados a eventos fortuitos como ser el daño de un equipo informático, los errores humanos involuntarios, catástrofes naturales, entre muchos otros. Todos estos riesgos pueden, potencialmente, tener un impacto negativo sobre los sistemas de información de una empresa y, por tanto, sobre el negocio.

Este escenario cambiante ha obligado a que la ciberseguridad, como un ecosistema completo, haya ido evolucionando y madurando. Se han llevado adelante numerosas iniciativas para ello, desde todos los sectores, como la industria, los gobiernos, las empresas, la Academia, y muchos otros. Entre otras cosas, se comprendió que la ciberseguridad no es un estado estático, sino que es un proceso continuo, de gestión, que requiere controles continuos que permitan medir, analizar, mejorar y controlar el estado de nuestros activos de información. Se han elaborado normas, estándares y *frameworks* tales como ISO 27000, COBIT, NIST CSF, PCI y otros, que buscan ser instrumentos de protección integral, sistematizada y continua de muchos aspectos de ciberseguridad para proteger a las compañías. Algunos de estos instrumentos, como por ejemplo la familia de norma ISO 27000, son generales y no están orientadas a un sector en particular. Otras como, por ejemplo, la norma PCI o HIPAA, están orientados a sectores muy específicos (sistemas de pago y salud en EEUU, respectivamente) y por tanto pueden no ser adecuados para empresas de otros sectores.

A pesar del nivel de madurez relativamente alto de estas normas y *frameworks*, éstas no suelen ser del todo adecuadas para un importante sector: las PYMEs. Las pequeñas y medianas empresas promedio, con una dependencia tecnológica baja a media, no tienen los recursos necesarios para implementar estas normas, las cuales requieren tiempo, conocimiento y recursos financieros significativos. Sin embargo, estas pequeñas y medianas empresas también son víctimas de ciberataques por lo que también deben realizar un esfuerzo por protegerse.

Aun así, es importante notar que los riesgos a los cuales están expuestas una PYME no son los mismos de una gran corporación multinacional, por lo que las prioridades con respecto a la implementación de controles deberán ser distintas. Por ejemplo, una gran empresa probablemente deba preocuparse por el riesgo de espionaje corporativo o gubernamental, debiendo invertir recursos significativos para protegerse ante este tipo de escenarios. Sin embargo, un caso de *ransomware* genérico, no dirigido, que afecte a un único empleado de la empresa, no le genere una disrupción de negocio ya que, al ser una corporación grande, por su propia naturaleza y dimensión, es muy probable que los procesos y la información de negocio estén distribuidos a lo largo de múltiples sistemas y personas. Sin embargo, este mismo escenario podría ser fatal para una PYME, donde por lo general no existe esta distribución: si un *ransomware* genérico afectara al empleado encargado de las finanzas de una PYME, es muy probable que esto genere un impacto directo y una disrupción total de las operaciones de negocio de la PYME. Por tanto, este riesgo, que en una empresa grande probablemente será categorizado como bajo, en una PYME será crítico, debiendo priorizar los esfuerzos en este sentido.

Por otra parte, a pesar de que muchas veces una PYME no es el objetivo final, es cada vez más frecuente que los cibercriminales las ataquen para, a través de ellas, hacer daños a terceros. Por ejemplo, en los últimos años han aumentado significativamente los ataques dirigidos del tipo *"watering hole "*, en los que los criminales infectan una web de confianza que luego es visitada por los empleados de la empresa o entidad objetivo. Muchas veces, esa web de confianza corresponde a una pequeña o mediana empresa, cuya protección es muy inferior que la empresa objetivo. Otra técnica que ha ido aumentando significativamente en los últimos años es la denominada "*supply chain attack*" o ataque a la cadena de suministro: los criminales buscan comprometer a una empresa proveedora de la empresa objetivo, para de esta manera llegar a comprometer a ésta última. Entre los casos recientes podemos mencionar el de NotPetya, un malware disruptivo cuyo objetivo eran varias empresas críticas de Ucrania, y en cuyo caso, el vector de ataque inicial fue una actualización infectada del software M.E.doc, muy utilizado por estas empresas críticas. M.E.doc era una compañía pequeña, poca protegida, que, aunque no fue el objetivo del ataque, tenía clientes que eran el objetivo de los cibercriminales. Otro ejemplo reciente es el de CCleaner, un software muy popular de una pequeña compañía de software llamada Piriform. Este año, cibercriminales aprovecharon vulnerabilidades de dicha compañía para reemplazar el software por una versión troyanizada, logrando de esta manera infectar a millones de clientes de esta compañía. La investigación del caso demostró que el objetivo del ataque a Piriform no era simplemente distribuir malware a una gran cantidad de víctimas, sino a ciertos clientes muy específicos: empleados de grandes empresas como Google, Microsoft, Samsung, Cisco, etc., que hubieran instalado la versión troyanizada (Greenberg, 2017). Nuevamente vemos como los cibercriminales se aprovechan de pequeñas y medianas empresas, menos protegidas, para a través de ellas atacar a otros objetivos.

Es por ello que se deben impulsar iniciativas que busquen fortalecer la seguridad de las PYMEs de una forma integral, efectiva y práctica. Este Trabajo Final de Master busca diseñar una guía de controles de seguridad de fácil implementación en una PYME. En este trabajo, a diferencia de otras guías y *framework* de seguridad, no se ha basado únicamente en las buenas prácticas y normas conocidos, sino se ha tenido en cuenta, principalmente, la realidad de estas micro, pequeñas y medianas empresas: las particularidades de las PYMEs, los riesgos más críticos al negocio y los controles más efectivas para estos riesgos, teniendo en cuenta los recursos de tiempo, dinero y conocimiento que una PYME podría destinar.

Objetivo General

Diseñar una guía de controles de seguridad para la protección integral, efectiva y eficaz de una PYME.

Objetivos Específicos

- Conocer los riesgos más críticos, de acuerdo a su probabilidad e impacto, que afectan a una PYME promedio
- Conocer los recursos que una PYME promedio es capaz de destinar para su protección
- Elaborar una lista de controles y medidas de protección para PYMEs
- Proponer una metodología de implementación para la guía de controles de acuerdo a la realidad de una PYME
- Elaborar herramientas para implementar la guía de controles para las PYMEs

Metodología

En la primera fase para la elaboración de este trabajo, se ha realizado un estudio exploratorio para conocer el panorama general promedio de las PYMEs en Paraguay: qué tipo de procesos tienen informatizados, qué tipo de datos almacenan, cuáles son los riesgos que más les preocupan, qué tipo de tecnologías utilizan, qué tipo de red tienen, cuál es su capacidad en recursos humanos, entre otros. El objetivo de este estudio ha sido identificar los riesgos más críticos de una PYME, teniendo en cuenta probabilidad e impacto, así como también cuantificar los recursos que puede destinar una PYME para la protección ante estos riesgos (tiempo, recurso humano, costo, etc.), de acuerdo a la realidad nacional.

Para este estudio se ha utilizado una combinación de diversas metodologías: recopilación de información relevante de estudios regionales y/o internacionales previos, encuestas a través de mecanismos no presenciales a una muestra representativa y significativa, entrevistas presenciales a PYMEs de diferentes sectores y/o entrevistas a organismos competentes en la materia. Cabe destacar que dicho estudio se ha realizado en mi país de residencia, Paraguay, por lo cual refleja la realidad y las características propias de PYMEs paraguayas.

A partir de los resultados del estudio de la primera fase, se ha elaborado una lista exhaustiva de posibles controles que ayuden a mitigar los riesgos identificados. Se ha realizado un análisis de factibilidad de estos controles, teniendo en cuenta su efectividad y los recursos necesarios para su implementación control (tiempo, costo, cantidad de recursos humanos, etc.). De esta manera, se ha podido seleccionar un conjunto acotado de controles, de manera a que se encuentren dentro del margen de recursos que el estudio reveló que una PYMEs podría dedicarle.

Por último, se elaboró algunos instrumentos que ayuden a una PYME a incorporar la guía de controles a su negocio de manera simple, práctica y efectiva, de modo a que pueda tener un nivel de protección razonable. Entre estos instrumentos se destaca un ejemplo de implementación de la guía de controles, con una o más opciones de implementación, con herramientas y técnicas simples, prácticas y concretas, al alcance de una PYME, así como también una planilla de generación de controles, adaptable a la realidad de una PYME.

Capítulo 2: Ciberseguridad en PYMEs

Antecedentes

Hace varios años que se ha identificado la necesidad de aumentar los esfuerzos orientados a la protección a pequeñas y medianas empresas frente a ciberataques, siendo éstas un blanco importante para cibercriminales. Esto ocurre, en gran medida, debido a que, por lo general, las PYMEs no cuentan con los mismos niveles de protección de empresas grandes. Existen diversas razones para este fenómeno, entre las cuales podemos citar:

- Las PYMEs suelen creer que no son de interés para los criminales, y que por tanto no serán blancos de un ciberataque
- Cuentan con recursos limitados (recursos financieros, humanos, de tiempo y de conocimiento)
- La gestión de la seguridad de la información, como un proceso continuo y sistemático, no está incorporado en sus procesos de negocio
- No conocen mecanismos simples y prácticos para la protección de sus activos, que estén adaptados a su realidad
- La mayoría de las normas, estándares, y guías de seguridad no están pensados para PYMEs y son difíciles de "bajar a tierra".

Habiéndose identificado esta problemática se ha ido trabajando en diversos proyectos para elaborar herramientas, guías y recomendaciones orientadas a las pequeñas y medianas empresas. Desde el punto de vista de las herramientas tecnológicas (hardware y software) se puede afirmar que existen una infinidad de herramientas, incluso gratuitas, de fácil uso, pensadas especialmente para pequeñas empresas, para casi todas las posibles necesidades que podrían surgir. La gran mayoría de las empresas de seguridad ofrecen hoy en día soluciones de *endpoint security* (antivirus, cortafuegos, etc.) básicas y gratuitas, adecuadas para PYMEs. Existen numerosas organizaciones sin fines de lucro, asociaciones profesionales, investigadores independientes e incluso gobiernos que ofrecen diversas herramientas gratuitas, por lo general *open-source* y de libre distribución, que pueden ser de suma utilidad para PYMEs. Por lo tanto, se puede afirmar como hipótesis inicial, que el problema no se debe a una ausencia de herramientas tecnológicas sino más bien a una ausencia de gestión de la seguridad de la información que permita incorporar dichas herramientas de protección en los procesos de negocio de las PYMEs.

Como ya mencionamos, existen numerosas normas, estándares, *frameworks* y guías de gestión de la seguridad de la información, pensadas para la protección integral de una empresa, pero complejas para una PYME. En general, muchas de estas normas y estándares pueden resultar complejas incluso a empresas grandes, que no tengan una madurez elevada en cuanto a sistemas de gestión y procesos. Uno de los principales problemas de estas normas es que son muy generales, de muy alto nivel, y resulta difícil llevarlo a un nivel más concreto, a acciones concretas. Por ello, hace algunos años ha habido iniciativas para elaborar *frameworks* de seguridad simplificados, orientados a empresas más pequeñas o de menor madurez.

Una de las primeras iniciativas que se puede mencionar es la guía de 20 Controles de Seguridad Críticos de SANS (*CIS Critical Security Controls*). Este proyecto inició debido a una solicitud del Departamento de Defensa de los Estados Unidos planteada en el 2008 a la NSA (*National Security Agency*) de dicho país para priorizar las inversiones en ciberseguridad, buscando protecciones efectivas contra ataques conocidos. Este planteamiento sirvió como puntapié inicial para una colaboración entre la NSA, el Instituto SANS, el Centro para la Seguridad en Internet (*Center for Internet Security*, CIS) y otros actores claves, quienes formaron un consorcio para elaborar de forma consensuada una lista de controles de seguridad claves para mitigar ciberataques. El espíritu de este proyecto se basó en la firme creencia que un control de seguridad debe ser agregado a lista solo de acuerdo a su pertinencia real para mitigar ciberataques, focalizando en riesgos críticos reales. Se identificaron así 20 controles de seguridad, que fueron ampliamente adoptado en múltiples organizaciones, tanto públicas como privadas, dentro y fuera de

Estados Unidos. Si bien, esta lista no fue elaborada teniendo en mente a las pequeñas y medianas empresas, debido a su simplicidad en cuanto a la comprensión de la misma y a su efectividad, resulta adecuada para empresas que no tienen un nivel de madurez elevado en cuanto a ciberseguridad.

En el 2011, Russell Eubanks presentó una guía de implementación de los 20 controles críticos para una pequeña empresa de presupuesto reducido, en la que detalla una gran cantidad de herramientas y metodologías simples, concretas y poco costosas para implementar cada uno de estos controles en una empresa pequeña (Eubanks, 2017). Si bien, este trabajo facilita aún más la implementación de los controles propuestos, como se trata de un trabajo de hace más de 6 años, la tecnología y los ataques han ido cambiando, por lo que existen muchas otras herramientas y técnicas nuevas a las mencionadas, que podrían ser más adecuadas para una implementación actual de los controles.

Por otra parte, hay que tener en cuenta que los 20 controles críticos propuestos incluyen algunos controles que podrían ser difíciles de implementar para una empresa pequeña. Por ejemplo, uno de los controles propuestos es la realización de pruebas de penetración y ejercicios del tipo *Red team* (simulación de ciberataques). Si bien es cierto que existen incluso herramientas gratuitas para este tipo de pruebas y mucha información en Internet sobre cómo realizarlo, este control demanda un conocimiento medio-alto y un tiempo significativo. En una empresa mediana, que como mínimo tiene una persona dedicada exclusivamente a seguridad, o un equipo pequeño de al menos dos personas dedicadas a TI podría ser factible implementarlo. Sin embargo, en una micro o pequeña empresa, de por ejemplo 5 personas, que no cuenta con ningún empleado dedicado exclusivamente a TI, sería prácticamente imposible implementar dicho control. Además, el beneficio adicional que representa un *pentesting* con respecto a los demás controles, es relativamente bajo en una empresa pequeña.

En vista a estos problemas, el Centro para la Seguridad en Internet (*Center for Internet Security*, CIS) ha seleccionado los 5 controles prioritarios de la lista de 20 controles, los cuales han demostrado una alta efectividad en la mitigación de alrededor del 85% de los ciberataques conocidos (Center For Internet Security). Esta selección, publicada en un documento llamado "*First 5 CIS Controls Guide*", simplifica y reduce aún más el costo de implementación de los controles de seguridad, llegando de esta manera a ser adecuado para una PYME.

Otra iniciativa que se puede mencionar es el Decálogo de la Ciberseguridad para Empresas, elaborado y publicado por INCIBE en el 2014 y actualizado hace pocos días. Esta guía contiene los diez aspectos más relevantes a tener en cuenta para proteger convenientemente la información de nuestra empresa. Se trata de un documento breve, de fácil comprensión, pero general, de nivel medio-alto, cuya implementación requeriría un trabajo significativo por parte de la empresa, que debería previamente identificar el "cómo" hacerlo.

Una iniciativa similar en Latinoamérica es la de Colombia, donde el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) elaboró y publicó una Guía para la Implementación de Seguridad de la Información en una MIPYME. A diferencia de las iniciativas que se mencionaron previamente, esta guía se enfoca más en cuanto a políticas de seguridad y gestión de la seguridad de la información, que, aunque es más breve y más simplificado que normas como la ISO 27000, sigue siendo muy general, haciéndolo muy difícil para una PYME de traducirlo a acciones concretas.

Otra iniciativa interesante, orientada a PYMEs es la herramienta de autodiagnóstico de INCIBE, que permite, de forma simple y gratuita, realizar un primer análisis de riesgo en no más de 5 minutos (INCIBE). Se trata de una plataforma web que permite, a través de preguntas cortas y concretas, medir el nivel general de riesgo de una PYMEs en cuanto a gestión de personas, procesos y tecnología. Esta herramienta podría servir como insumo para el estudio exploratorio de la primera fase del presente trabajo.

No se encontró información acerca de iniciativas que hayan tomado en cuenta, de forma directa, la realidad de una PYME promedio, ni que haya realizado una estimación real del esfuerzo necesario por parte de la PYME para implementar los controles propuestos. El presente trabajo se centrará

principalmente en esta cuestión, de modo a acercar la teoría propuesta con la realidad alcanzable por una PYME.

Si bien, todas las iniciativas citadas han sido de suma utilidad como bases del presente trabajo, se debe tener en cuenta que los mismos fueron elaborados de acuerdo a la realidad estadounidense, europea, o de otros países de mayor madurez que Paraguay. Y si bien existen muchísimos factores comunes entre diferentes regiones del mundo, especialmente cuando se trata de tecnología, no se puede dejar de lado las particularidades tales como diferencias económicas, culturales, sociopolíticas, idiomáticas, legislativas, de madurez de la industria de ciberseguridad, entre muchas otras. Por ejemplo, en Estados Unidos existen numerosas empresas dedicadas a brindar servicios de ciberseguridad, desde pequeñas hasta multinacionales. Por lo tanto, una PYME tiene un enorme abanico de posibilidades para la contratación de servicios especializados, con precios accesibles y alta calidad. Sin embargo, en Paraguay, al igual que en muchos países menos avanzados en la materia, el mercado es limitado, habiendo pocas empresas dedicadas a brindar servicios y soluciones especializadas y de calidad para empresas pequeñas debido a que, en la actualidad, no les parece rentable este nicho de mercado. La gran mayoría de empresas dedicadas a ciberseguridad ofrecen solamente servicios o productos orientados a grandes empresas como por ejemplo los bancos, grandes empresas de telecomunicaciones o empresas multinacionales, que son, hoy por hoy, prácticamente los únicos potenciales clientes de dichos servicios. En el plano legislativo, por ejemplo, en Paraguay no existen prácticamente consecuencias legales ante fuga de informaciones, mal manejo de la información u otro tipo de incumplimientos que, en otros países representarían un enorme riesgo para las empresas y, por tanto, son motivadores para invertir en ciberseguridad.

Panorama de la ciberseguridad en PYMEs en Paraguay y el mundo

En Paraguay, casi el 97% de las unidades productivas corresponden a micro, pequeñas y medianas empresas (MiPYMEs). La definición de MiPYMEs suele variar entre países. De acuerdo a la legislación paraguaya, la ley Nro. 4457/12, éstas se definen de acuerdo a acuerdo a los siguientes criterios:

- Microempresa: empresa familiar (únicamente) de hasta 10 personas con una facturación anual de hasta 500.000.000 Gs (alrededor de 75.000 Euros)
- Pequeña Empresa: hasta 30 empleados con una facturación anual de hasta 2.500.000.000 Gs (alrededor de 380.000 Euros)
- Mediana Empresa: hasta 50 empleados con una facturación anual de hasta 6.000.000.000 Gs (alrededor de 845.000 Euros)

Esta definición varía sustancialmente con respecto a la definición de la Unión Europea, por ejemplo, especialmente en cuanto a la categoría de mediana empresa (hasta 250 empleados en UE) y con respecto a la facturación anual máxima de las tres categorías, que es alrededor de 20 veces mayor. La definición en Estados Unidos se basa en varios factores adicionales (sector de la empresa, tipo de empresa, número de empleados y facturación) siendo mucho más compleja la categorización.

De acuerdo al Censo Económico Nacional de Paraguay del año 2011, el último que se realizó en el país, se contabilizaron 224.242 unidades productivas, de las cuales el 96.9% correspondían a micro, pequeñas y medianas empresas, es decir, alrededor de 217.250 empresas. Sin embargo, menos del 1% de las MIPYMEs se encuentran registradas formalmente ante el Viceministerio de MiPYMEs, entidad gubernamental encargada de promover e incentivar el crecimiento de este sector productivo.

De dicho censo y según la definición actual, la cual fue establecida luego de la realización del censo, se puede conocer la distribución de unidades productivas por categoría:

- Micro empresas: 90.9%
- Pequeñas empresas: 3.8%
- Medianas empresas: 2.2%
- Grandes empresas: 3.1%

En cuanto a estudios específicos de ciberseguridad en PYMEs, no existen antecedentes en Paraguay, pero existen numerosos estudios en otros países, llevados a cabo generalmente por empresas del sector privado y por organismos gubernamentales, tanto de América Latina como de Estados Unidos y Europa.

Existen estudios que han medido el costo o impacto de un ciberataque en pequeñas y medianas empresas, entre ellos se puede destacar un estudio reciente llevado a cabo por Kaspersky Lab y B2B International ha determinado que el costo promedio de un ciberataque a una PYME estadounidense es de 86.500 USD. Este costo, sin embargo, es muy distinto al obtenido por la Asociación de Empresas Pequeñas y Medianas (NSBA) de Estados Unidos, que realiza una encuesta anual a PYMEs de este país y que incluye una sección de ciberseguridad. En dicha encuesta, en el 2015, el costo promedio de un ciberincidente resultó ser de alrededor de 7.115 USD en aquellos casos que no se involucró cuentas bancarias de las empresas, y 32.020 USD en aquellos que sí. En la encuesta de 2016 no se incluyó la sección de ciberseguridad. Estos costos son también significativamente distintos del costo promedio estimado por INCIBE, que es entre 20.000 ~ 50.000 Euros para PYMEs en España. No se encuentra información sobre estudios similares específicos sobre Paraguay ni tampoco de la región.

Otro estudio de interés que ha sido llevado a cabo en España es la Encuesta sobre confianza digital en las empresas, llevada a cabo por ONTSI (Observatorio Nacional de las Telecomunicaciones y de la Seguridad de la Información) e INCIBE, que fue publicada en octubre de este año. Este estudio examina los activos tecnológicos y de información de las empresas españolas, así como también su modelo de gestión de seguridad de estos activos, su preparación en cuanto a ciberseguridad, las herramientas y medidas de seguridad que implementan, los incidentes y su impacto al negocio, así como también su comportamiento en materia de protección de datos personales y transacciones electrónicas. Este estudio brinda información que podría ser muy valiosa, ya que a partir de ella se puede tener un panorama general "promedio" de las PYMEs. Sin embargo, el ecosistema de las TICs y de la seguridad de España es muy diferente al de Paraguay. Además, también existen importantes diferencias legislativas, culturales y de formación. Por ejemplo, en Paraguay, la legislación referente a privacidad y protección de datos personales es prácticamente inexistente, muy distinta a España, y Europa en general, donde la legislación es muy estricta y contempla multas elevadas. Esto, en España, constituye un factor determinante para las decisiones que toma una empresa, aun las pequeñas, ya que el incumplimiento puede significar incluso la quiebra, convirtiéndose de esta manera en un motivador para la aplicación de medidas de control adecuadas. En Paraguay, sin embargo, al no existir dicha legislación, es poco frecuente que una empresa incorpore medidas de este tipo, ni es muy probable que estén dispuestas en invertir muchos recursos en ello, si no existe ninguna razón legislativa ni de negocio.

Otra diferencia se puede apreciar en cuanto al grado de madurez en estándares y normas de gestión de seguridad de la información, con 5.7% de las empresas certificadas en ISO 27001, por ejemplo (ONTSI, 2017). En Paraguay, en cambio, no existe todavía ninguna empresa certificada en ISO 27001, ni siquiera entre las grandes empresas, ya que el grado de madurez a nivel país es inferior. De hecho, la primera agencia certificadora para ISO 27001 fue habilitada hace unos pocos meses. Otra diferencia importantísima es la firma digital, que según el estudio de INCIBE y ONTSI, tiene un uso de casi 90% en empresas españolas. En Paraguay no existe un estudio al respecto, pero de acuerdo a los registros de la Dirección General de Firma Digital y Comercio Electrónico, el ente rector de firmas digitales, se ha emitido menos de 8.000 certificados de firma digital, lo que representa menos del 2% con respecto a la población paraguaya. En su gran mayoría, los usuarios de firma digital son funcionarios gubernamentales, empresas importadoras y exportadoras y abogados que realizan trámites ante el Poder Judicial. Esto se debe a diversos factores, entre ellos lo incipiente de la firma digital en Paraguay (menos de 2 años), la poca cantidad de trámites en línea que requieren firma digital que existen en el país, el alto costo asociado al

uso de la firma digital en Paraguay, la poca e inadecuada difusión de la firma digital en empresa, entre otros.

En Paraguay se cuenta con un Observatorio TICs, un organismo dependiente de la Secretaría Nacional de Tecnologías de la Información y Comunicaciones (SENATICs). En el año 2017 ha realizado la primera Encuesta sobre Uso y Acceso de Internet, uno de los pocos estudios recientes en la materia. Cabe destacar que el estudio estuvo orientado a ciudadanos y hogares, y no específicamente a empresas, por lo que la información, aunque pueda resultar un antecedente interesante, no podrá tomarse como una estadística válida para empresas. La encuesta contó con un apartado sobre incidentes cibernéticos. El 7.4% afirmó haber sido víctima de un incidente, principalmente estafa/fraude cibernético con fines económicos (casi 42%) y acceso a datos privados (40%). Del porcentaje de personas que sufrió un incidente, alrededor del 27% lo reportó. Menos del 17% sabía a ciencia cierta a donde debía reportarlo.

Encuesta de ciberseguridad en PYMEs

Debido a la falta de información específica, actualizada y veraz sobre el estado de la ciberseguridad en PYMEs paraguayas, se ha realizado un estudio de modo a conocer el panorama general promedio de las PYMEs: qué tipo de procesos tienen informatizados, qué tipo de datos almacenan, cuáles son los riesgos que más les preocupan, qué tipo de tecnologías utilizan, qué tipo de red tienen, cuál es su capacidad en recursos humanos, entre otros.

El objetivo de este estudio fue responder a dos preguntas principales:

1. ¿Cuáles son los riesgos más críticos de una PYME, teniendo en cuenta probabilidad e impacto?
2. ¿Cuántos recursos puede destinar una PYME en la protección ante estos riesgos (tiempo, recurso humano, costo, etc.)?

Para ello, se ha realizado una encuesta online anónima que fue difundida entre una gran cantidad de micro, pequeñas y medianas empresas paraguayas.

Para el diseño de la metodología de la encuesta se ha contado con la colaboración de integrantes de INCUPAR (Asociación Paraguaya de Incubadoras de Empresas y Parques Tecnológicos) quienes cuentan con amplia trayectoria, especialmente en cuanto a estudios y encuestas realizadas en PYMEs. Se ha hecho énfasis en la necesidad de elaborar una encuesta breve, minimizando la cantidad de texto que el encuestado debe completar y con un lenguaje sumamente simple de modo a maximizar las posibilidades de obtener una cantidad significativa de respuestas reales. El cuestionario de la encuesta se encuentra en el Anexo 1.

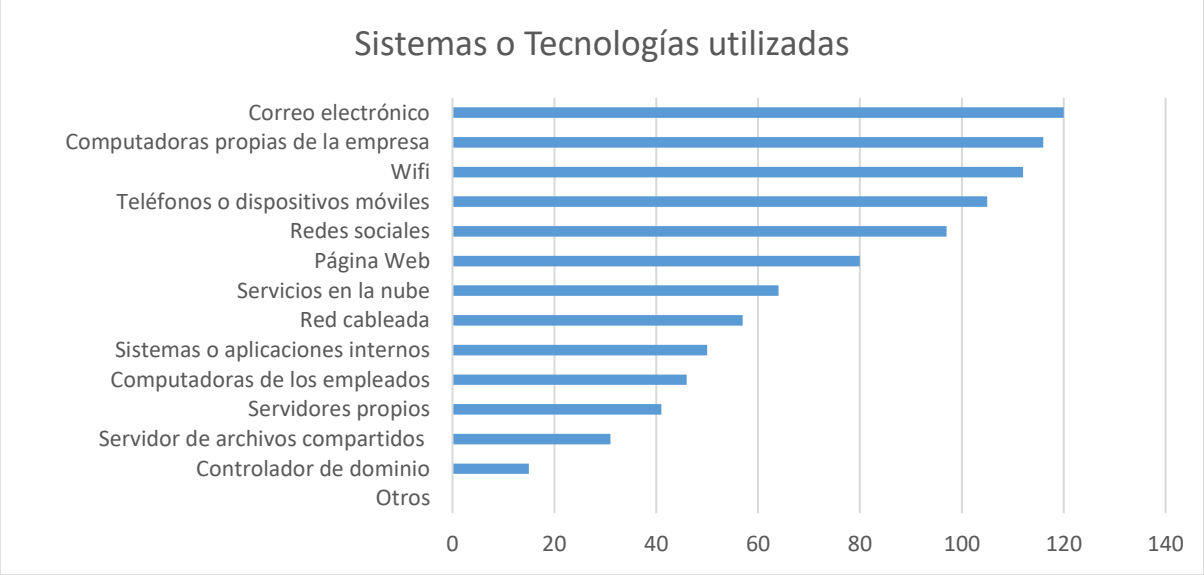
En cuanto a la difusión de la encuesta, se limitó a PYMEs paraguayas y se utilizaron diversos canales de difusión: correo electrónico, formulario de contacto de páginas web, Facebook y Whatsapp. Se ha difundido la encuesta entre empresas registradas en bases de datos del Viceministerio de Micro, Pequeñas y Medianas Empresas del Ministerio de Industria y Comercio, bases de datos públicas de miembros de diversos gremios, cámaras y asociaciones sectoriales, tales como CISOFT (Cámara de Industria del Software), CAFAPAR (Cámara de Farmacias del Paraguay), ASATUR (Asociación Paraguaya de Agencias de Viajes y Turismo), ATOLPAR (Asociación de Transitarios y Operadores Logísticos del Paraguay), AICP (Asociación Industrial de Confeccionistas del Paraguay), APAP (Asociación Paraguaya de Agencias Publicitarias), AIHPY (Asociación de Industria Hotelera del Paraguay), CCPY (Colegio de Contadores del Paraguay), CAP (Cámara de Anunciantes del Paraguay), CNCSP (Cámara Nacional de Comercio y Servicios del Paraguay) y UIP (Unión de Industrias Paraguayas), lista de contactos de organizaciones aglutinadoras de PYMEs, tales como CAPAPYME (Cámara Paraguaya de PYMEs), INCUNA (Incubadoras de Empresas de la Universidad Nacional de Asunción), ADEC (Asociación de Empresarios Cristianos), InfoPYME, AJE (Asociación de Jóvenes Empresarios), CEILAC (Centro de Emprendedurismo en Internet), INCUPAR, SENATICs (Secretaría

Nacional de Tecnologías de la Información y Comunicaciones). Además, se ha seleccionado aleatoriamente 10~15 empresas pequeñas y medianas de varios sectores (comercios minoristas, turismo, entretenimiento, salud, educación, tecnología, servicios, abogados, contadores, varios), a las cuales se ha enviado la encuesta.

Resultados del estudio exploratorio sobre estado de la ciberseguridad en PYMEs

La encuesta exploratoria se ha realizado durante una ventana de tiempo de 14 días, y ha recogido respuestas de 148 empresas, de las cuales 133 son micro, pequeñas y medianas empresas, tomando como factor determinante la cantidad de empleados (1 a 50 empleados).

Con respecto a los sistemas, herramientas o tecnologías que utilizan las PYMEs encuestadas, las estadísticas obtenidas son las siguientes:



Cuadro 1 Tecnologías, sistemas y herramientas utilizadas por PYMEs

1. Computadoras: la gran mayoría (88.5%) cuenta con computadoras propias de la empresa; en casi un tercio (33.8%) de las empresas, los empleados llevan sus computadoras. Un grupo de empresas se basa únicamente en BYOD (9%), otro grupo se basa en alguna combinación de BYOD y computadoras propias (25.6%), y otras utilizan únicamente computadoras propias (61.7%). Con eso se puede concluir que, aun con la limitación de presupuesto de las PYMEs y con la tendencia del BYOD, aun así, la amplia mayoría se basan fundamentalmente en computadoras propias.

2. Teléfonos o dispositivos móviles: la mayoría de las empresas (79%) utiliza teléfonos o dispositivos móviles, ya sea de la empresa o de los empleados. Debido a la naturaleza de los dispositivos móviles, en el marco de una PYME, es indiferente si el dispositivo pertenece a la empresa o al empleado, ya que, en cualquiera de los casos, la empresa tendrá poco o ningún control físico permanente sobre el dispositivo. Un reducido grupo (menos de 3%) se basa únicamente en dispositivos móviles, es decir, no cuentan con computadoras sino solamente con dispositivos móviles.

3. Página Web: la mayoría (60.2%) posee una página web corporativa. De esas empresas, el 40% la tiene alojada en servidores propios pero la mayoría lo tiene alojado en otro lugar (servidores compartidos, servicios tercerizados, etc.).

4. Correo electrónico: la gran mayoría (90.2%) utiliza correo electrónico, el cual es el activo más utilizado, incluso más que las computadoras.

5. Redes Sociales: la gran mayoría (73%) utiliza las redes sociales en su negocio. Llama la atención que existen más empresas PYMEs que poseen redes sociales que página web.

6. Sistemas o aplicaciones internas: la mayoría de las PYMEs (62.4%) no posee sistemas ni aplicaciones internas. Un grupo relativamente reducido (37.6%) utiliza sistemas internos tales como sistema de stock, sistemas contables, etc. Esto nos lleva a concluir que la mayoría de estas empresas manejan sus procesos internos con planillas electrónicas y documentos ofimáticos (finanzas, presupuestos, datos de clientes, stock de productos, etc.).

7. Servidores propios: solo un grupo reducido (30.8%) cuenta con servidores propios. De las PYMEs que poseen servidores propios, la mayoría lo utiliza para sus sistemas internos; estos sistemas, por lo general, son basados en web y por tanto deben ser alojados en algún servidor. Sin embargo, un pequeño grupo utiliza servidores propios para alojar la página web, servidores, compartición de archivos, u otros.

8. Servidor de archivos compartidos: solo un grupo reducido (23.3%) de las PYMEs utilizan servidores de archivos compartidos. De ese grupo, algunos cuentan con una controladora de dominio, es decir, cuentan con un modelo de red relativamente estructurado, pero la gran mayoría lo tiene como un sistema aislado (por ejemplo, servidores propios con Samba o similar, o a través del sistema de carpeta compartidas de Windows simplemente).

9. Wi-Fi: la gran mayoría de las PYMEs (84.2%) posee una red wifi. De éstas, un grupo lo combina además con una red cableada (47.3%) sin embargo la mayoría utiliza únicamente una red inalámbrica (52.7%). Sorprendentemente, un grupo considerable de microempresas utiliza una combinación de Wifi y red cableada: 30 empresas, de las 96 microempresas encuestadas.

10. Red cableada: un grupo de PYMEs (42.9%) utiliza redes cableadas, pero la mayoría de las PYMEs no lo utilizan. Menos del 5% lo utilizan como único mecanismo de conectividad; todas las demás lo utilizan como un mecanismo secundario, además del Wifi, probablemente solo para extender la conectividad a algún lugar donde la cobertura del Wifi sea débil.

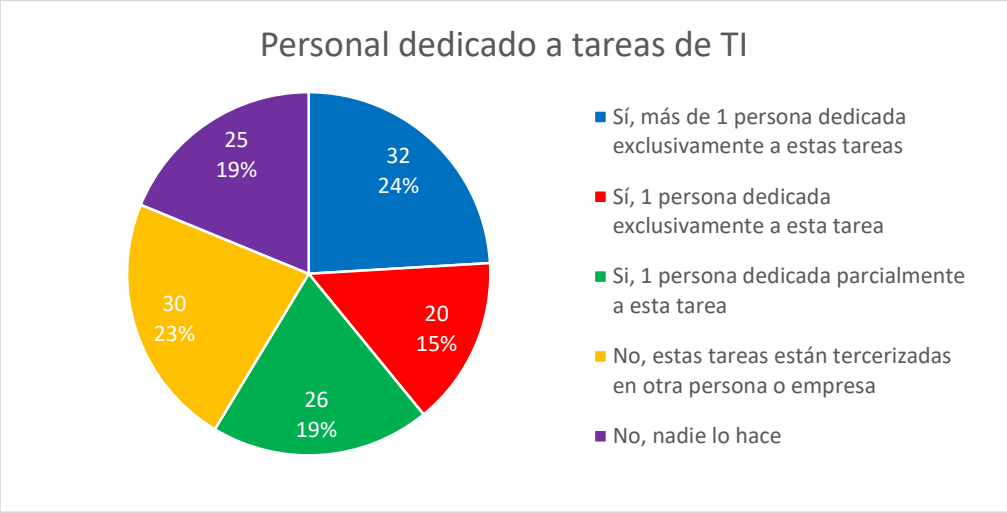
11. Controladora de dominios: un grupo muy reducido (15 empresas, 11.3%) posee una controladora de dominio. Sorprendentemente, 9 de estas empresas son microempresas (1 a 10 empleados), y solo 6 tienen más de 10 empleados, lo cual normalmente no justificaría la necesidad de una controladora de dominios.

12. Servicios en la nube: aproximadamente la mitad de las PYMEs (48.1%) utilizan servicios en la nube, tales como Google Drive, One Drive, Dropbox, etc.

Se puede concluir que los activos de información más utilizados por las PYMEs son los siguientes:

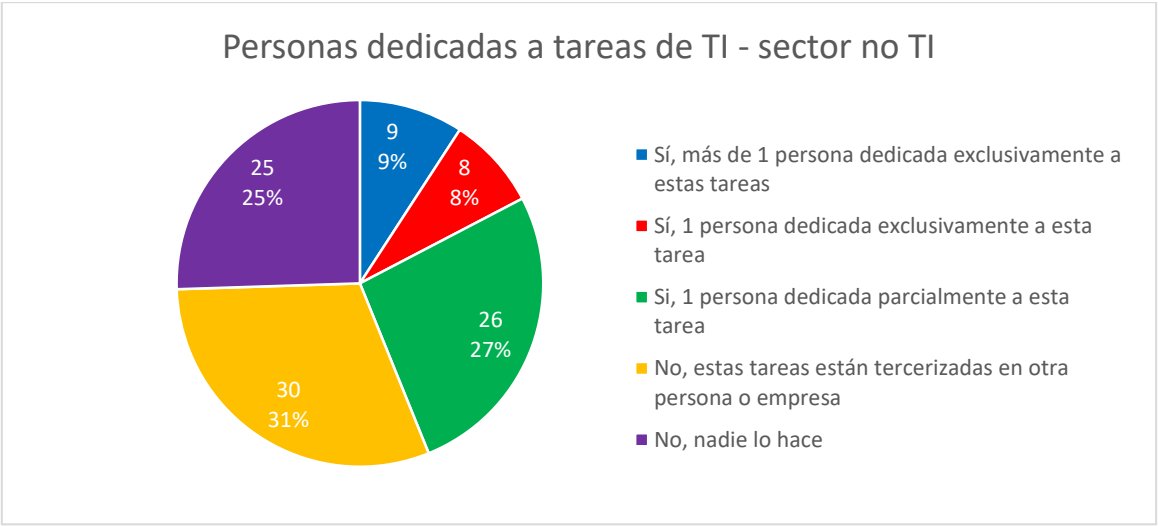
- Archivos (planillas, documentos de texto, pdf, etc.)
- Computadoras de la empresa y dispositivos móviles
- Correo electrónico
- Redes sociales
- Red Wifi

Con respecto a la cantidad de personas que dedican las PYMEs a las tareas de TI (desarrollo web, mantenimiento de la red, instalación de equipos, mantenimiento de los sistemas, etc.) no se observa una tendencia clara, ya que las respuestas se encuentran distribuidas de manera más o menos uniforme, desde más de una persona dedicada exclusivamente a las tareas, hasta ninguna.



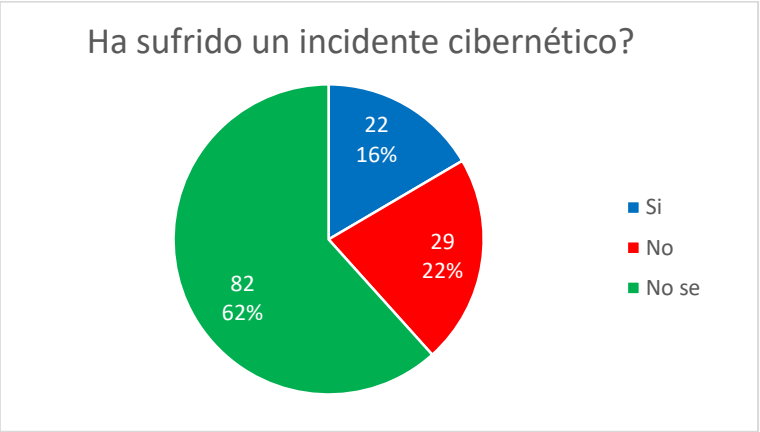
Cuadro 2 Dedicación de personal a tareas de TI en una PYME

Sorprendentemente, 24% de las microempresas encuestadas afirman contar con más de una persona dedicada exclusivamente a estas tareas. Es muy probable que estas microempresas estén dedicadas al rubro de tecnología. Excluyendo a este segmento, sin embargo, se observa una tendencia hacia la tercerización y la dedicación de una persona parcialmente. En un número importante de empresas (25%) nadie realiza tareas de TI. Esta alta disparidad entre empresas puede deberse, principalmente, a la variedad de rubros y también a la variedad de cantidad de personal. Una empresa mediana podría tercerizar o dedicar a una persona enteramente, pero una micro-empresa, cuyo negocio no esté directamente vinculado a los servicios de tecnología, probablemente no dedique a ninguna persona.



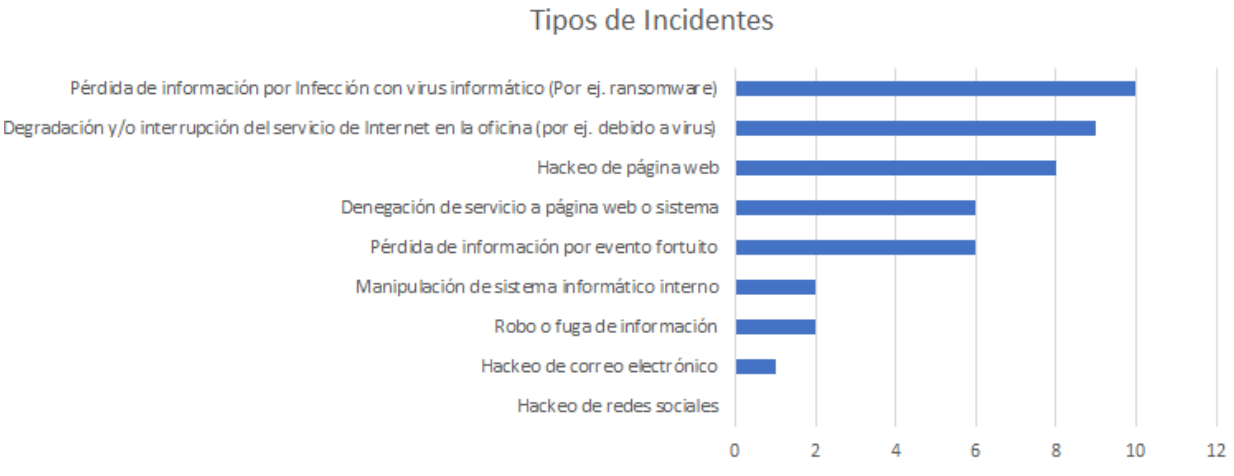
Cuadro 3 Dedicación de personal a tareas de TI en una PYME - normalizado

El 16% de las PYMEs encuestadas afirmaron haber sufrido un incidente cibernético. La gran mayoría (62%) afirmó que no lo sabía. Esto se debe, probablemente, a que no cuenten con mecanismos de monitoreo; incluso, es probable que hubieran ocurrido incidentes pero que los mismos hubieran pasado desapercibidos. Se debe tener en cuenta que, frecuentemente, los incidentes cibernéticos no son percibidos por la víctima; en ocasiones, la víctima no relaciona los problemas con un incidente cibernético: por ejemplo, un virus que estuviera implantado en todas las máquinas de la red podría estar generando una sobrecarga tal que las mismas estuvieran extremadamente lentas y no se pudiera trabajar normalmente. Sin embargo, si la empresa no investiga el problema, es muy poco probable que lo relacione con un incidente cibernético; es más probable que lo relacione simplemente a la antigüedad de la máquina.



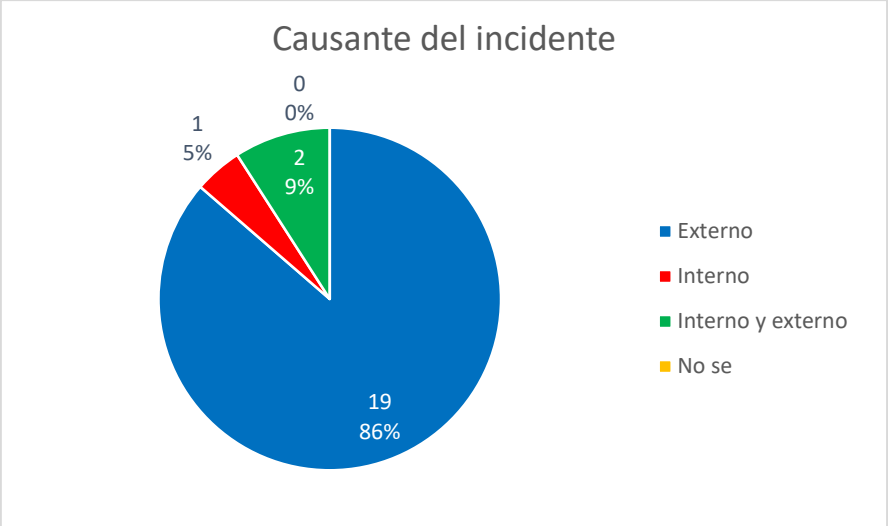
Cuadro 4 Ocurrencia de incidente cibernético en PYMEs

El tipo de incidente más frecuente es la pérdida de información por ransomware (7.5% del total de los incidentes), seguido de la degradación del servicio de internet debido a virus, botnet, etc. (6.8%) y hackeo de página web (6%). Algunas empresas afirmaron haber sufrido una denegación de servicio a su página web o a sus sistemas y la pérdida de información por eventos fortuitos. Nuevamente, esta estadística refleja el hecho de que las PYMEs solo perciben los incidentes más “visibles” como el ransomware, pero que probablemente no se enteren que han sufrido otros tipos de incidentes más silenciosos.



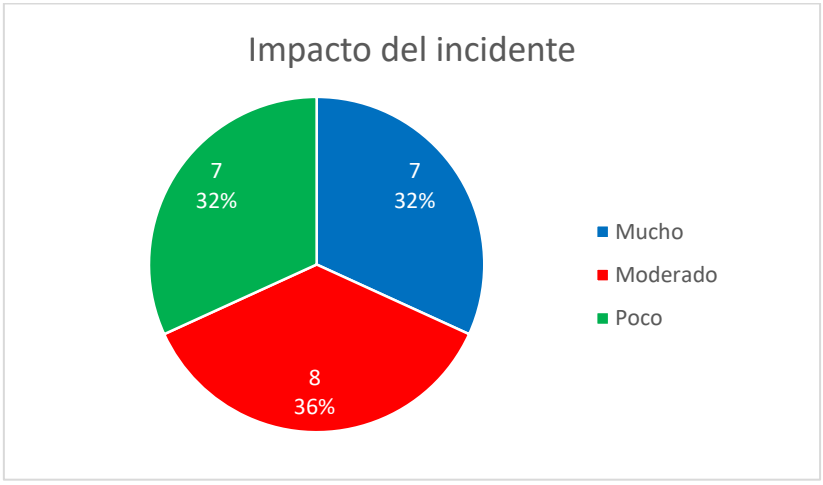
Cuadro 5 Tipos de incidentes en PYMEs

De estos incidentes, la gran mayoría de las PYMEs (86% de las que sufrieron incidentes) indicaron que se debió a un atacante externo. Un pequeño grupo de empresas (14%) manifestó que alguien interno estuvo involucrado en el incidente. Esto se debe probablemente a que los empleados internos de una PYME no tienen la intención, el conocimiento y/o la oportunidad de realizar algún daño a través de medios cibernéticos.



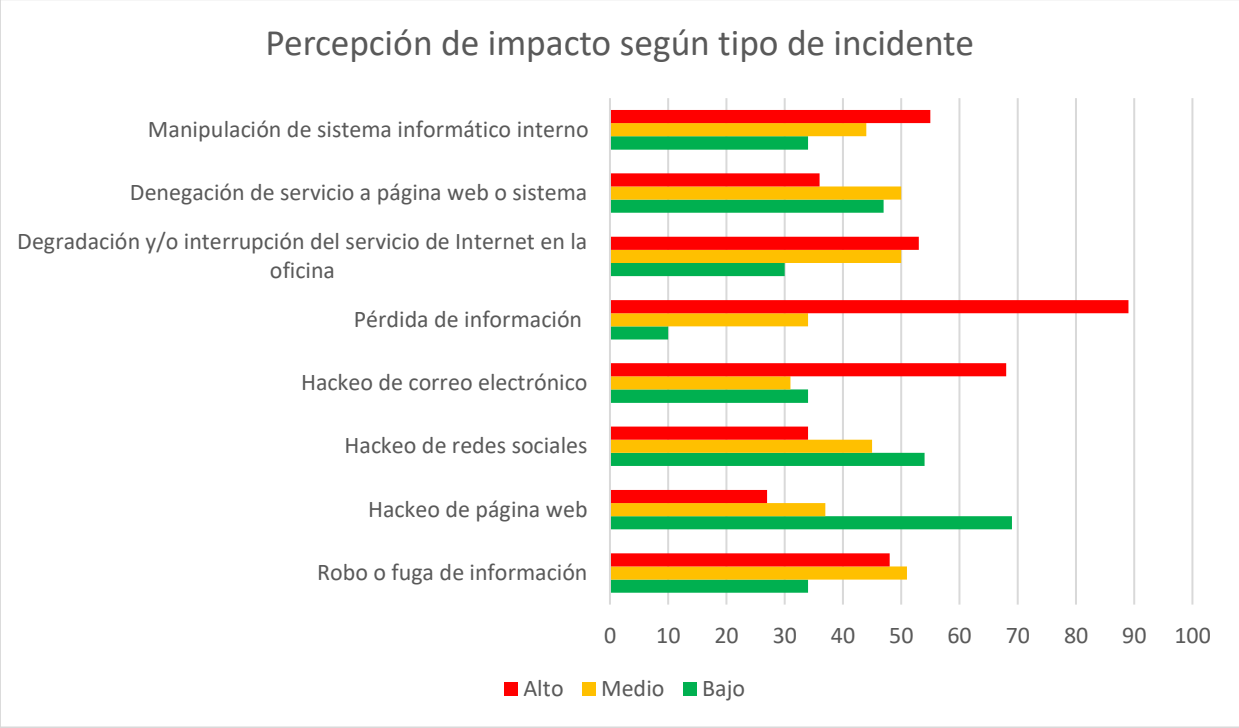
Cuadro 6 Tipos de causantes de incidentes en PYMEs

Tampoco hay una clara tendencia con respecto al impacto, la mayoría (36%) indicó que el impacto fue moderado, con una interrupción del negocio durante poco tiempo y/o pérdidas moderadas, pero que no fue un gran problema; sin embargo, un grupo también grande (32%) indicó que el impacto fue alto, interrumpiendo el negocio durante un tiempo significativo y/o generando pérdidas importantes, y otro grupo de las mismas proporciones (32%) indicó que el impacto fue bajo, sin ninguna interrupción al negocio ni pérdidas significativas.



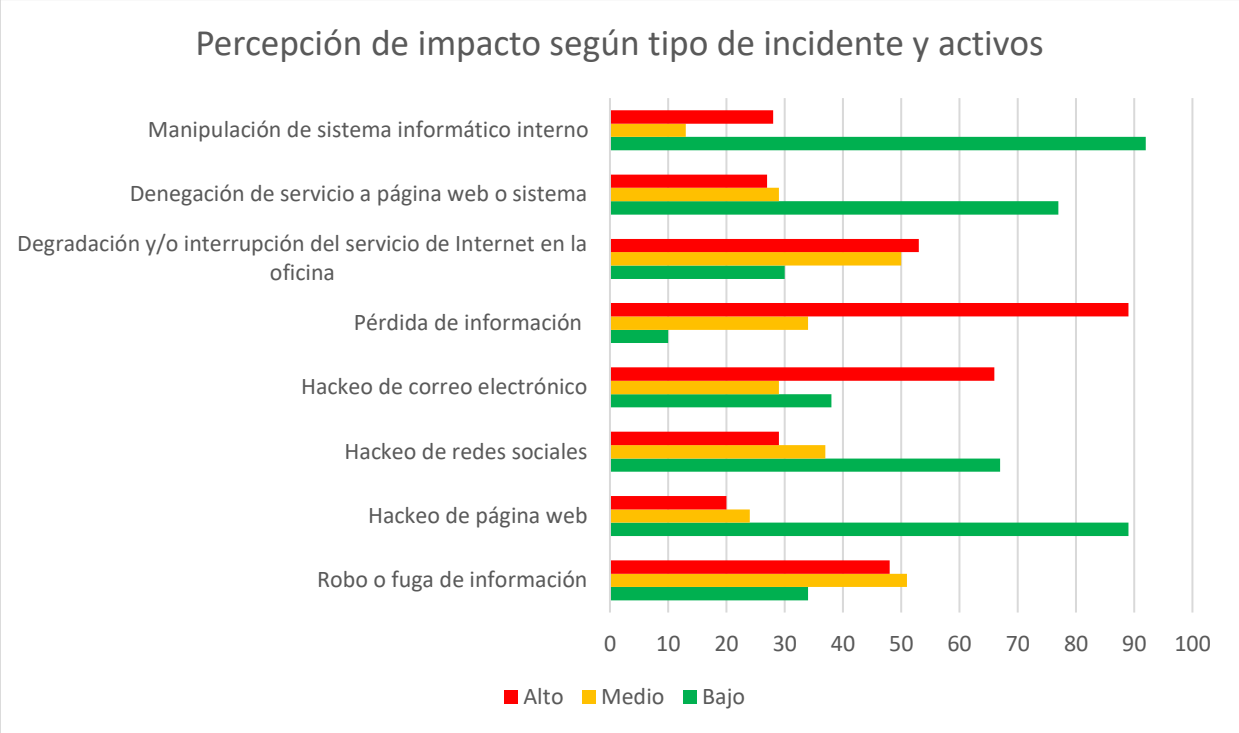
Cuadro 7 Impacto de incidentes en PYMEs

De las empresas que manifestaron que el impacto fue bajo, el 42.8% había sufrido un incidente por *ransomware* – lo que nos hace suponer que tenían copia de seguridad o que el equipo infectado no contenía información importante para el negocio; y el 57.2% restante había sufrido un hackeo a su página web. Sin embargo, en los otros casos de *ransomware*, el impacto fue moderado o alto (30% y 40% de todos los casos de *ransomware*, respectivamente). La mayoría de los incidentes de degradación del internet debido a virus tuvieron un impacto moderado o alto (50% y 30% respectivamente). La mayoría de los hackeos de páginas web tuvieron un impacto bajo (50% de los casos), pero un número importante indicó que el impacto fue alto (40% de los casos). En general, se nota una relación entre la indisponibilidad tanto se información como de servicios con el impacto.



Cuadro 8 Percepción de impacto según tipo de incidentes en PYMEs

Se debe tener en cuenta que esta estadística solo refleja la percepción teórica, ya que muchas empresas que, por ejemplo, manifestaron que un cierto tipo de incidente a un cierto tipo de sistema tendría un impacto alto, no poseen ese sistema. Por ejemplo, de las 55 empresas que manifestaron que una manipulación a un sistema o aplicación internos tendría un impacto alto a su negocio, solo 28 poseen efectivamente un sistema o aplicación interna. Por lo tanto, se calculó una estadística modificada de acuerdo a la percepción de impacto por tipo de incidente, pero según los sistemas o activos que posee la empresa.



Cuadro 9 Percepción de impacto según tipo de incidentes en PYMEs - normalizada

En este caso, se observa que los incidentes que más impacto generarían al negocio de una PYMEs, de acuerdo a los activos y sistemas que poseen, son la pérdida de información, el hackeo de correo electrónico y la degradación y/o interrupción del servicio de internet en el lugar de trabajo; es decir, aquellos incidentes que afecten la disponibilidad de sus recursos o servicios. El robo o la fuga de información preocupa también moderadamente a las PYMEs, probablemente debido a cuestiones de imagen o de competencia. A diferencia de otros países, debido a que en Paraguay no hay una ley de protección de datos y no hay sanciones a este tipo de incidentes, no suele ser una preocupación muy grande entre las empresas.

En cuanto a la percepción de impacto que tendría un determinado tipo de incidente en una PYMEs, se comprueba que la mayor preocupación se da con respecto a la pérdida de información (*ransomware*, evento fortuito, etc.), hackeo del correo electrónico y manipulación de un sistema interno. Se puede ver una tendencia en cuanto a la percepción del impacto que tendrían aquellos incidentes que afecten a la disponibilidad de recursos o servicios en la empresa, los cuales, en general, son percibidos como de alto impacto. En cambio, incidentes relacionados a página web o redes sociales son considerados de bajo impacto, probablemente porque muchas PYMEs no utilizan la página web para atraer clientes y porque saben que pueden reemplazar con relativa facilidad su perfil o página de una determinada red social.

Un hecho llamativo es el valor relativamente bajo que tiene la página web para el negocio de una PYME paraguaya, especialmente frente a las redes sociales que son consideradas más críticas para el negocio. Esto se debe a diversas razones, muy particulares de nuestra región.

- El acceso masivo a Internet en a Paraguay empezó entre los años 2004 a 2006, periodo en el cual empezaron a ofrecerse los primeros servicios de acceso a Internet accesibles para hogares y empresas pequeñas. Si bien, en esos años la tendencia era la web tradicional todavía, en muy poco tiempo empezó el auge de las redes sociales.

- El acceso a Internet en Paraguay, hoy en día, es principalmente móvil, a través de los planes de internet ofrecidos por las compañías telefónicas. Solo alrededor del 40% de la población paraguaya tiene acceso a banda ancha fija, sin embargo, prácticamente el 100% cuenta con acceso a Internet a través de móviles (Observatorio TICs, 2017). Esto significa que hay una porción importante de casi el 60% que nunca tuvo acceso a una computadora ni al Internet en el hogar, y que, por tanto, ha tenido su primer acercamiento a Internet a través de los smartphones, con los planes de las telefónicas, que normalmente son limitados en cuanto al volumen de tráfico. La mayoría de estos planes ofrecen acceso "gratuito" a Facebook, WhatsApp y algunos contenidos bien específicos.

- Esta realidad, sumada a otros factores culturales, explica que Paraguay sea el país que utiliza más redes sociales; especialmente Facebook (Beliz, y otros, 2016)

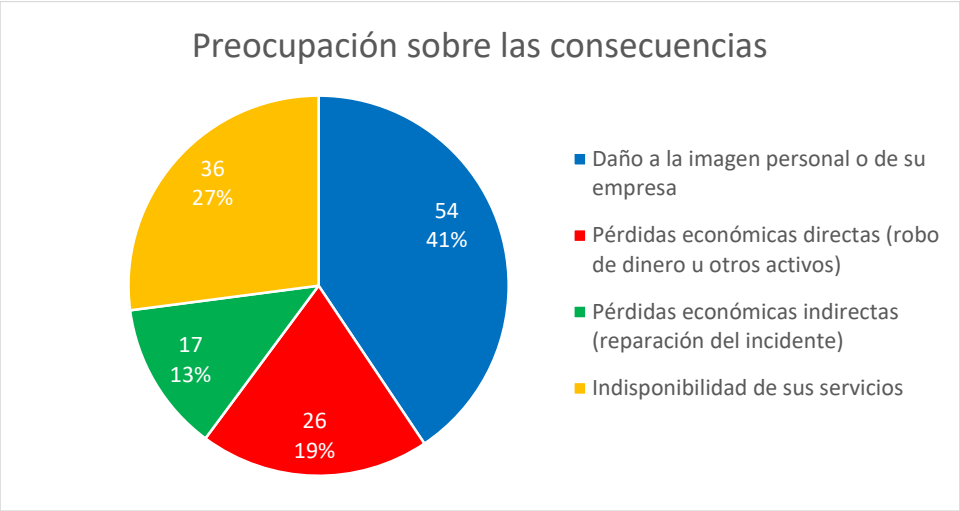
- Crear una web es relativamente económico, con precios que rondan los 1000 USD, sin embargo, el mantenimiento (servicio de alojamiento, dominio .py, actualización de contenido, noticias, fotos, etc.) suele tener un costo relativamente elevado para una PYME (alrededor de 1000 USD anuales, prácticamente como una web nueva).

Estos hechos explican que las empresas, especialmente las PYMEs optan por no tener una web sino redes sociales: su principal, y en muchos casos, único mecanismo de darse a conocer en el mundo digital es a través de Facebook u otras redes sociales. Los potenciales clientes de PYMEs, por lo general, no buscan servicios o comercios en buscadores como Google sino mayormente a través de redes sociales.

Para ciertos tipos de servicios como ser estudios contables, de abogados, u otras ramas más específicas, uno de los mecanismos de captación de clientes más efectivas son las referencias personales. Teniendo en cuenta que, además, Paraguay es un país con una población pequeña de apenas alrededor de 7.000.000 habitantes, con menos de 3.000.000 en el área central, es perfectamente posible encontrar empresas o profesionales simplemente a través de las relaciones personales. Muchas PYMEs captan clientes a través de las referencias personales o de grupos de personas afines, medios publicitarios tradicionales (pasacalles, panfletos, etc.) o posicionamiento estratégico (zona o lugar donde se ubica físicamente, precio, etc.), siendo los medios digitales un activo menos crítico.

Otra particularidad de Paraguay es que una gran parte del comercio electrónico, sobre todo en PYMEs, se realiza a través de redes sociales: las empresas publicitan sus productos a través de redes sociales (Facebook e Instagram, principalmente) y el comprador realiza el pedido a través de la propia red social (a través de mensaje directo, por ejemplo) o a través de algún canal alternativo (WhatsApp, por ejemplo). Se acuerda la compra y el cliente realiza el pago a través de plataformas de micro-pago, como por ejemplo giros de dinero a través del teléfono móvil. Esto también explica el auge que ha tenido en los últimos años las plataformas de micro-pago frente a las plataformas de pago online tradicionales. Esto ocurre, entre otras razones, porque hay una baja formalización bancaria; solo un pequeño porcentaje de la población paraguaya tienen una cuenta bancaria en los bancos, por ende, no todos tienen tarjetas de créditos. Sin embargo, el porcentaje de la población que tiene acceso a un smartphone es ampliamente mayor, por lo que los sistemas de micro-pago a través de teléfonos móviles son ampliamente utilizados.

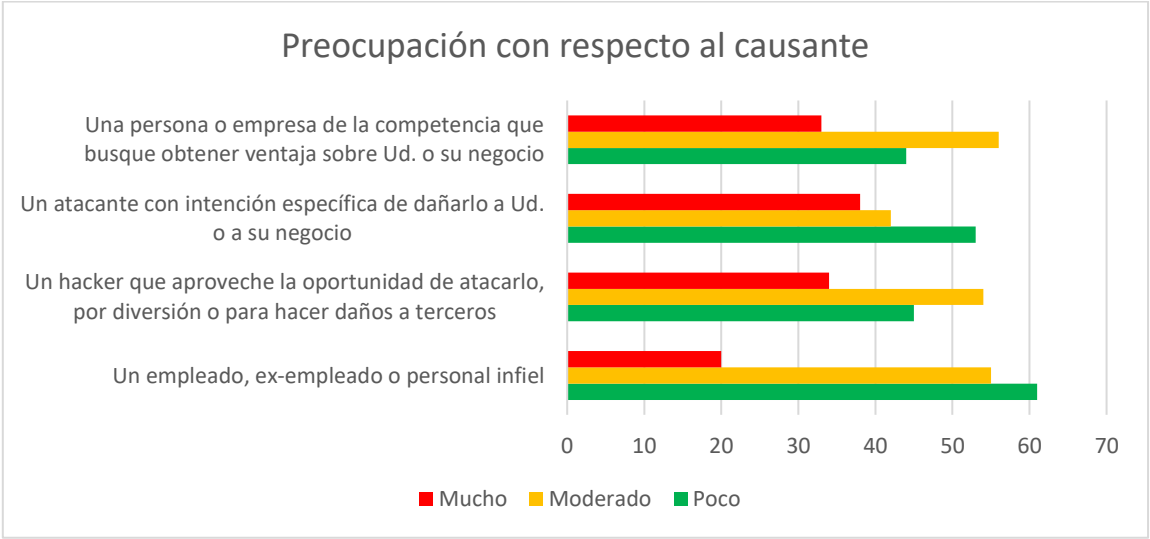
Con respecto a las consecuencias o daños ocasionados por un incidente, la mayoría de las PYMEs (41%) manifestó que le preocupa el daño a la imagen personal (de los directivos) o de la empresa. La segunda mayor preocupación es la indisponibilidad de los servicios brindados por la empresa (27%). Las pérdidas económicas, tanto directas como indirectas son preocupaciones menores. Esto se debe probablemente a que, en las PYMEs, el dinero o activos financieros no están directamente vinculados a los activos tecnológicos. Con respecto a las pérdidas indirectas, normalmente no existen sanciones por el mal manejo de los activos de información, por lo que esto no representa una preocupación para las PYMEs paraguayas; esto probablemente cambiaría si se creara alguna legislación rigurosa para la protección de datos personales. Además, sus activos tecnológicos muchas veces no tienen un alto valor monetario, por lo que el daño financiero que podría causarse no será muy elevado.



Cuadro 10 Preocupación en cuanto a consecuencias de un incidente en PYMEs

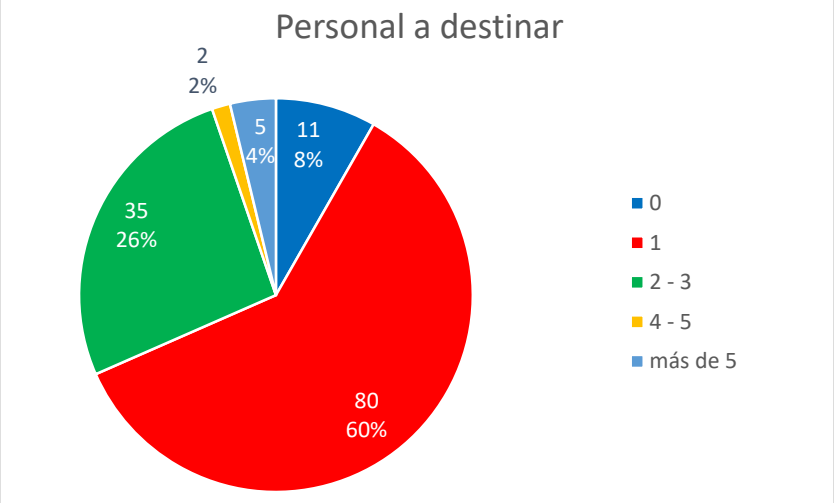
La mayoría de las PYMES (42.1%) manifestó una preocupación moderada con respecto a una persona o empresa de la competencia. Un atacante con intención específica de dañar a la empresa fue considerado una preocupación baja para la mayoría de las empresas (39.8%). Con respecto a un atacante que simplemente aproveche la oportunidad, pero sin una intención específica de dañarla a la empresa fue considerado una preocupación moderado por la mayoría de las PYMEs (40.6%). La mayoría de las empresas (45.9%) consideran que un atacante interno, ya sea un empleado, ex-empleado o similar sería una preocupación baja.

Es posible que muchas PYMEs solo hayan considerado la preocupación teórica y no la probabilidad, por lo cual expresaron una preocupación relativamente alta con respecto a atacantes dirigidos, por ejemplo. Pero en términos generales, de acuerdo a la respuesta de la mayoría por cada una de las amenazas, las dos amenazas que preocupan mayormente a las PYMEs son personas o empresas de la competencia y atacantes que simplemente aprovechen la oportunidad.



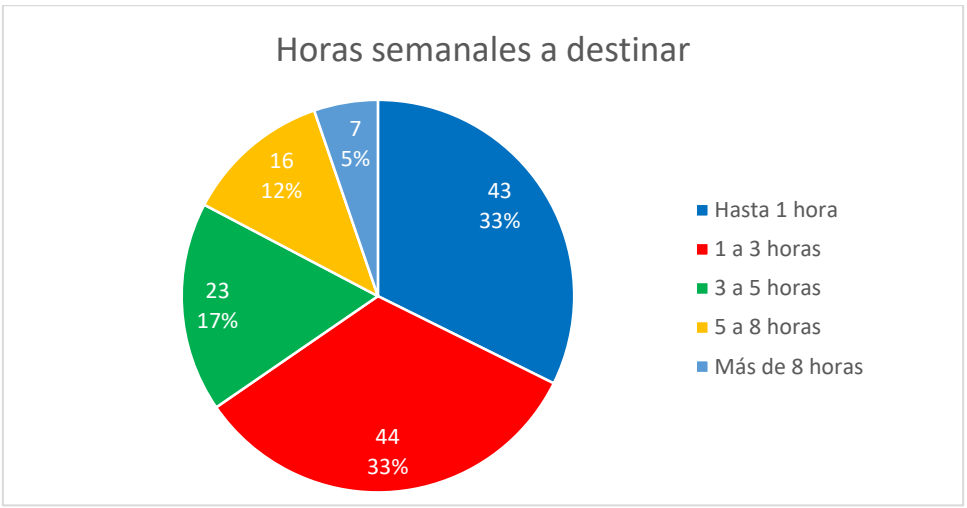
Cuadro 11 Preocupación en cuanto a las amenazas en PYMEs

La gran mayoría de las PYMEs (60%) indicó que estaría dispuesta a destinar una persona para dedicarse a la implementación de protecciones de seguridad.



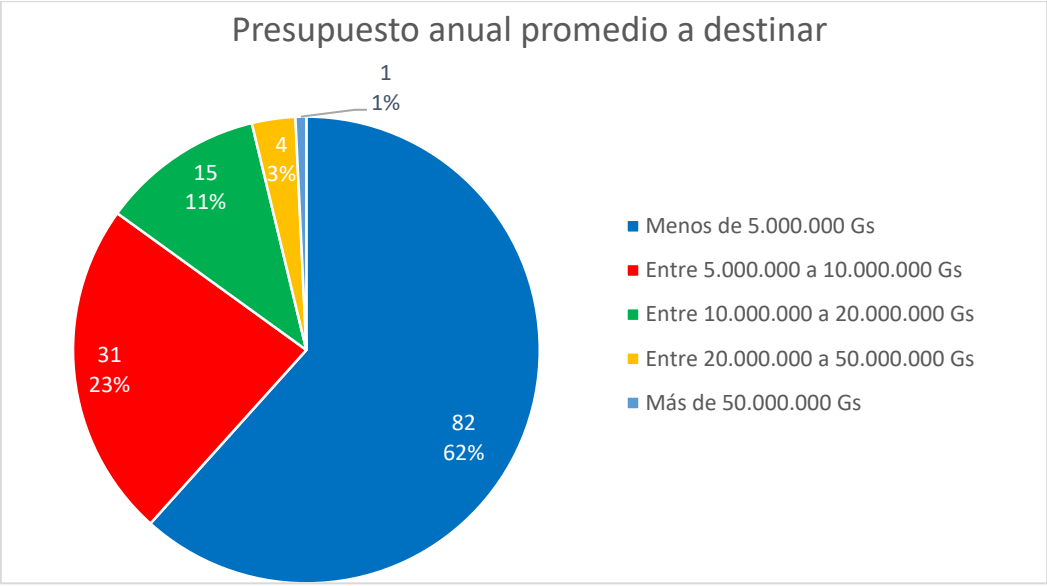
Cuadro 12 Cantidad de personal a dedicar por una PYME para cuestiones de seguridad

Con respecto a la cantidad de horas semanales que estarían dispuestas a destinar para las tareas relacionadas a protección de su seguridad, la mayoría de las PYMEs (33%) indicó que destinaría entre 1 a 3 horas, pero un porcentaje casi idéntico indicó que solo destinaría hasta 1 hora.



Cuadro 13 Tiempo de dedicación semanal por una PYME para cuestiones de seguridad

La gran mayoría de las PYMEs (62%) indicó que estaría dispuesta a destinar menos de 5.0000.000 Gs. (alrededor de 800 Euros) anualmente en medidas de protección, sin tomar en cuenta los costos del personal, pero incluyendo costos de tercerización, si se deseara tercerizar tareas. Un grupo reducido (23%) estaría dispuesto a destinar un presupuesto entre 5.000.000 a 10.000.000 Gs. (alrededor de 800 a 1.600 Euros). Muy pocas empresas estarían dispuestas a destinar montos mayores.

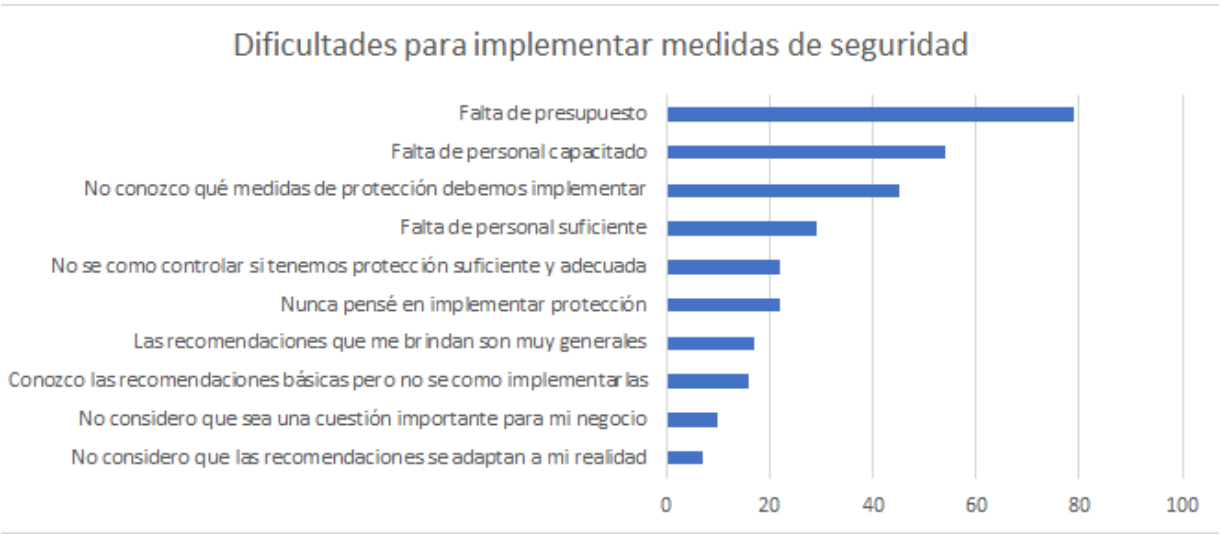


Cuadro 14 Prespuesto anual a dedicar por una PYME para cuestiones de seguridad

Con respecto a las dificultades o problemas a los que se enfrentan las PYMEs a la hora de implementar medidas de seguridad, las principales fueron:

- La falta de presupuesto fue atribuida por la gran mayoría de las PYMEs (59.4% del total)
- La falta de personal capacitado fue mencionada por un grupo grande de PYMEs (40.6%)
- Un grupo grande de empresas (33.8%) indicó que no conoce qué medidas de protección deben implementar.

Otras causas como falta de personal suficiente, desconocimiento sobre cómo controlar el nivel de protección, y otros problemas fueron mencionados por grupos reducidos de PYMEs.



Cuadro 15 Dificultades para implementación de medidas de seguridad en PYMEs

Esto nos indica nuevamente que la cuestión presupuestaria es la principal preocupación de una PYME, así como también el conocimiento específico que pueda tener el personal. En cierta medida, es posible que el problema de falta de presupuesto, en realidad, sea derivada de una falta de conocimiento o capacitación: es probable que las PYMEs que no estén especializadas en TICs no conozcan las múltiples de medidas de protección que existen, las cuales muchas veces son totalmente gratuitas. Ese desconocimiento, sumado al mito que la ciberseguridad se protege con herramientas caras y sofisticadas, les lleva a creer que con su limitación de presupuesto no están en capacidad de protegerse adecuadamente.

En definitiva, se han obtenido las siguientes conclusiones a partir del estudio de PYMEs:

- Los principales activos de información que poseen prácticamente todas las PYMEs son:
    - Archivos (planillas, documentos de texto, pdf, etc.)
    - Computadoras de la empresa y dispositivos móviles
    - Correo electrónico
    - Redes sociales
    - Red Wifi

  En este trabajo, se denominará a estos activos los “activos básicos de toda PYME”. Algunas empresas poseen además otros activos tales como página web, sistemas internos, servicios en la nube, servidores propios, etc. Sin embargo, a diferencia de una empresa grande, que normalmente poseen todos estos activos en simultáneo, muy pocas PYMEs posee todos estos activos, sino solo algunos.
- Sin tener en cuenta a las micro-empresas (hasta 10 empleados) que dedican a más de una persona exclusivamente a tareas de TI (rubro tecnológico, probablemente), en las demás PYMEs se observa una tendencia hacia la tercerización o la dedicación de una persona parcialmente para las tareas de TI.
- Con respecto a la ocurrencia de incidentes cibernéticos, se observa que aquellos incidentes que afectan a la disponibilidad de la información (por ej. *ransomware*) y de la red (virus, *botnets*, etc.) son los que tienen un mayor impacto al negocio de las PYMEs. Los incidentes que afectan a la confidencialidad no han tenido un impacto tan alto, y aquellos relacionados a integridad (manipulación de sistemas internos, por ejemplo), a pesar de tener un impacto medio, no son muy frecuentes. Los incidentes cibernéticos que afectan a las PYMEs se deben casi enteramente a personas externas.
- De acuerdo a la percepción de las PYMEs, y de acuerdo a su realidad, los incidentes que más impacto generarían a su negocio son la pérdida de información, el hackeo de correo electrónico y la degradación y/o interrupción del servicio de internet en el lugar de trabajo; es decir, aquellos incidentes que afecten la disponibilidad de sus recursos o servicios. Las amenazas que les preocupan más son aquellos atacantes genéricos que aprovechen la oportunidad (no dirigidos específicamente contra ellos) y personas de la competencia (dirigidos). En cuanto a las consecuencias de un ataque a la PYME, su mayor preocupación es el daño a su imagen personal o de la empresa.
- Los recursos que las PYMEs estarían dispuestos a destinar para la aplicación de medidas de seguridad son:
    - Recursos humanos: 1 persona
    - Tiempo: Hasta 1 hora o de 1 a 3 horas. Buscando un balance, se establece como límite 2 horas.
    - Recursos económicos: Hasta 5.000.000 Gs. anualmente (alrededor de 800 Euros). Esto no incluye el sueldo del personal a ser destinado, pero debe cubrir costos de tercerización, si fuera necesario.

Entonces, los controles y recomendaciones de la guía no deben requerir más de una persona para ser implementados, deben poder ser implementados en, a lo sumo, 2 horas semanales y no deben superar el costo de 5.000.000 Gs. anuales.

- En cuanto a las dificultades que debe ayudar a resolver esta guía están:
    - La falta de presupuesto, por lo que se debe basar enteramente en soluciones y herramientas gratuitas o con el menor costo posible.
    - La falta de personal capacitado, por lo que la guía y sus recomendaciones derivadas deben ser simples, tienen que poder ser implementadas sin necesidad de contrataciones externas y sin necesidad de conocimiento técnico.
    - El desconocimiento con respecto a las medidas a implementar, por lo que la guía debe ser concreta y práctica, no debe ser necesario que el personal de la empresa deba investigar adicionalmente. Entre los instrumentos adicionales de la guía se incluye referencias a tutoriales y guías de uso de las herramientas si fuera necesario, de modo a minimizar el esfuerzo, tiempo y el conocimiento requerido por parte del personal de la PYMEs.

Capítulo 3: Elaboración de guía de controles

Análisis de riesgo para la identificación de posibles controles

Primeramente, se ha identificado un conjunto de posibles controles y medidas de protección que puedan ser implementados por cada activo de información. Existen diversas metodologías para la identificación de controles. Actualmente, la tendencia es utilizar la metodología COSO II, la cual se basa en realizar un análisis de riesgos tomando en cuenta los procesos, en vez de los activos. De acuerdo a esta metodología, se identifican primeramente los procesos críticos de la empresa, luego se plantean todas las posibles amenazas a estos procesos y se estima el impacto y la probabilidad de cada una de las amenazas, lo que permite obtener un valor para cada riesgo. Se define un nivel de riesgo inaceptable, y de acuerdo a ese nivel se obtienen todos los riesgos que están por encima del nivel aceptable y que, por ende, deben ser controlados. Los controles se establecen para cada uno de estos riesgos inaceptables.

Esta metodología es adecuada para una empresa grande y con un nivel de madurez relativamente alto en cuanto a seguridad de la información, ya que permite obtener controles más acertados de acuerdo a sus procesos críticos, los cuales están establecidos de manera más formal (políticas, procedimientos de negocio, manuales de funcionarios, áreas de negocio y estructura organizacional bien definida, etc.). Es adecuada cuando se posee una gran cantidad de activos de información, muy variados, donde se debe tener en mente el panorama general (los procesos de negocio), más que los componentes individuales (archivos, sistemas, equipos, servidores, softwares, etc.). Los controles que derivan de este análisis son, en la mayoría de las veces, relativamente generales y, ocasionalmente, representan un proyecto de mejora de un aspecto, más que una acción específica.

Sin embargo, esta metodología es compleja de aplicar a una PYME, la cual difícilmente tenga procesos completamente definidos, sino tiene una realidad más dinámica, cambiante, con procesos y procedimientos informales que se van ajustando de acuerdo a las necesidades del día a día. Para esta realidad, es más adecuado utilizar la metodología que se basa en identificar controles de acuerdo a cada activo de información. Esto obedece a que, en una PYMEs, tal como nos demostró el resultado de la encuesta exploratoria, el conjunto de activos de información es relativamente limitado y estándar. Además, esta metodología tiene la ventaja de que los controles y medidas de protección que derivan del análisis de cada activo, son sumamente específicos, concretos y prácticos.

Para ello se ha planteado todas las posibles amenazas que pueden afectar a cada uno de los activos, para cada una de las dimensiones de la seguridad (confidencialidad, integridad y disponibilidad). Se ha analizado la criticidad de cada amenaza a cada tipo de activo de acuerdo a la probabilidad y al impacto de cada amenaza para dicho activo de una PYME.

Para cada una de las amenazas, se han propuesto controles y medidas de protección. Se ha analizado también la factibilidad de cada control de acuerdo a las limitaciones de recurso de una PYME (recursos humanos, tiempo y dinero máximo que puede ser destinado). Se ha enfocado solamente en controles o medidas de seguridad simples y económicas; no se han planteado controles o medidas de seguridad que claramente superen las limitaciones dadas.

Activos de información básicos de toda PYME:

- Archivos (planillas, documentos de texto, pdf, etc.): abarca los archivos desde el punto de vista de la información que contienen, principalmente los archivos almacenados en equipos de usuario.
- Computadoras de la empresa y dispositivos móviles: abarca los equipos de usuario desde el punto de vista del sistema operativo, sus programas y las cuentas de usuario vinculadas. No se tiene en cuenta la información contenida en los archivos de los equipos, ya que éstos ya fueron contemplados como activo de información en sí mismos.

- Correo electrónico: abarca las cuentas de correo electrónico, los mensajes de correo y el software de correo (en caso de utilizar un servidor de correo propio).
- Redes sociales: abarca las cuentas de redes sociales (perfiles, *fanpage*, etc.), el contenido publicado y los mensajes intercambiados.
- Red Wifi: abarca el *Access Point* (AP) y la red local que éste proporciona

Activos de información adicionales de algunas PYMEs:

- Página web: Incluye los archivos de la página web, la base de dato asociada, las cuentas de *webmaster*, editores u otros usuarios y el servicio de alojamiento y/o servidor web.
- Servicios en la nube: abarca la cuenta asociada al servicio y los archivos alojados en él
- Sistemas o aplicaciones internas: se centra en los archivos o ejecutables del sistema interno, la base de datos asociadas y las cuentas de usuarios asociadas al sistema (a nivel de aplicación).
- Servidores propios: abarca a los equipos servidores desde el punto de vista del sistema operativo, sus programas, los servicios que ejecutan y las cuentas de usuarios vinculadas.

El análisis de riesgo se encuentra en el Anexo 2. De acuerdo a cada uno de estos activos, se ha detallado todas las posibles amenazas, su probabilidad e impacto, de lo cual se han planteado todos los posibles controles o medidas de seguridad parar mitigar estas amenazas. Se ha utilizado la siguiente escala:

- Probabilidad:
    - Baja: es poco probable debido a que existen pocas personas con interés, oportunidad y recursos (tiempo, conocimiento, capacidad técnica) de llevar a cabo el ataque; se espera que ocurra un evento una vez en 10 años o más.
    - Media: es probable que existen personas con interés, pero no con la oportunidad o los recursos, o personas que tengan la oportunidad y/o los recursos, pero no la motivación para llevar a cabo el ataque; se espera que ocurra un evento en un periodo de 3 a 10 años.
    - Alta: es probable que existan personas con interés, oportunidad y recursos para llevar a cabo el ataque; se espera que ocurra un evento en un periodo de 3 años o menos.

- Impacto:
    - Bajo: el evento no supone una interrupción significativa al negocio, no se afecta la confidencialidad de datos personales sensibles y/o información sensible del negocio ni se afecta negativamente a la imagen de la empresa, no se producen consecuencias económicas significativas.
    - Medio: el evento supone una interrupción a algún proceso del negocio, se afecta la confidencialidad de algunos datos sensibles o se afecta negativamente la imagen, pero de manera temporal y reparable, se producen algunas pérdidas económicas, directas o indirectas, pero pueden ser asumidas por la empresa.
    - Alta: el evento produce una interrupción significativa a varios procesos del negocio, se afecta la confidencialidad de mucha información sensible o datos personales, se daña la imagen de la empresa y/o los costos directos o directos asociados al evento son importantes. Las pérdidas económicas no pueden ser asumidas fácilmente por la empresa.

- Criticidad: Nivel de Probabilidad + Nivel de Impacto

		Probabilidad		
		Baja	Media	Alta
Impacto	Alta			
	Media			
	Baja			

Criticidad
Baja
Media
Alta

Tabla 1: Matriz de riesgo y escala de criticidad utilizada en el análisis

De este análisis de riesgo, tomando como línea de corte aquellos riesgos medios y altos, se han identificado posibles controles, que se han descrito y analizado en la siguiente sección. Algunos controles o medidas de protección son transversales, tales como las referentes a la protección de contraseñas (elección de contraseñas robustas, uso de gestor de contraseña, por ejemplo), educación al usuario (sobre ingeniería social, especialmente), etc. Otros controles, que sirven para proteger un determinado activo, en realidad, están implementados en un activo diferente, como por ejemplo las contraseñas de inicio de sesión y bloqueo de pantalla, las cuales protegen, entre otras cosas, la información contenida en un equipo; sin embargo, se trata de un control que se implementa en el propio equipo, no en los archivos. Otros controles que han sido identificados como mecanismos de protección de un activo particular, podrían ser considerados un control global, como por ejemplo la educación de usuarios.

Descripción y análisis de los controles identificados

Se ha realizado un análisis de la efectividad de cada posible control y se ha planteado posibles maneras de implementarlas. Con este análisis, fue posible estimar los recursos necesarios para su implementación, en cuanto al tiempo, los recursos humanos y el costo económico a ser destinados. No se han considerado implementaciones que superen claramente las limitaciones identificadas en la encuesta exploratoria. En el Anexo 3 se detalla un ejemplo de implementación de los controles, con una o más opciones de implementación, en la que se describe el tipo de control, las herramientas requeridas, el tiempo estimado para su implementación, la cantidad de personal y el conocimiento técnico necesario, así como también el costo económico.

Archivos (en computadoras, teléfonos, dispositivos móviles, etc.)

1. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos:

Esta medida de protección es efectiva para aquellos escenarios en que un atacante con acceso físico a un equipo (por ejemplo, un empleado o visitante ocasional con malas intenciones) desea acceder a archivos que se encuentren en un equipo al cual no debería acceder. También es efectiva para el caso de pérdida o robo de un equipo, considerando un atacante con recursos bajos a intermedios. No será efectivo para proteger contra un atacante avanzado, que podrá evadir dicho control, por ejemplo, *booteando* el equipo desde un sistema operativo diferente o desde algún modo avanzado del sistema operativo. Las contraseñas deben ser robustas y diferentes una de otra, especialmente entre equipos que pertenecen o que deberían ser accedidos por personas diferentes. Si bien, este control o medida de protección protege, entre otras cosas, el acceso a archivos sensibles que se encuentran en un determinado equipo, se implementa en el equipo y no en los archivos, por lo que su implementación fue planteada como un control de equipos (computadoras, teléfonos y dispositivos móviles).

2. Cifrado de archivos sensibles:

Esta medida de protección es efectiva para aquellos casos en que un atacante logra el acceso al propio archivo, mediante el acceso al disco duro donde se aloja (infección de malware, robo del equipo, acceso físico al equipo, etc.). Con esta medida de protección, aunque el atacante pudiera evadir otros controles como la contraseña de inicio de sesión, por ejemplo, no podría visualizar el contenido del archivo ya que no posee la clave de cifrado y, por tanto, no podrá descifrarlo. El cifrado puede ser implementado de diversas formas, entre las que destacan:

- Cifrado de archivos: tiene la ventaja de tener un impacto mínimo en el rendimiento global, los archivos se cifran y descifran solo cuando se va a acceder a ellos. Existen múltiples soluciones, gratuitas y simples para implementarlo en la gran mayoría de los sistemas operativos. Algunas aplicaciones incluyen funcionalidades de cifrado de archivos (Microsoft Office, WinRAR, ZIP, 7zip). La desventaja es que deben cifrarse los archivos de manera individual. Además, si el equipo se compromete con un software malicioso que tenga la capacidad de extraer archivos y capturar pulsaciones de teclado, podrá obtenerse la clave y el cifrado del archivo podrá romperse. Sin embargo, un software malicioso de este tipo, y que además sea capaz de evadir la protección de un antivirus, se considera una amenaza avanzada, la cual es poco probable en PYMEs.

- Cifrado de disco: su ventaja es que se cifra el disco duro entero, por lo que el usuario no necesita preocuparse de identificar individualmente los archivos sensibles. La desventaja es el impacto en el rendimiento; tampoco protege en aquellos casos en que el equipo se ha comprometido (por ej: *malware* con capacidad de captura de pantalla), ya que luego del *booteo*, los datos se encuentran en texto claro. Sin embargo, un *malware* de este tipo, y que además sea capaz de evadir la protección de un antivirus, se considera una amenaza avanzada, poco probable en PYMEs.

- Cifrado de contenedor o disco virtual: combina las ventajas de ambos tipos de cifrado, creándose un disco duro virtual totalmente encriptado, sin embargo, como el disco duro virtual es finalmente, un archivo, los datos no se escriben en texto claro en el disco físico en ningún momento. La desventaja es que el archivo permanece cifrado en el contexto del contenedor, si el usuario, luego de haber montado el contenedor cifrado, copia el archivo a un lugar fuera del contenedor, el mismo se almacenará en texto claro, perdiéndose la protección. Una herramienta gratuita para este tipo de cifrado es VeraCrypt. Tampoco es del todo efectivo contra software malicioso avanzado, sin embargo, este escenario es poco probable en PYMEs.

Algunos sistemas operativos, tanto de computadoras como de dispositivos móviles, incluyen herramientas de cifrado, por lo general, a nivel de disco. Es el caso de Mac OS X, desde la versión 10.3 se incluye FileVault. Muchas distribuciones de Linux incluyen diversas herramientas de cifrado. En el caso de Android y iOS también cuentan con funcionalidad de cifrado de archivos a nivel de disco. En el caso de Windows, desde la versión Vista se cuenta con Bitlocker, sin embargo, solo está disponible en algunas ediciones, que, por lo general, no son las que se utilizan en PYMEs. Sin embargo, existen numerosas herramientas de terceros que pueden instalarse en casi todos los sistemas operativos, para todos los tipos de cifrado (archivos, disco, contenedor, etc.).

En las pruebas de implementación fue posible implementar dicho control a través de un software de terceros (AxCrypt) con un tiempo de dedicación de 2 a 3 minutos por equipo, sin requerir ningún conocimiento técnico y de manera gratuita, pudiendo una persona implementar el control en todos los equipos o cada empleado instalar y configurar individualmente el software en su equipo. En el caso de dispositivos móviles Android y iOS se ha optado por la configuración de la funcionalidad incluida en el sistema operativo por parte de cada empleado en menos de 2 minutos.

3. Distribución granular de permisos para accesos a archivos:

Este control es efectivo contra el abuso de confianza de personas internas, como por ejemplo empleados infieles. Evita que una única persona pueda acceder a todos los archivos sensibles de la empresa, limitando los permisos y accesos a aquella información estrictamente necesaria para la realización de las tareas asignadas. Este control, además, dificulta los ataques externos, en el sentido que, cuanto más segmentada y/o distribuida esté la información, el atacante tendrá que comprometer más de un equipo y/o cuenta para obtener lo que desea.

Este tipo de controles se deben implementar a nivel de procedimiento, principalmente. Primeramente, la organización debe realizar un inventario de activos de información, en la que, como mínimo, se debe recoger la siguiente información:

- ¿Qué tipo de datos o información poseemos en la empresa?
- De estos datos, ¿cuáles son sensibles?
- ¿Dónde están almacenados esos datos, en qué archivos, en qué máquinas, en qué cuentas?
- ¿Quiénes tienen acceso a esos datos actualmente?
- ¿Quiénes necesitan esos datos para realizar sus tareas?

Luego de haber respondido dichas preguntas, la empresa, es decir, alguna persona con autoridad, ya sea el dueño, directivo, gerente o a quien haya sido delegada la responsabilidad de llevar a cabo el proyecto de seguridad, debe tomar las decisiones necesarias para definir los niveles de permiso de acuerdo a cada empleado o grupo de empleados.

Mediante las pruebas de implementación se estimó que el tiempo de dedicación puede variar de 4 a 30 horas, dependiendo del nivel de conocimiento que tengan los directivos o empleados acerca de qué datos tienen y donde se encuentra. La implementación no requiere recursos económicos ni conocimiento técnico, pero requiere la dedicación de al menos una persona, con el apoyo activo de al menos un directivo o autoridad de la empresa, así como el apoyo de los demás empleados.

4. Copia de seguridad continua de archivos:

Este control es efectivo para minimizar el impacto causado por *ransomware*, borrado intencional o no intencional de archivos, eventos fortuitos como el daño de un equipo, y muchos otros incidentes que afecten a la disponibilidad de la información. Para que el control sea realmente efectivo, es fundamental que se tengan en cuenta tres propiedades:

- Frecuencia de la copia: si la copia de seguridad solo reflejará la información tal como se encontraba en el momento de la copia; si se trata de archivos que se modifican frecuentemente, la copia también debe realizarse con igual frecuencia.
- Almacenamiento de la copia: la copia de seguridad debe almacenarse en un lugar diferente al original, preferentemente en otro lugar físico; de lo contrario, si se daña el almacenamiento, se perderá el original y la copia.
- Verificación de la copia: se debe probar que la copia se esté realizando efectivamente y que la misma funcione, es decir que, al momento de restaurarla, se pueda recuperar la información que se deseaba.

Existen varias maneras de implementar este tipo de medidas:

- Copiar todos los archivos o los archivos importantes en un dispositivo de almacenamiento externo (USB o disco duro externo) con una cierta periodicidad, por ejemplo 1 vez al mes.
    - Ventajas: no se requiere ningún software o herramienta adicional (además del propio dispositivo externo); el límite de tamaño de los datos a copiar está limitado únicamente al tamaño del dispositivo externo

    - Desventaja: no es un mecanismo automatizado, depende de la acción humana de cada empleado; no se tendrá copia de seguridad de las modificaciones generadas en el periodo. En caso de utilizar un dispositivo externo para cada empleado, los costos son elevados.
- Sincronización de archivos a un servidor compartido, por ejemplo, con alguna herramienta basada en *rsync* o similar.
    - Ventaja: la copia de seguridad se puede hacer de manera más frecuente (dependiendo de la configuración de la herramienta – normalmente diaria); no requiere acción de parte de los empleados, la copia se realiza automáticamente; las copias de seguridad se almacenarán en un almacenamiento centralizado, bajo el control de la empresa.
    - Desventaja: se debe contar con algún medio de almacenamiento centralizado, que puede tener un costo relativamente alto y debe ser securizado; se debe contar con una herramienta o software (aunque existen varios, algunos gratuitos); la implementación requiere conocimiento técnico y tiempo.
- Sincronización de archivos mediante servicios en la nube, como Dropbox, OneDrive, ZohoDocs, Amazon S3 o Google Drive.
    - Ventaja: la copia se realiza de manera continua, por lo que la información de la copia siempre está actualizada; no requiere ninguna acción de parte de los empleados, la copia se realiza de manera automática; la instalación y configuración de la herramienta es rápida y fácil
    - Desventaja: el tamaño de la copia está limitado de acuerdo al espacio de almacenamiento ofrecido por el servicio de la nube, el espacio adicional tiene costo; como la sincronización es a través de Internet, la copia de seguridad de archivos grandes puede ser lenta y/o sobrecargar la red; en caso de que la empresa no cuente con un plan corporativo, las copias de seguridad se almacenarán en las cuentas individuales de los empleados.

Analizando las ventajas y desventajas de las tres posibles implementaciones, se ha descartado la copia de seguridad manual periódica, la cual es difícilmente sostenible a largo plazo, en cambio, se optó por alguna solución de sincronización de archivos. También se ha descartado la sincronización en red con almacenamiento offline centralizado, ya que esto supondría la adquisición, instalación, configuración y mantenimiento de un servidor o dispositivo de almacenamiento local, lo cual probablemente supere las limitaciones de una PYME. En muchos casos, aunque se pueda realizar la inversión inicial, será difícil de mantener, constituyendo un posible punto de fallo que introduzca más riesgos. Teniendo en cuenta las enormes ventajas de los servicios basados en *cloud*, que superan ampliamente las demás opciones, se ha optado por la tercera opción. En el caso de dispositivos móviles (teléfonos), también se puede implementar esta medida, con las herramientas nativas de Android y iOS.

En las pruebas de implementación se ha logrado implementar este control de 30 minutos a 1 hora para la configuración del servicio y 5 a 10 minutos por equipo a ser sincronizado. Se requiere la dedicación de una persona para la configuración del servicio y cada empleado puede instalar y configurar de manera individual el cliente de sincronización en su equipo, sin requerirse ningún tipo de conocimiento técnico y sin ningún costo.

Computadoras:

1. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña robustas y diferentes en todos los equipos:

Esta medida de protección había sido planteada como mecanismo para prevenir que alguien no autorizado acceda a los recursos de un equipo, especialmente a los archivos, y se implementará en los equipos (computadoras, teléfonos y dispositivos móviles) a nivel de sistema operativo, teniendo en cuenta

que todos los sistemas operativos traen dicha funcionalidad. Para que la medida de protección sea efectiva, las contraseñas deben ser robustas y diferentes una de otra, especialmente entre equipos que pertenecen o que deberían ser accedidos por personas diferentes. Debe ser combinada con una política de contraseñas que indique a los empleados qué características debe cumplir la contraseña (longitud, combinación de tipos de caracteres, tipos de contraseña a ser utilizadas, periodo de rotación o cambio, etc.). Adicionalmente, la política no debe ser solo verbal o escrita, sino estar implementada en el propio control, es decir, que el sistema operativo no permita al empleado elegir una contraseña que no cumpla la política. Política recomendada para una PYME (amenazas básicas hasta intermedias):

- Longitud mínima de caracteres de 10 a 12
- Combinar minúsculas, mayúsculas, números y símbolos, al menos un carácter de cada tipo
- Evitar contraseñas o palabras comunes (datos personales, fáciles de adivinar o palabras de diccionario)
- Cambiar la contraseña cada 3 a 6 meses.

Es posible implementar este control de al menos dos maneras distintas, en menos de 15 minutos por equipo, de manera gratuita, sin conocimiento técnico y por una única persona.

2. Soluciones de seguridad de Endpoint (*antivirus*, *antimalware*, anti-*spyware*, etc.)

Esta medida protege al equipo de infección de software malicioso y técnicas de ataque relacionadas a *malware*. Las herramientas más básicas y gratuitas sirven, por lo general, para detectar y remover software malicioso de acuerdo a firmas o patrones conocidos, mientras que las herramientas más avanzadas y de pago ofrecen funcionalidades adicionales como protección en tiempo real (análisis *on-the-fly*), *sandboxing*, inspección de paquetes basado en host, etc. Para una PYME, las herramientas básicas suelen ser adecuadas. Las versiones corporativas (por lo general, de pago) ofrecen, entre otras cosas, una gestión centralizada del agente de antivirus de los equipos de la red, mientras que, en las versiones personales, se debe gestionar y administrar el antivirus de cada equipo de manera individual y aislada. Existen muchas empresas que ofrecen soluciones de seguridad de *endpoint*, desde la propia solución integrada a Windows (Windows Defender, Security Essentials) u software de terceros.

Para una microempresa que cuenta con muy pocos equipos, es posible implementar este control con herramientas gratuitas, sin necesidad de conocimiento técnico, instalando cada empleado de manera individual con un tiempo de dedicación de 20 a 30 minutos. Sin embargo, para una empresa un poco mayor (10 o más empleados) es preferible optar por una implementación que permita una gestión centralizada, para lo cual se requiere la dedicación de 1 a 2 horas de una persona para la configuración de la solución central, la cual debe tener un conocimiento básico a intermedio. La implementación en cada equipo es de 15 a 25 minutos y puede ser realizada por cada empleado de manera individual. Los costos anuales varían de 20 a 40 USD por equipos dependiendo del tipo de licencia que se adquiera.

3. Cortafuego basado en Host

Esta medida de protección controla las conexiones permitidas y no permitidas, desde y hacia el equipo. Normalmente se configura de tal manera a permitir todas las conexiones salientes de la máquina y para rechazar todas las peticiones entrantes, lo cual es adecuado para aquellos casos en que el equipo no necesita exponer ningún servicio. Protege ante ataques locales y/o ciertos escenarios de explotación de vulnerabilidades (técnicas de movimiento lateral entre equipos comprometidos, por ejemplo), minimizando el contacto que pueda haber entre la máquina y otras. En el caso de necesitar compartir archivos, permitir control remoto del equipo, etc. es necesario habilitar las reglas específicas para permitir dichas conexiones específicas. Nunca se recomienda deshabilitar completamente el cortafuego sino personalizar las reglas. En algunos casos, puede ser recomendable limitar las conexiones salientes, por ejemplo, permitiendo

solo las conexiones a puertos conocidos; sin embargo, en la práctica esto es difícil de mantener, ya que existen múltiples servicios legítimos sobre puertos poco tradicionales. Para una PYME, es suficiente un cortafuego a nivel de host con una configuración estándar. La gran mayoría de sistemas operativos, entre ellos Windows, iOS, Linux, etc. incluyen cortafuegos de host; se puede utilizar dicha función o se puede utilizar software de terceros. Generalmente, las soluciones de seguridad de *endpoint* incluyen funcionalidad de cortafuegos.

Es posible implementar este control en 1 a 2 minutos por equipo sin ningún conocimiento técnico y de manera gratuita, ya sea por cada empleado de manera individual o por una persona que lo configure en cada equipo.

4. Actualización de sistema operativo y programas:

La actualización es, probablemente, uno de los controles más importantes, ya que es la principal manera de corregir vulnerabilidades que se descubren en el software, tanto en el sistema operativo como en las aplicaciones. Mantener el software actualizado protege ante la explotación de vulnerabilidades, una de las técnicas utilizadas por los atacantes para la distribución e implantación de software malicioso, así como otras técnicas más avanzadas. Una de las técnicas más peligrosas, que se aprovecha de la existencia de vulnerabilidades en el equipo de usuarios es la de *drive-by download* o descarga al paso, utilizada principalmente para distribución de malware. Con esta técnica, una persona que visita un sitio web que contiene código malicioso (infectada previamente y/o a través de *malvertising*, anuncios infectados), con solo abrir la página, el código malicioso explota alguna vulnerabilidad del equipo del visitante y lo infecta. Es especialmente peligroso porque no requiere interacción de la víctima. La principal defensa ante este tipo de técnicas es la actualización permanente de todo el software. Esta medida de protección, sin embargo, no será suficiente para aquellos escenarios en que el atacante utiliza ingeniería social ya que, en estos casos, por lo general, no se explota ninguna vulnerabilidad de software.

Si bien, la actualización puede realizarse de manera manual o automatizada, de manera individual o centralizada, son preferibles aquellos mecanismos automatizados y centralizados, que no dependen de la acción manual de los empleados, ya que de lo contrario se corre el riesgo de que éstos olviden de realizarlo con la frecuencia deseada. Muchas soluciones de seguridad de *endpoint* corporativas permiten la gestión centralizada y automatizada de actualizaciones, por lo general, incluido en el costo de la licencia.

Este control puede ser implementado de manera efectiva y eficiente con herramientas de terceros (Kaspersky Software Updater), con una dedicación de 30 minutos por equipo, por parte de una sola persona o por parte cada empleado de forma individual, sin conocimiento técnico y de manera gratuita. En caso de contar con una solución de seguridad de *endpoint* corporativa, es posible implementarlo de manera centralizada en 30 minutos, incluido en el costo de licencia del control 2 de este apartado (“Soluciones de seguridad de Endpoint”).

5. Protección de servicios expuestos con contraseñas robustas:

Algunos de los principales servicios de acceso remoto que pueden ser expuestos a Internet son SSH, RDP, TeamViewer. Estos accesos deben estar protegidos a través de una contraseña, como mínimo, la cual debe cumplir las políticas de contraseña que se han recomendado para contraseña de inicio de sesión de los equipos. Teniendo en cuenta que se trata de servicios accesibles desde Internet, los requerimientos podrían ser incluso más estrictos (contraseñas más largas, cambio de contraseña más frecuente, etc.). Como se trata de aplicaciones o servicios independientes del usuario de sistema operativo, a excepción de RDP, que es nativo de Windows y utiliza las credenciales de usuarios locales o de dominio, cada acceso deberá ser protegido y reforzado individualmente. Como medida práctica, se recomienda evitar

diversificar los mecanismos de acceso remoto, debido a que esto implicaría tener que contemplar procedimientos específicos para cada tipo de acceso.

Teléfonos y dispositivos móviles

1. Antivirus:

De manera similar al software antivirus en computadoras, esta medida protege a teléfonos y dispositivos móviles de infección de software malicioso. Algunas soluciones de antivirus corporativas incluyen soporte para teléfonos y dispositivos móviles, que se integran a la solución centralizada, sin embargo, las soluciones más económicas como AVAST Business Managed Antivirus no lo soporta. Otras como Panda Endpoint Protection, Kaspersky Small Office Security o Cloud Endpoint Security sí soportan dispositivos móviles (Android, iOS). Sin embargo, existen múltiples aplicaciones antivirus gratuitas que pueden instalarse de manera individual en los dispositivos móviles, los cuales son adecuados para los dispositivos de una PYME.

Es posible implementar este control a través de herramientas de terceros, con un tiempo de dedicación de a 1 3 minutos por equipo, sin conocimiento técnico, de manera gratuita, ya sea por una persona que lo instale en todos los dispositivos, o cada empleado de manera individual.

2. Restricción de instalación de apps no oficiales:

Tanto Android como iOS permiten restringir la instalación de aplicaciones que no provengan de los *app stores* oficiales. Esto minimiza el riesgo de instalar un software malicioso. Si bien, también existen aplicaciones maliciosas en los *app stores* oficiales, ya que a veces los controles para incluir una aplicación en el *app store* pueden fallar, esto es mucho menos frecuente. Es por eso que esta medida de protección debe ser complementada con el uso de un antivirus. No es una medida efectiva para aquellos casos en que un atacante obtuvo acceso físico al teléfono, ya que éste puede desactivar esta restricción, antes de implantar un software malicioso. Tampoco es efectivo para un atacante avanzado que sea capaz de evadir los controles del *app store* oficial y subir la aplicación maliciosa a él.

Esta configuración puede realizarse en 1 a 2 minutos por dispositivo, sin conocimiento técnico y de manera gratuita por cada empleado de manera individual.

3. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña

De manera similar a lo que es en computadoras, esta medida de protección ayuda a prevenir que alguien no autorizado acceda a los recursos de un dispositivo móvil, no solo archivos sino también acceso a las aplicaciones que están instaladas en los dispositivos. Una característica de las aplicaciones de los dispositivos móviles es que, la mayoría de éstas, están vinculadas a cuentas que están permanentemente abiertas (aplicaciones de redes sociales, de mensajería, clientes de correo, etc.) por lo que alguien que accede físicamente a un dispositivo móvil, accede también a estas cuentas. Esta protección se implementa a nivel de sistema operativo, teniendo en cuenta que todos los sistemas operativos traen dicha funcionalidad. Por lo general se puede establecer una contraseña, un PIN numérico, un patrón de desbloqueo o algún rasgo biométrico (huella dactilar, imagen facial, u otro). Para que la medida de protección sea efectiva, las contraseñas o su equivalente deben ser robustas y diferentes una de otra, especialmente entre equipos que pertenecen o que deberían ser accedidos por personas diferentes. A diferencia de las computadoras, no suele ser posible establecer una política de robustez de dicha credencial, las opciones específicas dependen del fabricante del dispositivo (modelo, marca, etc.). Por defecto no viene configurado ninguna contraseña ni equivalente.

Esta configuración puede realizarse en 2 a 3 minutos por dispositivo, sin conocimiento técnico y de manera gratuita por cada empleado de manera individual.

Correo electrónico

1. Contraseña segura:

Esta medida de protección previene que alguien no autorizada pueda acceder a la cuenta de correo electrónico, ya sea para evitar que pueda leer mensajes confidenciales o utiliza la cuenta para enviar *spam* o correos maliciosos. Las contraseñas de las cuentas de correo electrónico deberían cumplir con la política de contraseña de la empresa en cuanto a longitud, complejidad, etc. La implementación de esta medida de protección depende, en gran medida, del servicio de correo que se está utilizando, así sea un servicio de correo gratuito personal como Gmail, Hotmail/Outlook, un servicio de correo corporativo como Zoho, Office 365, o servidor de correo propio (Zimbra, MS Exchange, u otro).

La implementación es posible en 2 a 3 minutos por cuenta (o en total, en caso de servicios corporativos), con conocimiento técnico básico a nulo, por parte de una persona o cada empleado de manera individual y sin ningún costo.

2. Autenticación de doble factor:

Es una medida de protección adicional al usuario y contraseña, con la que, además de la contraseña, la cuenta solicita un código para poder acceder; ese código generalmente se envía o genera en el teléfono móvil. Previene que alguien no autorizada pero que ha logrado obtener la contraseña (ya sea adivinando la contraseña o a través de ingeniería social) pueda acceder a la cuenta de correo electrónico, ya que no tendrá manera de obtener el código. La implementación de esta medida de protección depende, en gran medida, del servicio de correo que se está utilizando, así sea un servicio de correo gratuito personal como Gmail, Hotmail/Outlook, un servicio de correo corporativo como Zoho, Office 365, o servidor de correo propio (Zimbra, MS Exchange, u otro). No todos los sistemas de correo incorporan la funcionalidad de autenticación de doble factor (por ejemplo, Zimbra solo lo incluye en la versión de pago).

Se probó que la implementación de este control requiere la dedicación de 10 a 15 minutos por cuenta por parte de cada empleado, con un nivel de conocimiento técnico básico y sin ningún costo.

3. Soluciones de seguridad de Endpoint (*antivirus*, *antimalware*, anti-*spyware*, etc.):

Teniendo en cuenta que existen malwares que infectan un equipo de usuario y utilizan el servicio de correo dentro de la red para generar spam, las soluciones de seguridad de *endpoint* minimizan el riesgo de quedar infectado con este tipo de software malicioso; sin embargo, se trata de una medida de protección a nivel de equipo y ya ha sido analizada en detalle en el apartado de dicho activo.

4. Configuración segura del servidor de correo, restricción del puerto 25:

Teniendo en cuenta que existen *malwares* que infectan un equipo de usuario y utilizan el servicio de correo dentro de la red para generar spam, con la restricción del puerto 25 se evita que estos *malwares* puedan establecer conexiones directas al puerto 25 para enviar los correos. El puerto 25 debería estar expuesto únicamente hacia el exterior de la red, solo se deben establecer conexiones SMTP con servidores de correo legítimos, no con máquinas infectadas. Todas las conexiones al puerto 25 deberían estar filtradas en la LAN. Esta restricción se debe configurar normalmente en el equipo de borde de red (*router*), por lo

que este control será analizado en el apartado de Wifi. Se debe tener en cuenta que algunos proveedores de servicio de Internet filtran el puerto 25 para los clientes con IPs dinámicas, por lo que en algunos casos no es necesario este control. Algunos modelos de *router* podrían no permitir la restricción de puertos.

5. Actualización del software de correo (si es propio):

Si la empresa cuenta con un servidor de correo propio, deberá actualizar regularmente el software de correo. Esto deberá ser llevado a cabo por el administrador del servicio de correo, las instrucciones específicas dependerán del software de correo a ser utilizado.

La implementación de este control es muy variable, pudiendo requerir de 15 minutos a 8 horas, debe ser llevada a cabo por una persona de conocimiento intermedio a avanzado; sin embargo, suele ser gratuito.

6. Configuración de información de recuperación:

La gran mayoría de los servicios de correo permiten establecer información de recuperación tal como una cuenta de correo alternativa, un número de teléfono móvil, etc. Esto permite que, cuando el usuario hubiera perdido acceso a la cuenta, pueda recuperarla. Esto es especialmente útil, por ejemplo, cuando una persona no autorizada ha logrado acceder a una cuenta y ha cambiado la contraseña. Si bien, esa persona puede cambiar también la información de recuperación, por lo general, cuando se detecta el nuevo acceso se envía un enlace de recuperación a las cuentas alternativas, por lo que el usuario legítimo lo puede recuperar. Cuando no se había establecido la información de recuperación o cuando esa información no fuera la correcta, el usuario legítimo no tiene manera de recuperar la cuenta.

Redes Sociales:

1. Contraseña segura:

Esta medida de protección previene que alguien no autorizada pueda acceder a la cuenta de la red social de la empresa (*fanpage*, perfil, etc.), ya sea para evitar que pueda leer mensajes confidenciales o utiliza la cuenta para publicar mensajes falsos o simplemente boicotearla. Las contraseñas de las cuentas de redes sociales deberían cumplir con la política de contraseña de la empresa en cuanto a longitud, complejidad, etc. La implementación de esta medida de protección depende, en gran medida, de cada red social. En la mayoría de los casos, las redes sociales se manejan como cualquier cuenta personal y la empresa solo puede instruir a los administradores de la red social a que utilices una contraseña robusta, pero dependerá de éstos obedecer ese requerimiento.

2. Autenticación de doble factor:

Al igual que en el correo electrónico, la implementación de esta medida de protección depende, en gran medida, de cada plataforma de red social (Facebook, Twitter, Instagram, etc.). La gran mayoría de estas plataformas incluyen la funcionalidad de autenticación de doble factor, la cual simplemente debe ser activada y configurada por los usuarios.

3. Configuración de información de recuperación:

Al igual que los servicios de correo electrónico, la gran mayoría de las plataformas de redes sociales permiten establecer información de recuperación tal como una cuenta de correo alternativa, un número

de teléfono móvil, etc. Esto permite que, cuando el usuario hubiera perdido acceso a la cuenta, pueda recuperarla. Esto es especialmente útil, por ejemplo, cuando una persona no autorizada ha logrado acceder a una cuenta y ha cambiado la contraseña. Si bien, esa persona puede cambiar también la información de recuperación, por lo general, cuando se detecta el nuevo acceso se envía un enlace de recuperación a las cuentas alternativas, por lo que el usuario legítimo lo puede recuperar. Cuando no se había establecido la información de recuperación o cuando esa información no fuera la correcta, el usuario legítimo no tiene manera de recuperar la cuenta.

4. Procedimiento de baja de usuario - transferencia de responsabilidades y accesos:

Si bien, cualquier empresa, así sea una PYME o una gran empresa, debería tener procedimientos de alta, baja y modificación de usuarios para todo tipo de accesos, esto es especialmente importante para la administración de cuentas de redes sociales, ya que, la mayoría de las veces, las cuentas de redes sociales oficiales de la PYME se encuentran delegada en una persona, sin ningún tipo de control sobre la plataforma de la red social. Cuando esa persona se retira de la empresa, si no se ha transferido ese rol a otra persona, se corre el riesgo de perder el acceso al perfil o cuenta oficial de la empresa. Existen diversas maneras de implementar este control, dependiendo de la plataforma y de la empresa, ya sea a través de la redundancia de roles (más de un usuario administrador, cuando la plataforma lo permite), resguardo de la contraseña en poder de una autoridad de la empresa, u otros mecanismos.

Wifi:

1. Contraseña segura del Wifi:

Esta medida de protección previene que alguien no autorizada pueda conectarse a la red local de la empresa, y por tanto aprovechar el ancho de banda de la empresa. Además, si una persona lograra conectarse a la red local, podría realizar una gran variedad de ataques locales (*man-in-the-middle*, ataques de capa 2, *sniffing* de tráfico, denegación de servicio local, u otros) por lo que esta medida de protección es efectiva para este escenario. La contraseña del wifi se establece a través del panel de administración del *Access Point* (AP). Las instrucciones específicas varían de acuerdo a la marca y modelo del AP, pero es similar en todos. La contraseña debe cumplir las políticas de contraseña de la empresa especialmente en cuanto a longitud y complejidad. La implementación de este control requiere de 1 a 2 minutos de tiempo y puede ser realizada por una persona, sin conocimiento técnico y de manera gratuita.

2. Configuración segura del Wifi – protocolos seguros:

Esta medida de protección previene que alguien en el rango de cobertura del wifi explote vulnerabilidades en los protocolos antiguos para conectarse a la red local de la empresa. Esta configuración se realiza a través del panel de administración del *Access Point* (AP), las instrucciones específicas varían de acuerdo a la marca y modelo del AP, pero es muy similar en todos. Para una PYME, el protocolo más adecuado es WPA2; nunca se debe utilizar WEP o WPA. La implementación de este control requiere de 1 a 2 minutos de tiempo y puede ser realizada por una persona, sin conocimiento técnico y de manera gratuita.

3. Contraseña segura del Access Point:

Esta medida de protección previene que alguien no autorizado, ya sea que esté conectado a la red local (un empleado, un invitado u otro) o alguien que explote una vulnerabilidad del AP (vulnerabilidad CSRF,

por ejemplo) pueda acceder al Access Point y modificar la configuración. La contraseña del AP se establece a través del panel de administración del AP. Las instrucciones específicas varían de acuerdo a la marca y modelo del AP, pero es muy similar en todos. La contraseña debe cumplir las políticas de contraseña de la empresa especialmente en cuanto a longitud y complejidad y debe ser distinta a la de la red Wifi. La implementación de este control requiere de 1 a 2 minutos de tiempo y puede ser realizada por una persona, sin conocimiento técnico y de manera gratuita.

4. Utilización de HTTPs para envío de credenciales:

Si bien, la utilización de HTTPs o HTTP depende del servidor web al que uno se conecta, es decir, no depende del usuario, es importante instruir a los usuarios a que presten atención, especialmente a la hora de introducir credenciales o información sensible, que la conexión se esté estableciendo bajo HTTPs.

Página Web:

1. Actualización de CMS, plugins, plantillas:

Esta medida de protección previene que una persona explote una vulnerabilidad del código de la página web, ya sea una vulnerabilidad presente en el código del CMS, de algún *plugin* o de la plantilla, que le permita leer contenido sensible, esconder código malicioso, ejecutar comandos u otro tipo de ataques. Cuando se utiliza algún *Content Management System* (CMS) como Wordpress, Drupal, Joomla, etc. no es necesario que nadie de la empresa corrija el código, ya que los desarrolladores del CMS publican las correcciones del código en la nueva versión; el administrador de la web simplemente debe actualizarlo. Lo mismo ocurre para los *plugins* y plantillas que cuentan con un equipo de desarrollo que ofrece soporte para los mismos. La gran mayoría de los CMS, *plugins* y plantillas pueden actualizarse a través del panel de administración del CMS, sin embargo, las instrucciones específicas pueden variar de acuerdo al CMS, al plugin y a la plantilla. Por ejemplo, existen *plugins* que deben ser actualizados reemplazando los archivos a través del gestor de archivos o FTP. Algunos proveedores de servicio de alojamiento ofrecen la funcionalidad de actualización automática de los componentes. Para una PYME que no cuenta con personal técnico, es preferible elegir un servicio de hosting que cuente con esta funcionalidad.

Dependiendo del tipo de CMS, *plugins* y/o plantillas utilizadas, así como también dependiendo del servicio de alojamiento, este control puede ser implementado de 5 a 30 minutos, por una única persona con conocimientos técnicos básicos a intermedios y sin ningún costo.

2. Contraseña segura para los usuarios del CMS:

Esta medida de protección previene que una persona no autorizada acceda al panel de administración de la página web y pueda modificarla, y, por tanto, controlar el servidor web. No previene que una persona explote una vulnerabilidad de la programación web. Las contraseñas de los usuarios de la web deberían cumplir con las políticas de contraseña de la empresa. La implementación depende de las funcionalidades del CMS y requieren, por lo general, 1 a 2 minutos de dedicación por cuenta, por parte de una persona con conocimiento técnico básico y sin ningún costo.

3. Auditoría de vulnerabilidades de la aplicación web (en caso de desarrollo propio):

Cuando la web se construyó en base a un código propio, desarrollado por la empresa o por una empresa que no se dedica al mantenimiento de dicho código, en caso de existir vulnerabilidades, no se publicarán

parches ni actualizaciones. La mayoría de las veces, la empresa no se entera de la existencia de la vulnerabilidad hasta que se haya explotado. Los servicios de auditoría de vulnerabilidades suelen estar fuera del alcance de una PYME, tanto por el conocimiento técnico requerido como por el costo. Existen herramientas que permiten descubrir algunas vulnerabilidades comunes y peligrosas que pueden ser utilizadas por una persona de conocimiento intermedio, como por ejemplo ZAP, VEGA Scanner y otros. Vulnerabilidades de SQLi, XSS, LFI/RFI y ejecución de comandos y de código deben ser consideradas críticas. En caso de no contar con los recursos (personal, conocimiento, tiempo) de realizar una auditoría de vulnerabilidades y si no se cuenta con el soporte de la persona o empresa que desarrolló el código, se debe considerar migrar la web a un CMS que cuente con soporte.

Es posible implementar dicho control utilizando herramientas de terceros gratuitas (por ejemplo, ZAP *Scanner*) con una dedicación de 15 a 30 minutos por parte de una persona, pero con conocimiento intermedio a avanzado, ya que los resultados de las herramientas deben poder ser interpretados correctamente para, posteriormente, ser corregidas de forma adecuada. Por lo general, este control no podrá ser llevado a cabo por personal de la PYME por el nivel de conocimiento requerido, sino ser tercerizado mediante una empresa o profesional especializados. Los costos pueden ser muy variados, entre alrededor de 500 a 1000 Euros para un servicio básico. Por lo general, esto no incluye la corrección de las vulnerabilidades si las hubiera, las cuales pueden tener un costo considerable. En caso de que la página web presente vulnerabilidades y/o que la empresa requiera cambios frecuentes en la programación, es recomendable que la empresa considere la opción de migrar la página web a un CMS que cuente con el soporte activo de una empresa y/o comunidad, quienes gestionan las vulnerabilidades de sus productos. Por lo general, esta migración implicará una construcción casi nueva de la web sobre una plataforma distinta, con un costo equivalente a una página web nueva, sin embargo, el mantenimiento a lo largo del tiempo será significativamente menor.

4. Contraseña segura para accesos del *hosting*:

Todos los accesos del servicio de alojamiento (gestor de archivos, FTP, SSH, u otros) deben contar con contraseñas seguras para evitar que una persona no autorizada acceda al mismo y pueda ver, editar, borrar archivos del mismo. Esta medida de protección, sin embargo, no protege de la explotación de vulnerabilidades en el hosting ni en la web. La mayoría de los servicios de alojamiento utilizados por PYMEs no permiten que la empresa fuerce el cumplimiento de una política de contraseña, por lo que las personas encargadas de las cuentas deben implementar este control de manera individual por cada cuenta. Se requiere un conocimiento técnico básico, un tiempo de dedicación de 3 a 5 minutos y no requiere recursos económicos.

5. Copia de seguridad del sitio web:

Se debe realizar una copia de seguridad del sitio web (archivos y base de datos) para evitar la pérdida del mismo por diversas causas (eventos fortuitos relacionados al alojamiento, *ransomweb*, errores humanos, compromiso del sitio web). La copia de seguridad se puede hacer de manera manual o de manera automatizada si es que el servicio de alojamiento lo permite. A diferencia de los archivos internos de una empresa, que cambian casi diariamente, los archivos del sitio web de una PYME no cambian frecuentemente, ya que en la mayoría de los casos son webs corporativas informativas, por lo que será suficiente con hacer una copia trimestral o incluso con menor frecuencia, de acuerdo a la frecuencia con la que se actualiza el sitio.

La copia de seguridad debe incluir, como mínimo, el directorio raíz del servidor web, el contenido de la base de datos y cualquier archivo de configuración del sistema operativo o servicios que la empresa haya personalizado. Es fundamental verificar que el sitio web pueda ser recuperado correctamente a partir de la copia de seguridad.

Para la implementación de este control es recomendable elegir un servicio de alojamiento que cuente con la funcionalidad de copia de seguridad frecuente automatizada, lo cual no tiene ningún costo adicional, puede ser configurado por una persona de conocimientos técnicos básicos en 3 a 5 minutos. Existen servicios de alojamiento económicos, a menos de 3 Euros mensuales, que ofrecen esta funcionalidad.

6. Separación de bases de datos y/o archivos sensibles del contenedor público:

En caso de que la empresa cuente con bases de datos sensibles, ésta debe estar en un servidor de bases de datos distinta al de la página web. Esto evitará que, en caso de que exista una vulnerabilidad que permita el acceso o manipulación indebida a la base de datos de la web, esto solo afectará al contenido de la base de datos de la página y no a las demás. Igualmente, se debe evitar alojar archivos sensibles en el directorio raíz del servidor, o idealmente evitar incluso alojarlo en el mismo servidor web, el cual debe ser utilizado exclusivamente para alojar archivos de la página web. Esto evita que, en caso de comprometerse el servidor web, esto afecta a archivos sensibles. El administrador del servidor web debe realizar una revisión para asegurar que esto se esté cumpliendo, en caso contrario, debe migrar el contenido sensible a otro servidor; un servidor virtual o un contenedor virtual distinto será adecuado. Se requiere un tiempo de 10 a 60 minutos y un conocimiento técnico intermedio, sin embargo, no requiere recursos económicos.

7. Cortafuego de aplicación web (WAF - *Web Application Firewall*):

Un WAF (*Web Application Firewall*) es un tipo de herramienta que bloquea peticiones HTTP que coinciden con patrones de ataques conocidos. Por lo general, es altamente dependiente del tipo de aplicación, el lenguaje utilizado, el CMS, entre otras características de la aplicación web. Este control protege a la página web de la explotación de vulnerabilidades a nivel de aplicación, tales como SQL, XSS, CSRF y otras vulnerabilidades conocidas. No es una protección adecuada para prevenir accesos no autorizados de atacantes que, previamente, han obtenido la contraseña del CMS o servidor. Para ser efectiva, la herramienta debe ser modelada y personalizada de acuerdo a la web de la empresa; en caso de CMS comunes, existen generalmente reglas adaptadas a ellos; en cambio, en caso de aplicaciones de desarrollo propio, las reglas deben ser ajustadas.

Existen varios tipos de implementaciones de WAF: *cloud*, integrado y *appliance*. Este tipo de controles muchas veces están fuera del alcance de una PYME debido, principalmente, al conocimiento y tiempo que requiere su implementación y su mantenimiento. Mod_security, por ejemplo, es un tipo de WAF integrado a la programación del sitio y es gratuito, pero requiere un nivel de conocimiento avanzado para ser implementado. Puede ser más adecuada una implementación del tipo *cloud*, como por ejemplo la de Cloudflare, la cual requiere un conocimiento técnico básico a intermedio pero que tiene un costo (planes de alrededor de 18 Euros al mes)

Servicios en la nube:

1. Contraseña segura:

Esta medida de protección previene que una persona no autorizada pueda acceder a la cuenta del servicio en la nube. Las contraseñas de las cuentas de servicios en la nube deberían cumplir con la política de contraseña de la empresa en cuanto a longitud, complejidad, etc. La implementación de esta medida de protección depende, en gran medida, de cada plataforma. En los servicios de nube vinculados a cuentas personales (Google Docs, OneDrive, etc.) la empresa solo puede instruir a los administradores de la red social a que utilices una contraseña robusta, pero dependerá de éstos obedecer ese requerimiento. En

los servicios de nube corporativos (GSuites, Azure, OneDrive for Business, etc..) por lo general se puede establecer políticas de contraseña desde el panel de administración. El tiempo requerido es de 2 a 3 minutos, no tiene ningún costo y cada empleado que administra una cuenta puede configurarlo individualmente. En caso de servicios corporativos, una única persona podría implementar el control sin necesidad de conocimiento técnico en menos de 5 minutos.

2. Autenticación de doble factor:

Esta medida de protección previene que una persona no autorizada que ha obtenido la contraseña de alguna manera (ingeniería social, adivinando la contraseña, u otro mecanismo) pueda acceder a la cuenta del servicio en la nube. La implementación de esta medida de protección depende, en gran medida, de cada plataforma. En los servicios de nube vinculados a cuentas personales (Google Docs, OneDrive, etc.) cada usuario tendrá que configurar la autenticación de doble factor a su cuenta personal (Gmail, Outlook, etc.). En los servicios de nube corporativos (GSuites, Azure, OneDrive for Business, etc..) por lo general se puede forzar a que el usuario deba utilizar autenticación de doble factor desde el panel de administración.

La implementación de este control requiere una dedicación de 10 a 15 minutos por cuenta por parte de los administradores de las cuentas, con un conocimiento técnico básico y sin ningún costo.

3. Configuración de información de recuperación:

Las plataformas de servicios en la nube también permiten establecer información de recuperación (correo alternativo, teléfono, pregunta de seguridad, etc.) de modo a que, si se pierde el acceso a la cuenta, por el motivo que sea, se pueda recuperar el acceso. Cada administrador de la cuenta del servicio debe asegurarse de haber completado de manera correcta esta información.

Sistemas internos:

Debido a la diversidad de sistemas que pueden existir, no es posible modelar una implementación estándar de los controles propuestos, ya que éstas serán sumamente diversas. Muchas veces estos sistemas fueron desarrollados específicamente para la empresa, no cuentan con soporte, por lo que la empresa debe gestionar las vulnerabilidades que pueda haber en el sistema, ya sea debido a fallas en la programación, ausencia de controles y funcionalidades, y otros problemas que afecten a la seguridad.

1. Control de acceso a los sistemas con contraseñas robustas y diferentes para cada usuario.

Este control dependerá de si el sistema o aplicación interna cuenta con un módulo de gestión de usuarios. Las contraseñas de los usuarios de los sistemas deberían cumplir con las políticas de contraseña de la empresa.

2. Control granular de los permisos concedidos a cada usuario.

Este control dependerá de su el sistema o aplicación interna cuenta con un módulo de gestión de usuarios con control de permisos y roles. Muchas veces el sistema cuenta con un único rol que tiene todos los permisos, por lo que cualquier usuario que tenga acceso podría realizar cualquier acción, incluidas aquellas a las que no debería tener permisos.

3. Copia de seguridad de los datos del sistema interno (base de datos y/o sistema de archivos)

Este control normalmente es implementado a nivel del servidor donde se aloja el sistema, pude ser implementado a través de una copia manual con una cierta periodicidad, o a través de un mecanismo de copia de seguridad automatizada. La frecuencia de la copia de seguridad debe ser acorde a la frecuencia con lo que cambian los datos del sistema. En caso de sistemas transaccionales, la copia de seguridad debe ser continua.

4. Auditoría de vulnerabilidades de los sistemas internos

Este tipo de controles es especialmente relevante en el caso de sistemas propios a medida, ya que no suelen contar con el soporte de los desarrolladores, por lo que la gestión de vulnerabilidades recae en la empresa. Generalmente, este tipo de servicios están fuera del alcance de una PYME, tanto por el costo, tiempo y conocimiento requerido para llevarlo a cabo. Además, el tipo de auditoría depende también del tipo de sistema, lenguaje en que está construido, etc. lo que lo hace más complejo que debe ser llevado a cabo por una persona de conocimiento intermedio a avanzado. En caso de no poder implementar este control, se debería analizar la posibilidad de contratar un servicio de soporte de la empresa desarrolladora o de otra empresa especializada, o, como alternativa, migrar el sistema a otra plataforma que cuente con soporte de una empresa y/o de una comunidad activa.

5. Actualización del software y demás componentes de los sistemas internos

Este control solo podría ser implementado en caso de que el software y los componentes tengan soporte de sus desarrolladores, una empresa especializada y/o una comunidad activa. La manera de implementarlo depende de cada componente. En caso de que el software o un componente no cuente con soporte, se debe analizar la posibilidad de migrar el sistema a otra plataforma que cuente con soporte de una empresa y/o de una comunidad activa.

6. Soluciones de seguridad de *endpoint* en equipos que interactúan y/o alojan los sistemas internos (*antivirus*, *antimalware*, ..)

Este control ya ha sido analizado en el apartado de Equipos.

7. Cortafuego basado en *host* en equipos que interactúan y/o alojan la aplicación interna:

Este control dependerá en gran medida del tipo de sistema. En el caso de un sistema basado en Web, una posible implementación sería un WAF (*Web Application Firewall*) como por ejemplo *mod_security*. En su implementación más simple, puede instalarse y configurarse un cortafuego a nivel de sistema operativo, de manera similar a lo que fue descrito en el apartado de este activo.

Servidores propios:

Si bien, pocas PYMEs cuentan con servidores propios, ya sea físicos o virtuales por ejemplo a través de un servicio de VPS, es frecuente que cuenten también con al menos un personal técnico encargado de su mantenimiento, ya sea personal propio o un servicio tercerizado en otra empresa. La mayoría de las medidas de protección y controles requeridos para una red con servidores propios, especialmente si estarán publicados hacia Internet, requieren un tiempo y conocimiento significativamente mayor que los controles e los demás activos; en caso de que la PYME no cuente con ningún personal, ni propio ni

tercerizado que esté administrando dichos servidores, es necesario que contraten los servicios de alguna persona para el efecto. Dependiendo de las características de la empresa y de la cantidad de servidores, sistema y otros activos tecnológicos que posean, se deberá elegir entre un servicio tercerizado o un personal propio permanente.

1. Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware, etc.):

Los servidores, al igual que los equipos de usuario, también deben contar con software de seguridad como un antivirus. A pesar de que, en teoría, el servidor tiene una menor interacción con los usuarios (no se usa para navegar, abrir correos, etc.), igualmente es susceptible a la implantación de malware, ya sea a través de explotación de vulnerabilidades de servicios expuestos, explotación de vulnerabilidades de las aplicaciones alojadas o incluso a través de la propagación de malware en la red. Cualquier servidor, independientemente del sistema operativo (Windows, Linux, BSD u otro) debe contar con software de seguridad. Algunas empresas de antivirus cuentan con soluciones específicas para servidores, acordes a las particularidades de un servidor; la gran mayoría de soluciones específicas para servidores son de pago, pero también existen soluciones gratuitas. En aquellos casos en que el servidor cumple funciones relativamente reducidas (servidor de archivos, o de alojamiento de una pequeña web informativa) podría ser suficiente utilizar un software de seguridad igual al de los equipos de usuario.

En las pruebas de implementación en servidores Linux fue posible implementar este control con herramientas gratuitas, con la dedicación de 10 a 20 minutos por servidor por parte de una persona con conocimiento técnico intermedio. En el caso de servidores Windows Server, en cambio, no se ha encontrado soluciones adecuadas gratuitas; los costos varían de 25 a 250 Euros por servidor.

2. Cortafuego basado en Host y/o en red:

Los servidores, al igual que los equipos de usuario, también deben contar con un cortafuego para controlar las conexiones entrantes y salientes. El cortafuego puede ser a nivel de host, es decir, instalado y configurado en cada servidor o puede ser a nivel de red, es decir, instalado en un equipo de borde y configurado de manera global para todos los servidores. El cortafuego a nivel de host permite un control más granular, incluyendo el filtrado de conexiones entre máquinas / servidores de la red local. El cortafuego a nivel de red, sin embargo, permite el filtrado de conexiones entre los servidores y el exterior de la red (WAN). La mayoría de los *routers* de gama baja incluyen funcionalidades de cortafuego básico, suficientes para una empresa que no cuenta con servicios publicados, sin embargo, no son adecuados para empresas que desean publicar servicios, ya que no permiten aplicar reglas específicas para la DMZ, la cual queda directamente desprotegida. En este caso, se puede optar por equipos de borde de mayores prestaciones o utilizar herramientas gratuitas como pfSense, que pueden ser instaladas incluso en una PC-servidor de bajas prestaciones como equipo de borde.

Las implementaciones a nivel de host han sido posible en un tiempo de menos de 45 minutos para la instalación y configuración por parte de una persona con conocimientos intermedios a avanzados y de manera gratuita. Las pruebas de implementación a nivel de red han requerido alrededor de 2 horas, así como también un nivel de conocimiento técnico avanzado.

3. IDS/IPS basado en Host y/o en red:

Un IDS/IPS (*Intrusion Detection System* / *Intrusion Prevention System*) es una medida de seguridad que es capaz de detectar y bloquear varios tipos de ataques de acuerdo a los patrones de tráfico (ataques de fuerza bruta, ciertos tipos de ataques de denegación de servicio, explotación de vulnerabilidades, entre otros). Es importante resaltar que esta medida de protección depende casi enteramente de las reglas de

detección que posee, no podrá proteger de un ataque para el cual no posea una regla de detección con un patrón específico para ese ataque. Es adecuado para proteger ante ataques conocidos y/o que coincidan con patrones de ataques conocidos, tanto a nivel de red como de aplicación. No es adecuado para proteger ante ataques que se inician desde la red (empleado interno, ingeniería social, algunos tipos de distribución de malware, etc.). Puede ser implementado a nivel de host de manera genérico, basado en la aplicación (WAF, por ejemplo) o en la red. Las soluciones pueden ser muy variadas, por lo que sería imposible cubrir todas las posibles implementaciones; en las pruebas se han implementado dos opciones para este control, ambas gratuitas.

6. Actualización de sistema operativo y programas:

Al igual que con los equipos de usuario, la actualización es uno de los controles más importantes, ya que es la principal manera de corregir vulnerabilidades que se descubren en el software, tanto en el sistema operativo como en las aplicaciones. Mantener el software actualizado protegerá ante la explotación de vulnerabilidades, una de las técnicas utilizadas por los atacantes para comprometer un servidor. La principal defensa ante este tipo de técnicas es la actualización permanente de todo el software. En el caso de servidores Windows, la actualización se puede realizar de la misma manera que como se realice en los equipos Windows, ya sea a través de Windows Update combinado con actualización manual de los demás componentes o a través de una herramienta de gestión de vulnerabilidades. En el caso de servidores Linux, existen herramientas de automatización de actualización (yum-cron o similar), tanto del sistema operativo como de los paquetes descargados de repositorios oficiales; en caso de software instalado desde orígenes distintos, debe verificarse y/o actualizarse manualmente. A diferencia de las políticas de actualización en equipos de usuarios, podría no ser recomendable la actualización automática en servidores debido al riesgo que una actualización tenga problemas de compatibilidad con alguna de las aplicaciones o sistemas que se ejecutan en el servidor. Sin embargo, esto solo es válido para sistemas críticos y muy específicos; para una PYME esto no suele ser el caso, por lo que generalmente se puede utilizar herramientas de actualización automática sin mayor riesgo. En distribuciones específicas para servidores y de alta estabilidad, como CentOS/RHEL o Ubuntu LTE, los problemas de compatibilidad son muy raros.

7. Protección de servicios expuestos con contraseñas robustas:

Muchos servidores cuentan con algún mecanismo de acceso remoto expuesto a Internet como por ejemplo SSH, RDP, TeamViewer, etc. Estos accesos deben estar protegidos a través de una contraseña, como mínimo, la cual debe cumplir las políticas de contraseña que se han recomendado para contraseña de inicio de sesión de los equipos. Teniendo en cuenta que se trata de servicios accesibles desde Internet, los requerimientos podrían ser incluso más estrictos (contraseñas más largas, cambio de contraseña más frecuente, etc.). Como medida práctica, se recomienda evitar diversificar los mecanismos de acceso remoto, debido a que implica tener que contemplar procedimientos específicos para cada tipo de acceso. En caso de RDP (Windows) las políticas de contraseña se gestionan a partir de las políticas del sistema operativo, ya que las credenciales de acceso son las mismas del equipo. En el caso de SSH (Linux, principalmente) las políticas de contraseña se establecen en el archivo de configuración del servicio SSH.

La implementación de este control requiere una dedicación de 5 a 10 minutos por servicio por parte de una persona con conocimientos técnicos intermedios, sin necesidad de herramientas adicionales ni costo.

8. Hardening de sistema operativo y de servicios expuestos:

El hardening es un conjunto de acciones, configuraciones y controles adicionales que buscan, principalmente, dificultar un ataque. Se trata de una línea de defensa adicional a las básicas. De por sí

sola, no evita la ocurrencia de un ataque, pero previene que el daño sea significativo, en algunos casos previene el daño completamente. Existen muchas guías de hardening para cada sistema operativo y para cada servicio o aplicación. El hardening puede limitarse a cambiar solo algunas de las configuraciones por defecto o puede realizarse de manera exhaustiva, intentando fortalecer cada punto débil del sistema operativo. Existen herramientas para automatizar el proceso de hardening, aun así, el conocimiento requerido para utilizarlas es intermedio, ya que se debe comprender las implicancias de cada cambio de configuración. Algunas de éstas son Security Compliance Manager (Windows), Lynis (Linux), OpenSCAP (multiplataforma). La implementación de este control puede ser realizada de manera gratuita, con una dedicación que varía de 30 minutos a varias horas por servidor.

9. Copia de seguridad continua del sistema operativo (imágenes o *screenshots* de S.O.):

La copia de seguridad de servidores puede realizarse a nivel de sistema operativo o a nivel de archivos o contenido. La ventaja de hacer una copia de seguridad de todo el sistema operativo es que se resguardan también configuraciones, paquetes instalados, y otros componentes de manera a que, ante un incidente, se pueda restaurar rápidamente todo el servidor a su estado original. Cuando la copia de seguridad se realiza solo a nivel de sistema de archivos y base de datos de la aplicación, ante un incidente, es necesario realizar una instalación nueva del sistema operativo, una configuración completa y una posterior migración del contenido, lo que demora mucho más tiempo. En caso de utilizar virtualización, las copias de seguridad mediante la generación de imágenes del sistema operativo son muy fáciles de realizar, por lo general desde el panel de administración gráfico con unos cuantos *clicks* (con VMware, Hyper-V, ProxMox, etc.). En caso de que el servidor no se encuentre sobre una plataforma de virtualización, o que la misma no ofrezca la funcionalidad de realizar imágenes del sistema operativo, se puede utilizar alguna utilidad como rsync, y se debe contar con un sistema de almacenamiento de las imágenes, ya sea otro servidor, físico o virtual o un dispositivo de almacenamiento específico. En aquellos casos en que la criticidad del servicio, especialmente desde el punto de vista de disponibilidad, no es alta, como ocurre en la mayoría de las PYMEs, será suficiente con contar con una copia de seguridad de los archivos y bases de datos de las aplicaciones y sistemas alojados. En caso de incidentes, la recuperación a partir de la copia puede demorar alrededor de 1 a 3 horas (instalación y configuración inicial del sistema operativo en un nuevo servidor y reinstalación de los sistemas a partir de la copia de seguridad).

10. Redundancia lógica y/o física del servidor:

La redundancia lógica y/ física del servidor permite que, en caso de que ocurra un incidente que afecte a la disponibilidad de un servidor, el segundo servidor pueda suplir la indisponibilidad del primero para seguir brindando el servicio, evitando las interrupciones de servicio. La redundancia lógica debe ser diseñada desde la arquitectura hasta la programación e implementación del sistema. En muchos casos, si el sistema o aplicación no fue diseñado de manera a ser redundante, se necesitará una re-ingeniería de la misma. La redundancia puede ser de distintos niveles, pudiendo tener bases de datos redundantes, sistemas de archivos redundante, o en general, cualquier componente necesario para el funcionamiento del sistema. En la mayoría de las PYMEs la criticidad del servicio, especialmente desde el punto de vista de disponibilidad, no es alta por lo que esta medida de seguridad no será indispensable; será suficiente con contar con una copia de seguridad de archivos y bases de datos de las aplicaciones y sistemas alojado para que, en caso de un incidente que afecte la disponibilidad del sistema, se pueda migrarlo a un nuevo servidor hasta tanto se resuelva el incidente. Por tanto, este control no formará parte de la guía de controles.

Controles transversales:

Se trata de controles que no están directamente vinculados a un único activo, sino que son intrínsecos de la organización y que afectan a varios activos.

1. Educación al usuario:

Esta medida pretende concienciar y capacitar a los empleados acerca de los riesgos y cuidados que deben tener en cuenta a la hora de utilizar la tecnología. Si bien, muchas herramientas y controles técnicos protegen al usuario, de modo a que éste no deba preocuparse por la seguridad, estas medidas son insuficientes para protegerlo ante ataques de ingeniería social o aquellos ataques que requieren una interacción humana como ser el *phishing*, engaños telefónicos o presenciales, instalación de software malicioso (programas piratas o "*cracks*", por ejemplo), dejar el teléfono desatendido, etc. Es un control transversal a todos los activos. Un plan de concienciación y educación debe contemplar lo siguiente:

- Debe ser periódico, al menos una vez al año.
- Se debe asegurar que los nuevos empleados que son incorporados a la empresa sean capacitados.
- Las metodologías deben ser diversas, desde charlas cortas, simulacros, técnicas lúdicas, etc.
- El lenguaje debe ser simple, se pueden hacer analogías con la realidad diaria y conocida
- Los temas deben estar enfocados a aquellas cuestiones que dependen del usuario, no se debe incluir cuestiones que están fuera del alcance de éste (por ejemplo, medidas de protección que dependen del administrador de la red, seguridad de la web que depende del *webmaster*, etc.)

El tiempo estimado para un plan de concienciación y educación puede ser de 3 a 5 horas anuales, preferentemente dividido en jornadas breves por temática y metodología. Existen muchos recursos gratuitos, desde materiales audiovisuales, guías, charlas, etc. ofrecidos por organismos públicos, empresas privadas u organizaciones sin fines de lucro para que la empresa pueda llevar a cabo este plan. Existen también empresas privadas que ofrecen este tipo de servicios sin embargo suelen estar orientados a empresas grandes y con un costo superior al que puede destinar una PYME.

2. Utilización de gestor de contraseña:

El gestor de contraseñas es una herramienta que permita almacenar de manera segura las contraseñas, tanto de cuentas de correo, redes sociales, servicios en la nube, etc., de modo a minimizar el riesgo de olvidar las contraseñas. De esta manera, el usuario puede utilizar contraseñas largas, complejas, distintas, lo más aleatorias posible, sin el riesgo de olvidarlas. El gestor de contraseñas almacena las contraseñas de manera cifrada, por lo que es mucho más seguro que guardarlas en un documento en texto claro. El usuario solo debe acordarse de la contraseña del gestor ("Contraseña maestra"). Existen diversos programas gratuitos que pueden utilizarse, ya sea un gestor de contraseña offline (un programa que se instala en el equipo) o servicios de gestor de contraseña online (servicios que almacenan las contraseña en una cuenta en la nube).

Es posible implementar este control con herramientas gratuitas, en 2 a 3 minutos con conocimientos técnicos básicos; puede ser implementado por una persona en todos los dispositivos o puede ser implementado por cada empleado de manera individual en su dispositivo.

Ordenamiento y selección de controles en cuanto al balance costo - efectividad

Primeramente, se ha seleccionado los mejores controles, por activos. Aquellos controles cuya implementación han superado los límites de recursos que las PYMEs pueden destinar y que han aportado poco a la protección general del negocio han sido descartados.

Controles de activos básicos:

1. Archivos (en computadoras, teléfonos, dispositivos móviles, etc.)
   1.1. Copia de seguridad continua de archivos
   1.2. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos que alojan archivos sensibles.
   1.3. Distribución granular de permisos para accesos a archivos
   1.4. Cifrado de archivos sensibles.
2. Computadoras:
   2.1. Actualización de sistema operativo y programas
   2.2. Soluciones de seguridad de *Endpoint* (antivirus, antimalware, anti-spyware, etc.)
   2.3. Protección de servicios expuestos con contraseñas robustas
   2.4. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña
   2.5. Cortafuego basado en Host
3. Teléfonos y dispositivos móviles:
   3.1. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña
   3.2. Restricción de instalación de apps no oficiales
   3.3. Antivirus
4. Correo electrónico:
   4.1. Contraseña segura
   4.2. Autenticación de doble factor
   4.3. Configuración segura del servidor de correo, restricción del puerto 25 (si se utiliza servidor de correo propio)
   4.4. Actualización del software de correo (si se utiliza servidor de correo propio)
   4.5. Configuración de información de recuperación
5. Redes Sociales:
   5.1. Contraseña segura
   5.2. Autenticación de doble factor
   5.3. Procedimiento de baja de usuario - transferencia de responsabilidades y accesos
   5.4. Configuración segura y completa de la información de recuperación
6. Wifi:
   6.1. Contraseña segura del Wifi
   6.2. Configuración segura del Wifi - protocolos seguros
   6.3. Contraseña segura del AP

Controles transversales a la organización:

7. Establecimiento de políticas de seguridad, especialmente políticas de contraseña y de roles y permisos.
8. Utilización de gestor de contraseña para administrar contraseñas de diversos activos
9. Educación de usuarios (concienciación y capacitación) – especialmente en cuanto a ingeniería social y buenas prácticas de usuario

Controles de activos adicionales:

10. Página web:
    - 10.1. Copia de seguridad del sitio web
    - 10.2. Actualización de CMS, *plugins*, plantillas.
    - 10.3. Contraseña segura para los usuarios del CMS
    - 10.4. Contraseña segura para accesos del hosting (Filemanager, FTP, SSH, ..)
    - 10.5. En caso de desarrollo propio, considerar auditoría de vulnerabilidades o migrar a un CMS con soporte
    - 10.6. Separación de bases de datos y/o archivos sensibles del contenedor público
11. Servicios en la nube:
    - 11.1. Contraseña segura
    - 11.2. Autenticación de doble factor
    - 11.3. Configuración de información de recuperación
12. Sistemas internos:
    - 12.1. Control de acceso a los sistemas con contraseñas robustas y diferentes para cada usuario.
    - 12.2. Control granular e los permisos concedidos a cada usuario
    - 12.3. Copia de seguridad de los datos del sistema interno (base de datos y/o sistema de archivos)
    - 12.4. Actualización del software y demás componentes de los sistemas internos
    - 12.5. Auditoría de vulnerabilidades de los sistemas internos (en caso de sistema de desarrollo propio)
    - 12.6. Soluciones de seguridad de *endpoint* en equipos que interactúan y/o alojan los sistemas internos (antivirus, antimalware, ..)
    - 12.7. Cortafuego basado en host en equipos que interactúan y/o alojan la aplicación interna
13. Servidores propios:
    - 13.1. Protección de servicios expuestos con contraseñas robustas
    - 13.2. Actualización de sistema operativo y programas
    - 13.3. Hardening de sistema operativo y de servicios expuestos
    - 13.4. Cortafuego basado en Host y/o en red
    - 13.5. Soluciones de seguridad de *endpoint* (antivirus, antimalware, anti-spyware, etc.)
    - 13.6. IDS/IPS basado en Host y/o en red

De acuerdo a los controles propuestos, las posibles implementaciones, el análisis de costo desde el punto de vista de tiempo, recursos humanos, conocimiento y dinero requerido, su efectividad de acuerdo a posibles ataques a PYMEs y de acuerdo a las prioridades de negocio de las PYMEs, se ha ordenado los controles de manera priorizada, en orden decreciente según su relación costo-beneficio. Este ordenamiento es aproximado ya que muchos factores son subjetivos, además, no se ha realizado una medición numérica de la relación costo-beneficio sino solo una apreciación aproximada y subjetiva de dicha relación. Se ha dividido los controles en primarios, secundarios y adicionales:

- Controles primarios: serán aquellos controles fundamentales que protegen, de por sí solos, a la organización de incidentes o ataques comunes y probables y de alto impacto y cuya ausencia implica un éxito muy probable de un ataque;
- Controles secundarios: serán aquellos controles adicionales a los fundamentales que constituyen una segunda línea de defensa ante un incidente o ataque común y probable pero que, cuya ausencia, no implica el éxito de un ataque;
- Controles adicionales: son buenas prácticas que, en caso de ocurrir un incidente o ataque, puede ayudar a mitigar parcialmente los daños de éste o que, en general, pueden ayudar a la organización a implementar otros controles (primarios y/o secundarios) de manera más fácil o eficiente, pero que, de por sí solo, no protegen de un incidente o ataque.

Aquellos controles que constituyen una línea de defensa ante algún ataque o incidente que no requiera ninguna condición especial poco común o probable son considerados primarios (debido a que el usuario no podría protegerse sin dicho control), sin embargo, aquellos controles que protegen ante ataques que requieren que se de alguna condición especial (contar con acceso físico, ingeniería social relativamente sofisticada, o similar) serán considerados secundarios. Aquellos controles que protegen ante ataques que, de por sí solos, tienen un bajo impacto a la organización, son considerados controles secundarios, independientemente a si se requiere o no alguna condición especial para el éxito del ataque.

Esta agrupación busca orientar a la PYME con respecto al orden en el cual puede ir implementando los controles, de manera gradual y priorizada. No busca acotar el conjunto de controles. A pesar de ser una guía de controles básicos para PYMEs, no se debe perder de vista la importancia del modelo de defensa en profundidad, ya que no existe ningún control que pueda proteger al 100% de un incidente o ataque.

Controles primarios:

1. Copia de seguridad continua de archivos (en computadoras, teléfonos, dispositivos móviles, etc.)
2. Protección de servicios expuestos a Internet con contraseñas robustas, en equipos de usuarios y/o en servidores
3. Contraseñas seguras en cuentas de correo electrónico
4. Contraseñas seguras en cuentas de servicios en la nube
5. Contraseñas seguras en cuentas de redes sociales
6. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos, especialmente aquellos que alojan archivos sensibles.
7. Distribución granular de permisos para accesos a archivos
8. Actualización del software de correo (si se utiliza servidor de correo propio)
9. Actualización de sistema operativo y programas de los servidores propios
10. Actualización de sistema operativo y programas de equipos de usuario
11. Copia de seguridad de los datos del sistema interno (base de datos y/o sistema de archivos)
12. Control de acceso a sistemas internos con contraseñas robustas y diferentes para cada usuario.
13. Control granular de los permisos concedidos a cada usuario de los sistemas internos
14. Soluciones de seguridad de *endpoint* (antivirus, antimalware, anti-spyware, etc.) en computadoras
15. Antivirus en teléfonos y dispositivos móviles
16. Copia de seguridad del sitio web (archivos y contenido de base de datos)
17. Actualización de CMS, *plugins*, plantillas de la página web
18. Contraseña segura para los usuarios del CMS de la página web
19. Contraseña segura para accesos del hosting (Filemanager, FTP, SSH, ..)
20. Actualización del software y demás componentes de los sistemas internos

Controles secundarios:

1. Autenticación de doble factor en cuentas de correo electrónico
2. Autenticación de doble factor en cuentas de servicios en la nube
3. Autenticación de doble factor en cuentas de redes sociales
4. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña en teléfonos y dispositivos móviles
5. Educación de usuarios (concienciación y capacitación) – especialmente en cuanto a ingeniería social y buenas prácticas de usuario
6. Cortafuego basado en *host* en equipos que interactúan y/o alojan alguna aplicación interna
7. Cortafuego basado en *host* en equipos de usuarios
8. Restricción de instalación de apps no oficiales en teléfonos y dispositivos móviles
9. Cifrado de archivos sensibles.

10. Configuración segura del servidor de correo, restricción del puerto 25 (si se utiliza servidor de correo propio)
11. Cortafuego basado en *host* y/o en red para la protección de la red (DMZ, LAN, etc.)
12. Hardening de sistema operativo y de servicios expuestos en servidores propios
13. Contraseña segura del Wifi
14. Configuración segura del Wifi - protocolos seguros
15. En caso de página web de desarrollo propio, considerar auditoría de vulnerabilidades o migrar a un CMS con soporte
16. Separación de bases de datos y/o archivos sensibles del contenedor público del servidor web
17. Soluciones de seguridad de *endpoint* (antivirus, antimalware, anti-spyware, etc.) en servidores propios
18. IDS/IPS basado en Host y/o en red
19. Cortafuego de aplicaciones web (WAF – *Web Application Firewall*)
20. Contraseña segura del AP

Controles adicionales:

1. Establecimiento de políticas de seguridad, especialmente políticas de contraseña y de roles y permisos.
2. Utilización de gestor de contraseña para administrar contraseñas de diversos activos
3. Procedimiento de baja de usuario - transferencia de responsabilidades y accesos, especialmente de redes sociales u otras cuentas de administración delegada en un usuario
4. Configuración de información de recuperación de la cuenta de correo electrónico
5. Configuración de información de recuperación de la cuenta vinculada al servicio de la nube
6. Configuración de información de recuperación de la cuenta de redes sociales
7. Auditoría de vulnerabilidades de los sistemas internos

Estimación del costo global de los controles

Se calculó el costo global, en término de recursos humanos, tiempo y recursos financieros, requeridos para implementar los controles propuestos, seleccionando una de las opciones por cada control. Algunas opciones son más adecuadas para microempresas, pero pueden ser poco adecuadas para una empresa mediana. Se ha comprobado que, en casi todos los controles, existe al menos una opción que no requiere un tiempo de implementación superior a 2 horas. El único control que, por lo general, requerirá un mayor tiempo es la distribución granular de permisos para accesos a archivos, ya que implica una revisión de la situación actual de la empresa en cuanto a la información que posee. Sin embargo, se trata de un control que se realizará de manera poco frecuente, solo una vez al iniciar el proceso. Posteriormente, será una verificación, que podría ser anual, y que llevará significativamente menos tiempo ya que se conocerá mejor qué información se posee, donde se encuentra y quién tiene acceso.

Con respecto al costo, se ha podido encontrar una alternativa gratuita para casi todos los controles fundamentales. Uno de los pocos controles que tiene un costo asociado es la implementación de soluciones de seguridad de *endpoint* y servidores (antivirus, antimalware, etc.) con consola de gestión centralizada, sin lo cual sería bastante compleja la administración en empresas de alrededor de 15 o más equipos. Para redes de menor cantidad de equipos, es perfectamente posible y práctico utilizar las versiones personales, que son gratuitas. Aun así, el costo de las soluciones de antivirus en su edición corporativa, para 1 año y 25 dispositivos, por ejemplo, están disponibles a partir de 675 Euros aproximadamente, lo cual está dentro de los límites de presupuesto que habían indicado la mayoría de

empresas. Para todos los demás controles fundamentales se ha encontrado alternativas viables y gratuitas.

En cuanto a los recursos humanos, la gran mayoría de los controles requieren una persona dedicada a tiempo parcial a la implementación de estos controles, así como también la colaboración de los demás empleados para instalar en sus máquinas algunas herramientas, de lo contrario, si una única persona tiene que instalar individual y secuencialmente en cada máquina, el tiempo se extenderá a varios meses de trabajo. En la gran mayoría de los casos, las herramientas necesarias se instalan con un par de *clicks*, por lo que es viable plantear la posibilidad que el propio usuario lo instale el mismo. Si bien, en una red corporativa lo ideal sería que el administrador de la red pudiera instalar, configurar y controlar de manera centralizada las herramientas y configuraciones que implementa en cada equipo de la red, este mecanismo de gestión centralizada suele requerir una controladora de dominio y/o la adquisición de soluciones corporativas, que tienen un costo superior al que las PYMEs están dispuestas a destinar. Estas soluciones deberían ser analizadas sobre todo en aquellas empresas de 20 o más equipos, donde la gestión sin centralización empieza a ser compleja, no solo desde el punto de vista de seguridad sino de la sostenibilidad de la red.

Capítulo 4: Instrumentos para PYMEs

Objetivo de la fase

Para que el presente trabajo pueda ser aprovechado por una PYME es necesario brindarle instrumentos que le permitan, de forma simple y práctica, conocer la guía, implementarla y medirla. Para ello, se han diseñado los siguientes instrumentos:

- Formulario de auto-diagnóstico inicial
- Flujograma generador de controles
- Guía de implementación de controles
- Formulario de medición de cumplimiento

En esta fase se diseñó y se elaboró una primera versión de estos instrumentos de apoyo para la PYME.

Diseño de instrumentos

Formulario de auto-diagnóstico inicial:

Se trata de un instrumento que busca determinar la situación inicial de la seguridad en la PYME, principalmente en cuanto a nivel de riesgo. Para ello, el usuario debe indicar algunos datos como:

- Activos de información que posee
- Tipo de comportamiento o prácticas en cuanto a los activos de información
- Controles o medidas de protección que ya ha implementado

El formulario es del tipo de selección múltiple e incluye las respuestas más frecuentes, desde las ideales a las poco recomendadas. De acuerdo a las respuestas, principalmente con respecto a qué tipos de activo se posee, se debe continuar con una pregunta u otra. Por ejemplo, si el usuario indicó que no posee una página web en la empresa, podrá ignorar la sección de preguntas con respecto a dicho activo.

Cada una de las respuestas referentes al tipo de comportamiento y controles y medidas de protección existente, tiene un determinado puntaje, de acuerdo a qué tanto se acercan a lo correcto o ideal. En este caso, se ha optado por medir riesgo inicial, por lo que el puntaje es directamente proporcional al riesgo que introduce cada respuesta, es decir, qué tan alejada está de lo ideal. Además, tendrán mayores puntajes aquellas respuestas que reflejan la ausencia de controles primarios y de activos críticos. Se ha buscado un balance entre el nivel de detalle requerido para el diagnóstico y la brevedad y simplicidad para el usuario que lo completa.

Finalmente, se ha adoptado la siguiente escala para calcular el nivel de riesgo:

- 0 a 33% = riesgo bajo
- 34 a 66% = riesgo medio
- 67 a 100% = riesgo alto

Flujograma generador de controles:

Se trata de un instrumento que busca indicar al usuario qué controles o medidas de seguridad debe implementar en la empresa, de acuerdo a qué activos tiene, qué tipo de comportamiento o prácticas tiene en cuanto a dichos activos y qué controles ya tiene implementado. Esta información ya se ha indicado en el formulario de auto-diagnóstico inicial, por lo que este instrumento, que ha sido implementado como una planilla electrónica, importa las respuestas que se habían brindado en el formulario del diagnóstico inicial.

El resultado obtenido a partir de este instrumento es una lista de controles de esta guía, ordenados y agrupados de acuerdo a los niveles de prioridad que se establecieron en el capítulo anterior. En un futuro, esa prioridad podría ser determinada a partir de datos brindados por la empresa referentes a niveles de criticidad de los activos con respecto al negocio, así como otros datos de entrada de la empresa.

Guía de implementación de controles:

Este instrumento contiene una selección de opciones de implementación de cada control, con referencias a herramientas, tutoriales y guías específicas que ayuden a la PYME a implementar un determinado control, así como también información acerca de los recursos necesarios para la implementación (estimación de tiempo, recursos financieros y personal necesarios). Se trata de un documento de texto (archivo pdf) que contiene algunas posibles implementaciones de todos los controles, aunque existen otras opciones de implementación que podrían ser incluidas. En el futuro, podría construirse este instrumento de manera a que la guía incluya solamente aquellas opciones de implementación que aplican a la empresa, de acuerdo a los resultados de los instrumentos previos.

Formulario de medición de cumplimiento:

Este instrumento tiene como objetivo brindar a la PYME un mecanismo de medición de avance en la implementación de los controles, especialmente aquellos controles obtenidos a partir de los instrumentos previos. Permite que el usuario vaya marcando los controles y medidas de seguridad que ya ha implementado; a partir de esto, se calcula el porcentaje de cumplimiento.

Ampliaciones del trabajo

Si bien, en este trabajo se ha diseñado y elaborado una primera versión de estos instrumentos, en su mayoría en formato de documentos ofimáticos (planillas y pdf), estos servirán de base para la construcción de un sistema más práctico y adecuado para ser utilizado por una PYME.

Por ejemplo, se podría construir una sencilla plataforma web que cuente con varias secciones:

1. Una sección de auto-diagnóstico que contenga un formulario que pueda ser completado por el usuario, principalmente para conocer los activos que posee y los controles con los que ya cuenta, y que, de acuerdo a eso, le indique el nivel de riesgo al que está expuesta la PYME. Será algo similar a la herramienta de “Análisis de riesgos en 5 minutos” de INCIBE, pero con preguntas que tengan en mente el presente trabajo.
2. Una sección que, a partir del resultado de la sección de autodiagnóstico, genere los controles específicos que aplican a la PYME en cuestión, de acuerdo a los activos de información y otros datos que el usuario haya indicado.
3. Una o varias secciones que le indiquen al usuario las diversas maneras de implementar los controles que le han sido generados. Esta sección podría pedirle datos adicionales al usuario (por ejemplo, “¿hasta cuánto está dispuesto a invertir en la implementación?”) y, de acuerdo a esos datos, desplegarle las posibles opciones de implementación que se ajusten a esos datos. Lo ideal sería que esta sección, además, le brinde al usuario referencias a tutoriales o guías simples para cada opción de implementación. Estos tutoriales podrían ser parte de la plataforma, lo cual implicaría tener que mantenerlos, o podrían ser referencias externas a otros portales
4. Una sección que, de acuerdo a los controles que fueron seleccionados para la PYME en cuestión, generen un formulario de medición de cumplimiento. Podría generarse en formato de planilla electrónica que el usuario puede descargar, guardar y completar de manera *offline* durante todo el proceso de implementación, como mecanismo de auto-control. Otra opción sería que la plataforma genere un formulario en la propia web, que permita al usuario tildar o indicar los controles que va implementando. Sin embargo, como ese proceso de implementación no se hará

en un único día sino será un proceso relativamente largo y continuo, es necesario que el estado de dicho formulario quede almacenado en la plataforma, de modo a que el usuario pueda regresar a la misma y continuar completándolo, hasta haber implementado todos los controles. Esta opción entonces, requerirá que la plataforma permita la creación de cuentas de usuarios y cuente con un módulo de gestión de usuarios; los controles que aplican a la PYME del usuario y el estado del formulario de medición de cumplimiento se almacenarán en el contexto del usuario.

Este sistema podría ser implementado, por ejemplo, con Drools, un sistema de gestión de reglas de negocio (BRMS, *Business Rule Management System*) que utiliza un motor de reglas basado en inferencia de encadenamiento hacia adelante (*forward chaining*) y de encadenamiento hacia atrás (*backward chaining*) y que utiliza una implementación avanzada del algoritmo Rete. Se programarán las reglas de tal manera a que el sistema, formulando una mínima cantidad de preguntas simples pero exhaustivas al usuario, sea capaz de modelar las recomendaciones precisas para la PYME, no solo las recomendaciones genéricas, sino incluso posibles implementaciones acordes a las necesidades y posibilidades de la PYME.

A pesar de que esta guía de controles busca ser algo mucho más simple que un sistema de gestión de seguridad de la información ya que está orientada a PYMEs, no debe perderse de vista que la seguridad es un proceso y no un estado estático. Por ello, es importante que la plataforma recuerde al usuario de revisar el estado de cumplimiento de manera periódica, por ejemplo, una vez al año. Esto podría implementarse a través de notificaciones por correo electrónico al usuario, que le recuerden que ya ha pasado un año desde la última vez que indicó que cumplió con los controles y que debería volver a verificar que, efectivamente, los controles sigan funcionando como se espera.

Conclusiones

Con el presente trabajo se ha buscado brindar a las micro, pequeñas y medianas empresas (PYMEs) una manera de fortalecer su seguridad de una forma integral, efectiva y práctica, a través de una guía de controles de ciberseguridad, teniendo en cuenta que las PYMEs representan un sector fundamental de la economía, que se encuentran expuestos a ciberataques muy diversos y que, muchas veces, no cuentan con los recursos necesarios para protegerse adecuadamente.

Se ha podido comprobar que las PYMES tienen características y necesidades únicas, distintas a las de una empresa grande, no solo en cuanto a los recursos financieros, de personal y de conocimiento, sino también con respecto a los tipos de activo de información con los que cuentan, los procesos de negocio, la relación entre éstos y la tecnología, la criticidad de determinados activos, entre otros factores. Además, se pudo determinar que estas características varían de acuerdo a la región, al tipo de economía, a factores culturales y al nivel de madurez tecnológico, entre otros factores, siendo diferente, por ejemplo, en Paraguay con respecto a otros países

Para que una guía de seguridad sea útil a una PYME, la misma debe ser simple, práctica, adaptada a su realidad e implementable. Es por ello que se ha hecho énfasis en conocer primeramente esa realidad para luego formular controles y medidas de seguridad que mejores de forma real, integral y práctica la seguridad de la empresa. Esto nos permitió obtener un conjunto acotado y concreto de 20 controles primarios, 20 controles secundarios y 7 controles adicionales, fuertemente vinculados a activos de información determinados.

Además, se ha diseñado los instrumentos de base para un sistema o plataforma que, de manera integral, permita a una PYME realizar un diagnóstico de su situación, determinar los controles y medidas de seguridad que debe incorporar, conocer de manera concreta cómo puede implementar estos controles, realizar un seguimiento al proceso de implementación de dichos controles y, por último, repetir este proceso de manera periódica.

Índice de cuadros y tablas

Referencias bibliográficas

ABC. 2016. Edición España - Economía. *ABC.es.* [En línea] 30 de Mayo de 2016. [Citado el: 12 de Octubre de 2017.] http://www.abc.es/economia/abci-pymes-objetivo-mas-vulnerable-para-ciberdelincuentes-70000-ataques-2016-201605302128_noticia.html.

Agencia EFE. 2017. EFE. [En línea] 28 de Enero de 2017. [Citado el: 03 de Octubre de 2017.] https://www.efe.com/efe/espana/economia/los-incidentes-en-ciberseguridad-se-duplicaron-2016-y-sumaron-115-000/10003-3162398#.

Beliz, Gustavo y Chelala, Santiago. 2016. El ADN de la integración regional. *IADB.* [En línea] Octubre de 2016. [Citado el: 30 de Diciembre de 2016.] https://publications.iadb.org/bitstream/handle/11319/7896/El-ADN-de-la-integracion-regional-La-voz-de-los-latinoamericanos-por-una-convergencia-de-calidad-innovacion-equidad-y-cuidado-ambiental.pdf?sequence=4.

Center For Internet Security. CISecurity. [En línea] [Citado el: 09 de Octubre de 2017.] https://learn.cisecurity.org/first-five-controls-download.

Dirección General de Estadística, Encuestas y Censos (DGEEC). 2011. *Censo Económico Nacional Paraguay.* Dirección General de Estadística, Encuestas y Censos, Secretaría Técnica de Planificación. 2011. Censo Económico Nacional.

Eubanks, Russell. 2017. A Small Business No Budget Implementation of the SANS 20 Security Controls. *SANS.* [En línea] 10 de Agosto de 2017. [Citado el: 08 de Octubre de 2017.] https://www.sans.org/reading-room/whitepapers/hsoffice/small-business-budget-implementation-20-security-controls-33744.

Greenberg, Andy. 2017. Wired. *Wired.* [En línea] 20 de Setiembre de 2017. [Citado el: 07 de Octubre de 2017.] https://www.wired.com/story/ccleaner-malware-targeted-tech-firms/.

INCIBE. 2017. INCIBE. [En línea] 03 de Octubre de 2017. [Citado el: 08 de Octubre de 2017.] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf.

—. Protege tu empresa. *INCIBE.* [En línea] [Citado el: 07 de Octubre de 2017.] https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos.

Kaspersky Lab. 2016. Kaspersky. [En línea] 2016. [Citado el: 08 de Octubre de 2017.] https://go.kaspersky.com/rs/802-IJN-240/images/KasperskyLabReport_Financial_US.pdf.

Ley 4457/11. 2012. MiPymes MIC. [En línea] 16 de Mayo de 2012. [Citado el: 07 de Octubre de 2017.] http://mipymes.mic.gov.py/application/files/1214/5521/2798/Ley_4457_de_las_Micro_Pequenas_y_Medianas_Empresas.pdf.

Ministerio de Economía, Industria y Competitividad. Portal PYME. [En línea] [Citado el: 09 de Octubre de 2017.] http://www.ipyme.org/es-ES/UnionEuropea/UnionEuropea/PoliticaEuropea/Marco/Paginas/NuevaDefinicionPYME.aspx.

Ministerio de TICs (Colombia). 2016. MINTIC. [En línea] 06 de Noviembre de 2016. [Citado el: 08 de Octubre de 2017.] https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf.

National Small Business Association. 2015. 2015 Year-End Economic Report. *National Small Business Association (NSBA).* [En línea] Diciembre de 2015. [Citado el: 17 de Octubre de 2017.] http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.

Observatorio TICs. 2017. Encuesta sobre acceso y uso de Internet en Paraguay. *SENATICs.* [En línea] 25 de Agosto de 2017. [Citado el: 12 de Octubre de 2017.] http://gestordocumental.senatics.gov.py/share/s/ntjnuNLeT8u3gbAHC6WeVw.

ONTSI. 2017. Encuesta sobre Confianza Digital en las Empresas | ontsi.red.es. *Observatorio Nacional de las Telecomunicaciones y de la SI.* [En línea] Octubre de 2017. [Citado el: 09 de Noviembre de 2017.] http://www.ontsi.red.es/ontsi/sites/ontsi/files/Encuesta%20sobre%20confianza%20digital%20en%20las%20empresas%20%28octubre%202017%29.pdf.

SANS Institute. CIS Critical Security Controls: A Brief History. *SANS.* [En línea] [Citado el: 03 de Octubre de 2017.] https://www.sans.org/critical-security-controls/history.

Wikipedia. Drools. *Wikipedia.* [En línea] [Citado el: 28 de Diciembre de 2017.] https://es.wikipedia.org/wiki/Drools.

—. Small and medium sized enterprises. *Wikipedia.* [En línea] [Citado el: 09 de Octubre de 2017.] https://en.wikipedia.org/wiki/Small_and_medium-sized_enterprises.

ANEXO 1

Cuestionario encuesta de ciberseguridad a PYMEs

1. Indique la cantidad de empleados de la empresa: (Selección múltiple)

- 1 – 10
- 10 – 30
- 30 – 50
- Más de 50

2. Indique la facturación anual aproximada de la empresa: (Selección múltiple)

- 500.000.000 Gs. o menos
- 500.000.000 a 2.500.000.000
- 2.500.000.0000 a 6.000.000.0000
- Más de 6.000.000.000

Obs.: pregunta opcional

3. ¿Qué tipo de sistemas o tecnologías utiliza en su empresa? Marque todos los que apliquen: (Check list)

- Computadoras propias de la empresa
- Computadoras de los empleados
- Teléfonos o dispositivos móviles de la empresa y/o de los empleados
- Página Web
- Correo electrónico
- Redes sociales
- Sistemas o aplicaciones internos (sistema de stock, sistema contable, etc.)
- Servidores propios
- Servidor de archivos compartidos
- Wifi
- Red cableada
- Controlador de dominio (Active/Directory, LDAP, o similar)
- Servicios en la nube (Google Drive, Dropbox, OneDrive, etc.)
- Otro: _____

4. ¿Cuenta con personal dedicado a tareas de informática en su empresa? (Selección múltiple)

- Sí, más de 1 persona dedicada exclusivamente a estas tareas
- Sí, 1 persona dedicada exclusivamente a esta tarea
- Si, 1 persona dedicada parcialmente a esta tarea
- No, estas tareas están tercerizadas en otra persona o empresa
- No, nadie lo hace

5. ¿Su empresa ha sido víctima de un ciberataque o delito informático? (Selección múltiple)

- Si
- No
- No sé

Obs.: Si respondió “No”, ir a la pregunta 9

6. Si respondió “Si”, ¿qué tipo de incidente sufrió? (Check list)

- Robo o fuga de información
- Hackeo de página web
- Hackeo de redes sociales
- Hackeo de correo electrónico
- Pérdida de información por Infección con virus informático (Por ej. ransomware: encripta la información y pide un “rescate” para recuperarla)
- Pérdida de información por evento fortuito (daño de equipo, pérdida del equipo, etc.)
- Degradación y/o interrupción del servicio de Internet en la oficina (por ej., red lenta debido a virus)
- Denegación de servicio a página web o sistema (colapso de la misma debido a un exceso de tráfico de forma intencional)
- Manipulación de sistema informático interno
- Otro _____

7. ¿El incidente se debió a un atacante externo o interno de su empresa? (Selección múltiple)

- Externo
- Interno
- Interno y Externo
- No sé

8. ¿Qué tanto le afectó el incidente? (Selección múltiple)

- Poco - No hubo interrupción al negocio ni pérdidas significativas
- Moderado – Interrumpió el negocio durante poco tiempo y/o generó pérdidas moderadas, pero no fue un gran problema
- Mucho – Interrumpió el negocio durante un tiempo significativo y/o generó pérdidas importantes

9. ¿Qué tanto impacto económico le generarán los siguientes incidentes a su negocio? (Bajo, medio, alto) (Matriz de Selección múltiple)

- Robo o fuga de información
- Hackeo de página web
- Hackeo de redes sociales
- Hackeo de correo electrónico
- Pérdida de información
- Degradación y/o interrupción del servicio de Internet en la oficina
- Denegación de servicio a página web o sistema (colapso de la misma debido a un exceso de tráfico de forma intencional)
- Manipulación de sistema informático interno

10. Con respecto al daño generado por un incidente informático, ¿qué es lo que más le preocupa? (Selección múltiple)

- Daño a la imagen personal o de su empresa
- Pérdidas económicas directas (robo de dinero u otros activos)
- Pérdidas económicas indirectas (reparación del incidente)
- Indisponibilidad de sus servicios

11. ¿Qué tan probables cree que son las siguientes amenazas para Ud. o su empresa? (poco, moderado, mucho): (Matriz de Selección múltiple)

- Un empleado, ex-empleado o personal infiel
- Un hacker que aproveche la oportunidad de atacarlo, por diversión o para hacer daños a terceros
- Un atacante con intención específica de dañarlo a Ud. o a su negocio
- Una persona o empresa de la competencia que busque obtener ventaja sobre Ud. o su negocio

12. ¿Cuántas personas de su personal estaría dispuesto a destinar para aplicar medidas de seguridad de la información? (Selección múltiple)

- 0
- 1
- 2-3
- 3-5
- Más de 5

13. ¿Cuántas horas semanales estaría dispuesto a destinar a la aplicación y control de las medidas de seguridad de la información? (Selección múltiple)

- Hasta 1 hora
- 1 a 3 horas
- 3 a 5 horas
- 5 a 8 horas
- Más de 8 horas

14. Cuánto presupuesto anual estaría dispuesto a destinar en la adquisición y/o implementación de medidas de seguridad de la información? (Obs: contemplar también costos de tercerización de servicios, si es que se tiene pensado tercerizar tareas de seguridad) (Selección múltiple)

- Menos de 5millones Gs.
- Entre 5 a 10millones Gs.
- Entre 10 a 20millones Gs.
- Entre 20 a 50 millones Gs.
- Más de 50millones Gs.

Obs.: 1 Gs. (moneda paraguaya) = 0,00015 EUR

15. ¿Cuáles son las principales dificultades para implementar medidas de protección de la información en su empresa? Marque hasta 3 razones (Check list)

- Falta de presupuesto
- Falta de personal suficiente

- Falta de personal capacitado
- No conozco qué medidas de protección debemos implementar
- Las recomendaciones que me brindan son muy generales
- Nunca pensé en implementar protección
- Conozco las recomendaciones básicas, pero no sé cómo implementarlas
- No sé cómo controlar si tenemos protección suficiente y adecuada
- No considero que sea una cuestión importante para mi negocio
- No considero que las recomendaciones se adaptan a mi realidad
- Otro _____

La encuesta online fue elaborada utilizando Google Forms y está disponible en el siguiente enlace: https://goo.gl/forms/FZBYiOtCvRzaABbJ3

Duración total de la encuesta: 14 días

Cantidad de respuestas obtenidas: 148

ANEXO 2

Análisis de riesgo en PYMEs

Activo	Dimensión	Amenaza	Tipo	Posibles ataques	Probabilidad	Impacto	Criticidad	Control
Archivos almacenados en equipos de usuarios (computadoras o teléfonos)	Confidencialidad	Una persona desea obtener información sensible y/o de valor de la empresa, ya sea para aprovechar dicho conocimiento o para divulgarlo.	Externo	Implantación de un software malicioso que permita la filtración de archivos; vector de ataque ingeniería social Acceso físico al equipo que contiene los archivos	Baja; es muy poco probable que una PYME tenga un enemigo con los recursos e intención específica para exfiltrar información, cuyo valor es relativamente limitado	Alto; las PYMEs suelen almacenar toda la información del negocio en archivos, incluida información personal sensible de clientes	Media	Cifrado de archivos sensibles
			Interno	Acceso indebido a un equipo de la empresa al que no debería tener acceso. Copia no autorizada de archivos a los que tiene acceso	Media; podría haber pocas personas que tuvieran la intención de robar información de sus empresas, pero tendrán fácilmente la oportunidad y los recursos para hacerlo.	Alto; las PYMEs suelen almacenar toda la información del negocio en archivos, incluida información personal sensible de clientes	Alta	Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos. Cifrado de archivos sensibles. Distribución granular de permisos para accesos a archivos
	Disponibilidad / Integridad	Alguien borra o inutiliza un archivo	Externo o Interno	Una infección por ransomware. Acción no intencional de un empleado o persona interna. Falla de un componente físico (ej.: disco duro)	Alta; los ataques de ransomware son uno de los más frecuentes, son fáciles de llevar a cabo, los eventos fortuitos son frecuentes	Alto; las PYMEs suelen almacenar toda la información del negocio en archivos	Alta	Copia de seguridad de archivos
	Integridad	Una persona modifica el contenido de un archivo con el objetivo de boicotear a la empresa u obtener un beneficio personal	Externo	Implantación de un software malicioso que permita la manipulación de archivos; vector de ataque ingeniería social	Baja; es muy poco probable que una PYME tenga un enemigo con los recursos e intención específica para modificar información	Alto; dependiendo de la criticidad del proceso asociada al archivo, su modificación podría tener graves consecuencias (cambios en un historial médico, cambios en un archivo contable, etc.)	Media	Cifrado de archivos sensibles
			Interno	Manipulación de un archivo al que tiene acceso	Media; podría haber pocas personas que tuvieran la intención de robar información de sus empresas, pero tendrán fácilmente la oportunidad y los recursos para hacerlo.	Alto; dependiendo de la criticidad del proceso asociada al archivo, su modificación podría tener graves consecuencias (cambios en un historial médico, cambios en un archivo contable, etc.)	Alta	Separación de roles - Generación de información y verificación de la información sensible antes de su uso

Computadoras		Un software malicioso infecta al equipo y daña o manipula el sistema operativo	Externo o Interno	Infección con interacción humana (ingeniería social, programa falso o "crack") Infección mediante explotación de vulnerabilidades locales (drive-by download, gusano en la red) Infección mediante explotación de un servicio expuesto (RDP)	Alta; las infecciones con malware de todos los tipos son frecuentes y fáciles de realizar	Media; si bien, desde el punto de vista del equipo este puede ser recuperado, se interrumpen o degradan las operaciones normales	Alta	Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware, etc.) Firewall basado en Host Actualización de sistema operativo y programas Protección de servicios expuestos con contraseñas robustas Educación al usuario
		Un desperfecto físico o un evento fortuito daña el equipo	-	Daño del disco duro u otro componente importante Daño al arranque del sistema operativo	Media; hoy en día la estabilidad y durabilidad de los equipos es bastante alta, pero aun así se puede esperar que es algo que ocurrirá al menos una vez en un par de años	Baja; suponiendo que se cuente con copia de seguridad de la información, el impacto será solo una interrupción parcial hasta poder reemplazar el componente o equipo	Baja	Copia de seguridad continua de archivos
		Pérdida del equipo	-		Media; si bien, no es algo que ocurre frecuentemente, pero aun así se puede esperar que es algo que ocurrirá al menos una vez en un par de años	Baja; suponiendo que se cuente con copia de seguridad de la información, el impacto será solo una interrupción parcial hasta poder reemplazar el equipo, es poco probable que quien encuentre el equipo desee obtener la información	Baja	Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos. Copia de seguridad continua de archivos
		Robo del equipo	Externo		Media; si bien, no es algo que ocurre frecuentemente, pero aun así se puede esperar que es algo que ocurrirá al menos una vez en un par de años	Baja; suponiendo que se cuente con copia de seguridad de la información, el impacto normalmente será solo una interrupción parcial hasta poder reemplazar el equipo, normalmente el ladrón robaría el equipo por su valor comercial más que por su información	Baja	Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos. Copia de seguridad continua de archivos.
Teléfonos o dispositivos móviles		Un software malicioso infecta al equipo y daña o manipula el sistema operativo	Externo o Interno	Infección con interacción humana (ingeniería social, aplicación falsa) Infección mediante explotación de vulnerabilidades	Media; las infecciones con malware en teléfonos móviles son frecuentes, pero por lo general requieren una interacción humana, la infección sin interacción es poco frecuente.	Baja si bien, el malware en dispositivos móviles degrada el funcionamiento del mismo, esto suele tener un menor impacto en las operaciones de una empresa	Baja	Antivirus Actualización del firmware y aplicaciones Restricción de instalación de apps no oficiales
		Alguien implanta un software malicioso del tipo RAT (remote access tool) para obtener	Externo	Infección con interacción humana (ingeniería social, aplicación falsa)	Media; no es muy probable que la empresa tenga un enemigo con la intención de implantar un RAT en un dispositivo móvil, sin embargo, es relativamente fácil cuando hay interacción humana	Alta; suele haber mucha información sensible en los teléfonos, tanto personal como de la empresa, el control que se obtiene con un RAT es prácticamente total	Alta	Antivirus Restricción de instalación de apps no oficiales Educación al usuario

		información y/o realizar acciones específicas	Interno	Infección con interacción humana (ingeniería social, aplicación falsa) Acceso Físico al teléfono	Media; no es muy probable que la empresa tenga un enemigo con la intención de implantar un RAT en un dispositivo móvil, sin embargo, es relativamente fácil cuando hay interacción humana	Alta; suele haber mucha información sensible en los teléfonos, tanto personal como de la empresa, el control que se obtiene con un RAT es prácticamente total	Alta	Antivirus Contraseña de inicio de sesión y bloqueo de pantalla con contraseña Restricción de instalación de apps no oficiales
		Un desperfecto físico o un evento fortuito daña el equipos	-		Media; hoy en día la estabilidad y durabilidad de los equipos es bastante alta, pero aun así se puede esperar que es algo que ocurrirá al menos una vez en un par de años	Baja; suponiendo que se cuente con copia de seguridad de la información y los accesos a las cuentas vinculadas al teléfono, el impacto será solo una interrupción parcial hasta poder reemplazar el componente o equipo	Baja	Copia de seguridad continua de datos (aplicaciones, archivos, contactos)
		Pérdida del equipo	-		Media; si bien, no es algo que ocurre frecuentemente, pero aun así se puede esperar que es algo que ocurrirá al menos una vez en un par de años	Baja; suponiendo que se cuente con copia de seguridad de la información, el impacto será solo una interrupción parcial hasta poder reemplazar el equipo, es poco probable que quien encuentre el equipo tenga un interés grande en obtener la información	Baja	Copia de seguridad continua de datos (aplicaciones, archivos, contactos) Contraseña de desbloqueo de pantalla Borrado remoto de archivos
		Robo del equipo	Externo		Media; si bien, no es algo que ocurre frecuentemente, pero aun así se puede esperar que es algo que ocurrirá al menos una vez en un par de años	Baja; suponiendo que se cuente con copia de seguridad de la información, el impacto normalmente será solo una interrupción parcial hasta poder reemplazar el equipo, normalmente el ladrón robaría el equipo por su valor comercial más que por su información	Baja	Copia de seguridad continua de datos (aplicaciones, archivos, contactos) Contraseña de desbloqueo de pantalla Borrado remoto de archivos
Correo Electrónico	Confidencialidad / Integridad	Una persona malintencionada accede a la cuenta de correo para leer los mensajes o enviar mensajes en nombre del dueño de la cuenta	Externo	Ingeniería social (phishing) Keylogger implantado en la empresa o un lugar visitado por el dueño de la cuenta Contraseña fácil, fuerza bruta Explotación de vulnerabilidad en software de correo	Media; si bien, no todas las PYMEs tendrán un enemigo con la intención específica de acceder a un correo electrónico de la empresa para obtener información o para suplantar a alguien de la empresa, es un ataque muy fácil de llevar a cabo.	Alto; las PYMEs utilizan frecuentemente el correo electrónico e intercambian todo tipo de información a través de este medio (información interna, información de cliente, contratos, etc.), además lo utilizan muchas veces como libro de registro.	Alta	Contraseña segura Autenticación de doble factor Educación del usuario Actualización del software de correo (si es propio)

	Integridad / Disponibilidad	Una persona accede a la cuente de correo para desde ella enviar spam	Externo	Ingeniería social (phishing) Contraseña fácil, fuerza bruta Malware genérico de robo de credenciales	Alta; estos ataques son muy utilizados y son fáciles de realizar	Media; se interrumpen o degradan las comunicaciones normales poque la IP suele entran en lista negra de spam	Alta	Contraseña segura Autenticación de doble factor Educación del usuario Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware, etc.) Configuración segura del servidor de correo, restricción de puerto 25 (si es propio)
	Disponibilidad	Un usuario olvida la contraseña de su cuenta	Interno		Media; cuando se usan contraseñas medianamente complejas, las personas las olvidan frecuentemente	Media; suele haber una interrupción temporal en las comunicaciones, hasta tanto se logre recuperar el acceso - en caso de contraseña de administrador el impacto es mayor	Media	Utilización de gestor de contraseña Configuración de información de recuperación
Redes Sociales	Confidencialidad / Integridad	Una persona malintencionada accede a la cuenta de redes sociales para leer los mensajes o publicar mensajes en nombre de la compañía	Externo	Ingeniería social (phishing) Keylogger implantado en la empresa o un lugar visitado por el administrador de la cuenta Contraseña fácil, fuerza bruta Explotación de vulnerabilidad en la plataforma de la red social	Baja; es muy poco probable que una PYME tenga un enemigo con la intención específica de acceder a una cuenta o perfil de la empresa para obtener información o para suplantar a la empresa	Medio; suelen usar las redes sociales como mecanismo de comunicación con sus clientes o potenciales clientes, por lo que es importante para la imagen, pero no suelen intercambiar información muy sensible a través de este medio.	Baja	Contraseña segura Autenticación de doble factor Educación del usuario
	Disponibilidad	Una persona accede a la cuenta sin intención específica contra la empresa, pero para valerse de la cuenta para realizar actividades criminales	Externo	Ingeniería social (phishing) Contraseña fácil, fuerza bruta Explotación de vulnerabilidad en la plataforma de la red social	Media; cada vez es más frecuente que cibercriminales genéricos comprometan cuentas de redes sociales desprotegidas para, a través de ellas, hacer daños a terceros	Media; se interrumpen o degradan las comunicaciones normales, a veces se pierde el acceso a la red social	Media	Contraseña segura Autenticación de doble factor Educación del usuario Configuración segura y completa de la información de recuperación
		Una persona con intención específica contra la empresa accede a la cuenta y modifica la información de recuperación de modo a que la empresa pierde el control sobre la misma	Externa o interna	Ingeniería social (phishing) Contraseña fácil, fuerza bruta Keylogger implantado en la empresa o un lugar visitado por el administrador de la cuenta	Media; si bien, no todas las PYME tendrán un enemigo con la intención de boicotearla, es un ataque relativamente fácil de hacer y de alto impacto.	Alta; se interrumpen o degradan las comunicaciones normales poque se pierde el acceso a la red social, cuando hay una intención específica de sabotearla, el atacante cambia la información de recuperación de modo a que sea prácticamente imposible la recuperación	Alta	Contraseña segura Autenticación de doble factor Educación del usuario Configuración segura y completa de la información de recuperación

		El administrador de la cuenta olvida la contraseña de su cuenta	Interno		Media; cuando se usan contraseñas medianamente complejas, las personas las olvidan frecuentemente	Media; suele haber una interrupción temporal de las operaciones en la red social, hasta tanto se logre recuperar el acceso	Media	Utilización de gestor de contraseña Configuración de información de recuperación
		El administrador de la red social deja la empresa y/o pierde el acceso a la cuenta	Interna		Media; es frecuente que un empleado se retire y/o que pierda el acceso a su cuenta, con lo que se habrá perdido el acceso a la red social oficial	Media; se interrumpen o degradan las comunicaciones normales, a veces se pierde el acceso a la red social	Media	Procedimiento de baja de usuario - transferencia de responsabilidades y accesos Configuración de mecanismos de recuperación
Red Wifi	Disponibilidad	Una persona físicamente cercana utiliza el Wifi sin estar autorizada	Externa	Acceso desprotegido, sin contraseña o con protocolo débil Contraseña fácil, fuerza bruta	Media; muchas personas buscan puntos de Wifi poco protegidos en las cercanías	Media; normalmente el ancho de banda contratado es relativamente limitado, por lo que una o más personas utilizando el Wifi para ver streaming online, descargar archivos grandes, etc. puede afectar negativamente el rendimiento de la red	Media	Contraseña segura del Wifi Configuración segura del Wifi - protocolos seguros
		Una persona manipula la configuración del Wifi, ya sea para utilizarlo o boicotearlo	Externa	Ingeniería social + Explotación de vulnerabilidades del firmware del AP Expotación de servicios expuestos	Baja; los casos drigidos son poco frecuentes y los casos no dirigidos no suelen ser tan sofisticados	Media; el ancho de banda contratado y las capacidades del equipo AP suelen ser limitados, por lo que un uso indebido del mismo tiene un impacto medio	Baja	Contraseña segura del AP Configuración segura del Wifi - restricción de servicios expuestos
			Interna		Media; si bien, los casos no son tan frecuentes, son muy fáciles de realizar	Media; el ancho de banda contratado y las capacidades del equipo AP suelen ser limitados, por lo que un uso indebido del mismo tiene un impacto medio	Media	Contraseña segura del AP
	Confidencialidad	Una persona manipula la red para visualizar el tráfico interno	Externa	Ataque Man-in-the-Middle	Baja; el atacante debe tener acceso físico a la red (ataque de capa 2 o mediante pivoting), es muy poco probable que alguien externo tenga el interés, oportunidad y recursos para realizarlo	Medio; la gran mayoría de las páginas y sistemas utilizan HTTPs y canales seguros para autenticarse, los sistemas internos, si no estuvieran sobre HTTPs podrían suponer un cierto riesgo	Baja	Utilización de HTTPs para envío de credenciales
			Interna	Ataque Man-in-the-Middle	Media el atacante debe tener acceso físico a la red (ataque de capa 2 o mediante pivoting), alguien interno ya tiene este acceso, pero no necesaiamente tendrá el interés y el conocimiento para realizarlo	Medio; la gran mayoría de las páginas y sistemas utilizan HTTPs y canales seguros para autenticarse, los sistemas internos, si no estuvieran sobre HTTPs podrían suponer un cierto riesgo	Media	Utilización de HTTPs para envío de credenciales

Página web	Integridad / Disponibilidad	Alguien desfigura el sitio web	Externo	Explotación de vulnerabilidad de la aplicación Acceso indebido al panel de administración de la web Acceso indebido al servidor (Filemanager, FTP, ..)	Media; si bien, los atacantes genéricos no suelen tener una preferencia específica hacia una PYMEs, son ataques frecuentes y fáciles de realizar	Media; la encuesta mostró que la página web no suele ser un activo fundamental para el negocio, pero aun así genera un problema de imagen e interrupción de la presencia web	Media	Actualización de CMS, plugins, plantillas. En caso de desarrollo propio, considerar auditoría de vulnerabilidades o migrar a un CMS con soporte Contraseña segura para usuarios del CMS Firewall de aplicación web (WAF) Contraseña segura para accesos del hosting (filemanager, FTP, SSH, ..) Copia de seguridad del sitio web
		Alguien utiliza el servidor web para alojar contenido malicioso (sitio de phishing, scripts maliciosos, exploit kits, malware, ..)	Externo	Explotación de vulnerabilidad de la aplicación Acceso indebido al panel de administración de la web Acceso indebido al servidor (Filemanager, FTP, ..)	Alta; los cibercriminales atacan frecuentemente sitios web para esconder contenido malicioso en el	Medio; como se trata de ataques silenciosos e invisibles, no tienen un impacto directo sobre el negocio, el daño es a terceros que visitan el sitio infectado, aunque en el caso de exploit kits, esto podría afectar directamente a cliente y/o empleados de la PYME	Alta	Actualización de CMS, plugins, plantillas. En caso de desarrollo propio, considerar auditoría de vulnerabilidades o migrar a un CMS con soporte Contraseña segura para los usuarios del CMS Firewall de aplicación web (WAF) Contraseña segura para accesos del hosting (filemanager, FTP, SSH, ..) Copia de seguridad del sitio web
	Disponibilidad	El webmaster olvida las credenciales del panel de administración, cpanel u otro mecanismo de administración de la web	Interno		Media; cuando se usan contraseñas medianamente complejas, las personas las olvidan frecuentemente	Baja; se imposibilita temporalmente la gestión del sitio web, sin embargo, éste seguirá visible y operativo.	Baja	Utilización de gestor de contraseña Configuración de información de recuperación
	Confidencialidad	Explotando una vulnerabilidad de la página o del servidor, se accede a bases de datos o archivos confidenciales	Externo	Explotación de vulnerabilidad de la aplicación Acceso indebido al panel de administración de la web Acceso indebido al servidor (Filemanager, FTP, ..)	Media; si bien, los atacantes genéricos no suelen tener una preferencia específica hacia una PYMEs, son ataques frecuentes y fáciles de realizar	Medio a alto; el impacto dependerá de si el hosting se usa para alojar bases de datos o archivos sensibles, además de los datos de los usuarios del portal (el del webmaster, generalmente).	Media	Actualización de CMS, plugins, plantillas. En caso de desarrollo propio, considerar auditoría de vulnerabilidades o migrar a un CMS con soporte Contraseña segura para usuarios del CMS Firewall de aplicación web (WAF) Contraseña segura para accesos del hosting (filemanager, FTP, SSH, ..) Copia de seguridad del sitio web Separación de bases de datos y/o archivos sensible del contenedor público

Servicios en la nube	Confidencialidad / Integridad	Una persona malintencionada accede a la cuenta para ver los archivos y/o manipularlos	Externo	Ingeniería social (phishing) Keylogger implantado en la empresa o un lugar visitado por el administrador de la cuenta Contraseña fácil, fuerza bruta Explotación de vulnerabilidad en software del servicio de la nube	Media; si bien no toda PYME tendrá un enemigo con la intención específica de acceder a sus archivos, es un ataque muy fácil de llevar a cabo.	Alto; las PYMEs almacenan todo tipo de información en los servicios de la nube (información interna, información de cliente, contratos, etc.)	Alta	Contraseña segura Autenticación de doble factor Educación del usuario
	Integridad / Disponibilidad	Una persona accede a la cuente para almacenar en ella recursos maliciosos	Externo	Ingeniería social (phishing) Contraseña fácil, fuerza bruta Malware genérico de robo de credenciales	Baja; si bien, es un ataque muy fácil de hacer, un cibercriminal tiene múltiples maneras de alojar y distribuir recursos maliciosos, los servicios en la nube no son tan utilizados para ello	Bajo; por lo general el proveedor del servicio notificará y/o suspenderá temporalmente a la cuenta comprometida, pero el daño se revierte casi inmediatamente	Baja	Contraseña segura Autenticación de doble factor Educación del usuario
	Disponibilidad	El administrador de la cuenta de la nube olvida la contraseña	Interno		Media; cuando se usan contraseñas medianamente complejas, las personas las olvidan frecuentemente	Media; suele haber una interrupción temporal en el servicio, hasta tanto se logre recuperar el acceso	Media	Utilización de gestor de contraseña Configuración de información de recuperación
Sistemas o aplicaciones internas	Integridad / Confidencialidad	Una persona con intención específica de acceder a información del sistema y/o manipularla	Externo	Implantación de un software malicioso que permita el control remoto de equipos de la red local y/o permita explotar vulnerabilidades de la aplicación desde la red interna; vector de ataque ingeniería social Acceso físico al equipo que contiene el sistema	Baja; es muy poco probable que una PYME tenga un enemigo con los recursos e intención específica para manipular sistemas internos	Alto; las PYMEs que poseen sistemas internos suelen basar sus operaciones enteramente en la información de estos sistemas, que no suelen ser redundantes ni suelen auditarse	Media	Control de acceso a los sistemas con contraseñas robustas Auditoría de vulnerabilidades de los sistemas internos Actualización del software y demás componentes de los sistemas internos Soluciones de seguridad de endpoint en equipos que interactúan y/o alojan los sistemas internos (antivirus, antimalware, ..) Firewall basado en host en equipos que interactúan y/o alojan la aplicación interna
			Interna	Usuario con acceso legítimo abusa de sus privilegios y accede o modifica información	Media; podría haber pocas personas que tuvieran la intención de robar y/o manipular intencionalmente información de sus empresas, pero tendrán fácilmente la oportunidad y los recursos para hacerlo.	Alto; las PYMEs que poseen sistemas internos suelen basar sus operaciones enteramente en la información de estos sistemas, que no suelen ser redundantes ni suelen auditarse	Alta	Control de acceso a los sistemas con contraseñas robustas y diferentes para cada usuario. Control granular e los permisos concedidos a cada usuario

	Disponibilidad	Corrupción de los datos del sistema por evento fortuito	-		Media; los fallos debido a incidentes físicos (por ej. daño de disco), lógicos o errores humanos (sobrescritura de un archivo de configuración) pueden ocurrir con relativa frecuencia.	Alto; las PYMEs que poseen sistemas internos suelen basar sus operaciones enteramente en la información de estos sistemas	Alta	Copia de seguridad de los datos del sistema interno (base de datos y/o sistema de archivos)
Servidores propios	Integridad / Confidencialidad	Un software malicioso infecta al equipo y daña o manipula el sistema operativo del servidor	Externo o Interno	Infección mediante explotación de vulnerabilidades locales (gusano en la red) Infección mediante explotación de un servicio expuesto (RDP, SSH, servidor web, FTP, correo)	Alta; los ataques mediante explotación de vulnerabilidades a servidores expuestos a Internet son muy frecuentes y fáciles de realizar	Media; si bien, desde el punto de vista del equipo este puede ser recuperado, se interrumpen o degradan las operaciones normales	Alta	Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware, etc.) Firewall basado en Host y/o en red IDS/IPS basado en Host y/o en red Actualización de sistema operativo y programas Protección de servicios expuestos con contraseñas robustas Hardening de sistema operativo y de servicios expuestos
	Disponibilidad	Un desperfecto físico o un evento fortuito daña el servidor	-	Daño del disco duro u otro componente importante Daño al arranque del sistema operativo	Media; hoy en día la estabilidad y durabilidad de los equipos es bastante alta, pero aun así se puede esperar que es algo que ocurrirá al menos una vez en un par de años	Media; suponiendo que se cuente con copia de seguridad de la información, el impacto será una interrupción de los servicios del servidor hasta poder reemplazarlo.	Media	Copia de seguridad continua del sistema operativo (imágenes o screenshots de S.O.) Redundancia lógica del servidor

Anexo 3

Ejemplo de implementación de la guía de controles para PYMEs

Para la implementación se ha considerado un escenario de redes planas (no segmentadas), conectadas a uno o más puntos de conectividad Wifi, en una red corporativa (*work group*, con compartición de archivos), pero sin existencia de un dominio, lo cual es el escenario en la gran mayoría de las micro, pequeñas y medianas empresas.

Para realizar las pruebas de implementación de los activos básicos, se utilizaron dos máquinas virtuales Windows 7 con 2GB de RAM con una instalación por defecto o común y con programas comunes (navegador, suite de ofimática, lector de pdf, etc.), conectadas a una red Wifi estándar con un AP TP-Link de gama baja, en modo de Work Group. Como dispositivo móvil se utilizaron teléfonos Android (versión 6.x) y iPhone (versión 7.x). Los archivos en los que se ha centrado los controles son documentos de texto, planillas electrónicas, presentaciones, archivos pdf e imágenes. Como cuentas de correo, se utilizaron cuentas personales de Gmail y Outlook, y la suite corporativa Zoho, servicio que hoy en día ofrece hasta 25 usuarios corporativos gratuitos + 25 usuarios de bono, con dominio propio. Se utilizó también la suite corporativa de Microsoft, OneDrive for Business en su versión de prueba; de amplio uso en empresas; sin embargo, la misma no es gratuita. Se utilizó las redes sociales más comunes para PYMEs, Facebook, Twitter e Instagram. Para la página web se utilizó una web en Wordpress, el CMS más utilizado, en un web hosting compartido en un servidor externo con CPanel. Como servicios en la nube se implementó controles para Google Docs, Dropbox y OneDrive, los servicios más utilizados, sobre todo en PYMEs. Como servidores propios, se ha centrado en implementaciones para servidores Linux (CentOS, Debian) y servidores Windows Server 2012, con servicios de web (Apache, XAMPP y IIS), correo (*sendmail*, *postfix*) y SAMBA.

Para los sistemas internos, teniendo en cuenta la amplia variedad de sistemas o tecnologías que puede utilizar una PYME, y teniendo en cuenta que solo un grupo reducido cuenta con sistemas internos, se plantearon diversas recomendaciones generales y se estimaron los recursos aproximados (tiempo, recursos humanos y costo) que podrían requerir su implementación.

Para la estimación de recursos necesarios para la implementación de los posibles controles se tuvo en cuenta el tiempo de instalación de cualquier software o componente adicional que no está incluido por defecto, el tiempo de lectura de tutoriales o guías específicas que fueran necesarias para la implementación (no se incluyó el tiempo de lectura de material adicional o de soporte), el tiempo de configuración de la herramienta, software o componente necesario para el control, los conocimientos específicos que fueran necesarios para su implementación (se asumió un nivel de conocimiento de operador básico-intermedio). Tampoco se tuvo en cuenta el tiempo de montaje y preparación del laboratorio ni la creación de cuentas, ya que se asume que una PYME que implemente esta guía ya cuenta con los activos mencionados, instalados y configurados de manera básica y funcional. Todas las implementaciones se han realizado de manera secuencial y por una única persona.

Archivos (en computadoras, teléfonos, dispositivos móviles, etc.)

1. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos:

La implementación de este control fue planteada como un control de equipos (computadoras, teléfonos y dispositivos móviles).

2. Cifrado de archivos sensibles:

Cifrado de archivos en computadoras:

Opción 1:

Haciendo una prueba de implementación de VeraCrypt, el tiempo de implementación aproximado es de 30 minutos por equipo. Si bien, la instalación y configuración es sencilla y no requiere conocimientos avanzados, su uso no es simple para un operador básico, ya que cada vez que se desee visualizar un archivo de la partición encriptada, se debe abrir Veracrypt, montar la partición virtual, introducir la contraseña y hacer doble click sobre la partición. Recién allí se abrirá una ventana de exploración de archivos que permitirá acceder al contenido. Fuera de esa ventana no se podrá visualizar los archivos.

Tipo de control: Herramienta a nivel de equipo

Herramientas: Software Veracrypt

Tiempo estimado: 30 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: nivel intermedio

Costo: ninguno

Opción 2:

El cifrado a nivel de archivos se puede realizar con la función de Password Protection de Microsoft Office para los documentos de texto, planillas electrónicas y presentaciones. No puede utilizarse para archivos de otro formato; en estos casos tendrá que utilizarse alguna utilidad adicional, como por ejemplo 7zip para crear un archivo comprimido (.rar, .zip o similar) con contraseña. 7zip no viene instalado con Windows, por lo que debe instalarse adicionalmente. Se integra al menú contextual del explorador de archivos de Windows, sin embargo, para el establecimiento de la contraseña se debe entrar a la opción de compresión personalizada.

Tipo de control: Herramienta a nivel de equipo

Herramientas: 7zip

Tiempo estimado: 2 a 3 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 3:

AxCrypt es un programa de código abierto y gratuito que permite el cifrado a nivel de archivos, de manera simple e integrada al menú contextual del explorador de archivos de Windows (también disponible para iOS). El usuario simplemente debe hacer click derecho sobre el archivo que quiere cifrar y elegir la opción de cifrar. Se puede cifrar carpetas enteras. Posee un gestor de contraseñas integrado (opcional), de manera a que el usuario no necesite ingresar la contraseña cada vez que quiere abrir el archivo.

Tipo de control: Herramienta a nivel de equipo

Herramientas: AxCrypt

Tiempo estimado: 2 a 3 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Cifrado de archivos en Teléfonos o dispositivos móviles:

Los teléfonos Android y iOS ya traen una funcionalidad de cifrado de archivos a nivel de disco (*full-disk encryption*). En algunos modelos, viene activo por defecto; se utiliza el PIN, patrón o huella de desbloqueo para el cifrado y descifrado. Existen múltiples aplicaciones de cifrado a nivel de archivos, que son adecuadas para el uso personal o en PYMEs.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 2 minutos por equipo

Personal necesario: cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

3. Distribución granular de permisos para accesos a archivos:

Este tipo de controles se deben implementar a nivel de procedimiento, principalmente. Primeramente, la organización debe realizar un inventario de activos de información, en la que, como mínimo, se debe recoger la siguiente información:

- ¿Qué tipo de datos o información poseemos en la empresa?
- De estos datos, ¿cuáles son sensibles?
- ¿Dónde están almacenados esos datos, en qué archivos, en qué máquinas, en qué cuentas?
- ¿Quiénes tienen acceso a esos datos actualmente?
- ¿Quiénes necesitan esos datos para realizar sus tareas?

Luego de haber respondido dichas preguntas, la empresa, es decir, alguna persona con autoridad, ya sea el dueño, directivo, gerente o a quien haya sido delegada la responsabilidad de llevar a cabo el proyecto de seguridad, debe tomar las decisiones necesarias para definir los niveles de permiso de acuerdo a cada empleado o grupo de empleados. Entre los instrumentos de la presente guía, se ha elaborado un formulario para este inventario de información. La estimación inicial del tiempo requerido para la implementación de este control (responder a las preguntas y definir los niveles de permisos de acuerdo a las tareas) es de aproximadamente 4 a 30 horas, dependiendo de si los empleados de la empresa sepan, con relativa certeza, qué datos tienen y donde se encuentra, en cuyo caso 4 horas serán suficientes para completar el formulario, replantear los niveles de permisos y asegurar que los datos que se encuentren en manos no autorizadas se retiren. En caso de que el grado de certeza sea bajo, al menos un empleado tendrá que realizar una revisión manual, más o menos exhaustiva, de los archivos de cada equipo, en

coordinación de los demás empleados, se puede estimar un tiempo aproximado de 15 a 30 minutos por equipo de empleado (una computadora y, en algunos casos, un dispositivo móvil). En el peor de los casos, en una empresa mediana con 50 empleados esto puede tomar 25 horas, a lo que hay que sumar el tiempo de consolidación de la información verificada (1 hora) y el tiempo de completar el formulario, replantear los permisos y realizar los ajustes (4 horas).

Tipo de control: Procedimiento de la organización

Herramientas: Formulario de inventario de información

Tiempo estimado: 4 a 30 horas

Personal necesario: 1 persona completa y apoyo de un directivo o autoridad de la empresa, como mínimo; adicionalmente, apoyo de los demás empleados.

Conocimiento técnico: ninguno

Costo: ninguno

4. Copia de seguridad continua de archivos:

Opción 1:

Se implementará la sincronización de archivos con OneDrive for Business. Se trata de un servicio corporativo que ofrece, entre otras cosas, la sincronización de archivos en la nube de OneDrive de Microsoft, mediante una cuenta corporativa. En caso de que la empresa ya cuente con una suscripción, desde la más básica, el servicio ya está incluido, con un almacenamiento de 1TB, solo debe instalarse el software cliente en las máquinas que se deseen sincronizar. En caso de que la empresa no posea una suscripción y no desee pagar suscripciones, cualquier empleado que posea una cuenta de Microsoft o Outlook puede usar la versión personal de OneDrive (5GB de almacenamiento). En este caso, se ha considerado que ya se posee la suscripción y que la misma se encuentra configurada y con los usuarios de la empresa creados.

Tipo de control: Funcionalidad incluida en servicio - suscripción

Herramientas: software para OneDrive for Business

Tiempo estimado: 5 a 10 minutos por equipo (adquisición y configuración del servicio OneDrive for Business 30 minutos a 1 hora)

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno – Obs.: incluido con la suscripción básica de OneDrive for Business, 5 dólares al mes por usuario; alternativa gratuita: OneDrive Personal, incluido con el servicio gratuito de cuenta personal de Microsoft o de Outlook.

Opción 2:

Se implementará la sincronización de archivos con Zoho Docs. Se trata de un servicio corporativo que ofrece, entre otras cosas, la sincronización de archivos en la nube de Zoho, mediante una cuenta corporativa. Posee un plan gratuito para 25 usuarios (ampliable hasta 50 a través del programa de

Referrers), con un almacenamiento de 5GB por usuario, solo debe instalarse el software cliente en las máquinas que se deseen sincronizar.

Tipo de control: Funcionalidad incluida en servicio - suscripción

Herramientas: software cliente para Zoho Docs

Tiempo estimado: 5 a 10 minutos por equipo (adquisición y/o configuración del servicio Zoho 30 minutos a 1 hora)

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno hasta 25 usuarios (ampliable a 50 mediante Referrers)

Computadoras:

1. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos:

Opción 1:

El establecimiento de contraseña de inicio de sesión y pantalla de bloqueo con contraseña en Windows con forzado de cumplimiento de política a través de la edición manual de Local Security Policy permitirá que la empresa se asegure que los empleados están cumpliendo con la política de contraseña para el acceso al equipo.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 15 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala y configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 2:

El establecimiento de contraseña de inicio de sesión y pantalla de bloqueo con contraseña en Windows con forzado de cumplimiento de política a través de la importación de un *template* securizado con la herramienta LGPO y Security Compliance Manager (SCM) permitirá que la empresa se asegure que los empleados están cumpliendo con la política de contraseña para el acceso al equipo. Tiene la ventaja que no se necesita modificar la política de manera manual en cada equipo, sino se puede simplemente editarla de acuerdo a las necesidades en un equipo (por defecto, el *template* ya está securizado para cumplir con los requerimientos comunes) y luego puede importarse en las demás máquinas con la herramienta LGPO. Podría generar problemas si el *template* restringe alguna funcionalidad que la empresa necesita, en cuyo caso el *template* debe ser modificado previamente, lo cual requiere un nivel de conocimiento intermedio/avanzado. La ventaja es que el *template* ofrece no solo hardening de políticas de contraseña sino muchas otras configuraciones seguras, que se aplicarán en pocos minutos.

Tipo de control: Herramienta a nivel de equipo

Herramientas: LGPO y Security Compliance Manager (SCM)

Tiempo estimado: 30 minutos a 1 hora para la personalización del *template* (opcional) y 2 a 3 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos

Conocimiento técnico: intermedio

Costo: ninguno

En ambas opciones se requiere que, luego de aplicar la política, los usuarios existentes cambien sus contraseñas, ya que las políticas se aplican a contraseñas nuevas, no a los existentes.

2. Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware, etc.)

Opción 1:

Se ha probado la implementación de este control con el antivirus de Kaspersky, en su versión gratuita. La misma ofrece análisis de archivos, páginas web, contenido de correo y mensajería, detección y eliminación (básica) de malware, servicio de VPN para navegación (limitado). No requiere ninguna configuración adicional, la instalación por defecto es adecuada para la mayoría de los escenarios, especialmente en PYMEs.

Tipo de control: Herramienta a nivel de equipo

Herramientas: antivirus Kaspersky Free

Tiempo estimado: 30 a 45 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 2:

Se ha probado la implementación de este control con el antivirus Avast, también con la versión gratuita. Adicionalmente, ofrece la funcionalidad de notificación de actualizaciones faltantes, integrada al antivirus, gestor de contraseñas, navegación a través de VPN, entre otras.

Tipo de control: Herramienta a nivel de equipo

Herramientas: antivirus AVAST

Tiempo estimado: 20 a 30 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 3:

Si bien, la herramienta Windows Defender ha mejorado enormemente a partir de Windows 10, que ya la incluye por defecto, la misma no está disponible para Windows 7. Si la empresa tuviera un equipo Windows 10, podría utilizarla, activando simplemente la función desde el panel de control.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos por equipo

Personal necesario: 1 persona para la activación en todos los equipos o cada empleado lo activa individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 4:

Alternativamente, se podría optar por alguna solución corporativa. La mayoría de las empresas de antivirus ofrecen versiones para PYMEs, con precios accesibles, funcionalidades adicionales a las gratuitas, entre ellas la más importante, acceso a una consola de administración central. Para una PYMEs, suele ser más adecuada la consola de administración central basada en Cloud, de lo contrario se requerirá un servidor dedicado, integración a controlador de dominio u otros mecanismos poco usuales en PYMEs. Los precios varían de acuerdo al software; los más económicos rondan de 20 a 40 USD, dependiendo de la cantidad de equipos y tiempo de licencia a adquirir. Para probar la implementación de esta opción se optó por AVAST Business Managed Antivirus (versión de prueba), una de las soluciones de mejor relación costo-beneficio, así como también simplicidad en su uso.

Tipo de control: Herramienta a nivel de equipo + servicio Cloud

Herramientas: antivirus AVAST Business Managed Antivirus

Tiempo estimado: 1 a 2 horas para la configuración de la consola central + 15 a 25 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o 1 persona para la configuración de la consola central y cada empleado instala individualmente el software antivirus.

Conocimiento técnico intermedio

Costo: planes anuales (1, 2 o 3 años), 20 a 40 USD por equipo por año; precio unitario inversamente proporcional a la cantidad de equipos y tiempo de licencia.

3. Firewall basado en Host

Opción 1:

Este control puede ser implementado activando el firewall de Windows. La configuración por defecto es adecuada. Normalmente, ya viene activado por defecto, por lo que, si el empleado no lo desactivó explícitamente, no debería ser necesaria ninguna acción adicional.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 2:

Este control puede ser implementado a través de la funcionalidad de firewall ofrecida por varios antivirus, como, por ejemplo, Baidu o FortiClient. Anteriormente, otros antivirus gratuitos como Avast ofrecían dicha funcionalidad, pero la tendencia es no incluirlo.

Tipo de control: Herramienta de nivel de equipo

Herramientas: antivirus (por ejemplo, FortiClient u otro que incluya firewall)

Tiempo estimado: 1 a 2 minutos por equipo (se considera que la herramienta de antivirus ya se encuentra instalada y configurada)

Personal necesario: 1 persona para la activación en todos los equipos o cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

4. Actualización de sistema operativo y programas:

Opción 1:

La gran mayoría de sistemas operativos, entre ellos Windows, iOS y Linux permiten la actualización automática. En el caso de Windows, se cuenta con la funcionalidad de Windows Update, que permite actualizar el sistema operativo y los programas de Microsoft en segundo plano, de manera automática, sin que el usuario deba realizar nada. Sin embargo, esta herramienta no permite la actualización de aplicaciones que no sean de Microsoft (navegadores, lector pdf, reproductores de audio, algunos plugins, etc.). En el caso de iOS y Linux, también cuentan con utilidades de actualización automática, que permiten actualizar el sistema operativo y cualquier software descargado de repositorios oficiales. Cualquier aplicación descargada e instalada desde una fuente distinta a los repositorios oficiales deberá actualizarse a través de otros mecanismos.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos por equipo

Personal necesario: 1 persona para la configuración en todos los equipos o cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 2:

Muchas aplicaciones incluyen la funcionalidad de verificación de versión y actualización automática en la propia aplicación, sin embargo, esto tiene la desventaja que la comprobación se hará únicamente cuando el programa se estuviera ejecutando. Sin embargo, si se hubiera publicado un parche de seguridad desde la última vez que se ejecutó el programa, un atacante intermedio a avanzado podría explotar la vulnerabilidad, antes de que el programa tenga la oportunidad de notificar y/o actualizar la versión. Sin embargo, este escenario dependerá, en gran manera, de la ventana de tiempo que tenga el atacante. Si se trata de una vulnerabilidad relativamente nueva de un programa que el usuario no utiliza frecuentemente, es posible que el usuario no haya ejecutado, y, por tanto, no se haya actualizado el programa. Sin embargo, este tipo de ataques son menos probables en PYMEs, donde es poco probable que el atacante busque explotar una vulnerabilidad de pocos días, por lo que la verificación de versión y actualización automática incluida como funcionalidad en muchos programas podría ser suficiente para la mayoría de las empresas pequeñas y medianas. Otra desventaja es que la configuración debería realizarse programa por programa, aunque la mayoría la trae activa por defecto. Otras aplicaciones no ofrecen dicha funcionalidad, por lo que el usuario o administrador debe realizar una comprobación individual, programa por programa. Por tanto, no se considera una solución sostenible en el tiempo.

Opción 3:

Existen herramientas de gestión de actualizaciones que realizan un análisis de qué aplicaciones están instaladas en el equipo, verifican si existe una versión posterior y, en caso de comprobar que se encuentra desactualizado, notifica al usuario o administrador. Algunas herramientas permiten aplicar automáticamente la actualización, pero otras se limitan a notificarlo, debiendo el usuario o administrador actualizarla manualmente.

Ejemplos de herramienta de este tipo: AVAST (funcionalidad integrada al antivirus) y Kaspersky Software Updater. AVAST, en su versión gratuita, solo notifica la existencia de actualizaciones. Se ha probado la implementación con Kaspersky Software Updater, una herramienta gratuita que actúa localmente en el equipo en que está instalada.

Tipo de control: Herramienta de nivel de equipo

Herramientas: Kaspersky Software Updater

Tiempo estimado: 30 minutos por equipo

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 4:

Microsoft ofrece una herramienta para gestión centralizada de actualizaciones en redes corporativas llamada Microsoft Windows Server Update Services (WSUS), incluida como un rol desde Windows Server 2008 R2, sin ningún costo adicional. Sin embargo, es poco práctica para una red de equipos que no estén agrupadas en un dominio. Si bien, es posible añadir los equipos del grupo de trabajo al WSUS, requiere

un conocimiento avanzado (modificación de registros, configuración y mantenimiento de un servidor Windows Server) además del costo del propio servidor. WSUS, al igual que Microsoft Update, gestiona las actualizaciones de productos de Microsoft, sin embargo, puede ser combinada con otro software de gestión de actualizaciones complementarios, como por ejemplo Local Update Publisher.

Tipo de control: Herramienta de nivel de equipo y funcionalidad de sistema operativo (servidor)

Herramientas: Local Update Publisher y WSUS

Tiempo estimado: 8 a 24 horas (se asume que ya se cuenta con un servidor Windows Server 2008 R2 o superior instalado y configurado de manera funcional)

Personal necesario: 1 persona

Conocimiento técnico: avanzado

Costo: ninguno (se asume que ya se ha adquirido una licencia válida de Windows Server)

5. Protección de servicios expuestos con contraseñas robustas:

Algunos de los principales servicios de acceso remoto que pueden ser expuestos a Internet son SSH, RDP, TeamViewer. La implementación de este control debe ser realizada individualmente a cada tipo de acceso a través de guías o tutoriales que indiquen cómo cambiar la contraseña para cada tipo de servicio. En algunos servicios es posible implementar este control mediante el establecimiento de políticas de contraseña que fuercen el uso de contraseñas robustas. En el caso de RDP, se aplican las políticas de contraseñas del equipo o del dominio, por lo que el control 1 de la presente sección ya cubre este control. En el caso de otros mecanismos, como SSH, se debe establecer la política mediante el cambio de configuración del servicio.

Opción 1:

Configuración de políticas de contraseña del servicio SSH.

Tipo de control: Funcionalidad del servicio

Herramientas: ninguna

Tiempo estimado: 15 minutos por equipo

Personal necesario: 1 persona

Conocimiento técnico: intermedio

Costo: ninguno

Teléfonos y dispositivos móviles

1. Antivirus:

Existen múltiples aplicaciones antivirus gratuitas que pueden instalarse de manera individual en los dispositivos móviles, los cuales son adecuados para los dispositivos de una PYME, entre ellos, por ejemplo:

- ESET Mobile Security & Antivirus
- AVG Antivirus
- AVAST Antivirus

- Antivirus Free-Mobile Security (NQ Security Lab)
- Antivirus Kaspersky para móviles y tablets

Tipo de control: Herramienta de nivel de equipo

Herramientas: diversas aplicaciones de los *app stores* oficiales

Tiempo estimado: 1 a 3 minutos

Personal necesario: 1 persona para la instalación en todos los dispositivos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

2. Restricción de instalación de apps no oficiales:

Tanto Android como iOS permiten restringir la instalación de aplicaciones que no provengan de los *app stores* oficiales, mediante una configuración del sistema operativo.

Tipo de control: Configuración a nivel del sistema operativo

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos

Personal necesario: 1 persona para la configuración de todos los dispositivos o cada empleado lo configura individualmente. Obs.: Por defecto, ya viene configurado de esta manera, por lo que, a menos que alguien lo hubiera cambiado manualmente, no sería necesario realizar ninguna acción adicional, más que verificar que está configurado de esta manera.

Conocimiento técnico: ninguno

Costo: ninguno

3. Contraseña de inicio de sesión y bloqueo de pantalla con contraseña

Andoid y iOS permiten establecer una contraseña, un PIN numérico, un patrón de desbloqueo o algún rasgo biométrico (huella dactilar, imagen facial, u otro). A diferencia de las computadoras, no suele ser posible establecer una política de robustez de dicha credencial, las opciones específicas dependen del fabricante del dispositivo (modelo, marca, etc.). Por defecto no viene configurado ninguna contraseña ni equivalente.

Tipo de control: Funcionalidad del sistema operativo

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por equipo

Personal necesario: Cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Correo electrónico

1. Contraseña segura:

Opción 1:

En caso de que cada empleado utilice su cuenta personal de Gmail, Hotmail u otro similar, la empresa solo puede instruir a cada empleado a que utilice una contraseña robusta, pero dependerá de cada empleado de obedecer ese requerimiento.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta

Personal necesario: Cada empleado lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 2:

En caso de que utilizar un servicio de correo corporativo como Zoho Mail es posible establecer una política de contraseña a través del panel de administración, de modo a asegurar que todos los empleados estén utilizando contraseñas robustas en las cuentas de correo electrónico. Igualmente, si se cuenta con un servidor de correo propio como por ejemplo Zimbra (un software de correo *open source* y gratuito) es posible configurar la política de contraseña desde el panel de administración.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

2. Autenticación de doble factor:

Opción 1:

En caso de que cada empleado utilice su cuenta personal de Gmail, Hotmail u otro similar, las cuales incluyen la funcionalidad de autenticación de doble factor, la empresa debe instruir a cada empleado a que la active y configure.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: depende del servicio (por ej., Google Authenticator)

Tiempo estimado: 10 a 15 minutos por cuenta

Personal necesario: Cada empleado lo configura individualmente.

Conocimiento técnico: básico

Costo: ninguno

Opción 2:

En caso de que utilizar un servicio de correo corporativo como Zoho Mail es posible activar y forzar el uso de autenticación de doble factor a través del panel de administración, de modo a asegurar que todos los empleados sean forzados a configurarla en su cuenta.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: teléfono móvil, cuenta de correo alternativa o Google Authenticator

Tiempo estimado: 1 a 2 minutos para la activación desde el panel de administración, 10 a 15 minutos por cuenta

Personal necesario: 1 persona para la activación y cada empleado lo configura individualmente para su cuenta.

Conocimiento técnico: básico

Costo: ninguno

3. Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware, etc.):

Se trata de una medida de protección a nivel de equipo y su implementación ha sido probada en el apartado de dicho activo.

4. Configuración segura del servidor de correo, restricción del puerto 25:

Para implementar este control, se debe incluir las siguientes reglas en el cortafuego a nivel de red:

- Restringir el tráfico desde y hacia la LAN por puerto 25
- Permitir el tráfico desde la IP del servidor de correo hacia la WAN por puerto 25

Una PYME puede implementar esta restricción en el equipo de borde de red (router) o en un sistema dedicado (físico o virtual). En el caso de redes que no cuentan con IPs públicas estáticas, la gran mayoría de los proveedores de servicio de internet nacionales restringen el tráfico desde y hacia el puerto 25.

Tipo de control: Funcionalidad del equipo de red

Herramientas: ninguna

Tiempo estimado: 3 a 5 minutos

Personal necesario: 1 persona

Conocimiento técnico: intermedio a avanzado

Costo: ninguno

5. Actualización del software de correo (si es propio):

Si la empresa cuenta con un servidor de correo propio, deberá actualizar regularmente el software de correo. Esto deberá ser llevado a cabo por el administrador del servicio de correo, las instrucciones específicas dependerán del software de correo a ser utilizado.

Opción 1:

En caso de que utilizar por ejemplo Zimbra, la instalación de parches de seguridad, en una misma versión, se realiza desde la consola del servidor. En caso de que se trate de una versión nueva, se debe hacer una migración de versión, también desde la consola.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: ninguna

Tiempo estimado: 15 minutos a 8 horas (dependiendo de si la actualización es de una nueva versión)

Personal necesario: 1 persona

Conocimiento técnico: intermedio - avanzado

Costo: ninguno

6. Configuración de información de recuperación:

La gran mayoría de los servicios de correo permiten establecer información de recuperación tal como una cuenta de correo alternativa, un número de teléfono móvil, etc. La implementación específica depende del tipo de servicio de correo utilizado.

Tipo de control: Funcionalidad del servicio de correo

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta

Personal necesario: cada empleado lo configura individualmente para su cuenta.

Conocimiento técnico: básico

Costo: ninguno

Redes Sociales:

1. Contraseña segura:

La implementación específica de esta medida de protección depende de cada red social. En la mayoría de los casos, las redes sociales se manejan como cualquier cuenta personal y la empresa solo puede instruir a los administradores de la red social a que utilices una contraseña robusta, pero dependerá de éstos obedecer ese requerimiento.

Tipo de control: Funcionalidad de la plataforma de red social

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta

Personal necesario: Cada empleado que administra una cuenta lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

2. Autenticación de doble factor:

Al igual que en el correo electrónico, la implementación de esta medida de protección depende, en gran medida, de cada plataforma de red social (Facebook, Twitter, Instagram, etc.). La gran mayoría de estas plataformas incluyen la funcionalidad de autenticación de doble factor, la cual simplemente debe ser activada y configurada por los usuarios.

Tipo de control: Funcionalidad del servicio de red social

Herramientas: teléfono móvil, cuenta de correo alternativa o Google Authenticator

Tiempo estimado: 10 a 15 minutos por cuenta por plataforma

Personal necesario: cada empleado que administra una cuenta lo configura individualmente para la cuenta.

Conocimiento técnico: básico

Costo: ninguno

3. Configuración de información de recuperación:

La implementación específica depende de la red social utilizada, pero la gran mayoría (Facebook, Twitter, Instagram) lo permite. Muchas veces, el número telefónico configurado para la autenticación de doble factor constituye la información de recuperación.

Tipo de control: Funcionalidad de la red social

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta por plataforma

Personal necesario: cada empleado que administra una cuenta lo configura individualmente para la cuenta.

Conocimiento técnico: ninguno

Costo: ninguno

4. Procedimiento de baja de usuario - transferencia de responsabilidades y accesos:

Existen diversas maneras de implementar este control, dependiendo de la plataforma y de la empresa, ya sea a través de la redundancia de roles (más de un usuario administrador, cuando la plataforma lo permite), resguardo de la contraseña en poder de una autoridad de la empresa, u otros mecanismos por lo que no se ha probado la implementación, sin embargo, puede realizarse sin conocimientos técnicos y sin costo económico.

Wifi:

1. Contraseña segura del Wifi:

La contraseña del wifi se establece a través del panel de administración del Access Point (AP). Las instrucciones específicas varían de acuerdo a la marca y modelo del AP, pero es muy similar en todos. La contraseña debe cumplir las políticas de contraseña de la empresa especialmente en cuanto a longitud y complejidad.

Tipo de control: Configuración a nivel de equipo (AP)

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos

Personal necesario: 1 persona

Conocimiento técnico: ninguno

Costo: ninguno

2. Configuración segura del Wifi – protocolos seguros:

La configuración se realiza a través del panel de administración del Access Point (AP), las instrucciones específicas varían de acuerdo a la marca y modelo del AP, pero es muy similar en todos. Para una PYME, el protocolo más adecuado es WPA2; nunca se debe utilizar WEP o WPA.

Tipo de control: Configuración a nivel de equipo (AP)

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos

Personal necesario: 1 persona

Conocimiento técnico: ninguno

Costo: ninguno

3. Contraseña segura del Access Point:

La contraseña del AP se establece a través del panel de administración del AP. Las instrucciones específicas varían de acuerdo a la marca y modelo del AP, pero es muy similar en todos.

Tipo de control: Configuración a nivel de equipo (AP)

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos

Personal necesario: 1 persona

Conocimiento técnico: ninguno

Costo: ninguno

4. Utilización de HTTPs para envío de credenciales:

Opción 1:

Este control puede ser implementado mediante la herramienta HTTPS Everywhere, un complemento para navegadores que fuerza el uso de HTTPs durante la navegación.

Tipo de control: Herramienta de nivel de equipo

Herramientas: HTTPS Everywhere

Tiempo estimado: 2 a 3 minutos

Personal necesario: 1 persona para la instalación en todos los equipos o cada empleado lo instala individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Página Web:

1. Actualización de CMS, plugins, plantillas:

La gran mayoría de los CMS, plugins y plantillas pueden actualizarse a través del panel de administración del CMS, sin embargo, las instrucciones específicas pueden variar de acuerdo al CMS, al plugin y a la plantilla. Por ejemplo, existen plugins que deben ser actualizados reemplazando los archivos a través del FileManager o FTP. Algunos proveedores de servicio de alojamiento ofrecen la funcionalidad de actualización automática de los componentes. Para una PYME que no cuenta con personal técnico, es preferible elegir un servicio de hosting que cuente con esta funcionalidad.

Tipo de control: Funcionalidad del hosting o procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 5 a 30 minutos, dependiendo del CMS, plugin o plantilla

Personal necesario: 1 persona

Conocimiento técnico: básico a intermedio

Costo: ninguno

2. Contraseña segura para los usuarios del CMS:

Tipo de control: Funcionalidad del CMS

Herramientas: ninguna

Tiempo estimado: 1 a 2 minutos por cuenta

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

3. Auditoría de vulnerabilidades de la aplicación web (en caso de desarrollo propio):

Opción 1:

Un análisis de vulnerabilidades básico de una web puede ser realizado con scanners gratuitos como ZAP.

Tipo de control: Herramienta y procedimiento de la empresa

Herramientas: ZAP Scanner

Tiempo estimado: 15 a 30 minutos para análisis

Personal necesario: 1 persona

Conocimiento técnico: avanzado

Costo: ninguno

Opción 2:

Se puede contratar un servicio de análisis de vulnerabilidades básico, pudiendo incluir o no la corrección de vulnerabilidades encontradas. En las PYMEs, raramente habrá los recursos para corregir las vulnerabilidades, por lo que el servicio debe incluirlo, o se debe contratar otro servicio para ello.

Tipo de control: Servicio tercerizado

Herramientas: No aplica

Tiempo estimado: No aplica

Personal necesario: 1 persona para acompañamiento del proceso

Conocimiento técnico: básico a intermedio

Costo: 500 a 1000 Euros

4. Contraseña segura para accesos del hosting:

Tipo de control: Funcionalidad del hosting

Herramientas: ninguna

Tiempo estimado: 3 a 5 minutos

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

5. Copia de seguridad del sitio web:

Opción 1:

Se puede hacer una copia manualmente, copiando el contenido del sistema de archivos, del directorio raíz del servidor web, y el contenido de la base de datos. Se puede comprimir todo el contenido o crear un archivador con los archivos y se debe guardar offline, preferentemente, ya sea en un dispositivo de almacenamiento (USB, disco duro externo o similar) u online, pero fuera del servidor web.

Tipo de control: Procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 5 a 15 minutos

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

Opción 2:

Algunos servicios de alojamiento ofrecen la funcionalidad de copia de seguridad automática, solo se debe indicar la frecuencia con la que se desea realizar la copia, la cantidad de copias que se desea almacenar, el lugar donde se desea almacenar, etc. La mayoría de las veces, solo se permite guardar localmente en el mismo servicio de hosting, lo cual podría constituir un riesgo en caso de que el incidente se da con el servicio de hosting justamente. En caso de que el servicio no permita configurar un almacenamiento externo, el administrador deberá descargar regularmente la copia de seguridad de manera manual.

Tipo de control: Funcionalidad del servicio de alojamiento + procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos

Personal necesario: 1 persona

Conocimiento técnico: básico

Costo: ninguno

6. Separación de bases de datos y/o archivos sensibles del contenedor público:

En caso de que la empresa cuente con bases de datos sensibles, ésta debe estar en un servidor de bases de datos distinta al de la página web. El administrador del servidor web debe realizar una revisión para asegurar que esto se esté cumpliendo, en caso contrario, debe migrar el contenido sensible a otro servidor; un servidor virtual o un contenedor virtual distinto será adecuado.

Tipo de control: Procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 10 a 60 minutos

Personal necesario: 1 persona

Conocimiento técnico: intermedio

Costo: ninguno

Servicios en la nube:

1. Contraseña segura:

Opción 1:

Si se trata de un servicio en la nube orientado a uso personal, la empresa debe dar la directiva a los usuarios que administran la cuenta del servicio para que éstos establezcan una contraseña segura.

Tipo de control: Funcionalidad de la plataforma

Herramientas: ninguna

Tiempo estimado: 2 a 3 minutos por cuenta

Personal necesario: Cada empleado que administra una cuenta lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 2:

Si se trata de un servicio en la nube orientado a uso corporativo, el administrador del servicio debe configurar la política de contraseña a través del panel de administración de la nube. La implementación de este control dependerá de la plataforma.

Tipo de control: Funcionalidad de la plataforma

Herramientas: ninguna

Tiempo estimado: 5 minutos por plataforma

Personal necesario: 1 persona.

Conocimiento técnico: ninguno

Costo: ninguno

2. Autenticación de doble factor:

Opción 1:

Si se trata de un servicio en la nube orientado a uso personal, la empresa debe dar la directiva a los usuarios que administran la cuenta del servicio activen y configuren la autenticación de doble factor a la cuenta asociada al servicio.

Tipo de control: Funcionalidad de la plataforma

Herramientas: depende de la plataforma (teléfono, Google Authenticator, etc.)

Tiempo estimado: 10 a 15 minutos por cuenta

Personal necesario: Cada empleado que administra una cuenta lo configura individualmente.

Conocimiento técnico: ninguno

Costo: ninguno

Opción 2:

Si se trata de un servicio en la nube orientado a uso corporativo, el administrador del servicio puede activar el uso obligatorio de autenticación de doble factor a través del panel de administración de la nube, de modo a que cada usuario de una cuenta del servicio tendrá que configurarlo luego individualmente.

Tipo de control: Funcionalidad de la plataforma

Herramientas: depende de la plataforma (teléfono, Google Authenticator, etc.)

Tiempo estimado: 2 a 3 minutos por plataforma

Personal necesario: 1 persona.

Conocimiento técnico: ninguno

Costo: ninguno

3. Configuración de información de recuperación:

Las plataformas de servicios en la nube también permiten establecer información de recuperación (correo alternativo, teléfono, pregunta de seguridad, etc.) de modo a que, si se pierde el acceso a la cuenta, por el motivo que sea, se pueda recuperar el acceso. Cada administrador de la cuenta del servicio debe asegurarse de haber completado de manera correcta esta información.

Sistemas internos:

Debido a la diversidad de sistemas que pueden existir, no es posible modelar una implementación estándar de los controles propuestos, ya que éstas serán sumamente diversas, por lo que no se ha probado la implementación de los mismos.

Servidores propios:

1. Soluciones de seguridad de Endpoint (antivirus, antimalware, anti-spyware, etc.):

Opción 1:

Para servidores Linux, algunos softwares de seguridad son ClamAV (antivirus/antimalware), rkhunter, chrootkit (antirootkit), todos gratuitos. Pueden ser configurados para ejecutarse automáticamente de manera periódica y enviar reportes al administrador.

Tipo de control: Herramienta de nivel de equipo

Herramientas: ClamAV, rkhunter o chrootkit

Tiempo estimado: 10 a 20 minutos por servidor

Personal necesario: 1 persona.

Conocimiento técnico: intermedio

Costo: ninguno

Opción 2:

Para servidores Windows Server, la mayoría de empresas de antivirus ofrecen productos de seguridad específicos, pero ninguno gratuito. Por lo general, se integra a la consola de administración del antivirus corporativo.

Tipo de control: Herramienta de nivel de equipo

Herramientas: Kaspersky Windows Server Security o Security 10 for Windows Server, Bitdefender fow Windows Server o for File Server (Windows), Symantec Endpoint Protection Small Business Edition, u otros

Tiempo estimado: 30 minutos a 1 hora por servidor

Personal necesario: 1 persona.

Conocimiento técnico: intermedio a avanzado

Costo: desde 30 a 300 USD por servidor

2. Firewall basado en Host y/o en red:

Opción 1:

Como firewall a nivel de host, para servidores Windows se puede utilizar el firewall de Windows y para servidores Linux se puede utilizar *iptables*, ambos sin costo. Se debe modelar las reglas de modo a permitir solo las conexiones entrantes a los puertos de servicios que deben estar expuestos y denegar las demás; en caso de que algún servicio deba estar expuesto solo desde un origen determinado (por ejemplo, solo desde la LAN o solo desde otro servidor) se debe permitir las conexiones entrantes desde ese único origen. Por lo general, se configura el firewall para permitir todas las conexiones salientes del servidor, sin embargo, teniendo en cuenta que el servidor raramente necesite iniciar conexiones (para actualizarse, para descargar un paquete, para conectarse a una base de datos, etc.), se puede limitar las conexiones a puertos y/o destinos conocidos, únicamente.

Tipo de control: Herramienta de nivel de equipo

Herramientas: Iptables (Linux) o firewall de Windows (Windows Server)

Tiempo estimado: 5 a 10 minutos para la instalación, 30 a 45 minutos para configuración granular

Personal necesario: 1 persona.

Conocimiento técnico: intermedio a avanzado

Costo: ninguno

Opción 2:

pfSense es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Router, entre otras funcionalidades. Es gratuito y puede ser instalado en una PC-servidor de bajas prestaciones o incluso en una máquina virtual; también están disponibles en versión *appliance* físico desde 150 USD

Tipo de control: Herramienta a nivel de red

Herramientas: pfSense (opcional, *appliance* pfSense)

Tiempo estimado: 1 a 2 horas

Personal necesario: 1 persona.

Conocimiento técnico: avanzado

Costo: ninguno (*appliance* físico desde 150 USD)

3. IDS/IPS basado en Host y/o en red:

Opción 1:

Fail2ban es una herramienta gratuita para Linux que protege principalmente contra ataques de fuerza bruta y otras actividades maliciosas contra servicios como SSH, cuentas de correo, servidor web, etc, a través del bloqueo de las IPs que originan el tráfico malicioso. La configuración por defecto suele ser suficiente para las necesidades de una PYME, sin embargo, puede ser personalizada.

Tipo de control: Herramienta a nivel de equipo

Herramientas: fail2ban

Tiempo estimado: 10 a 15 minutos por servidor

Personal necesario: 1 persona.

Conocimiento técnico: intermedio a avanzado

Costo: ninguno

Opción 2:

Snort es un IDS/IPS a nivel de red gratuito, de código abierto y uno de los más utilizados en todo tipo de organizaciones, en todo el mundo. Puede ser instalado en un equipo dedicado; sin embargo, pfSense ofrece el paquete de Snort y de Suricata (un *fork* de Snort) entre sus utilidades, debiendo ser activado simplemente. Las reglas de un IDS/IPS, especialmente a nivel de red, deben ser personalizadas o ajustadas de acuerdo a la necesidad de la empresa, de lo contrario se corre el riesgo de que se bloqueen intentos legítimos de conexión, lo que puede ocasionar problemas. La configuración inicial es adecuada para muchos escenarios, pero el ajuste de las reglas requiere mucho tiempo y conocimiento antes de ser implementado de forma definitiva. Requiere una administración casi permanente.

Tipo de control: Herramienta a nivel de red

Herramientas: pfSense, Snort o Suricata

Tiempo estimado: 20 a 30 minutos para la activación y configuración inicial (se asume que pfSense ya se encuentra implementado correctamente) – 2 a 3 meses de monitoreo, configuración y ajuste adicional

Personal necesario: 1 persona.

Conocimiento técnico: avanzado

Costo: ninguno

4. Actualización de sistema operativo y programas:

Opción 1:

En el caso de servidores Linux existen herramientas de automatización de actualización (yum-cron o similar), tanto del sistema operativo como de los paquetes descargados de repositorios oficiales; se debe

tener en cuenta que, en caso de software instalado desde orígenes distintos, debe verificarse y/o actualizarse manualmente. En distribuciones específicas para servidores y de alta estabilidad, como CentOS/RHEL o Ubuntu LTE, los problemas de compatibilidad son muy raros.

Tipo de control: Herramienta a nivel de equipo

Herramientas: yum-cron o similar

Tiempo estimado: 5 a 10 minutos por servidor

Personal necesario: 1 persona.

Conocimiento técnico: intermedio

Costo: ninguno

Opción 2:

En el caso de servidores Windows, la actualización se puede realizar de la misma manera que como se realice en los equipos Windows, ya sea a través de Windows Update combinado con actualización manual de los demás componentes o a través de una herramienta de gestión de vulnerabilidades.

5. Protección de servicios expuestos con contraseñas robustas:

En algunos servicios se permite establecer políticas de contraseña, sin embargo en otros, dependerá del usuario. En caso de RDP (servidores Windows) las políticas de contraseña se gestionan a partir de las políticas del sistema operativo, ya que las credenciales de acceso son las mismas del equipo. En el caso de SSH (servidores Linux, principalmente) las políticas de contraseña se establecen en el archivo de configuración del servicio SSH.

Tipo de control: Funcionalidad del sistema operativo o servicio

Herramientas: ninguna

Tiempo estimado: 5 a 10 minutos por servicio

Personal necesario: 1 persona

Conocimiento técnico: intermedio

Costo: ninguno

6. Hardening de sistema operativo y de servicios expuestos:

Opción 1:

Se puede realizar un hardening de manera manual, eligiendo alguna guía como por ejemplo CIS Benchmarks. Algunas de las medidas de protección que se implementan en el proceso de hardening es deshabilitar los usuarios administrativos, limitar los intentos de acceso fallido, desinstalación de paquetes innecesarios, establecimiento de políticas de contraseña robusta, restricción de permisos a lo estrictamente necesario, etc. Los cambios pueden incorporarse gradualmente.

Tipo de control: Procedimiento de la organización

Herramientas: ninguna

Tiempo estimado: 2 a 8 horas por servidor

Personal necesario: 1 persona

Conocimiento técnico: avanzado

Costo: ninguno

Opción 2:

Se puede realizar un hardening de manera automatizada o semi-automatizada con OpenSCAP, una herramienta basada en *baselines* ampliamente aceptados por la industria, para varios sistemas operativos y usos comunes. Consta de dos fases: primeramente, un escaneo inicial del servidor a ser protegido, en el que se identifican potenciales problemas, seguida de la fase de corrección, en la que se puede aplicar las correcciones que se desean, de manera manual, siguiendo las recomendaciones de la herramienta (incluye tutoriales específicos, paso a paso, de cómo aplicar la corrección) o se puede optar por la aplicación automatizada de las correcciones. Con el OpenSCAP Framework se puede auditar las máquinas de manera remota y centralizada.

Tipo de control: Herramienta a nivel de equipo

Herramientas: OpenSCAP framework, OpenSCAP Scanner y baselines

Tiempo estimado: 30 minutos por servidor

Personal necesario: 1 persona

Conocimiento técnico: intermedio - avanzado

Costo: ninguno

7. Copia de seguridad continua del sistema operativo (imágenes o *screenshots* de S.O.):

Opción 1:

Rsync es una de las herramientas de sincronización más conocidas y versátiles para servidores Linux que permite realizar una copia de seguridad de manera periódica e incremental. Funciona por línea de comandos y permite realizar sincronización remota, en un modelo cliente-servidor.

Tipo de control: Herramienta a nivel de equipo

Herramientas: rsync

Tiempo estimado: 20 a 30 minutos para instalación y configuración de servidor de almacenamiento y 10 a 15 minutos por servidor (cliente)

Personal necesario: 1 persona

Conocimiento técnico: intermedio - avanzado

Costo: ninguno. Obs.: requiere un dispositivo de almacenamiento externo, ya sea físico o virtual donde copiar los archivos (servidor rsync)

Opción 2:

Existen herramientas de sincronización similares a rsync para servidores Linux, pero con interfaz gráfica, como por ejemplo Simple Backup Suite.

Tipo de control: Herramienta a nivel de equipo

Herramientas: Simple Backup Suite (sbackup)

Tiempo estimado: 15 a 20 minutos por servidor

Personal necesario: 1 persona

Conocimiento técnico: intermedio

Costo: ninguno. Obs.: requiere un dispositivo de almacenamiento externo, ya sea físico o virtual donde copiar los archivos.

8. Redundancia lógica del servidor:

La redundancia lógica debe ser diseñada desde la arquitectura hasta la programación e implementación del sistema; si el sistema o aplicación no fue diseñado de manera a ser redundante, se necesitará una re-ingeniería de la misma. Teniendo en cuenta que la criticidad de servicios brindados por PYMEs,, especialmente desde el punto de vista de disponibilidad, no es extremadamente alta, y teniendo en cuenta la complejidad que le supone implementarlo, no se ha probado este control. Para una PYME será suficiente con contar con una copia de seguridad de los archivos y bases de datos de las aplicaciones y sistemas alojado para que, en caso de un incidente que afectara la disponibilidad del sistema, se pueda migrarlo a un nuevo servidor hasta tanto se resuelva el incidente.

Controles transversales:

1. Educación al usuario:

El tiempo estimado para un plan de concienciación y educación puede ser de 3 a 5 horas anuales, preferentemente dividido en jornadas breves por temática y metodología. Existen muchos recursos gratuitos, desde materiales audiovisuales, guías, charlas, etc. ofrecidos por organismos públicos, empresas privadas u organizaciones sin fines de lucro para que la empresa pueda llevar a cabo este plan. Existen también empresas privadas que ofrecen este tipo de servicios sin embargo suelen estar orientados a empresas grandes y con un costo superior al que puede destinar una PYME.

Opción 1:

INCIBE cuenta con una serie de recursos para concienciación y sensibilización de usuarios de una empresa, para el desarrollo de una cultura en seguridad. Entre estos recursos se encuentran infografías, videos, cuestionarios de auto-evaluación y cursos masivos a distancia (MOOC).[1]

[1] https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad

Opción 2:

El CERT-PY, de Paraguay, cuenta con una serie de iniciativas para la concienciación y sensibilización de usuarios de empresas, entre ellas, un taller mensual abierto a todo público en la que se abarca la gran mayoría de los temas específicos vinculados a usuarios de la tecnología e Internet, de manera no técnica y con énfasis en herramientas y medidas de protección al alcance del usuario. El taller tiene una duración de 3 horas y los materiales son públicos[2]. Este mismo taller está disponible en formato de curso virtual, abierto a todo público (previo registro), y con un enfoque teórico-práctico, que le permite al usuario entender la problemática y le guía a través de la implementación de las medidas de protección que están a su alcance[3].

2. Utilización de gestor de contraseña:

Opción 1:

Un posible gestor de contraseña gratuito es Kaspersky Password Manager.

Tipo de control: Herramienta de nivel de equipo

Herramientas: Kaspersky Password Manager

Tiempo estimado: 5 minutos

Personal necesario: 1 persona para la instalación en todos los dispositivos o cada empleado lo instala individualmente.

Conocimiento técnico: básico

Costo: ninguno

Opción 2:

Un posible gestor de contraseña gratuito y online es LastPass, una extensión para la gran mayoría de los navegadores. También tiene una versión offline, para escritorio.

Tipo de control: Herramienta de nivel de equipo

Herramientas: LastPass

Tiempo estimado: 2 a 3 minutos

Personal necesario: 1 persona para la instalación en todos los dispositivos o cada empleado lo instala individualmente.

Conocimiento técnico: básico

Costo: ninguno

[2] https://www.cert.gov.py/index.php/download_file/view/565/209
[3] http://cursos.gov.py/categorias/area-informatica/seguridad-en-internet