Contador Público Nacional y Perito Partidor

EL IMPACTO GENERADO POR LA SEGURIDAD INFORMÁTICA EN LAS PYMES DE MENDOZA

Trabajo de Investigación

POR

DEMARTINI, María Victoria - N° Registro 24286; vickydemartini@live.com.ar
RIOS, María Julieta - N° Registro 25883; mjulirios@gmail.com

Profesor Tutor

MAJOWKA, Pablo David

Mendoza-2019

RESÚMEN

El presente trabajo de investigación tiene que ver con el impacto que genera la seguridad informática en Pymes de Mendoza, buscando como objetivo aportar información a entes analizados con el fin de implementar herramientas propuestas, concientizar respecto del impacto económico de la gestión de seguridad informática en la gestión empresarial y así poder detectar brechas y vulnerabilidades del sistema establecido y posibles oportunidades de mejora. Ayudará a las PYMES de Mendoza a tomar conciencia en la protección de sus datos y sistemas informáticos, teniendo en cuenta que cuando nos referimos a datos informáticos, es toda la información virtual que se encuentra almacenada y disponible en la red privada de las pymes, siendo dicha información fundamental y vital para que las pymes funcionen correctamente y alcance sus objetivos propuestos. El objetivo es obtener un nivel considerable de seguridad para las pymes, el cual se logrará con los resultados obtenidos en la investigación y posteriormente recomendando e indicando una propuesta para gestión y prevención de seguridad informática, la cual podrá ser aplicable para la mayoría de pymes de diferentes rubros o giros de negocio, el único requisito es que la pyme se proponga implementar la propuesta de seguridad informática resultante.

En la primera parte se llevará a cabo un análisis teórico del tema a tratar, definiendo los conceptos generales a utilizar durante el desarrollo del trabajo de investigación. Luego en la segunda parte del trabajo, se realizará un análisis, una evaluación y una gestión de riesgos a los cuales se encuentra expuesta una Pyme con el objeto de poder determinar, analizar, valorar y clasificar el riesgo en la seguridad informática, así como también el impacto económico que genera en su actividad. Todo esto se logró mediante la búsqueda bibliográfica. A continuación, se llevó un análisis práctico a través del diseño de una encuesta con preguntas en su mayoría cerradas y algunas abiertas para relevar información necesaria para evaluar las dificultades que se producen cuando se desean implementar acciones para proteger la integridad y la privacidad de la información. Por último, se concluye con una serie de propuestas básicas de mejora a fin de que que puedan ayudarte a proteger a tu Pyme de cualquier amenaza.

Palabras claves: SISTEMA INFORMÁTICO - PYMES - SEGURIDAD INFORMÁTICA - IMPACTO ECONÓMICO - GESTIÓN DE RIESGOS.

ÍNDICE

Introducción…….....4
CAPÍTULO I – PYMES Y SEGURIDAD INFORMÁTICA
PYMES…….....6
1.1. Definición de PYMES…….....6
1.2. Ventajas de las PYMES…….....6
1.3. Desventajas de las PYMES…….....7
1.4. Registro PYMES…….....7
1.5. Clases de PYMES……..…….....15
2. SEGURIDAD INFORMÁTICA…..…….....16
2.1. Origen…… ..…….....16
2.2. Definición..…….. ……....16
2.3. Ventajas de la seguridad informática.....17
2.4. Desventajas de la seguridad informática.....17
3. Empresas atacadas en su seguridad informática……..…….19
4. Impacto de la seguridad informática en el perfeccionamiento de la gestión empresarial……20
5. La Ciberseguridad……....21
CAPÍTULO II – GESTIÓN DE RIESGOS E IMPACTO ECONÓMICO
1. Análisis, evaluación y gestión de riesgos……..……...26
2. Impacto en la actividad económica de una PyME……...27
CAPÍTULO III – APLICACIÓN PRÁCTICA
1. Trabajo de campo…..……33
2. Recomendaciones…….……43
Conclusiones…….....46
Referencias bibliográficas.....47

Introducción

El trabajo de investigación se dedicará al estudio del impacto generado por la seguridad informática en Pymes de Mendoza.

La correcta gestión del sistema de seguridad informática, así como el conocimiento de su impacto económico contribuirá a que los directivos, usuarios y el personal de la actividad informática de las entidades estén capacitados para ver la eficiencia, eficacia y el triunfo del negocio a través de procesos informáticos.

La seguridad informática es un asunto prioritario, pero ¿cómo poder cuantificar el valor de negocio que aporta una red segura?, ¿cómo poder evaluar y justificar la inversión en productos de seguridad de red?

De esta manera, al sufrir filtraciones de información, las empresas gastan cantidades enormes de tiempo y dinero en tareas de detección y corrección técnica, en la identificación y el bloqueo de ataques, así como en la valoración de los daños causados y en la aplicación de medidas correctivas.

Expresado lo anterior, las dificultades que el trabajo de investigación plantea en cuanto a la implementación de seguridad informática tiene su significancia en la resistencia al cambio organizacional (no sólo por los trabajadores de las organizaciones sino también por quienes dirigen la misma), en la capacidad de inversión, en la falta de metodología (por parte de quien tiene que asesorar, en este caso el contador de la empresa), y en la falta de conocimiento (por parte de otros asesores y usuarios) al momento de definir pilares esenciales en la aplicación de los sistemas de seguridad informática. Este trabajo se encuentra dirigido especialmente a estudiantes y profesionales en ciencias económicas, para que permita conocer y tener en cuenta los obstáculos e inconvenientes que surgen cuando se desea implementar la seguridad informática en una PYME. De este modo el lector se encontrará más preparado y consciente de los problemas que se producen en las organizaciones, tomando un rol y un punto de vista más protagónico y primordial (agregando valor a la organización).

Objetivos de Investigación

General:

- ➔ Determinar el impacto de la seguridad informática en Pymes de Mendoza.

Específicos:

- ➔ Identificar los problemas de gestión de sistemas de seguridad informática en Pymes de Mendoza.
- ➔ Análisis, evaluación y gestión de riesgos de ataques cibernéticos en la Pymes de Mendoza.
- ➔ Determinar el impacto en la actividad económica de Pymes.
- ➔ Enumerar medidas a implementar para disminuir el riesgo e impacto en la gestión empresarial.

Se trata de un estudio cuantitativo de tipo explicativo. Se realiza un relevamiento de información a través de encuestas y análisis de documentación.

Estructura del trabajo

Este trabajo tendrá como punto de partida, en el primer capítulo, la definición de conceptos generales que permitan comprender la complejidad del tema a tratar, con el objeto de proponer mecanismos de solución a los problemas que puedan plantearse. En el segundo se expondrá un análisis, una evaluación y una gestión de riesgos a los cuales se puede exponer una Pyme en cuanto a riesgos de seguridad informática e implementar medidas para minimizar los riesgos, y a su vez para ir solucionando los impactos. En el capítulo tres llevar adelante una encuesta realizada a una muestra de empresas mediante un cálculo estadístico con el fin de obtener información, y así analizar, evaluar y confirmar la hipótesis de la investigación, mencionando a continuación una serie de recomendaciones básicas que pueden ayudarte a proteger a tu Pyme de cualquier amenaza. Por último, daremos una breve conclusión del tema desarrollado.

CAPÍTULO I: PYMES Y SEGURIDAD INFORMÁTICA

En esta primera etapa del trabajo se desarrollarán definiciones y conceptos de PyMES, seguridad Informática y ciberseguridad como así también abordaremos el tema de cómo una empresa puede ser atacada en su seguridad informática y cómo esto impacta en su gestión empresarial.

1. PYMES

1.1. DEFINICIÓN DE PYME

Una PyME es considerada como una micro, pequeña o mediana empresa que realiza sus actividades en el país, en alguno de los sectores como servicios, comercial, industrial, agropecuario, construcción o minero; puede estar integrada por una o varias personas y su categoría se establece de acuerdo a la actividad declarada, a los montos de las ventas totales anuales o a su cantidad de empleados (Definición obtenida de https://pymes.afip.gob.ar).

Se trata de una empresa que se caracteriza por tener un número reducido de trabajadores, que registra ingresos moderados. También suele escribirse como PYME y PyME. Toma en cuenta las modalidades de empresa más reducidas, tales como las unipersonales; su definición varía según el país. En Argentina, por ejemplo, las empresas se clasifican de acuerdo a sus ventas anuales y a su rubro (una pyme industrial puede tener un volumen de facturación que, en otro sector económico, la ubicaría entre las de mayor volumen). Podemos decir que las pymes tienen necesidades específicas que deben ser atendidas por el Estado, que este tipo de empresas genera, en conjunto, grandes riquezas para cada país además de ser uno de los principales motores del empleo. Sin embargo, por sus particularidades, necesitan protección e incentivos para competir frente a las grandes corporaciones. Las líneas de crédito con condiciones especiales, los beneficios impositivos y la consultoría sin cargo son algunos de los instrumentos que suelen ofrecerse desde el Estado a las pymes para desarrollarse. (Porto & Gardev, 2009)

1.2. VENTAJAS DE LAS PYMES

Una de las ventajas tiene que ver con que presentan más flexibilidad que empresas convencionales en el sistema de producción; permiten entablar una relación mucho más cercana con los clientes; así es que, gracias a la mayor sencillez de su infraestructura, es más sencillo cambiar de nicho de mercado (el espacio donde se encuentran los potenciales usuarios o consumidores de un servicio o producto).

Los puestos de trabajo son más amplios, menos estrictos, y los trabajadores están más abiertos al cambio; el mayor nivel de conocimiento específico y know how, que se da gracias a la cercanía de los integrantes con el día a día de la empresa, puede convertirse en una importante ventaja con respecto a la competencia.

Además, el tiempo que requiere la toma de decisiones estratégicas puede ser considerablemente menor, dado que los procesos de gestión resultan menos complejos; presentan una visión menos estricta, más enfocada en las necesidades y demandas de los clientes que en sus propias raíces, lo cual da lugar a importantes modificaciones a nivel estructural, adoptando las tecnologías y el personal necesario para encarar los desafíos que se presentan a cada paso. (Porto & Gardev, 2009)

1.3. DESVENTAJAS DE LAS PYMES

Dado que se mueven por procesos de tipo emergente, la desventaja que presentan es que no cuentan con lineamientos específicos relacionados con su creación, sino que experimentan constantes cambios y evoluciones. (Porto & Gardev, 2009)

No gozan de un importante respaldo financiero, lo cual les impide embarcarse en negocios de gran envergadura; requieren de una constante revisión de su estructura, dado que su naturaleza adaptable puede convertirse en la razón de su disolución a causa de la pérdida del control organizativo. Suele ocurrir que no exista un control estricto de la entrada y la salida del dinero.

La mayor cercanía entre los trabajadores puede ser negativa si éstos trasladan sus problemas personales a la oficina.

Otra de las desventajas es que el reducido volumen de producción se refleja en la cuantía de los pedidos realizados a los proveedores, lo cual puede derivar en *sobrecosto*; si no se realiza una campaña publicitaria efectiva y constante, la empresa puede pasar desapercibida ante los consumidores.

1.4. REGISTRO DE UNA PYME

En la página https://www.produccion.gob.ar se puede realizar el registro de tu empresa bajo la categorización de MiPyME, y así, poder pagar menos impuestos y acceder a beneficios.

¿Cómo funciona el registro?, ¿cómo solicito la categorización MiPyME y los beneficios fiscales?, deberás:

- Tener CUIT con estado administrativo “Activo. Sin limitaciones”.
- Tener Clave Fiscal.
- Declarar y mantener actualizado el domicilio fiscal, así como los domicilios de los locales y establecimientos.

- Tener declaradas correctamente las actividades económicas - de acuerdo al nomenclador vigente F. 883.
- En caso de corresponder, tener presentadas las declaraciones juradas de IVA de los últimos 3 períodos fiscales cerrados.
- Tener declarado tu correo electrónico. Para ello se ingresa al servicio con clave fiscal "Sistema Registral" y en el menú "Registro Tributario", seleccionar la opción "Administración de Emails". Allí podrás ingresar tu correo electrónico.
- Tener declarado ante esta Administración Federal el "Domicilio Fiscal Electrónico". Para conocer cómo declararlo podés ingresar a la Guía Paso a Paso - Domicilio Fiscal Electrónico: ¿Cómo se adhiere y dónde se consultan las notificaciones?

1.4.1. Guía Paso a Paso para la registración de una PyME en A.F.I.P.

Imagen Nº I: Pasos para la registración. Paso 1.

Imagen N° II: Pasos para la registración. Paso 2

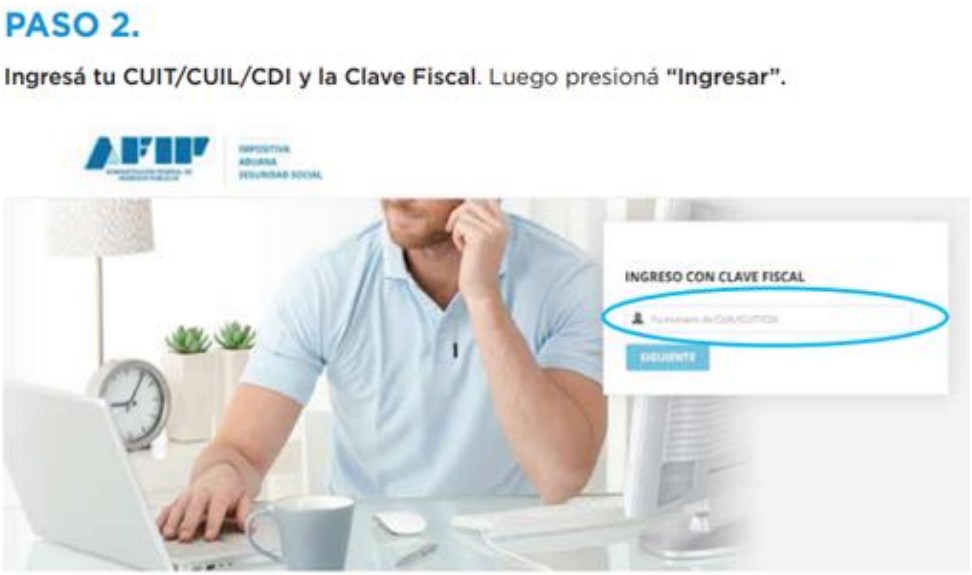
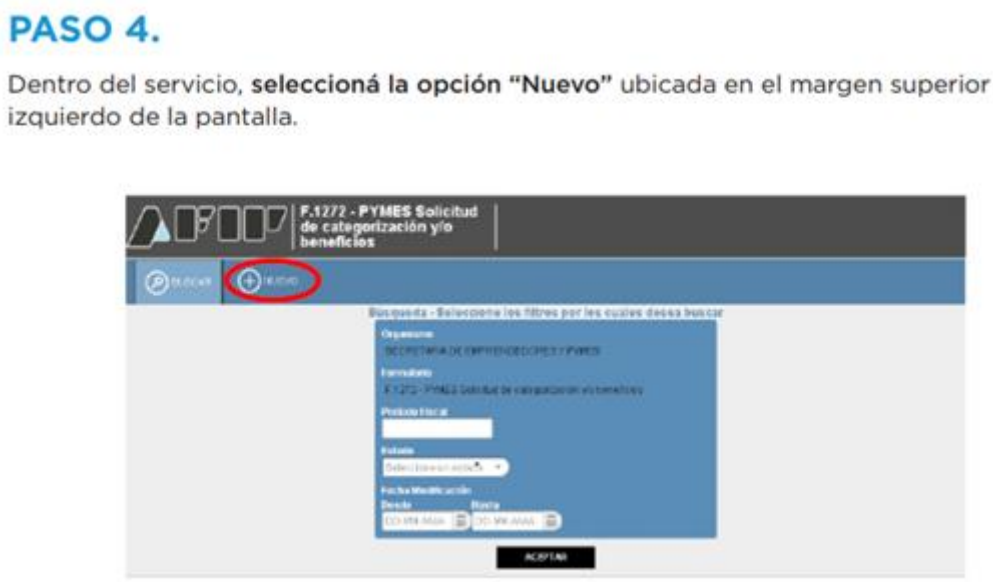


Imagen N° III. Pasos para la registración. Paso 3

Imagen N° IV. Pasos para la registración. Paso 4



Como consecuencia se abrirá una nueva ventana donde el sistema pedirá que complete los siguientes campos:

- Organismo: Secretaría de Emprendedores y PyMEs
- Formulario: F 1272 – PYMES Solicitud de categorización y/o beneficios

Imagen N° V. Pasos para la registración. Selección organismo y formulario.

A continuación, el sistema mostrará la siguiente pantalla, compuesta por la solapa "Datos informativos" y por los períodos fiscales cerrados en los que estuviste inscripto en el Impuesto al Valor Agregado. Los períodos fiscales que figuran dependerán de la fecha de tu inscripción en el Impuesto al Valor Agregado. Serán considerados los últimos 3 períodos fiscales cerrados. En caso de que la

inscripción sea posterior a los últimos 3 períodos fiscales cerrados, deberá informarse la suma de las ventas correspondientes a los períodos fiscales cerrado en que se estuvo inscripto en el impuesto.

En “Datos Informativos” deberás manifestar que mediante esta declaración jurada estás solicitando la categorización como Micro, Pequeña o Mediana Empresa Tramo 1 y 2. Asimismo, el sistema te consultará si deseas solicitar la opción para cancelar el IVA por trimestre, para ello deberás seleccionar la opción “SÍ”. En caso de que únicamente quieras categorizarte deberás seleccionar la opción “NO”.

Una vez contestada la pregunta, hacé clic en “Siguiente”

Imagen N° VI. Pasos para la registración. Solicitud de beneficios y datos informativos.

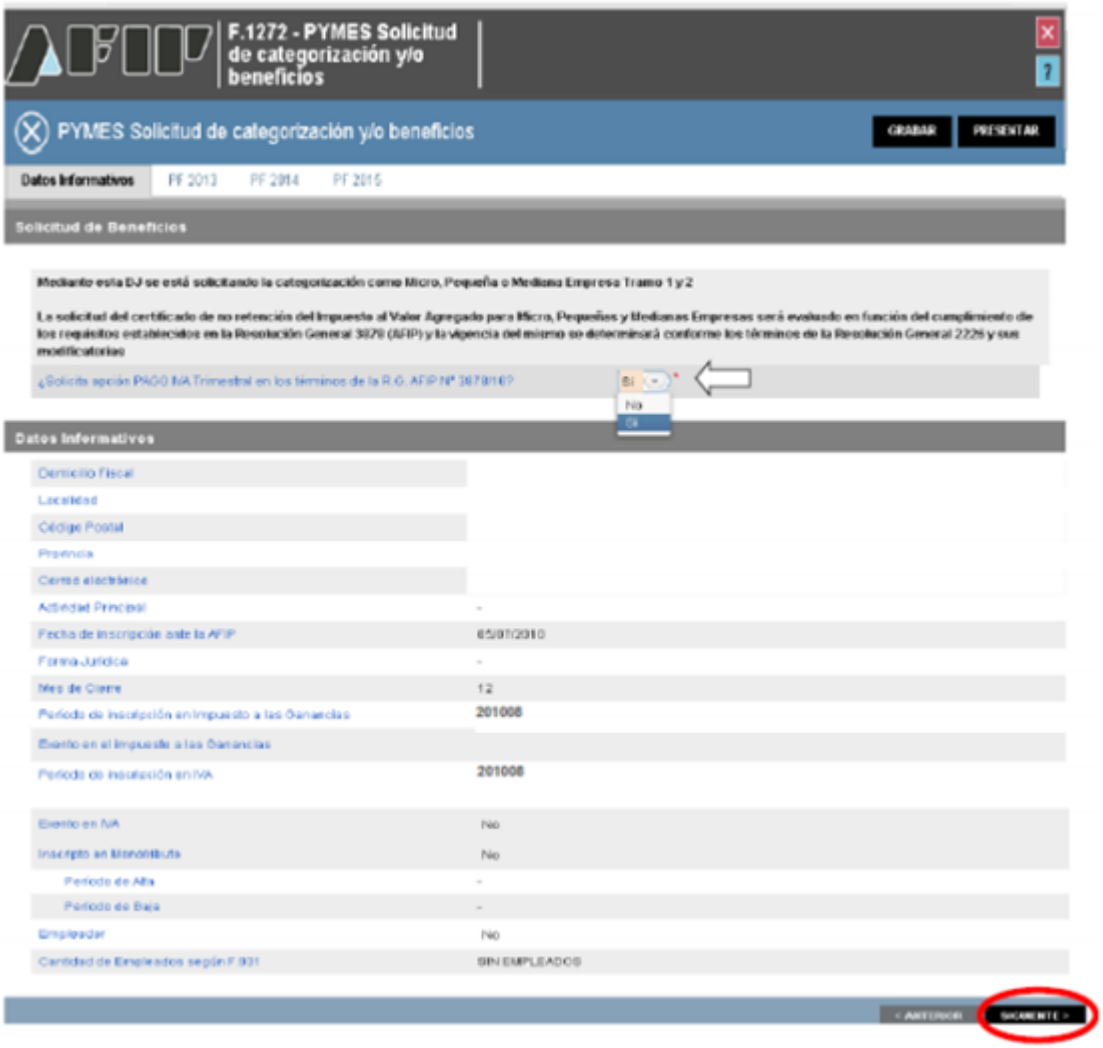


Imagen N° VII. Pasos para la registración. Paso 6.

PASO 6.

En las **solapas de los períodos fiscales deberás informar la suma de las ventas obtenidas por cada actividad,** incluyendo, en caso de corresponder según la actividad declarada, el 50% de las exportaciones netas de impuestos internos e IVA, conforme a período seleccionado.

La suma total de las ventas anuales por cada actividad que informes deberá coincidir con el total de ventas anuales que mostrará el sistema.

Para pasar al próximo período seleccioná **"Siguiente"**

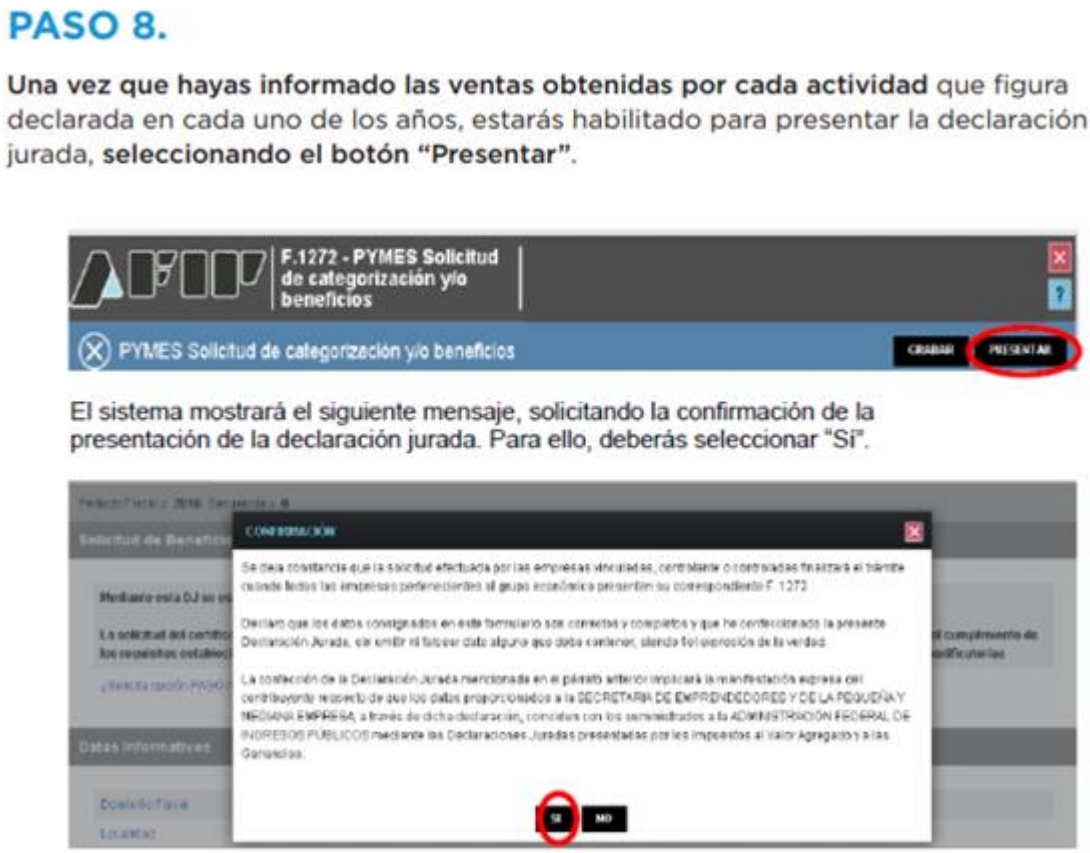
Imagen N° VIII. Pasos para la registración. Paso 7.

PASO 7.

Realizá el procedimiento anteriormente detallado en cada una de las solapas de los períodos que tengas disponibles.

Recordá que la suma total de las ventas anuales por cada actividad que informes deberá coincidir con el total de ventas anuales que mostrará el sistema.

Imagen N° IX. Pasos para la registración. Paso 8.



Por último, para conocer la resolución de tu solicitud, ingresá al servicio con Clave Fiscal "E – Ventanilla". Allí, te notificarán la categoría "MIPyME" y los beneficios fiscales obtenidos. (https://pymes.afip.gob.ar).

¿Cuáles son los beneficios?

- Pago de IVA a 90 días
- Compensación del impuesto al cheque en el pago de ganancias
- Eliminación del Impuesto a la Ganancia Mínima Presunta
- Incentivos fiscales para PyMEs que invierten
- Simplificación en la solicitud del certificado de no retención de IVA
- Reducción de retenciones para micro empresas de comercio

El panorama actual de la pequeña y mediana empresa, en general, indica la presencia de un sentimiento generalizado de desaliento, excepto en algunos pocos ramos. Aún resulta arriesgada la hipótesis, parecía ser una constante de este tipo de organizaciones el estado de crisis permanente.

Mendoza figura quinta en el ránking de los distritos con PyMEs (Pequeñas y Medianas Empresas) que salieron a buscar financiamiento en el mercado de capitales, que en el último trimestre del año pasado movió un total de $15.146 millones impulsado por las necesidades que generó la crisis económica. (Boyer, 2019)

Según el último informe de la Comisión Nacional de Valores (CNV), en diciembre del año pasado un total de 8 compañías radicadas en el territorio mendocino decidieron emitir deuda para adquirir recursos. (Boyer, 2019)

Durante el 2018, el número de PyMEs que salieron al mercado se incrementó un 70% respecto al año anterior. El crecimiento se explica por la puesta en marcha de una herramienta para facilitarles el acceso al crédito (la Obligación Negociable Simple), pero también por las crecientes urgencias que surgieron en medio de una profunda crisis económica con extremas tasas de interés.

Durante el cuarto trimestre de 2018 el financiamiento obtenido por las PyMEs ascendió a $15.146 millones, monto que representa el 35% del total del financiamiento en el mercado de capitales", indicó el documento de la CNV (Comisión Nacional de Valores).

En la CNV resaltaron que, a diciembre de 2018, el 44% de las empresas con oferta pública revisten el carácter de PyME y que, desde la entrada en vigencia en junio 2017 de la Resolución General N° 696 del "Régimen ON Simple", el número de emisoras PyME pasó de 74 a 144, esto es, 70 ingresos netos en 18 meses. (https://www.cnv.gov.ar/SitioWeb/Informes)

1.5. CLASES DE PYMES

La Secretaría de Emprendedores y PyMEs del Ministerio de Producción publicó la nueva clasificación para determinar qué empresas se encuadran dentro de la categoría PyME.

A través de la resolución 154/2018, se elevan los límites de facturación anual contemplando las especificidades propias de los distintos sectores y la evolución reciente de los mismos. Para el sector de industria, por ejemplo, actualmente se considera una microempresa la que facture en promedio durante los últimos 3 años hasta $13,4 millones, una pequeña hasta $81,4 millones; una mediana tramo 1 hasta $661,2 millones y una mediana tramo dos hasta $966,3 millones.

Asimismo, se incorpora la variable de personal empleado de manera concurrente con las ventas, con el objetivo de lograr un encuadre más preciso en la categorización PyME. Para las empresas que realicen actividades de comisión o consignación, se tomará sólo la variable empleo, lo cual les permitirá encuadrarse dentro de la categoría que más se ajuste a su tamaño real.

Por otro lado, y con el objetivo de incentivar las ventas al mercado externo de las pequeñas y medianas empresas, se redujo el porcentaje de las exportaciones a considerar para la categorización PyME, de un 50% a un 25% (https://www.argentina.gob.ar/noticias/nuevas-categorias-para-ser-pyme).

Tabla N° I: Clases de PyMEs 2019

Categoría	Construcción	Servicios	Comercio	Industria y minería	Agropecuario
Micro	12.710.000	6.740.000	23.560.000	21.990.000	10.150.000
Pequeña	75.380.000	40.410.000	141.680.000	157.740.000	38.180.000
Mediana tramo 1	420.570.000	337.200.000	1.190.400.000	986.080.000	272.020.000
Mediana tramo 2	630.790.000	481.570.000	1.700.590.000	1.441.090.000	431.450.000

Fuente: Montos publicados en la página web de la SEPYME sobre la base de la Resolución 220/19 SEPyME.

2. SEGURIDAD INFORMÁTICA

2.1. ORIGEN

La historia de la seguridad informática comienza a partir de los años 80´s con lo común que era usar un computador personal y la preocupación por conservar la integridad de los datos almacenados. De aquí en adelante se empiezan a producir los virus y gusanos más exactamente en los años 90´s, donde se crea una alerta para los ordenadores y la conexión a internet, empezando a identificarse ataques a sistemas informáticos, comenzando a definir la palabra Hacker, a final de los 90s las amenazas empezaron a generalizarse, aparecen nuevos gusanos y malware generalizado, ya a partir del año 2000 los acontecimientos hacen que se tome muy en serio la seguridad informática. (Julio, 2016)

2.2. DEFINICIÓN

Según la ISO 27001(norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan) la seguridad informática es una rama de la ingeniería de sistemas que se encarga de coordinar acciones para proteger la integridad y la privacidad de la información que ha sido almacenada en un sistema informático. Tiene que ver con plantear prácticas para la implementación de sistemas que permitan mitigar los riesgos a los que se exponen dichos sistemas.

¿En qué consiste la seguridad informática? Proteger la integridad de la información no sólo es una cuestión de almacenamiento. Está bien ordenarla y clasificarla, pero no es suficiente. Las amenazas que rondan a los datos tienen estrategias sofisticadas. Los virus informáticos, por ejemplo, son programas dañinos que se instalan en la memoria RAM de los ordenadores del usuario e impiden el normal acceso a la información. También están los denominados hackers o profesionales del saqueo informático, que se encargan de bloquear los sistemas para acceder a bases de datos confidenciales y

usar dicha información para fines desconocidos. Todas las empresas tienen información de carácter confidencial. En mayor o menor medida, las empresas deben poner en marcha sistemas de protección para no verse afectadas por estos sofisticados programas de saqueo, sobre todo cuando la información implica un elemento importante dentro de sus actividades comerciales.

La seguridad informática es un área de la informática que se enfoca en la protección de la infraestructura, computación, información contenida o circulante en un ordenador o red de ordenadores respectivamente. Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, con el fin de mantener un sistema de información seguro y confiable.

Esta consiste en garantizar que el material y los recursos de software se usen únicamente para los propósitos que fueron creados.

Cualquier sistema de seguridad informática que se ponga en marcha en una empresa u organización debe apuntar a tres principios básicos (Sistemas de Gestión la Seguridad de la Información ISO 27001):

1. Confidencialidad: Habla del carácter privado de los datos almacenados en un sistema informático. Es especialmente aplicable cuando los equipos operan físicamente distantes del centro de operaciones de la empresa.

2. Integridad: Se refiere a la validez y la consistencia de la información. Los sistemas deben, por lo tanto, evitar duplicidades y velar por una buena sincronización

3. Disponibilidad: Se trata de la continuidad de acceso a los datos por parte los usuarios. El objetivo es velar por la permanencia del sistema informático. (ISOTools, 2015)

2.3. VENTAJAS DE LA SEGURIDAD INFORMÁTICA

Se encarga de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios, creando buenas medidas de seguridad que eviten daños y problemas que pueden ocasionar intrusos.

Crea barreras de seguridad que no son más que técnicas, aplicaciones y dispositivos de seguridad que, utilizando aplicaciones de protección como matafuegos, antivirus, antiespias y usos de contraseñas, protege la información y los equipos de los usuarios.

Capacita a la población general sobre las nuevas tecnologías y las amenazas que pueden traer.

2.4. DESVENTAJAS DE LA SEGURIDAD INFORMÁTICA

La seguridad absoluta es imposible y la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.

En los equipos más desactualizados, un antivirus realmente efectivo puede ser muy pesado, puede hacerlo más lenta, y ocupar mucho espacio en memoria.

Los requisitos para la creación de contraseñas son cada vez más complejos, la mayoría de los sitios web requieren inicios de sesión y el cambio de contraseñas con frecuencia se ha vuelto obligatorio en muchos lugares de trabajo, recordarlas en ocasiones es muy difícil.

Tal vez la mayor problemática que posea una PyME para encarar ISO- 27001, es lograr convencer a su Dirección de la importancia que reviste todo el proceso de implementación de la misma.

La puesta en funcionamiento de un verdadero SGSI (Sistema de Gestión de la Seguridad de la Información) requiere los controles que a continuación avanzamos.

a. El análisis de riesgo

En la secuencia natural para obtener resultados del análisis de riesgo, es: La identificación, definición, descripción y valoración de los activos. El cálculo de impacto (debilidades, riesgo, grado de exposición, popularidad, criticidad, etc.) que podría ocasionar cualquier problema sobre cada uno de ellos. El riesgo concreto que se posee de producirse determinados hechos. Las salvaguardas que se pueden aplicar para minimizar el riesgo. Conjunto de acciones que pueden realizarse (En lo posible agrupadas por similitud o área). Propuesta de varios cursos de acción posibles (desde el de máxima, intermedios al de mínima).

Finalmente: Elección y Aprobación de un curso de acción por parte de la Dirección. Es decir, el compromiso que asume en virtud de su propia estrategia (Coste/Beneficio/Negocio), para tratar las acciones de ese curso de acción y asumir el riesgo residual que quedará con lo que no esté dispuesto a abordar el máximo nivel de la empresa.

El último paso que trato es el más importante de todos, pues recién a partir de éste, se puede iniciar el conjunto de medidas para minimizar los riesgos, y a su vez para ir solucionando los impactos que SÍ esté dispuesta a abordar la Dirección ("por escrito": Declaración de intenciones).

El discurso final y convincente del análisis de riesgo se logra cuando se han sabido llegar a identificar claramente los "Procesos de negocio", y sobre ellos centrar la máxima atención de seguridad. Esto es lo que da de comer a la empresa, y todo Director necesita dormir tranquilo sobre ellos. Por lo tanto, si esto se ha hecho bien, tenemos grandes posibilidades de haber ganado esta "primer batalla", logrando que a través del curso de la acción que la Dirección haya elegido, podamos empezar nuestro trabajo.

b. Sistema de Gestión de la Seguridad de la Información.

La segunda estrategia para obtener el éxito de nuestra problemática, pasa por el SGSI, el cual como su nombre indica, es un proceso de gestión, cosa que también conoce con alto grado de detalle un director. Lo mejor que podemos hacer es respetar estrictamente lo que propone la norma como PDCA (Plan-Do-Check- Act), y asegurar que desde el primer día el sistema entrará en "rodaje".

Esto implica que se pueden planificar seriamente sus acciones, hitos y evolución. Si se sabe presentar bien el SGSI, éste es otro logro, pues un sistema que "rueda", a través de los ciclos que va sufriendo, puede demostrar con máxima eficiencia su evolución la cual, en términos jerárquicos de la empresa, indica claramente, cómo se emplean los recursos que nos dieron. A través de cuadros de mando, pueden verificar cuantitativamente si se están empleando con corrección los mismos, cosa que, en nuestro trabajo diario en seguridad, se nos suele hacer muy difícil de "poner en el escaparate directivo". Es decir, los planteos que ISO-27001 hace para implementar un SGSI, son discursos netamente convincentes.

Lograr que el empresario decida abordar los costos que implican un análisis de riesgo y la implantación de un sistema de gestión de seguridad de la información, siguiendo la norma ISO - 27001, puede ser una tarea difícil de completar, convirtiéndose estos costos en una desventaja. Al iniciar este conjunto de tareas, no cabe duda que se está sobrecargando el ritmo habitual de trabajo de toda la organización, por lo tanto, se debe ser consciente de que exigirá un esfuerzo adicional.

3. EMPRESAS ATACADAS EN SU SEGURIDAD INFORMÁTICA

Actualmente las empresas más afectadas son las redes sociales como Facebook. Estos ataques tienen el objetivo principal de obtener información de usuarios que utilizan estas redes, información detallada como correos electrónicos, direcciones, números telefónicos. Se dedican a ganar información de usuarios, aunque particularmente recientemente se dio un ataque que impedía a la empresa concluir con las transacciones y compras de productos.

Otros ataques más que ganar información de los usuarios, su objetivo principal es obtener un ingreso monetario o una contratación interna con la empresa, comunicando que ingresó a su sistema y revelando la forma de cómo solucionar el problema.

Muchos de los ataques a bancos públicos y privados o empresas son para realizar transacciones internas, cuentas en países extranjeros.

La empresa Microsoft es la empresa con más ataques, debido a su sistema operativo Windows, con el fin de conseguir apoyo económico o ser contratados por esta empresa.

Los troyanos bancarios son un subconjunto de malware que persigue el robo de datos y cuentas bancarias electrónicos, estos troyanos especialmente bancarios empezaron a desarrollarse y operar en el año 2004. Suelen recoger y actualizar listados de entidades bancarias que se crean o se descargan desde un servidor malicioso, tienen cantidades de listas de cadenas de monitorización de actividad bancaria.

A la hora de interpretar los datos, es necesario aclarar que los equipos que alojan malwares bancarios no necesariamente termina en una situación de fraude, para que un fraude se produzca se han de dar tres circunstancias precedidas:

- Que el equipo esté infectado.

- El espécimen ataca a la entidad bancaria.
- Rellenar formulario con datos personales que solicitan desde sitios sospechosos.

Una de las características con las que funciona un troyano bancario son:

- Registro de teclas pulsadas.
- Captura de formularios.
- Capturas de pantalla y grabación de video.
- Inyección de campos de formulario fraudulentos.
- Inyección de páginas fraudulentas.
- Redirección de páginas bancarias.

Ya con todos estos datos extraídos de los usuarios el infractor puede extraer dinero de las diferentes cuentas bancarias, ejecutando así el robo.

La información robada puede pasar a un tercer equipo, pero algunos antes de hacerlo encriptan la información, evitando así que la información sea vista y descifrada.

Otros ataques consisten en obtener acceso a una cámara web de algún ordenador con el fin de espiar o sentir tener el control sobre esa persona.

Algunos hackers pretenden hacer esto como una forma de chantaje, si encuentra algo comprometedor de esta persona, visualizado por su cámara web. Es una de las prácticas más usadas en el mundo, y algunos aprovechan para ganar grandes sumas de dinero a cambio de no publicar el contenido multimedia.

Lo que se recomienda es tener un buen antivirus o para más seguridad, tapar tu webcam cuando no la estés utilizando.

4. IMPACTO DE LA SEGURIDAD INFORMÁTICA EN EL PERFECCIONAMIENTO DE LA GESTIÓN EMPRESARIAL

Cada día, y cada vez con más frecuencia, leemos, escuchamos, vemos en las noticias incidentes de ciberseguridad. Estos ataques se publican únicamente cuando afectan a grandes empresas, pero eso no significa que, diariamente, no se estén produciendo miles de ataques a miles de usuarios individuales y PYMES.

Las tecnologías de la información y las comunicaciones actuales, permiten a nuestras empresas, innovar, llegar a nuevos mercados, ganar en eficiencia.

Estas ventajas, sin embargo, exponen a nuestra empresa a nuevos retos, protegernos contra hackers, ciberdelincuentes, pérdidas de información, es decir, ciberdelincuencia en general.

Lamentablemente, vivimos en un entorno en el que la pregunta no es si nos va a suceder, sino cuándo nos va a suceder.

La seguridad absoluta, bien sea física o lógica, sabemos que no es un objetivo alcanzable, pero evidentemente, eso no significa que no debamos intentar protegernos al máximo.

Sabiendo que debemos proteger nuestra empresa contra estos ciberdelincuentes, la pregunta es la siguiente, ¿cuánto debo invertir en Seguridad Informática? La respuesta a esta pregunta tampoco es fácil. Evidentemente dependerá de muchos factores.

Para ayudarnos a tomar esta decisión, existen varios informes sobre el impacto financiero de un ciberataque en una PYME.

En el siguiente trabajo se propone un acercamiento al impacto económico de la Gestión de Seguridad Informática en las PYMES de Mendoza, para dar respuesta al desequilibrio existente entre los especialistas de Tecnologías de la Información (TI) y las administraciones de las entidades y empresas, respecto a la necesidad de invertir en "Seguridad" y que tengan en cuenta que las TI son determinantes en la gestión y el negocio de estas, es decir, debemos mirar e interpretar a las empresas y al éxito del negocio a través de la Informática.

Nuestro objetivo es demostrar que el Sistema de Gestión de la Seguridad Informática impacta directamente en la gestión y el negocio de las entidades y que se debe invertir en seguridad proactivamente ya que los costos son superiores cuando no se invierte y sucede un suceso.

5. LA CIBERSEGURIDAD

El término “ciberseguridad” hace alusión a una disciplina de la seguridad que busca proteger la integridad, la disponibilidad y confidencialidad de la información a través de diferentes mecanismos y prácticas. Una pyme, como cualquier otra organización, cuenta con este activo y debe ser protegido. La relación entre las pymes y la ciberseguridad es algo que, si no existe, debería hacerlo. Para que el vínculo cumpla con su objetivo principal, es decir, proteger la información de la organización, se deben combinar técnicas que involucren la gestión, el personal y la tecnología. (American Express, s.f.)

Las nuevas tecnologías alcanzan no sólo a las compañías sino también a los ciberdelincuentes, que transforman vulnerabilidades en riesgos organizacionales. ¿Cómo lograr un cambio de paradigma que permita estar un paso adelante de los ciberatacantes?

Aceleradamente las nuevas tecnologías de la información avanzan, ocupando espacios insospechados y alcanzando una posición preponderante dentro de la estructura organizacional, haciéndose imprescindibles debido al nivel de dependencia que se va adquiriendo. La idea prevaleciente en directivos, funcionarios y especialistas consiste en garantizar que los sistemas instalados brinden los servicios y utilidades que de ellos se espera.

Pero en este escenario prácticamente tranquilo sucede algo inesperado, se produce un evento relevante que compromete la seguridad con consecuencias adversas para el funcionamiento de los sistemas instalados y las operaciones que se realizan: ha ocurrido un incidente de seguridad informática.

A consecuencia del incidente se produce gran tensión pues generalmente nadie imaginaba que pasara algo semejante. La posibilidad de que algún sistema no respondiera según lo previsto no estaba en la mente de ningún miembro de la organización. Por lo que los propietarios buscan que el problema sea resuelto en un plazo breve, tratando de entender lo que pasó e intentando buscar soluciones.

Comienzan a improvisarse diversas alternativas de solución aplicando métodos de prueba y error; se revisan documentos de fabricantes y bibliografía, consultan sitios web y foros en internet se contacta con especialistas en informática.

Cuando se soluciona el incidente se regresa a la normalidad. Sin embargo, la falta de previsión y preparación ha provocado el gasto innecesario de valiosos recursos de todo tipo, al trabajar al mismo tiempo demasiadas personas sobre un mismo tema o con la insuficiente preparación para la solución del incidente, la pérdida de información valiosa sobre las causas y efectos del incidente, y el surgimiento de usuarios insatisfechos.

Al mismo tiempo este avance de las tecnologías de la información y su influencia en casi todas las áreas de la vida social han propiciado una serie de comportamientos ilícitos o no autorizados que de manera general pudieran agruparse en aquellos dirigidos contra las redes y sistemas informáticos, por ejemplo ataques a servidores, desfiguración de sitios web, denegación de servicio, creación introducción y propagación de códigos maliciosos, envío masivo de correos no deseados (spam) y los ejecutados con la utilización de los sistemas y redes como medios para cometer ilegalidades como el fraude, robo espionaje, pornografía, actividad económica ilícita entre otros.

El problema ya existe y avanza a una velocidad que nos obliga a hacer sonar las necesarias señales de alarma.

En las últimas décadas, y de forma exponencialmente acelerada, el desarrollo de la sociedad y de la economía globalizada ha hecho que dependamos absolutamente de la informática y de las telecomunicaciones. La realidad es que las empresas, las grandes, pero también las medianas y pequeñas, dependen casi al 100% del correcto funcionamiento de aplicaciones informáticas y de sistemas de telecomunicaciones para sus actividades. (Navarrete, 2015)

Este nuevo escenario económico y social, supone enormes ventajas y posibilidades en el desarrollo económico. El mundo globalizado se hace accesible para todos. Los emprendedores tienen a su alcance cualquier posibilidad de intercambio comercial y, todos tenemos acceso a una gran cantidad de información.

El panorama ha hecho que aparezcan nuevos riesgos para las empresas, unos de carácter técnico, pero, los más preocupantes son los intencionados. Las consecuencias de estas amenazas suponen para las empresas afectadas importantes daños económicos, graves problemas en la reputación,

incumplimientos de la obligación de custodiar datos de carácter personal, y la peor de todas, es la sensación de impotencia e inseguridad.

La conectividad digital desempeña un papel fundamental para desbloquear la innovación y la prosperidad en todo el mundo, pero el aumento de la amenaza cibernética representa un obstáculo importante para nuestro camino continuo y colectivo hacia el progreso.

Se prevé que la pérdida económica debida al delito cibernético alcanzará los 3 billones de dólares para 2020, y el 74% de las empresas del mundo pueden esperar ser pirateadas el próximo año. Los esfuerzos actuales para contener el delito cibernético, si bien son importantes, siguen siendo en gran medida insuficientes a medida que el impacto global de las amenazas cibernéticas continúa creciendo.

Las pequeñas empresas son el alma de la economía global. Proporcionan todo tipo de servicios esenciales: a individuos, al gobierno, a organizaciones más grandes y entre sí. Para las pequeñas empresas, cuando se trata de delitos informáticos, los riesgos son grandes. Las estadísticas muestran que el 58% de los delitos cibernéticos se dirige a pequeñas empresas, con un costo global de 600 mil millones de dólares en 2018.

Estas cifras pueden parecer sorprendentes, en gran parte debido al hecho de que la mayoría de la cobertura de ciberataques en los medios de comunicación se centra en las grandes empresas, lo que afecta a un gran número de clientes. Lo que muchas personas no saben, sin embargo, es que las pequeñas empresas suelen ser la forma más fácil de llegar a las grandes empresas. Los atacantes, por ejemplo, obtendrán acceso a las credenciales de una pequeña empresa en la cadena de suministro de una gran empresa como un camino hacia la compañía más grande, y la infracción a menudo pasará desapercibida hasta después de que se haya llevado a cabo el ataque. Ya sea el objetivo principal de un ataque o una ruta hacia una organización más grande, una pequeña empresa puede verse afectada por un ataque cibernético. La recuperación de un ataque es difícil en el mejor de los casos; en el peor de los casos, podría significar cerrar la pyme. Ignorar el riesgo cibernético no es una opción. La prevención es, con mucho, el mejor curso de acción.

Según un nuevo estudio de Mimecast, la compañía internacional especializada en administración de correo electrónico, informó que hoy por hoy nos podemos encontrar un enlace malicioso por cada 50 emails que ingresan en nuestra bandeja. En su investigación, en base a más de 142 millones de correos electrónicos que atravesaron los filtros de seguridad de correo electrónico de empresas de todo el mundo en el último trimestre, se descubrieron 203.000 enlaces engañosos en más de 10 millones de correos electrónicos.

Por otro lado, Mimecast dio a conocer que más de 19 millones de correos no deseados, 13.176 correos electrónicos que contienen tipos de archivos peligrosos y 15.656 archivos adjuntos de malware, fueron omitidos por los proveedores de seguridad. Esto deja a las organizaciones en riesgo de una violación de datos y pérdidas financieras.

Estos son ataques difíciles de identificar sin capacidades de seguridad especializadas, y estas pruebas muestran que los sistemas comúnmente utilizados no están haciendo un buen trabajo para atraparlos.

Pero ¿por dónde empezar? Hay una gran cantidad de consejos disponibles sobre qué hacer, pero a menudo es confuso y, a veces, contradictorio. La gran mayoría de las pequeñas empresas carecen de los conocimientos técnicos necesarios para prevenir los ataques cibernéticos y no cuentan con los recursos financieros para invertir en seguridad a nivel empresarial. Los propietarios de pequeñas empresas pueden preguntarse: "¿Por qué alguien querría atacarme?" O quizás prefieran concentrarse en generar ingresos. Pero la verdad es que las pequeñas empresas no solo tienen información valiosa, sino que también pueden actuar como un trampolín hacia organizaciones más grandes a las que los piratas informáticos pueden llegar a dirigirse.

La tendencia general es pensar que los cibercriminales atacan principalmente a las grandes compañías. Esto es un error: los principales destinatarios de estos ataques son las pequeñas y medianas empresas.

Estos delitos no siempre llegan a los titulares de los medios de comunicación, como sí lo hacen los ataques que golpean a naciones o a grandes empresas: el 44% de las PyMEs han sido víctimas de ciberataques. Y lo que es peor: el 60% de éstas cierra seis meses después del ataque.

Las ciberamenazas actuales son más sofisticadas que nunca, lo que permite que los grandes delincuentes ataquen a empresas de pequeñas ciudades. Los criminales cibernéticos pueden ser hacktivistas con un programa social que buscan interrumpir sus operaciones diarias o grupos criminales organizados que quieren obtener datos personales o financieros de sus clientes.

Las PyMEs suelen dedicar menos tiempo y dinero a la seguridad de red que las empresas más grandes. Eso hace que sean blancos fáciles para los criminales cibernéticos. Pero aun cuando las empresas no son un blanco específico, los ataques automatizados analizan internet de manera constante en busca de datos vulnerables y computadoras con poca protección que se puedan usar como recurso.

Robar a muchas pequeñas empresas en lugar de a una única compañía grande mantiene la atención de los medios y del Gobierno alejada de los atacantes y, aun así, les permite obtener grandes ganancias de varios blancos. Las PyMEs suelen ser el eslabón más débil de un ataque de cadena de confianza en el que los atacantes acechan la seguridad de pequeños blancos de la cadena de suministro con escasa protección para llegar a los grandes socios comerciales.

Incluso las pequeñas y medianas organizaciones almacenan datos valiosos que significan dinero para los cibercriminales, quienes pueden apuntar a segmentos verticales del mercado que les permitan aprovechar vulnerabilidades comunes y, a su vez, lograr grandes ganancias a partir de varias víctimas.

A pesar de las amenazas de rápida evolución en la avenida principal, muchas PyMEs y organismos locales aún se concentran en estrategias de defensa heredada, como un firewall sencillo. El primer paso es actualizar a una protección con un firewall de última generación (NGFW) o una

aplicación de gestión unificada de amenazas (UTM) que combine todas las defensas necesarias en un único dispositivo fácil de gestionar y económico.

El segundo paso es determinar los dispositivos sofisticados de seguridad que tienen controles para descubrir diferentes partes de un ataque, pero los atacantes, aún así, pueden encontrar formas de evadir las defensas. La defensa profunda cierra las brechas y quiebra la kill chain del atacante. La teoría de fondo de la kill chain es que cuantas más capas (o eslabones) de defensa crea para evitar diferentes tipos de ataques, más se perfecciona su protección. Cada eslabón representa una parte de la metodología del atacante, pero también representa una oportunidad para que implemente una defensa.

Por último, debe verse la amenaza para poder defenderse. Las pequeñas empresas sufren vulneraciones todos los días, pero solo un tercio admite desconocer si fueron atacadas o no. Tanto para organizaciones pequeñas como grandes, a las empresas les toma un promedio de 80 días notar si fueron vulneradas. A esa altura, el daño ya está hecho. Estas vulneraciones no se notan porque nos inundamos en un océano de datos. Ya que nunca puede tener una defensa perfecta, el tercer paso crítico en su estrategia de seguridad es implementar herramientas de detección y respuesta que le ayuden a ver y controlar los incidentes que superan sus defensas. Necesita una herramienta que reúna los datos de todos los controles de seguridad y correlacione diferentes interruptores de seguridad en un único incidente de forma tal que no pierda los indicios de un ataque más sofisticado de varios vectores.

Bien el cierre del capítulo

CAPÍTULO II: GESTIÓN DE RIESGOS E IMPACTO ECONÓMICO

En el presente capítulo, se desarrollará un análisis y gestión de riesgos informáticos con el objeto de comprender las amenazas y vulnerabilidades a las cuales se encuentran expuestas las Pymes y así poder disminuir, aceptar, evitar o transferir dicho riesgo. Además, se expone la percepción de este riesgo, la falta de concientización como motivo principal, así como también el impacto económico que genera el hecho de invertir por parte de las empresas en ciberseguridad.

1. ANÁLISIS, EVALUACIÓN Y GESTIÓN DE RIESGOS

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir.

Toda empresa cuenta, o al menos debería contar, con un área de gestión del riesgo. Este equipo debe ser capaz de determinar, analizar, valorar y clasificar el riesgo en la seguridad informática.

Una vez procesada esa información se podrá conocer con certeza cuáles son esos datos cuya vulneración provocaría un mayor impacto. Conocer y poder acotar este área de información es la única forma de poder llevar un control sobre ella, y para lograrlo es necesario: (Power Data, 2013)

- Implementar mecanismos de control de la información: eligiendo el método adecuado según las necesidades reales de la empresa.
- Gestionar esos mecanismos: apoyándose en una regulación, como es el marco normativo; ya que sólo así se puede acotar el riesgo y tenerlo bajo control, evitando fugas.

Hay que tener en cuenta que la gestión del riesgo no debe plantearse como una acción puntual, sino como un proceso que requiere adaptabilidad para garantizar la corrección de conductas que puedan poner en peligro la integridad de los datos y, al mismo tiempo, la imagen de la compañía. En definitiva, el propósito de un área de control de riesgo es, no sólo identificar y tratar la información, sino también hacer los ajustes convenientes para facilitar la toma de decisiones en este sentido. Y no hay que confundir su misión con la de seguridad informática, que es responsabilidad del Departamento de Informática, aunque ambas estén íntimamente relacionadas; ya que mientras que estos últimos protegen la estructura de la información y lo hacen mediante antivirus, firewalls, etc., el área de control de riesgo por lo que vela es por la integridad del contenido, de los datos en sí.

¿Se requiere mucho tiempo y personal especializado para evaluar los riesgos? En el contexto de la seguridad, una medida a tener presente en las Pymes se relaciona con la identificación y tratamiento

de riesgos asociados a la información, al igual que en las grandes organizaciones. En otras palabras, se debe realizar una evaluación de riesgos, que si bien, puede considerarse un desafío, puede ser resuelto a través del uso de algún método o metodología.

Por ejemplo, se han desarrollado opciones específicas para organizaciones más pequeñas, como es el caso de OCTAVE-S, pensado para empresas de 100 o menos personas. Todas las versiones cuentan con documentación disponible de forma gratuita y emplean un enfoque autodirigido, por lo que la puede llevar a cabo por personal sin especialización en evaluación de riesgos.

¿Qué pasos puedo seguir para atender un incidente en una Pyme? Existen opciones enfocadas completamente en Pymes. Una de ellas es el método de los Seis Pasos desarrollado por SANS Institute, ajustado a las pequeñas y medianas empresas. El primer paso consiste en la preparación y se refiere a la definición previa de las acciones a seguir en caso de que se presente un incidente. La segunda etapa es la identificación, donde distintos factores pueden dar la pauta para la identificación de un potencial incidente (por ejemplo, el bajo desempeño de los sistemas y de la red), por lo que el personal de la Pyme puede ser un agente de identificación.

En función de las instrucciones generadas, se llega a la fase de contención, en la que como su nombre lo indica, se busca controlar la actividad anormal a través de la realización de los cambios necesarios en la configuración de los sistemas o red. Además, incluye otras actividades como la generación de respaldos.

La etapa posterior es la erradicación, que tiene como propósito remover o eliminar las causas del incidente, así como las consecuencias que haya generado. De esta forma, se puede llegar de forma gradual a la fase de recuperación y finalmente a las lecciones aprendidas.

¿Los planes de continuidad solo se aplican en grandes organizaciones? Otros planes de gestión de la seguridad también pueden ser aplicados en las Pymes, principalmente porque siguiendo los mismos pasos y requisitos para realizar actividades como un análisis de impacto al negocio se pueden tener resultados aceptables dentro de las pequeñas y medianas empresas, con la principal diferencia de que el alcance se reduce considerablemente.

Esto se debe principalmente al hecho de que la complejidad entre procesos, así como las interacciones entre los mismos, es menor con relación a empresas de mayor tamaño. Por lo tanto, es muy probable que la cantidad de activos disminuya, acotando la recuperación y/o la continuidad de las operaciones, así como el tiempo dedicado al desarrollo y aplicación de estas medidas. (Mendoza, 2015)

2. IMPACTO EN LA ACTIVIDAD ECONÓMICA DE UNA PYME

Existe una débil apuesta de las pymes por la seguridad informática. La inversión de las empresas con menos de 250 empleados en ciberseguridad es inversamente proporcional al riesgo que tienen de ser atacadas. La mayoría de las grandes multinacionales son conscientes de los riesgos que asumen al manejar su información a través de ordenadores, móviles o tabletas y lo reflejan con cada vez mayores

inversiones en ciberseguridad. Sin embargo, la percepción de este peligro en empresas más pequeñas es reducida y son pocas las que tienen entre su lista de prioridades proteger sus sistemas. (Cortéz, 2017)

Entre muchas pymes existe la falsa creencia de que, por ser pequeñas, no están en el punto de mira de los ciberataques. Es normal que esto suceda porque piensan en el delincuente informático como una persona de carne y hueso a la que no le interesan los datos de una pequeña empresa. Piensan que no son objetivos de los *hackers*, pero la realidad es que normalmente estos no son personas atacando ordenadores, sino máquinas atacando a máquinas; es totalmente indiscriminado. Sin embargo, en muchas ocasiones estos ataques informáticos son de máquina a máquina, es decir, son indiscriminados y lo único que puede salvarte de ellos es la prevención y la protección. Para evitar riesgos, se recomienda contar con protocolos y planes de seguridad.

La pyme no suele tropezar dos veces con la misma piedra. Muchas han aprendido la lección después de haber sufrido un ataque o tras haber visto cómo otras a su alrededor lo sufrían.

La falta de concientización es el motivo principal por el que las compañías no destinan

recursos a prevenir ataques, pero no el único. A veces, sencillamente, no los tienen. El ecosistema de pymes dispone, por lo general, de medios reducidos y no puede dedicar tiempo

y esfuerzos a esta tarea.

Respecto al coste, en apariencia inasumible para los comercios más modestos, se considera que no es necesaria una gran inversión para estar protegido. A veces, una auditoría pequeña les puede dar unos pasos a seguir y le pueden bastar. No todas las empresas tienen las mismas necesidades.

Los virus aprovechan cualquier vía de entrada para colarse en un sistema.

Imagen Nº X: Robo de información

Fuente: Cortéz, J. (12 de Junio de 2017). *https://retina.elpais.com*. Obtenido de https://retina.elpais.com/retina/2017/06/01/tendencias/1496307759_889133.html

La ventaja fundamental de estas empresas frente a las grandes es su velocidad de reacción. Una oficina con cinco empleados no tiene problemas para cortar la red diez minutos e instalar la última actualización de un sistema operativo, un proceso que en algunas multinacionales es tan tedioso como ineficiente. Normalmente, realizan análisis de vulnerabilidad de los sistemas que potencialmente van a cubrir para buscar sus deficiencias antes de centrarse en la prevención.

Las soluciones en la nube evitan en parte el problema de la seguridad y garantizan una mayor disponibilidad, pero algunas empresas tienen reparos con alojar su información en un servidor que no les pertenece.

La lucha contra los ciberdelitos debe partir de una nueva cooperación entre sociedad civil y administración, con la necesaria presencia de todos los actores implicados: las empresas, los especialistas, las universidades.

Hace falta voluntad, especialistas y recursos económicos concretos e importantes. Las empresas así lo demandan. Aunque no queramos mirar, la realidad sigue corriendo a velocidad de gigas.

Todas las empresas son conscientes de que la Gestión de la Seguridad Informática es un asunto prioritario. Pero, ¿cómo pueden cuantificar el valor de negocio que aporta una red segura? ¿cómo pueden evaluar y justificar la inversión en productos de seguridad de red, como firewalls de próxima generación,

sistemas de prevención de intrusiones y dispositivos de gestión unificada de amenazas? No existe una fórmula exacta ni una herramienta para calcular el "costo de los ataques".

Los daños causados por los ataques, independientemente de la fuente, se dividen en dos categorías principales: la filtración de datos y la pérdida de servicio.

La filtración de datos siempre da lugar a noticias sensacionalistas, pues la extracción de información corporativa confidencial va a parar a manos de criminales o competidores. Los daños causados por las filtraciones de datos son visibles y muy graves. Pueden ser daños de carácter financiero (pérdida de ingresos, costos legales y normativos, costes derivados de procesos judiciales y multas), costes 'blandos' (pérdida de la confianza y fidelidad de los clientes) y pérdida de competitividad (como resultado de la pérdida de propiedad intelectual).

Después de sufrir filtraciones de información, las empresas se gastan cantidades enormes de tiempo y dinero en tareas de detección y corrección técnica, en la identificación y el bloqueo de ataques, así como en la valoración de los daños causados y en la aplicación de medidas correctivas. Además, los casos de filtración de datos generan una publicidad negativa que dura mucho más que el ataque en sí.

Los ataques por denegación de servicio resultan en la degradación o en la total inoperatividad de los sistemas informáticos, tanto de estaciones de trabajo como de servidores web, de aplicaciones o de bases de datos. Pero los daños colaterales en el ámbito financiero de estos daños también pueden ser catastróficos. El comercio se ralentiza o se detiene por completo, lo cual repercute directamente en los ingresos. Los procesos cotidianos se interrumpen o los empleados no pueden desempeñar sus tareas porque la red está fuera de servicio.

En realidad, no existe un modelo de costos universal aplicable a todos los casos. Lo que sí queda claro lo costosos que resultan estos ataques para los resultados, la reputación y la competitividad de las empresas.

Con el siguiente gráfico vemos cómo diseñar un plan de seguridad de la información partiendo de nuestros objetivos de negocio a nivel estratégico, definiendo a partir de estos los objetivos de seguridad. (INCIPE, Instituto Nacional de Ciberseguridad, 2015)

Gráfico N° I: Riesgos y objetivos de seguridad.

Cada Pyme tiene sus riesgos y sus objetivos de seguridad, por lo tanto cada una necesitará sus propias métricas vinculadas a sus estrategias de negocio. A modo de ejemplo estos podrían ser algunos de los objetivos de seguridad de tu Pyme:

- Definir el plan de seguridad teniendo como referencia un análisis de riesgos sobre los activos de información.
- Establecer una organización de seguridad para administrar la seguridad de la entidad.
- Establecer políticas y procedimientos de seguridad.
- Optimizar las inversiones en seguridad de la información al ejecutar planes de acción que apoyen la consecución de los objetivos de la organización.
- Evaluar la situación actual de seguridad de la empresa respecto a un estándar de buenas prácticas.
- Conocer y planificar las inversiones y costos necesarios para alcanzar el nivel de seguridad adecuado.
- Mejorar los niveles de Seguridad de la Información al fomentar la adopción de una cultura de seguridad de la información a todos los niveles.

Siguiendo adelante en el gráfico los procesos necesarios serían, entre otros:

- Identificar los activos de información críticos para el proceso de negocio de producción, contabilidad o gestión de personal.
- Realizar un análisis de riesgos bajo una metodología de riesgos identificando los riesgos y amenazas en cada uno de los activos de información. Asegurarse de que los riesgos son efectivamente comprendidos y controlados.
- Identificar el nivel de seguridad existente en los sistemas, servicios, aplicaciones e infraestructura (incidentes, actualizaciones, etc.).
- Definir y planificar los planes de acción a realizar (a corto, mediano y largo plazo) teniendo como referencia la diferencia existente entre el nivel de seguridad actual y el nivel de seguridad objetivo.
- Implementar mecanismos de seguridad en servidores, estaciones de trabajo y dispositivos de red para reducir el tiempo de inactividad y los incidentes.
- Formar a los empleados para el uso seguro de las TIC. Asegurarse de que todos los usuarios entienden las responsabilidades de seguridad.

Pero no basta con saber cuáles son los riesgos y dónde están, sino también poder determinar el valor de los activos amenazados y el tiempo que será necesario invertir en reparar daños o prevenirlos. Con el objetivo de mitigar los riesgos la empresa establece controles, no exclusivamente técnicos, que se implementan según el plan de seguridad.

CAPÍTULO III: APLICACIÓN PRÁCTICA

Para realizar el trabajo de campo se tuvo en cuenta como universo los datos del Ministerio de la Producción de la Nación, donde Mendoza registra un total de 34.665 pymes, de las que se tomaron 42 empresas como muestra para inferir en el desarrollo de la investigación, que surge según la aplicación de un cálculo estadístico a través de un margen de error del 10%, nivel de confianza del 80%, y nivel de heterogeneidad del 60%.

De este modo, se han tenido en cuenta para el análisis de la investigación 28 PyMes (muestra) radicadas en el gran Mendoza, dentro del cual se encuestaron diferentes empresas como: Verdini, Andrés Merino Pinturerías, Proal, Ferretería ALEO, Lagus, Cocucci, etc. para obtener información, y así analizar, evaluar y confirmar la hipótesis de la investigación.

Se presentan los resultados estadísticos obtenidos de las encuestas realizadas en el primer semestre del año 2019. De modo que se diseñó una encuesta con preguntas en su mayoría cerradas y algunas abiertas para relevar información necesaria para evaluar las dificultades que se producen cuando se desean implementar acciones para proteger la integridad y la privacidad de la información El instrumento se probó en una población limitada para asegurar su calidad y claridad. La información se almacenó de tal manera de poder analizar y obtener los datos buscados.

Cabe señalar que las organizaciones encuestadas han omitido contestar algunas preguntas de la encuesta, en algunos casos por no ser aplicables y en otros por criterios propios de confidencialidad, que se ha respetado. También en muchos casos, se ha reservado el nombre de la empresa que completó la encuesta a pedido de esta última.

A continuación, presentamos los resultados obtenidos.

1. UBICACIÓN DEL SISTEMA CONTABLE

Tabla N°II: Ubicación del S.I.C.

UBICACIÓN DEL S.I.C.	TOTAL	PORCENTAJES
Propio de la Empresa	18	64%
Estudio Contable	7	25%
Ambos	3	11%
TOTAL GENERAL	28	100%

Gráfico N°II: Sistema de Información Contable

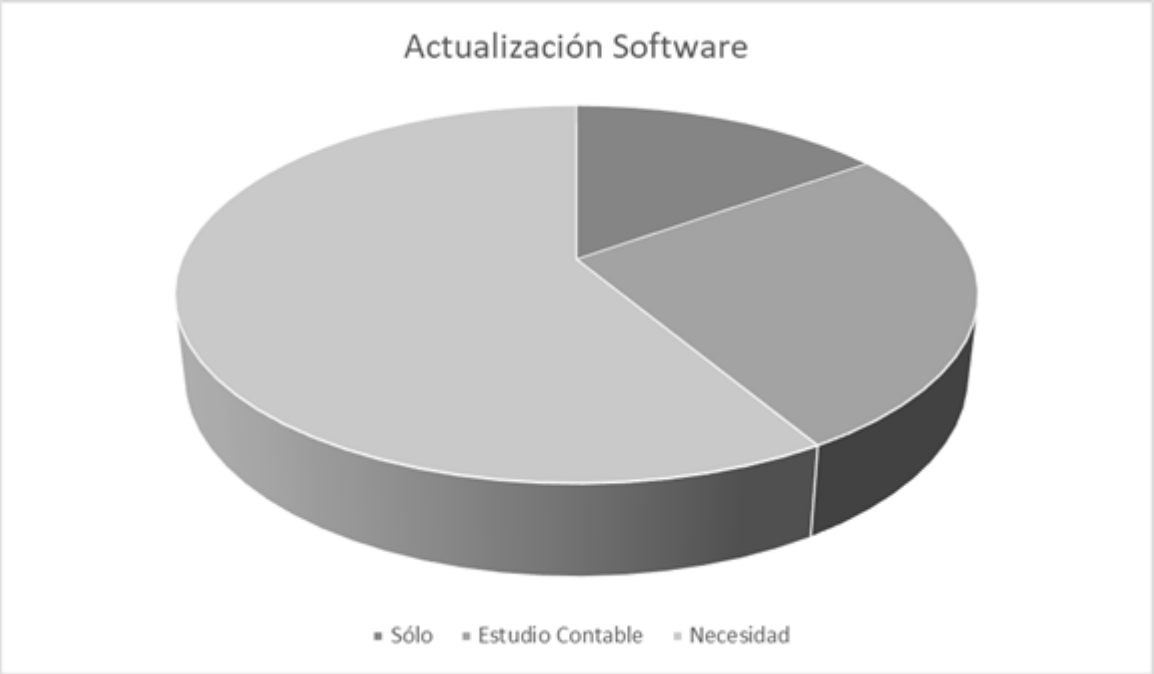
De la totalidad de los entes consultados, el 100% posee un S.I.C. De este número se desprende que el 64% lo posee implementado en su propia empresa, el 25% en un estudio contable, y el 11% en ambos. Vale decir que hoy en día todas las compañías sean pequeñas, medianas y grandes, cuentan con un S.I.C.

2. CUÁNDO REALIZAN UNA ACTUALIZACIÓN DEL SOFTWARE

Tabla N°III: Actualización del Software

ACTUALIZACIÓN DEL SOFTWARE	TOTAL	PORCENTAJES
Se actualiza sólo	4	15%
Lo realiza el Estudio Contable	7	26%
Cuando surge la necesidad	16	59%
	27	100%

Gráfico N°III: Actualización del Software



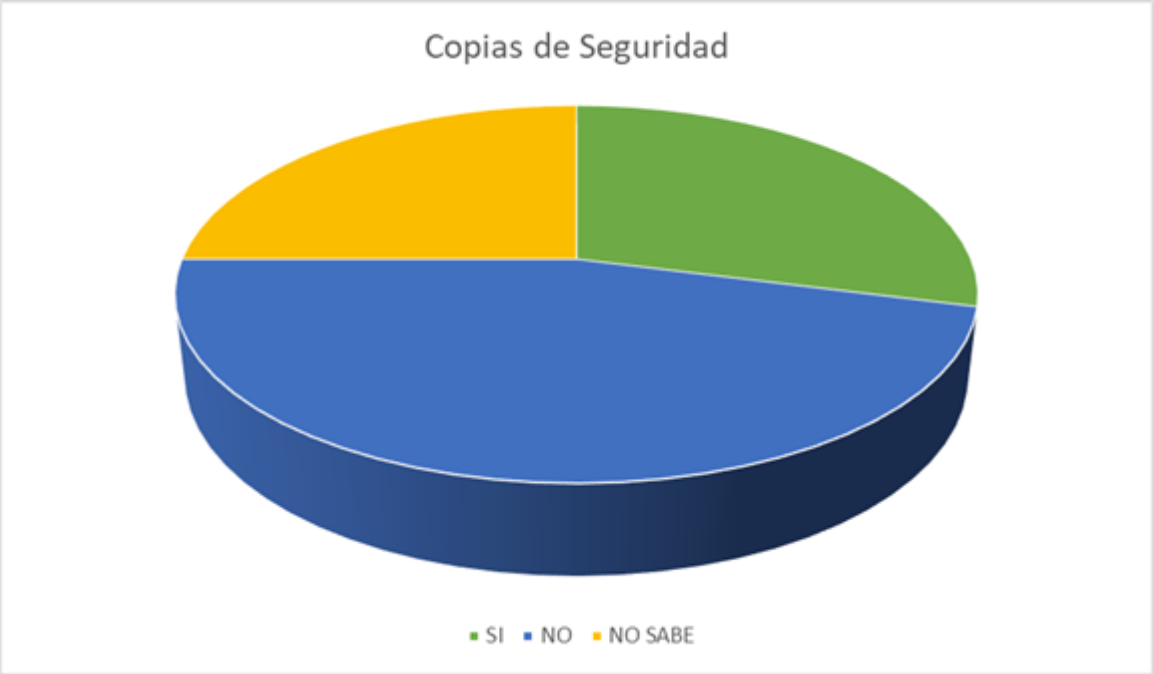
Observamos que el 59% de las PyMES consultadas sólo deciden implementar una actualización ante una necesidad, reaccionan a las situaciones que se les van planteando en lugar de prevenirlas. En base a lo que nos comentaron el motivo es que prefieren gastar en otro tipo de cosas, desconociendo el impacto económico que les puede producir tener un software desactualizado y vulnerable. Todos los equipos deben estar perfectamente actualizados con la última versión de Windows. Este es uno de los factores que se pueden analizar para asegurar que el software se actualice regularmente para mejorar la seguridad informática.

3. REALIZAN COPIAS DE SEGURIDAD PERIÓDICAMENTE

Tabla N°IV: Copias de Seguridad

COPIAS DE SEGURIDAD	TOTAL	PORCENTAJES
SÍ	8	29%
NO	13	46%
No sabe, es responsabilidad del Estudio Contable	7	25%
	28	100%

Gráfico N°IV: Copias de Seguridad



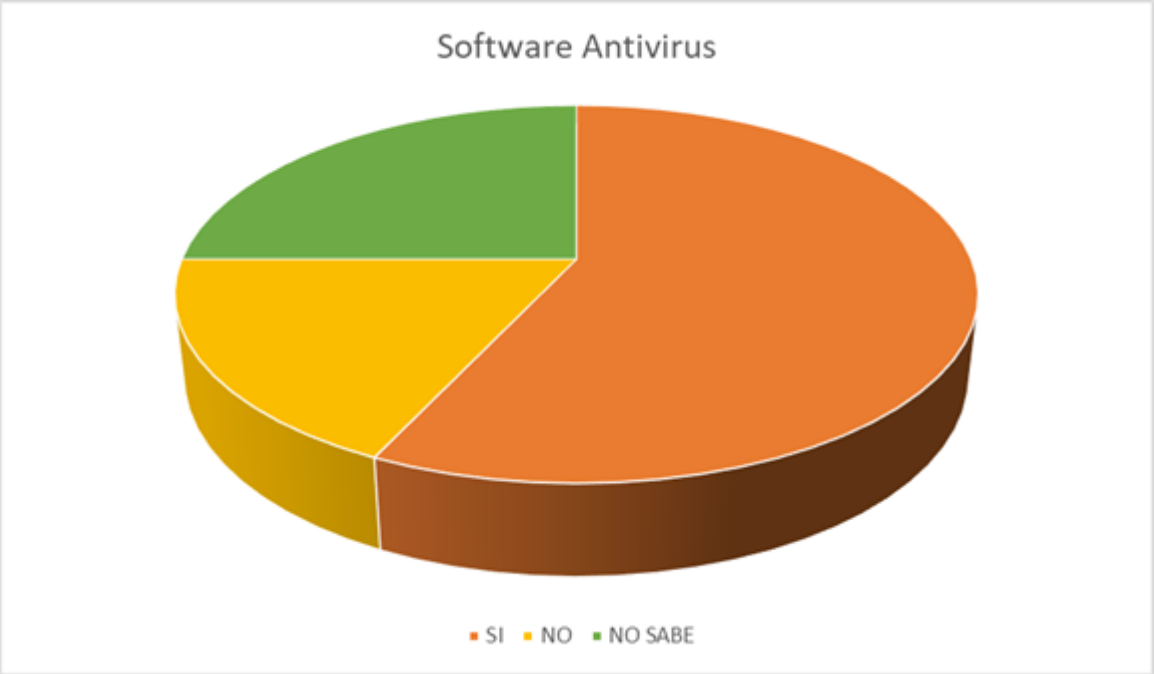
Como podemos observar en el gráfico, realizar copias de seguridad no es una prioridad para las PyMES, ignorando la posibilidad de la pérdida de información, ya sea por un virus, por una falla en el hardware; entre otras, que traiga como consecuencia la no recuperación de datos. Esto sumado a lo que vimos en la tabla N°2 en la que el 59% de las PyMES no prioriza la actualización de su software, genera que la información quede expuesta a ser robada o perdida.

4. TIENE INSTALADO UN SOFTWARE ANTIVIRUS ACTUALIZADO

Tabla N°V: Software Antivirus

SOFTWARE ANTIVIRUS	TOTAL	PORCENTAJES
SI	16	57%
NO	5	18%
No sabe, es responsabilidad del Estudio Contable	7	25%
	28	100%

Gráfico N°V: Software Antivirus



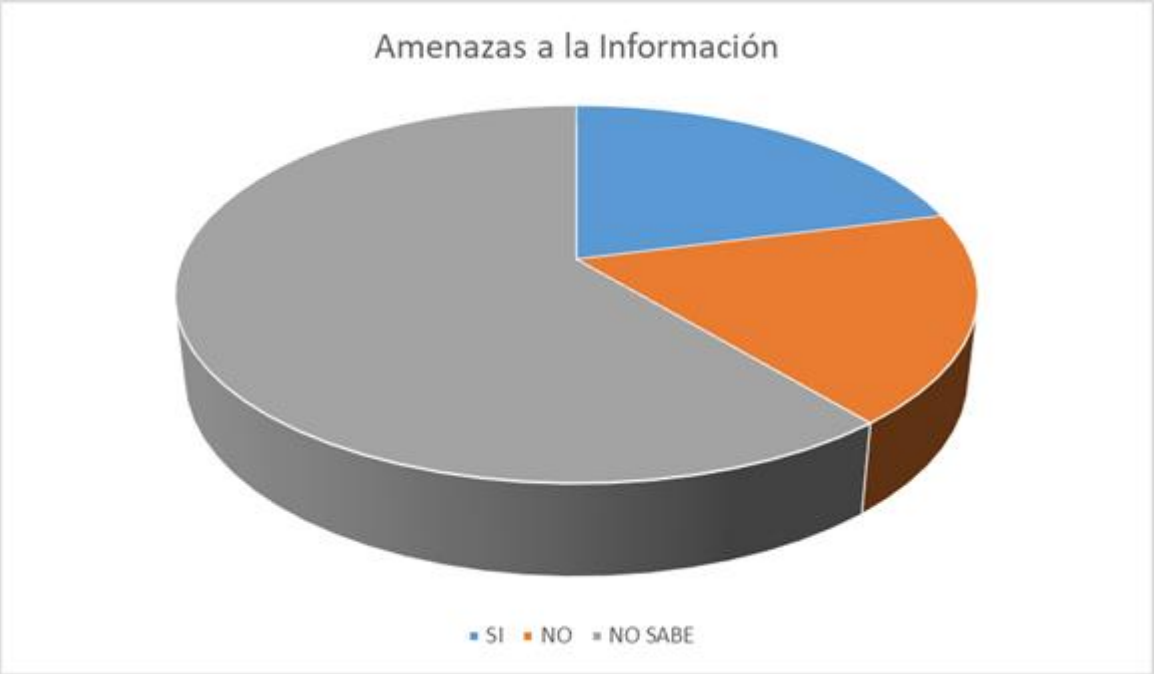
En este punto, si se puede observar una medida de seguridad informática, ya que del total de PyMES consultadas el 57%, más de la mitad, tiene un software antivirus. Es esencial que cada entidad cuente con un software antivirus actualizado de manera que los virus puedan mantenerse lejos. Un antivirus es uno de esos factores que necesita ser actualizado regularmente, lo que permite que sea extremadamente seguro.

5. CONOCE LAS AMENAZAS A LAS CUALES SE ENCUENTRAN EXPUESTOS LOS DATOS INFORMÁTICOS DE SU PYME.

Tabla N°VI: Conocimiento de las amenazas a la información

AMENAZAS A LA INFORMACIÓN		
SI	6	21%
NO	5	18%
NO SABE	17	61%
	28	100%

Gráfico N°VI: Conocimiento de las amenazas a la información



En este gráfico se ve claramente cómo el 61% de empresas consultadas desconoce totalmente las amenazas que rondan a la información de ellas. En estas amenazas es donde existe el riesgo; es por eso que resulta necesario poder gestionar ese riesgo instalando sistemas de control que minimicen tanto la probabilidad de que ocurran sucesos negativos como su severidad (pérdida económica que supondría para el emprendedor).

6. ESTARÍA DISPUESTO A INVERTIR EN SEGURIDAD INFORMÁTICA

Tabla N°VII: Inversión en seguridad informática

INVERSIÓN EN SEGURIDAD INFORMÁTICA	TOTAL	PORCENTAJES
SI	8	29%
NO ME PARECE NECESARIO	4	14%
NO TENGO LA CAPACIDAD FINANCIERA	16	57%
	28	100%

Gráfico N°VII: Inversión en seguridad informática

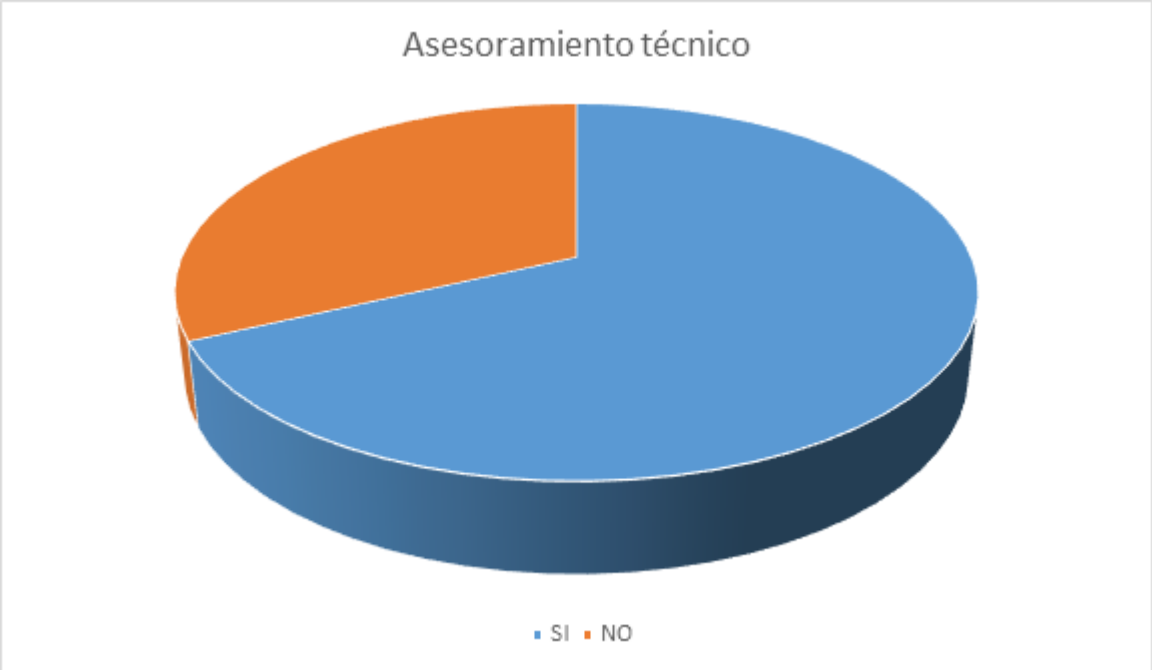
Podemos observar que el 57% de las empresas entrevistadas respondieron que no cuenta con la capacidad financiera para invertir en seguridad informática, quedando nuevamente expuesto que prefieren correr riesgos, sin tener conocimientos de lo costoso que puede resultar la pérdida de la información, sobre la opción de prevenir estos costos.

7. TIENE ASESORAMIENTO TÉCNICO PARA LA GESTIÓN DE LA INFORMACIÓN

Tabla N°VIII: Asesoramiento técnico

ASESORAMIENTO TÉCNICO	TOTAL	PORCENTAJES
SI	19	68%
NO	9	32%
	28	100%

Gráfico N°VIII: Asesoramiento técnico



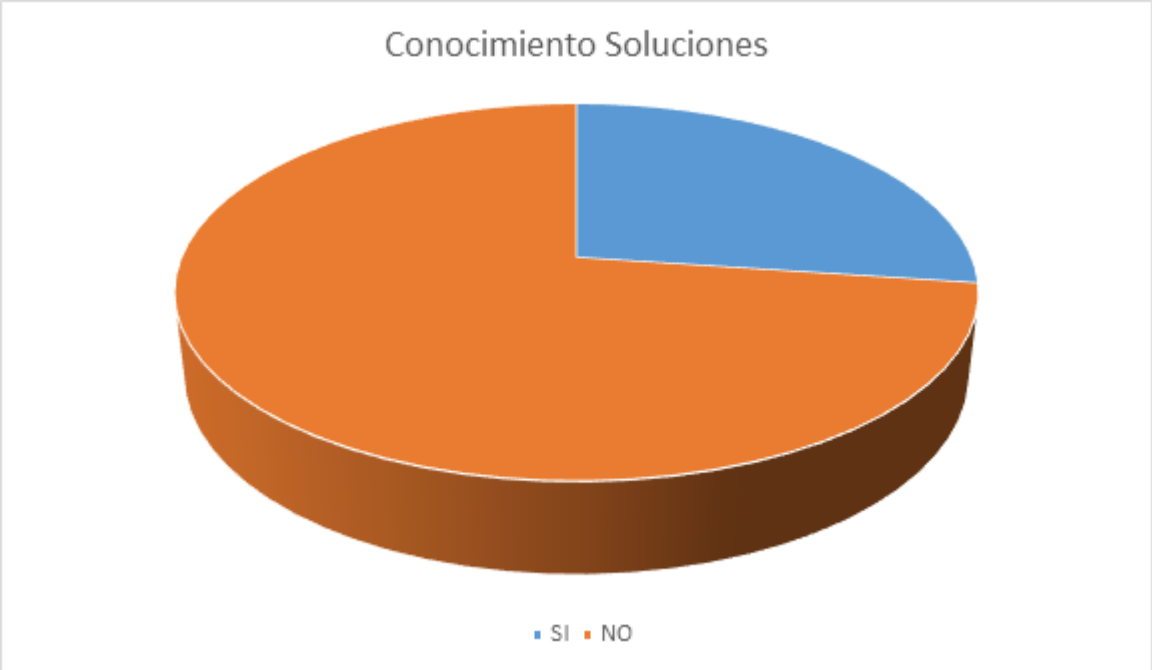
A través del siguiente gráfico se observa que la gran mayoría, el 68%, opta por asesorarse en cuanto a la gestión de la información, siendo esto positivo en lo que respecta a la búsqueda de soluciones para tener la información completa y oportuna.

8. CONOCE LAS SOLUCIONES SOBRE SEGURIDAD INFORMÁTICA QUE OFRECE EL MERCADO DE SOFTWARE.

Tabla N°IX: Conocimiento de soluciones sobre seguridad informática

CONOCIEMIENTO SOLUCIONES	TOTAL	PORCENTAJES
SI	7	25%
NO	21	75%
	28	100%

Gráfico N°IX: Conocimiento de soluciones sobre seguridad informática



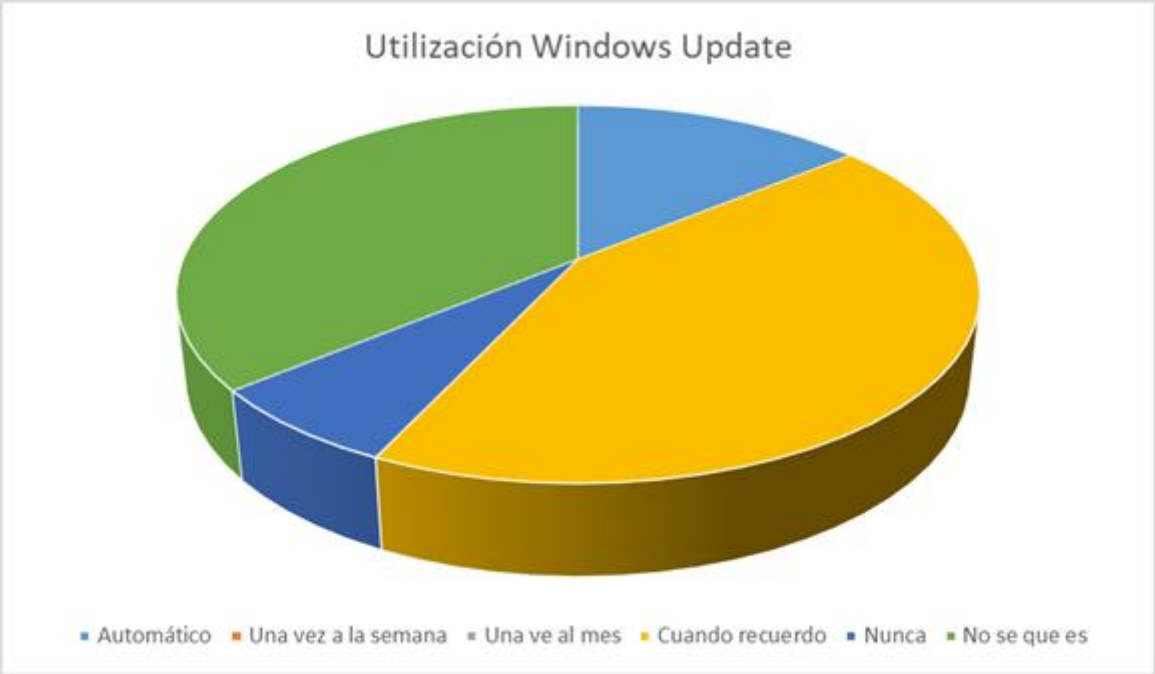
De esta manera se observa cómo un 75% de estas Pymes encuestadas tiene conocimiento respecto de soluciones sobre seguridad informática, lo que permite de alguna manera que ante cualquier amenaza o riesgo al cual se enfrente dicha entidad; la misma pueda adoptar distintos caminos que puedan llevar a la continuidad del emprendimiento llevado a cabo.

9. ¿CON QUÉ FRECUENCIA UTILIZAS WINDOWS UPDATE?

Tabla N°X: Utilización Windows Update

UTILIZACIÓN WINDOWS UPDATE	TOTAL	PORCENTAJES
Se actualiza automaticamente	4	14%
Al menos una vez a la semana	0	0%
Al menos una vez al mes	0	0%
De vez en cuando, si recuerdo	12	43%
Nunca	2	7%
No sé qué es Windows Update	10	36%
	28	100%

Gráfico N°X: Utilización Windows Update



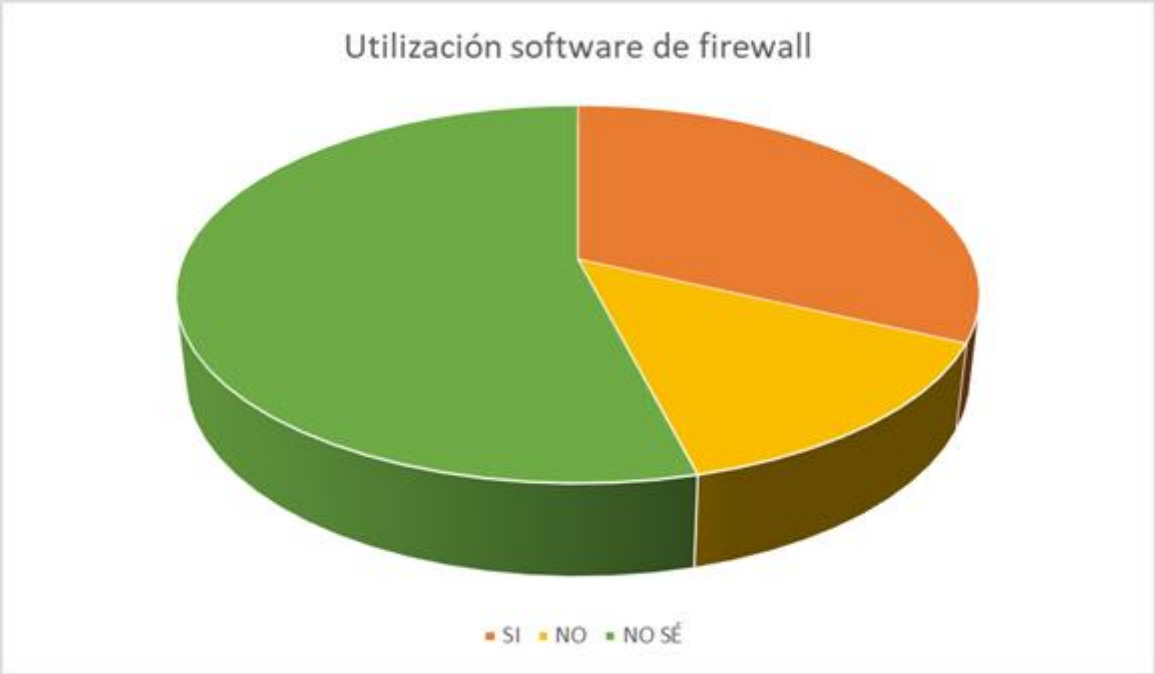
Podemos observar como solo el 14% de estas empresas utiliza Windows Update; mientras que en su gran mayoría lo realiza de vez en cuando si lo recuerda; lo que preocupa es ese 36% que desconoce lo que es, debido a que los equipos de una entidad necesitan ser actualizados regularmente para poder contar con las configuraciones estándar. Hay actualizaciones que se producen de forma consecutiva y pueden no ser realizadas normalmente por las organizaciones. Algunas personas prefieren llevar a cabo sólo actualizaciones importantes, mientras que otros realizan regularmente todas y cada una de las actualizaciones de Windows.

10. ¿UTILIZAS UN SOFTWARE DE FIREWALL EN TU ORDENADOR?

Tabla N°XI: Utilización Software de firewall

UTILIZACIÓN SOFTWARE DE FIREWALL	TOTAL	PORCENTAJES
SI	9	32%
NO	4	14%
NO SÉ	15	54%
	28	100%

Gráfico N°XI: Utilización Software de firewall



Como podemos observar el 54% de dichas empresas desconoce respecto de la utilización de un firewall; en contraposición de un 32% que si lo utiliza; permitiendo que entidades o personas no autorizadas no pueden acceder al equipo, lo que reduce las posibilidades amenazas a la seguridad.

2. RECOMENDACIONES

No existe una solución única para todos los riesgos de ciberseguridad debido a que los ataques evolucionan, haciéndose más sofisticados y difíciles de detectar. Sin embargo, hay algunas recomendaciones básicas que pueden ayudarte a proteger a tu Pyme de cualquier amenaza. Algunas recomendaciones a tener en cuenta: (PRESTIGIA, 2018)

- Dispón, como mínimo, de un antimalware y cortafuegos. También es importante mantener el antivirus actualizado o realizar auditorías para detectar posibles agujeros de seguridad.
- Presta atención a las actualizaciones de seguridad de tu sistema operativo para estar al día.
- Realiza *backups*, es decir, copias de seguridad en función de tus necesidades y cifra la información.
- Mantente informado sobre estafas e incidentes recientes. De esta manera, podrás identificar posibles riesgos.
- Protege la navegación de tus empleados y utiliza contraseñas seguras, implementando un plan de claves seguras.

- Sentido común. Es el mejor y más útil de los consejos. Si detectas una situación sospechosa navegando por internet, ten precaución y no caigas. Si sospechas de un enlace, email o archivo adjunto…¡no lo abras, bórralo!
- Trabajar en la concientización de los usuarios y educarlos para el buen manejo de los datos.
- Establecer un plan de protección de la información para contener incidentes, prevenir potenciales ataques, resguardar la información, controlar la información (que no llegue a manos equivocadas).
- Contar con equipos y recursos operativos que permitan dar respuesta a estos eventos.
- Pensar en la seguridad de la información y la continuidad del negocio.
- Motivar a las gerencias a que escuchen a sus especialistas en seguridad y no esperar a hacerlo cuando ocurre un incidente. Tomar la seguridad informática como una inversión y no como un gasto. La seguridad es un trabajo continuo, todos los días se debe hacer algo para prevenir.
- Considerar los recursos de la empresa. Una de las principales acciones a tomar de forma proactiva es saber cuáles son los recursos disponibles. La cantidad de horas hombre y la evaluación de sus capacidades técnicas para la resolución de diversos incidentes será necesaria para crear un equipo de respuestas, pero esto no alcanzará para mitigar un incidente. También es importante contar con hardware y soluciones de seguridad personalizadas para cada ambiente, herramientas imprescindibles que deben estar actualizadas para una mayor eficiencia.
- Crear un plan de acción. En todo sistema de gestión de la seguridad de la información debe existir un plan sólido de continuidad del negocio para una eventual contingencia. Es el caso de los BCP (Business Continuity Plan), que permiten restaurar las actividades críticas para el negocio de una forma rápida y controlada.
- Categorizar los posibles incidentes. La evaluación del tipo de incidente en cuanto a variables como el tiempo de resolución, impacto al negocio. Teniendo en cuenta estas problemáticas se deberá decidir qué tipo de incidente procesar en primera instancia, ya que como vimos anteriormente, los recursos son limitados y se deben establecer prioridades. Este proceso variará mucho teniendo en cuenta el tipo de institución afectada y su negocio; por ejemplo, no tiene el mismo impacto que una PyME dedicada a la producción de artículos cosméticos sufra una denegación de servicio, que le suceda a una empresa dedicada al almacenamiento en la nube. Por supuesto que en este último caso la problemática es mucho más crítica y debe ser solucionada cuanto antes.
- Dedicar tiempo a la investigación. Es importante entender la causa del incidente, la profundidad de la brecha, en dónde faltaron controles o cuáles fallaron. Resolver estas incógnitas servirá como base para la prevención de un futuro incidente. Para esta etapa es muy útil contar con gente con conocimientos de informática forense.

- Utilizar un antivirus que analice todas las descargas. Asegúrate de tener un antivirus instalado, actualizado al día para que reconozca el mayor número de virus, y realiza análisis regularmente de todo el sistema.
- Mantener el sistema operativo y el navegador actualizados. Los virus aprovechan los agujeros del SO y navegador para infectar los dispositivos. Como contramedida los fabricantes corrigen los programas a través de actualizaciones. La mejor forma para estar protegido es activar las actualizaciones automáticas.
- Cuidar las contraseñas. Al introducirlas se debe estar seguro de que es la página correcta, ya que puede parecer idéntica a la legítima y tratarse de una suplantación. No se debe utilizar la misma contraseña en diferentes servicios porque si acceden a una cuenta fácilmente podrán acceder al resto. Tampoco se ha de compartir las contraseñas con nadie, aunque digan que son del servicio técnico, los servicios respetables nunca solicitarán las contraseñas por propia iniciativa.
- Confiar en la web, pero sin ser ingenuo. Hay que permanecer alerta, no todo lo que se dice en internet tiene por qué ser cierto. Ante la duda, contrastar la información en otras fuentes de confianza.
- No hacer clic en enlaces que resulten sospechosos. Se debe ser precavido antes de seguir un enlace al navegar, en el correo, en la mensajería instantánea o en una red social. Los mensajes falsos que los acompañan pueden ser muy convincentes con el fin de captar la atención del usuario y redirigir a páginas maliciosas.
- Tener cuidado con lo que se descarga. No hay que precipitarse y descargarse cualquier cosa, ya que nuevas amenazas surgen cada día y los antivirus no pueden combatirlas todas. Hay que descargar los ficheros solo de fuentes confiables y los programas desde sus páginas oficiales.
- Desconfiar de los correos de remitentes desconocidos. Ante la duda, es recomendable no responder a los mismos y eliminarlos directamente.
- Pensar antes de publicar. Los servicios actuales de internet facilitan las relaciones sociales, lo que conlleva a su vez se publiquen mucha información sobre las personas (datos personales, imágenes, gustos, preferencias, etc.). Dado el valor que tiene esta información, y las repercusiones negativas que puede tener su uso inadecuado por parte de otras personas, es necesario que se gestionen adecuadamente.

CONCLUSIONES

Tal como se presentó en la introducción, este trabajo de investigación se ha escrito con el objetivo de ser una herramienta que sirva especialmente a Pymes; de manera que permita conocer y tener en cuenta el impacto generado por la seguridad informática.

En conclusión, la seguridad informática es un tema de muy alto impacto en la realidad virtual y tecnológica del mundo, ya que, así como se desarrollan software para el beneficio y facilidad de algunas actividades, también se crean software que su fin es robar información de manera desautorizada a diferentes entidades, entre ellas las PYMES, hasta usuarios individuales.

Sin embargo, existe una ligera diferencia entre seguridad informática y seguridad de la información y esta se basa en la implementación y el campo de ejercicio en el cual se ejecuta.

Existen miles de personas que se encargan de una manera constante de tratar de robar información, con el fin de obtener dinero vendiendo esa información o por cuestiones más que nada de honor y demostrar poder.

Las empresas más afectadas son entidades como bancos, entidades financieras, y tiendas On Line, las cuales son más propensas por la cantidad de dinero virtual manifestado en transacciones de alto contenido monetario. Actualmente las empresas son más vulnerables que en años anteriores, ya que se están descubriendo más formas de cómo llegar a obtener información de usuarios y empresas a través de señuelos, que parecen ser correctas páginas web o formularios confiables, pero en realidad son trampas de hacker para obtener información de los usuarios. Por tal motivo lo más conveniente es tomar medidas preventivas manuales y no dejar todo automáticamente a un software.

En función de las encuestas realizadas y el material recolectado hemos observado que las PyMES están expuestas a estos ataques y/o amenazas por no darle la necesaria atención e importancia a las consecuencias y al impacto que puede generar la seguridad informática en lo que respecta a la continuidad de dichas empresas por no estar lo suficientemente informadas o por creer que invertir en ello resulta innecesario, y por lo tanto encontrarse más vulnerables a un posible acceso y/o daño a su sistema.

Para concluir entendemos que el sistema de información no es más que la información mantenida en servidores o grandes contenedores, que solo se hacen sensibles cuando se mantienen en movimiento, en una transacción, en una red de datos, identificando el hacker que hay un movimiento y escudriñando qué se puede ver a través de ello.

REFERENCIAS BIBLIOGRÁFICAS

American Express. (s.f.). *https://www.amexcorporate.com.ar*. Obtenido de https://www.amexcorporate.com.ar/multitaskers/nota.php?id=843&cat=7

Avilés Gómez, M. (2010). *www.books.google.com.bo*. Obtenido de https://books.google.com.bo/books?id=Om1hC1sn3oIC&printsec=frontcover&dq=delitos+y+delincuentes+informaticos&hl=es-419&sa=X&ved=0ahUKEwj15JO52bzkAhXOo1kKHQ2pDAUQ6AEIJzAA#v=onepage&q=delitos%20y%20delincuentes%20informaticos&f=false

Boyer, L. (13 de Febrero de 2019). Mendoza, una de las provincias con más pymes que se financiaron en el mercado de capitales. *Diario Los Andes*, pág. 1.

Capodiferro Cubero, D. (2017). La libertad de información frente a internet. *Revista de Derecho Político*, 701-737.

Corletti, A. (13 de Marzo de 2008). *http://seguridad-informacion.blogspot.com*. Obtenido de http://seguridad-informacion.blogspot.com/2008/03/problemtica-ventajas-y-desventajas-de.html

Cortéz, J. (12 de Junio de 2017). *https://retina.elpais.com*. Obtenido de https://retina.elpais.com/retina/2017/06/01/tendencias/1496307759_889133.html

Cuervo Alvarez, J. (2013). *http://www.informatica-juridica.com*. Obtenido de http://www.informatica-juridica.com/trabajos/delitos-informaticos-proteccion-penal-de-la-intimidad/

Espinoza Santos, B. F., & Terán Viteri, L. F. (Marzo de 2015). *www.eumed.net*. Obtenido de http://www.eumed.net/rev/cccss/2015/01/internet-seguridad.html

iLifebelt Times. (16 de Noviembre de 2012). *www.ilifebelt.com*. Obtenido de http://ilifebelt.com/uso-de-internet-en-latinoamerica-infografía/2012/11

INCIPE, Instituto Nacional de Ciberseguridad. (21 de Septiembre de 2015). *https://www.incibe.es*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/mide-seguridad-informacion

ISOTools. (22 de Septiembre de 2015). *https://www.isotools.org*. Obtenido de https://www.isotools.org/2015/09/22/4-documentos-en-pdf-para-aprender-sobre-seguridad-informatica/

Julio, I. (25 de Marzo de 2016). *https://grupo4herramientasinformatica.blogspot.com*. Obtenido de https://grupo4herramientasinformatica.blogspot.com/2016/03/la-seguridad-informatica.html

Mendoza, M. A. (11 de Febrero de 2015). *https://www.welivesecurity.com*. Obtenido de https://www.welivesecurity.com/la-es/2015/02/11/desafios-planes-seguridad-para-pymes/

Navarrete, J. G. (22 de Octubre de 2015). *Fundación Empresa Seguridad y Sociedad*. Obtenido de https://www.fundacionesys.com/es/noticias/opinionciberseguridad-estan-suficientemente-protegidas-nuestras-empresas

Porto, J. P., & Gardev, A. (2009). *Definición de*. Obtenido de https://definicion.de/pyme/

Power Data. (11 de Abril de 2013). *https://www.powerdata.es/*. Obtenido de https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/234639/C-mo-evaluar-el-riesgo-de-la-seguridad-inform-tica-de-una-empresa

PRESTIGIA. (10 de Abril de 2018). *https://seguridad.prestigia.es*. Obtenido de https://seguridad.prestigia.es/riesgos-de-ciberseguridad-en-pymes/

Zelaya, V. (s.f.). *https://www.academia.edu*. Obtenido de https://www.academia.edu/13709765/LA_MEDIANA_EMPRESA

Páginas Web Consultadas

https://pymes.afip.gob.ar

https://www.cnv.gov.ar/SitioWeb/Informes.

https://www.argentina.gob.ar/noticias/nuevas-categorias-para-ser-pyme.

DECLARACIÓN JURADA RESOLUCIÓN 212/99/CD

Los autores de este trabajo declaran que fue elaborado sin utilizar ningún otro material que no hayan dado a conocer en las referencias, que nunca fue presentado para su evaluación en carreras universitarias y que no transgrede o afecta derecho de terceros.

Mendoza, 12 de Septiembre de 2019

Firma y aclaración	Número de registro	DNI
Rios Maria Julieta	25883	38582583
Demarchini, M. Victoria	24286	31902606