1502/1059

Universidad de Buenos Aires

Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

TEMA:

SEGURIDAD DE LA INFORMACIÓN EN EL ÁMBITO EMPRESARIAL

TÍTULO:

PROPUESTA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA PEQUEÑA O MEDIANA EMPRESA

Autor:

Miguel Eduardo Álvarez Espinoza

Directora: Mg. Patricia Prandini

Agosto del 2016

Cohorte 2015

DECLARACIÓN JURADA DEL ORIGEN DE LOS CONTENIDOS

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la Legislación Nacional e Internacional de Propiedad Intelectual.

Álvarez Espinoza Miguel Eduardo
FIRMADO

RESUMEN

La gran mayoría de las empresas que conforman el motor laboral de Latinoamérica son de carácter PyMe; es decir, pequeñas y medianas empresas mercantiles, industriales o de otro tipo, que tienen un número reducido de trabajadores y registran ingresos moderados, pero que en conjunto constituyen un eje fundamental que sustenta la generación de riqueza y desarrollo para nuestros países. Es menester entonces que este nicho empresarial tan importante y a la vez tan vulnerable por sus propias particularidades, proteja mínimamente sus sistemas informáticos, a las personas que los gestionan y a la información que generan, con un impacto manejable para la disponibilidad limitada de recursos que las caracteriza.

A partir del análisis de modelos y metodologías existentes, el presente trabajo final de especialización desarrolla un modelo de política de seguridad de la información (PSI), que incluye un sistema de controles de seguridad aplicable a una PyME. Este modelo procura brindar un marco lo suficientemente amplio y flexible como para facilitar la protección de la información de las organizaciones de este tipo, consumiendo una cantidad acotada de recursos.

PALABRAS CLAVE

- PyMe
- Política de seguridad de la información - PSI
- Seguridad de la información.
- ISO/IEC 27002:2013

ÍNDICE

DECLARACIÓN JURADA DEL ORIGEN DE LOS CONTENIDOS II
RESUMEN III
ÍNDICE IV
INTRODUCCIÓN 6
CAPITULO I 8
1.1 DEFINICIÓN Y CARACTERIZACIÓN DE UNA PYME 8
1.2 PROBLEMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA REGIÓN, DESDE LA PERSPECTIVA LAS PYME. 10
1.2 BREVE INTRODUCCIÓN AL ESTÁNDAR ISO 27002:2013 [8] 13
CAPÍTULO II 16
2.1 ANÁLISIS DE LA PYME MULTISERVICIOS 16
2.1.1 ANTECEDENTES 16
2.1.2 INSTALACIONES 16
2.1.3 CURSO DE ACCIÓN A SEGUIR 17
2.2 RELEVAMIENTO DE HARDWARE 17
2.2.1 CONCLUSIONES RESPECTO AL HARDWARE 18
2.3 RELEVAMIENTO DE SOFTWARE 18
2.3.1 CONCLUSIONES RESPECTO AL SOFTWARE 18
2.4 PERCEPCIÓN DE LA PYME SOBRE LA SEGURIDAD DE LA INFORMACIÓN 19
2.5 INCIDENTES DE SEGURIDAD EN LAS PYME 21
2.5.1 IMPACTO Y CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD 21
2.5.2 RESPUESTA DE LAS PYME FRENTE A LOS INCIDENTES DE SEGURIDAD 23
CAPITULO III 24
3.1 PROPUESTAS PARA OPTIMIZAR LA SEGURIDAD 24
3.2 ACCIONES A APLICAR 27
3.2.1 TIPOS DE MEDIDAS 27
3.2.2 ACCIONES A APLICAR PARA PROTEGER EL HARDWARE 28
3.2.3 ACCIONES A APLICAR PARA PROTEGER EL SOFTWARE 31
3.2.4 ACCIONES A APLICAR PARA PROTEGER LA RED 33
3.2.5 ACCIONES A APLICAR PARA LA PROTECCIÓN DE LOS DATOS 35
3.2.6 ACCIONES A APLICAR PARA PROTEGER AL PERSONAL 37
CAPITULO IV 40
4.1 ALCANCE DEL CAPÍTULO 40
4.2 PORQUÉ USAR UN MODELO DE PSI 40
4.3 OBJETIVOS DE LA POLÍTICA 42

4.4 DISTRIBUCIÓN Y DIFUSIÓN 43
4.5 ALCANCE Y USO 43
4.6 GLOSARIO DE TÉRMINOS 44
4.7 PRESCIPCIONES PARA ACCESO DE USUARIOS 46
4.8 PRESCIPCIONES PARA ACCESO A SISTEMAS Y APLICACIONES 48
4.9 PRESCIPCIONES PARA EL MANEJO DE INFORMACIÓN 49
4.10 PRESCRIPCIONES DE SEGURIDAD A NIVEL EMPRESA 50
4.11 PRESCRIPCIONES PARA EL USO RESPONSABLE DE EQUIPOS INFORMÁTICOS 51
4.12 PRESCRIPCIONES PARA ACCESO FÍSICO RESPONSABLE 54
4.13 PRESCIPCIONES PARA EL CONTROL DE ACCESO A RED 54
4.14 PRESCRIPCIONES SOBRE EL ACCESO A INTERNET 55
CONCLUSIONES 57
RECOMENDACIONES 61
ANEXOS 64
ANEXO A 64
A.1 DIAGRAMA DE INSTALACIONES DE PYME MULTISERVICIOS 64
ANEXO B 65
B.1 INVENTARIO DE LOS RECURSOS DE HARDWARE DE PYME MULTISERVICIOS 65
B.2 SOFTWARE INSTALADO EN COMPUTADORES DE PYME MULTISERVICIOS 66
ANEXO C 68
C.1 CUESTINARIOS EFECTUADOS A PYME MULTISERVICIOS 68
ANEXO D 79
D.1 CONTROLES DE LA ISO/IEC 27002:2013 APLICABLES A UNA PYME 79
BIBLIOGRAFÍA 93

INTRODUCCIÓN

Este trabajo de especialización busca brindar una perspectiva sobre la prioridad que las empresas pequeñas y medianas deben dar a las normas de seguridad de la información en aras de proteger sus activos de información.

Es consabido que los ataques o amenazas informáticas están a un clic de distancia, y su rápida propagación por la red es muy difícil de controlar, aún por las compañías especializadas. Se deben establecer parámetros mínimos que refuercen la seguridad para la protección de los datos y recursos informáticos de las PyME, que no cuentan con personal especializado para este tipo de labor, y cuyo personal comúnmente no ha recibido ningún tipo de capacitación que prevenga el mal uso o la desidia cuando se utilizan recursos informáticos, ante la falta de normas y mecanismos de seguridad.

Este trabajo final de especialización se desarrolla en cuatro capítulos de la siguiente manera:

El Capítulo I presenta la definición y la caracterización de una PyME y una breve descripción de su problemática en la región, desde la perspectiva de uso de las Tecnologías de Información y su seguridad. Además, se hace una introducción al estándar ISO/IEC 27002:2013, su historia y el porqué de la conveniencia de implantar sus lineamientos en una empresa pequeña o mediana.

En el Capítulo II se hace mención al relevamiento realizado a la PyME "Multiservicios", ubicada en la ciudad de Bahía de Caráquez, Provincia de Manabí, Ecuador, presentándose una serie de conclusiones sobre su situación. Adicionalmente, se presenta un breve análisis sobre cómo "Multiservicios" y en general las PyME, perciben el tema de la seguridad de la información y los riesgos a los que se exponen frente a los incidentes de seguridad que pudieran afectarlas. Este relevamiento se realizó con la idea de conocer mejor la realidad

de una PyME en materia de protección de su información y de los recursos utilizados para gestionarla.

En el Capítulo III se efectúa una propuesta de controles y medidas preventivas aplicables a una PyME, detallando cursos de acción para atender las dificultades que se presenten en cuanto a la protección del hardware, software, redes informáticas, información y recursos humanos.

Finalmente, en el Capítulo IV se presenta una serie de lineamientos para el desarrollo de una PSI dentro una PyME. Se detalla cómo se debe elaborar un documento de este tipo, ofreciendo una guía práctica y sencilla para los responsables de llevarla a cabo, con el fin de facilitar su aplicación e implementación por parte de personal sin experiencia profunda en el uso de tecnologías de la información, ni en la gestión de incidentes informáticos.

En línea con lo anterior, se identificaron y seleccionaron los controles de los 14 dominios principales que conforman la norma ISO/IEC 27002:2013, en función de su aplicación a la realidad de las PyME. Dicho análisis se expone en el ANEXO D. El criterio utilizado para esta selección se basó en la practicidad para aplicar cada uno de los controles mencionados en la norma, tomando en cuenta además los recursos que demandaría su implementación a una empresa de este tipo.

El texto se cierra con las conclusiones y una serie de recomendaciones que puede seguir una PyME para fortalecer la protección de su información.

Este trabajo final de especialización puede ser usado como guía para la implementación de tareas relacionadas a la gestión de la seguridad de la información y de los riesgos de seguridad en una PyME, además de facilitar la redacción de una Política de Seguridad de la Información. Se aclara que no es aplicable a empresas especializadas en TI, las que requieren controles más estrictos y generalmente cuentan con personal especializado en el tema.

CAPITULO I

1.1 DEFINICIÓN Y CARACTERIZACIÓN DE UNA PYME

Se conoce como PyME al conjunto de pequeñas y medianas empresas que, en razón a su volumen de ventas, capital social, cantidad de trabajadores, nivel de producción o la disponibilidad de activos, presentan una serie de características distintivas de este tipo de entidades económicas. Entre estas características se encuentran las siguientes:

- Falencias en sus estrategias e instancias de planificación.
- Débiles encadenamientos productivos.
- Costos elevados por desperdicio de materia prima.
- Insuficiente producción para exportar o aumentar su alcance geográfico.
- Falta de adecuación de la maquinaria y de procedimientos vinculados a la calidad, necesaria para contar con procesos eficientes y efectivos y mejorar la producción o prestación de servicios.

En muchos países, se las caracteriza en función de la cantidad de empleados o de los ingresos. A manera de referencia, en Ecuador las compañías se clasifican de la siguiente forma:

1.- Microempresas: Entre 1 a 9 trabajadores ó Ingresos menores a $100.000.00

2.- Pequeña empresa: Entre 10 a 49 trabajadores o Ingresos entre $100.001.00 y $1.000.000.00

3.- Mediana empresa: Entre 50 a 199 trabajadores o Ingresos entre $1.000.001.00 y $5.000.000.00

4.- Empresa grande: Más de 200 trabajadores o Ingresos superiores a los $5.000.001.00 [1]

La principal ventaja de las pequeñas empresas se basa en la facilidad con la que pueden manejarse administrativamente, ya que no existen engorrosos procesos burocráticos para llevar una tarea a cabo.

El limitado presupuesto que manejan se presenta como su principal desventaja. Suelen ser más susceptibles a los vaivenes de la economía, como la inflación o las devaluaciones, y viven de sus ingresos diarios. La falta de recursos financieros es evidente y por lo tanto, se les dificulta crecer, poniendo de esta manera en peligro su existencia. A esto se suma una administración rudimentaria por parte del o los propietarios que afecta el rendimiento general de la empresa.

En el caso de las medianas empresas, cabe mencionar que generalmente, padecen los mismos problemas que las pequeñas empresas. Pueden tener como ventaja un mejor manejo administrativo, pero también presentan altos costos de operación, dificultades para la renovación del equipamiento y maquinaria, escasez de ganancias extraordinarias y limitaciones para pagar altos salarios. Esto último conlleva a que no cuenten con personal especializado, además de carecer de efectivos controles de calidad.

> En Latinoamérica, las pequeñas y medianas empresas (PyME) representan el 99% del total de empresas no financieras y generan empleos para aproximadamente el 70% del total de la fuerza laboral. [2]

Las PyME son fundamentales desde el punto de vista económico y social para las economías, ya que generan oportunidades de negocio de distinta naturaleza y en diferentes estratos, contribuyendo así al crecimiento económico de los países.

> "Según un estudio del 2012 de la Comisión Económica para América Latina y el Caribe (Cepal), Perú es el país donde, por ejemplo, más microempresas existen, seguido de Ecuador y México. En el caso de las pequeñas, el mayor porcentaje lo ocupa Argentina y de las medianas Uruguay. Colombia es el país en el que el 50,6% de los empleos que se genera corresponde a las microempresas (17,5% a las pequeñas y 12,8% a las medianas). Mientras que en Ecuador, según el estudio, el 44% corresponde a las micro (17% a las pequeñas y 14% a

las medianas). En Ecuador además, de acuerdo al informe, el 99,8% de empresas son micro, pequeñas y medianas." [3]

1.2 PROBLEMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA REGIÓN, DESDE LA PERSPECTIVA LAS PYME.

En el lapso de unas pocas décadas, Internet ha saltado de ser una plataforma desconocida, utilizada casi exclusivamente por académicos y especialistas en tecnología, a convertirse en una red cuyos servicios son aprovechados por infraestructuras críticas a nivel nacional y en múltiples actividades humanas. En efecto, el acceso a esta gran red ya se considera un servicio básico, tal como tener energía eléctrica o acceder al servicio de agua potable, y se encuentra presente en casi todos los aspectos de nuestra vida cotidiana.

Las ventajas de tener conectividad son enormes y la región ha adoptado estas nuevas tecnologías con entusiasmo. Sudamérica es actualmente el cuarto mayor mercado móvil del mundo, la mitad de su población usa el Internet y los gobiernos de la zona emplean cada vez más medios digitales para comunicarse y brindar servicios a los ciudadanos.

Sin embargo, a pesar del importante uso de Internet que registra la región, no se presentan grandes avances en temas de seguridad cibernética, mucho menos en el ámbito de las PyME. Si bien se sabe que es sustancial contar con una estrategia de este tipo, poco se ha logrado a nivel general en el continente, más allá de la etapa de tener una idea básica sobre qué hacer. Solo los países más ricos de la región cuentan con distintas organizaciones dedicadas a la seguridad cibernética pero incluso donde están presentes tales organizaciones, las posibilidades de éxito se encuentran limitadas por la falta de coordinación entre los distintos sectores de la economía y las entidades públicas.

"Según el Centro de Estudios Estratégicos e Internacionales, América Latina tiene 300 millones de usuarios de Internet, más de la

mitad de la población de la región, por lo que riesgos cibernéticos son cada vez más preocupantes y se están convirtiendo en un factor de mayores consideraciones en seguridad y formulación de políticas económicas. La conciencia de seguridad cibernética ha ido creciendo a medida que se ha reconocido que las amenazas y vulnerabilidades tienen el potencial de frenar la innovación y el avance de la economía basada en Internet, a la vez que ponen en riesgo a los individuos y las organizaciones." [4]

Los esfuerzos hasta ahora realizados si bien han ayudado, aún resultan insuficientes, demostrando que queda pendiente mucho por hacer, ya que tanto instituciones públicas y compañías privadas se encuentran expuestas a sufrir ataques.

Los países de Latinoamérica no son ajenos a este fenómeno y como el resto del mundo, sus organizaciones, gobiernos y población en general, sufren las consecuencias de las actividades ilícitas y de las vulnerabilidades propias de las tecnologías y de Internet. Efectivamente, estos ataques se presentan bajo las mismas formas que en otros países, ya sean casos de robo de identidad, "PHISHING", denegación de servicio, robo de información, violaciones a la propiedad intelectual, etc. [5]

El sector privado ha superado al estatal, en general, en su reconocimiento de la importancia de la seguridad cibernética, mientras que el nivel de concientización en el público varía en toda la región. Dicho nivel seguramente aumentará a medida que más servicios estatales pasen a estar en línea y se generen más debates sobre las implicancias de la seguridad en distintas actividades en línea, como es el caso del comercio electrónico.

"De acuerdo al Estudio Global sobre la Seguridad TI Empresarial, realizado por B2B Internacional a distintas empresas de 22 países de Latinoamérica, y dado a conocer por Kaspersky Lab, el 68% de ellas ha sufrido algún tipo de ciberataque con virus en los últimos doce meses. **Las microempresas (63% de las pequeñas y 60% de las medianas) han sido víctimas de virus, gusanos, spyware y otros programas maliciosos, a diferencia de las compañías más grandes**, que son el blanco de otro tipo de ataques, como el ciberespionaje, phishing y ataques de DDoS. Frente a esta situación, el sondeo mostró que **sólo**

> **un 25% de las Pymes invierten en seguridad en tecnologías de la información (TI) de forma preventiva**, mientras que el 19% de las pequeñas empresas y el 15% de las medianas empresas son reactivas frente a los ciberataques, preocupándose por la seguridad informática **sólo luego de que fueron víctimas del ataque."** [6]

Por otra parte, en el frente de la seguridad cibernética, están surgiendo varios cambios importantes, como el que propicia la adopción de estándares de seguridad de la información para reducir las vulnerabilidades presentes en los sistemas y preparar a América Latina para el futuro. Así mismo existe una fuerte tendencia hacia la mejora en la concientización sobre los riesgos cibernéticos, es decir, proponer y enseñar técnicas básicas de prevención a las personas y organizaciones para defenderse de ataques.

La ventaja de la concienciación cibernética es que puede ser implementada de forma barata y difundida ampliamente y no reducirse solo a una lista de comportamientos o una sesión básica de entrenamiento, adaptándose de esta manera a las limitaciones presupuestarias de las economías latinoamericanas.

A pesar de lo dicho y en materia de inversión, la región aún se encuentra muy lejos de las potencias mundiales en cuanto al aprovechamiento que estas hacen de las Tecnologías de la Información.

> Si bien es cierto que cada vez más empresas invierten en tecnología, en Argentina aún estamos muy lejos de los niveles de los países más desarrollados del mundo, donde es habitual una inversión en tecnología informática de entre un 5% y un 6% de su facturación. En Argentina, las empresas que más recursos destinan llegan, en el mejor de los casos, al 1%. Esto es porque muchos aún lo ven como un gasto y no como una inversión. [7]

En el caso particular de las PyME estas empresas no cuentan con mecanismos y controles adecuados para proteger sus datos sensibles. Las pequeñas y medianas empresas deben tener muy en cuenta que no necesitan proteger toda la información que se genera dentro de la organización, sino solo la que es realmente confidencial,

como ciertos archivos o datos que son de valor para la empresa misma y para sus clientes, tanto por las ganancias que pueden generar como en las pérdidas que representaría su extravío, sea en oportunidades o multas.

Desgraciadamente, para un encargado de tecnología o de seguridad de la información, resulta muy complicado poder convencer a sus empleadores y gerentes para que se invierta en este rubro. Sin embargo, a partir de la difusión pública de casos de ataques cibernéticos con fuerte impacto económico o sobre la reputación, y con un gran esfuerzo, se está tratando de superar esta situación, observándose que todo tipo de empresas está incorporando paulatinamente prácticas, sistemas y dispositivos que protegen su actividad y su información.

Con una buena cultura de seguridad de la información al interior de la organización, y una conciencia clara de cuáles son los recursos que se deben proteger, la inversión en seguridad para una PyME no debería ser muy grande y las soluciones más fáciles de aplicar.

1.2 BREVE INTRODUCCIÓN AL ESTÁNDAR ISO 27002:2013 [8]

El estándar ISO/IEC 27002:2013 (originalmente denominado ISO/IEC 17799) es una norma de seguridad de la información publicada por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La versión más reciente fue difundida en el año 2013.

El estándar tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995. En el año 2000 la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional publicaron el estándar ISO/IEC 17799:2000, con el título de Information Tecnology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar, surgió en el año 2005 el documento modificado ISO/IEC 17799:2005.

Con la aprobación de la norma ISO/IEC 27001 en octubre de 2005 y la reserva de la numeración 27000 para la Seguridad de la Información, el estándar ISO/IEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007.

La versión de 2013 del estándar describe los siguientes catorce dominios principales:

- Políticas de Seguridad.
- Organización de la Seguridad de la Información.
- Seguridad de los Recursos Humanos.
- Gestión de los Activos.
- Control de Accesos.
- Criptografía.
- Seguridad Física y Ambiental.
- Seguridad de las Operaciones.
- Seguridad de las Comunicaciones.
- Adquisición de Sistemas, Desarrollo y Mantenimiento.
- Relaciones con los Proveedores.
- Gestión de Incidencias que afectan a la Seguridad de la Información.
- Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio.
- Conformidad.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica, asimismo, una guía para su implantación. El número total de controles suma 114 entre todas las secciones. Cada organización debe considerar previamente cuántos de esos controles serán realmente los aplicables, según sus propias necesidades.

De acuerdo a lo señalado en el propio estándar, y como un complemento a la meta que se persigue con este trabajo, se preparó adicionalmente el cuadro que se adjunta en el ANEXO D, conteniendo los controles que, de acuerdo sus características, consumo estimado de recursos y complejidad de implementación, podrían ser aplicados en una PyME, con el fin de proveer una guía práctica que encamine a la empresa a minimizar riesgos y garantizar la continuidad del negocio. Es menester dejar muy en claro que, si bien no se podrá alcanzar la seguridad total, se podrá estar más cerca de ella mediante las buenas prácticas que se sugieren.

CAPÍTULO II

2.1 ANÁLISIS DE LA PYME MULTISERVICIOS

2.1.1 ANTECEDENTES

Alvarado PC surgió como un pequeño emprendimiento familiar el 20 de marzo de 2006. En sus inicios se dedicaba a la venta de partes y equipos de computación. Se ubica en el centro de la turística ciudad de Bahía de Caráquez, provincia de Manabí, Ecuador.

Originalmente estaba conformada por 4 personas quienes se dedicaban a tiempo completo a las actividades de la pequeña empresa. Con el pasar del tiempo y debido al buen servicio que brindaba, la clientela y la demanda aumentaron. Esta nueva situación llevó a la necesidad de reinventar su enfoque original para pasar a llamarse "Multiservicios", dedicándose en su nueva faceta a la asesoría de diseño gráfico, venta y soporte de software con licencia, servicio de fotocopias, venta de souvenirs de la ciudad y servicio fotográfico profesional. Adicionalmente, se sumó una oferta de reparación y venta de equipos tecnológicos de diferentes marcas. Actualmente emplea a 16 personas entre personal administrativo, de ventas y asesoramiento técnico.

La elección de esta PyME como caso de estudio se justifica por el valor que este tipo de empresas tiene en el ámbito local, ya que se constituye en un ente dinamizante de la economía que conoce bien el mercado en el que se desenvuelve. A pesar de que su administración ha sido relativamente fácil, su crecimiento se ha dado en forma desorganizada.

2.1.2 INSTALACIONES

En el ANEXO A.1 de este documento se puede obtener un diagrama de las instalaciones físicas de la PyME Multiservicios.

2.1.3 CURSO DE ACCIÓN A SEGUIR

Con el fin de conocer el estado de situación de la PyME Multiservicios en cuanto a la seguridad de su información, se realizaron las siguientes actividades:

- Relevamiento en las oficinas de la empresa, con el propósito de ponerse en contacto con los encargados de la misma para tratar de conocer cuál es su apreciación sobre la seguridad de la información. Se hizo hincapié en conocer los activos de información con los que cuenta y tratar de conocer que se hace para proteger la información del negocio.
- Análisis de la percepción del personal y de los propietarios de la PyME respecto a la seguridad de la información, con el propósito de conocer de primera mano las limitaciones que se tienen en cuanto a recursos, conocimientos y falencias.

A partir de este relevamiento, y en consonancia con las buenas prácticas de la ISO/IEC 27002:2013, se elaboraron recomendaciones, de cara a mantener la seguridad de la información dentro de una PyME, plasmadas en el Capítulo III (Propuesta de controles y medidas preventivas) de este Trabajo de Especialización.

2.2 RELEVAMIENTO DE HARDWARE

En términos amplios, el relevamiento o inventario es el recuento detallado de los bienes que una entidad posee en un momento determinado.

Una labor de importancia en el día a día de cualquier organización, incluyendo las PyME, es mantener actualizado el inventario con el hardware disponible y su estado. Se realiza con la finalidad de que se pueda determinar la cantidad y el tipo de equipos

con los que cuenta la empresa, para así poder hacer el seguimiento respectivo y aplicar planes de mantenimiento preventivo o correctivo, aumentando la eficiencia y eficacia en el soporte tecnológico de los equipos.

En el ANEXO B.1 se presenta un compendio del inventario de los recursos de hardware de la PyME Multiservicios. Este informe incluye código, la ubicación y el usuario a quien pertenece.

2.2.1 CONCLUSIONES RESPECTO AL HARDWARE

Respecto al hardware con el que Multiservicios realiza sus actividades, se puede indicar que dispone de equipamiento lo suficientemente robusto para cubrir sus necesidades. Sin embargo, se evidencian varias falencias en cuanto a las medidas de seguridad para el acceso y protección del mismo.

La instalación, operación y mantenimiento de la red están bajo la responsabilidad del personal técnico interno de la PyME.

2.3 RELEVAMIENTO DE SOFTWARE

De igual forma que en el apartado anterior, se indicará de una forma general el software instalado en las estaciones de trabajo y su configuración. Se puede encontrar un detalle pormenorizado en el Anexo B.2.

2.3.1 CONCLUSIONES RESPECTO AL SOFTWARE

Si bien Multiservicios cuenta con el software necesario para poder brindar un servicio eficiente, carece de la mayoría de las licencias de uso respectivas ya que se decidió ahorrar en ese rubro, exponiéndose a sanciones legales y a la falta de soporte del proveedor. Solo disponen de software antivirus con licencia paga como única herramienta para proveer seguridad a sus programas y sistemas.

2.4 PERCEPCIÓN DE LA PYME SOBRE LA SEGURIDAD DE LA INFORMACIÓN

> Las pequeñas y medianas empresas (pymes) desempeñan un papel importante en las economías nacionales. Cuando sus clientes les confían datos, las pymes también asumen la responsabilidad de proteger esta información contra atacantes en línea. Sin embargo, como se detalla en el Estudio comparativo sobre capacidades de seguridad 2015 de Cisco, las pymes muestran indicios de que sus defensas contra atacantes son más débiles de las que sus desafíos exigen. A su vez, estas debilidades pueden poner en riesgo a los clientes de las pymes. Los atacantes que pueden violar la red de una pyme también pueden encontrar una vía hacia una red empresarial. Los encuestados en este estudio señalaron que no tienen un ejecutivo a cargo de la seguridad y no cree que sus empresas sean objetivos de gran valor para los delincuentes en línea. Esta convicción insinúa que hay un exceso de confianza en la capacidad de la empresa para frustrar los sofisticados ataques en línea de hoy, o, lo que es más probable, que esta nunca será atacada. [9]

Crear y ejecutar políticas de seguridad como medida de prevención es una de las prácticas que permite a una PyME disponer de una estrategia para el aumento progresivo del nivel de protección de sus activos. La información que poseen las empresas, cualquiera sea su tamaño y finalidad, es un activo de gran valor que los atacantes tratan de obtener para conseguir alguna ganancia económica, sobresalir como hackers o simplemente para dañar la reputación de la empresa atacada. Las limitaciones en cuanto a la disponibilidad de sus recursos técnicos y humanos y una menor conciencia sobre la importancia de las políticas de seguridad, respecto a las grandes empresas, implica una mayor exposición frente a estos sucesos y, a su vez, mayores consecuencias de los mismos en el caso de producirse, pudiendo llegar incluso a afectar a la continuidad de las operaciones. La diversidad que registran las empresas en cuanto a su preparación frente a posibles riesgos se refleja así mismo, en la forma de responder y combatir estos incidentes.

Las PyME se caracterizan generalmente por tener una confianza excesiva respecto a su nivel de exposición, menospreciando el hecho de que un atacante les podría robar eventualmente su información. En efecto, tienen muy arraigada la convicción de que no son susceptibles de sufrir ataques y suelen asumir que es muy remota la posibilidad de que algo les pase.

Sin embargo, existe también la percepción de que asegurar la información es una medida deseable, aunque las restricciones al presupuesto son generalmente un obstáculo para adoptar procesos de protección adecuados.

En el ámbito web donde los atacantes desarrollan tácticas más sofisticadas para acceder a redes y mantenerse inadvertidos. Ninguna empresa, grande, mediana o pequeña puede dejar sus redes desprotegidas ni retrasar la aplicación de procesos que puedan ofrecer conocimientos sobre cómo se produjo una vulnerabilidad para poder evitarla en el futuro.

Es muy probable también que una PyME no se dé cuenta de que sus propias vulnerabilidades se traducen en un peligro potencial para sus clientes. Los delincuentes pueden ser capaces de obtener acceso a una red como medio para encontrar un punto de ingreso a otra red que les provea mayor beneficio, y una PyME puede ser el punto de partida de ese ataque.

En este marco y del relevamiento realizado, es posible afirmar que Multiservicios, al ser una típica PyME, carece de una real percepción sobre lo expuesta que se encuentra a situaciones que pueden resultar en una vulneración de su red, su información y sus sistemas. En este sentido, existe despreocupación sobre su seguridad de la información debido que nunca se han implementado en esa compañía buenas prácticas que ayuden a superar estas limitaciones.

2.5 INCIDENTES DE SEGURIDAD EN LAS PYME

Un incidente de seguridad de la información es cualquier tipo de acción, realizada por algún atacante externo o interno, que tenga por objetivo violentar a una política o mecanismo de seguridad de la organización.

"Entre los incidentes de seguridad que afectan a pequeñas y medianas empresas se encuentran:

- Ciberespionaje
- Fallas de seguridad en los proveedores
- Intrusiones en la red
- Ataques de denegación de servicio
- Phishing
- Fuga intencional de información
- Vulnerabilidades de software
- Fraude de los empleados
- Fuga accidental de información
- Malware" [10]

2.5.1 IMPACTO Y CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD

Una violación a los sistemas de seguridad de una empresa suele conducir irremediablemente a serios problemas de negocios. Sin embargo, y dando por sentado que el daño pueda ser muy diverso, es difícil que las víctimas puedan estimar el costo total ocasionado por incidentes de este tipo.

Las posibles consecuencias que podrían sufrir las empresas pueden calificarse en dos grupos:

- Las que afectan la capacidad operativa del negocio, es decir que causan una interrupción momentánea,

prolongada o permanente de la producción, generando una pérdida considerable de oportunidades.

- Las que se relacionan con los gastos adicionales en servicios profesionales reactivos, asesoramiento con personal capacitado y gastos inherentes a la reconstrucción de imagen o reputación de la empresa.

Las empresas perjudicadas ven la afectación a su productividad como una primera muestra del impacto de un ataque, consecuencias que resultan evidentes desde un primer momento.

La pérdida económica que surge por la indisponibilidad de los sistemas es tema de preocupación. Por ejemplo, es relativamente fácil poder realizar ataques del tipo DoS (*denial of service* o denegación de servicio) que podrían ser ejecutados con el único motivo de frenar las actividades productivas de una organización, destruyendo horas/hombre invertidas.

Los incidentes, cualquiera sea su naturaleza, pueden ser resueltos de varias maneras, ya sea por el propio personal de la empresa, mediante asesoramiento de un servicio profesional externo, o a través de la contratación de una persona de confianza con conocimientos informáticos, todo lo cual redundará en un gasto adicional al presupuesto.

Las empresas para ser competitivas, además de contar con productos o servicios de calidad, deben desarrollar la confianza de los consumidores y socios de negocio. El tener una reputación intachable desempeña un papel clave en la construcción de esa relación. Los daños a la reputación dependen directamente de si el incidente de seguridad se hizo público o no. El reporte a las autoridades competentes es una forma de mejorar el escenario general de la seguridad, siendo en algunos casos obligatorio para evitar sanciones.

2.5.2 RESPUESTA DE LAS PYME FRENTE A LOS INCIDENTES DE SEGURIDAD

"Incluso la empresa mejor protegida experimentará en algún momento una violación de seguridad de la información, por lo que la pregunta clave para afrontar la seguridad de la información no es si sucederá, sino cuándo sucederá" [11]. Por lo tanto, la forma en que una empresa se prepara para responder a un incidente es una manera de medir su madurez.

Un obstáculo que enfrentan las empresas PyME respecto a la gestión de incidentes de seguridad de la información es su falta de sensibilidad para propiciar planes reactivos y de iniciativa para actuar ante las consecuencias derivadas de incidentes que afectan la continuidad del negocio y la seguridad de su información.

> Uno de los principales argumentos para no acometer medidas preventivas, que reduzcan o mitiguen los riesgos, es la falta de concienciación de los altos cargos de dichas compañías que no estiman oportuno invertir en estas medidas, ya que siempre esperan un retorno de esa inversión, y es por ende poco "justificable" inicialmente. [12]

La inversión necesaria para prevenir estos incidentes debería ser menor que lo que le cueste a la empresa si la amenaza se llega a materializar. Hay que tener en cuenta que cualquier disposición que se tome solo servirá para reducir los riesgos, ya que estos nunca podrán anularse. Por ello, resulta muy importante evaluarlos y considerar como posibilidad asumir los que se consideren menos críticos.

En términos empresariales, perder dinero es dejar de ganarlo, por lo que este debería ser uno de los principales argumentos que se deba usar para persuadir al alto mando de la PyME y comprometerlo a ejecutar algún tipo de medida en pos de la seguridad de la información, por lo que es necesario establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a estos incidentes. Estos procesos deben contribuir a lograr la mejora continua en la evaluación y monitoreo de los sucesos que afecten a la seguridad.

CAPITULO III

3.1 PROPUESTAS PARA OPTIMIZAR LA SEGURIDAD

Se hace necesario proteger tanto los aspectos físicos de los activos de información así como también a su ámbito lógico, el cual está conformado por los programas y sistemas que gestionan la información en sí. Los daños que puede sufrir una organización no se dan solo sobre los propios medios físicos, sino también contra la propia información almacenada y procesada. Por lo tanto, la seguridad física es sólo una parte del amplio espectro que se debe cubrir, ya que es apenas una de las múltiples aristas a considerar para tratar de llegar a una adecuada protección de la información.

Hecha esta aclaración, entre las primeras medidas preventivas a tomar en cuenta en cualquier organización, incluyendo las PyME, se encuentra la protección física del equipamiento informático. Cualquier equipo en general debe situarse en lugares protegidos al que sólo el personal autorizado pueda ingresar. Las medidas aplicables van desde las más elementales, como una habitación cerrada bajo llave, a los más avanzados dispositivos tecnológicos, como el acceso por mecanismos biométricos o el uso de cámaras de vigilancia o detectores de movimiento.

En la cotidianidad de las PyME, esto debe llevarse a cabo siempre y cuando todas estas medidas armonicen con el reducido presupuesto con el que cuentan para garantizar la seguridad de la información. En estos contextos, medidas simples como la colocación de cerraduras con llave y la ubicación de servidores en salas internas de uso exclusivo, que requieran sobrepasar uno o varios niveles de acceso o de ingreso muy limitado, ya constituyen un aporte importante a la seguridad de estos recursos y no representan un gasto exagerado para una PyME.

Sería ideal considerar también la adopción de medidas básicas para prevenir no solo las amenazas provocadas por el hombre, sino también a las producidas por la naturaleza, como son los casos de los

desastres naturales, inundaciones, terremotos y cualquier otro evento natural que pudiera afectar a la operatividad física de los equipos informáticos.

Por otro lado, y como ya se dijo, el activo más importante que cualquier empresa posee es la información, por lo tanto se deben utilizar técnicas que la protejan a través de la utilización de mecanismos vinculados a la seguridad lógica, la cual consiste en la implementación de barreras y procedimientos que resguarden los datos y sistemas y sólo se permita que accedan a ellos las personas autorizadas.

Los objetivos que la seguridad lógica persigue son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Procurar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Procurar que la información recibida sea la misma que ha sido transmitida.
- Asegurar que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Asegurar que se disponga de pasos alternativos de emergencia para la transmisión de información.

"La seguridad de la información en su faceta preventiva abarca todas aquellas acciones que van orientadas a evitar que se materialice una amenaza a la confidencialidad, integridad y disponibilidad de la información. Para estos fines y entre otros mecanismos, se debe proporcionar herramientas que controlen el acceso, con el fin de garantizar la identificación y gestión de perfiles, para determinar qué usuario y bajo qué condiciones puede acceder al recurso solicitado para ejecutar la acción seleccionada.

> No es suficiente que el aumento de la conectividad a Internet sea sostenible: también es necesario que dicha conectividad sea segura y resistente. De hecho, nuestra dependencia de esta compleja infraestructura ha venido con un precio: al conectar tantos aspectos de nuestra economía y servicios vitales a Internet, también nos hemos expuesto a una serie de actividades cibernéticas nefastas que pueden socavar la disponibilidad, integridad y resiliencia de esta infraestructura central, lo que ha amenazado los beneficios económicos y también tecnológicos, políticos y sociales de Internet. [13]

Esta afirmación demuestra que resulta indispensable contar con las mínimas medidas de seguridad adecuadas, por lo que la cultura de la seguridad de la información debe cuidarse y mejorarse en el tiempo para estar al día respecto a todas y cada una de las nuevas modalidades delincuenciales que van surgiendo, buscando adelantarse a cualquier tipo de ataques o vulneración.

Sin embargo, garantizar la seguridad absoluta de la información es inviable, tal cual lo sostiene el escritor y consultor en seguridad Glenn S. Phillips, quien menciona cuatro puntos por los que la seguridad total de información no es posible:

> Existe gente involucrada. No existe seguridad absoluta simplemente porque la gente forma la mayor parte del área de riesgo. Ya sea que tenga malas intenciones, o que tenga buenas intenciones, pero comete errores.
>
> El cambio es constante. Aunque el día de hoy logremos asegurar algo, mañana habrá nuevos riesgos. Cambio de gente, tecnología y forma de hacer negocios. El parche que instalé hoy protege contra los riesgos de ayer, no contra los de mañana.
>
> Seguridad es un concepto, no una definición. Se puede definir "entorno seguro" para una situación particular pero no se puede generalizar. Pasar la auditoria únicamente demuestra que se revisó lo que creemos revisable. Esto no cubre riesgos particulares de negocio y riesgos nuevos.
>
> La tecnología es una herramienta, no una solución completa. Demasiados líderes asumen que la seguridad es un problema de tecnología. Citando a Zygmunt Bauman: "las cerraduras pueden

ayudarnos a soslayar el problema o a olvidarlo, pero no pueden obligarlo a dejar de existir." [14]

3.2 ACCIONES A APLICAR

3.2.1 TIPOS DE MEDIDAS

Entre las medidas a emplear para minimizar los riesgos y dotar a la empresa de un nivel adecuado de seguridad, se pueden distinguir dos tipos:

- Medidas preventivas: Aquellas que se deberán implantar para evitar la posible explotación de una vulnerabilidad por parte de una amenaza.
- Medidas correctivas: Medidas que se deberán implantar para solucionar o reparar las consecuencias de ataques o fallas debido a amenazas que se han materializado.

Pueden existir amenazas en la PyME que no necesariamente se materializarán en hechos que afecten a la seguridad de la organización, por lo que no representan un riesgo para la misma, o bien dicho riesgo podría ser asumido por la empresa. Por consiguiente, estas amenazas pueden no ser tenidas en cuenta a la hora de establecer las medidas de seguridad pertinentes.

En la norma ISO/IEC 27002:2013 por ejemplo, existe una gran cantidad de controles, cuya aplicación no sería posible en una PyME, debido a su alto costo de implementación, o porque simplemente la probabilidad de ocurrencia de la amenaza a enfrentar es mínima.

En base a lo expresado, para reducir los riesgos que atentan contra la confidencialidad, integridad y disponibilidad de la información de una PyME, se detallan a continuación las medidas más relevantes que se pueden emplear para proteger adecuadamente su información y recursos informáticos. Se las categoriza en acciones para proteger el hardware, el software, la red, los datos y al personal (ver Gráfico N° 1).

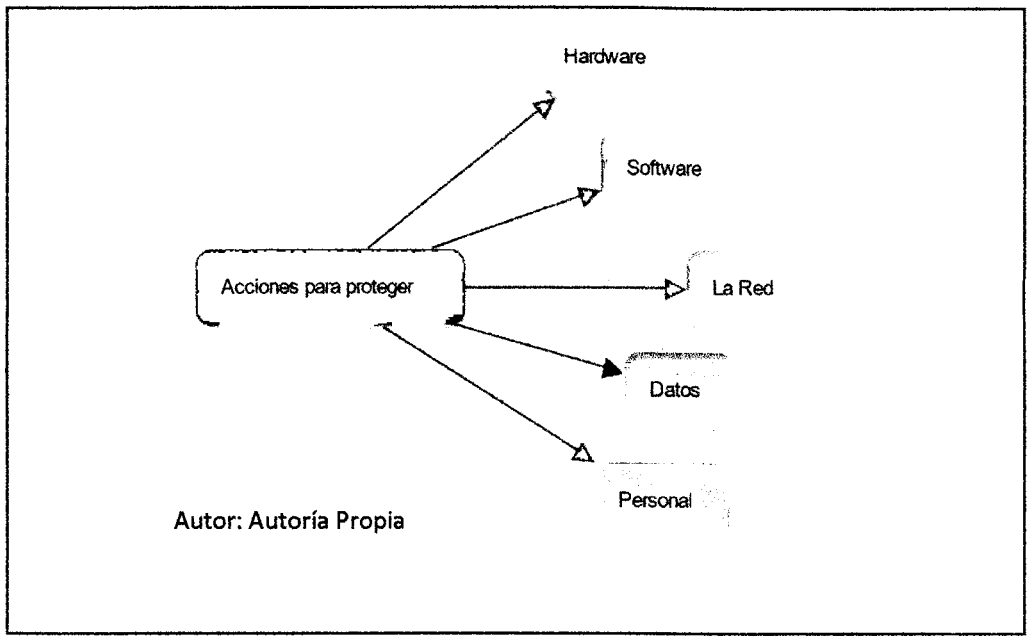


Gráfico N° 1 Categorías de Medidas de Protección

3.2.2 ACCIONES A APLICAR PARA PROTEGER EL HARDWARE

> El hardware es el equipamiento informático con el que contamos para el desarrollo de nuestras tareas cotidianas, ya sea para almacenar los datos de nuestros clientes o para subir nuevos datos e informaciones. Más allá de todas las opciones que hoy nos brindan los servicios online o el *cloud computing*, sigue siendo imprescindible disponer del hardware adecuado para gestionar cualquier proyecto. Y, sin embargo, es uno de los grandes olvidados. [15]

Si se detectan fallas en el correcto funcionamiento y en la seguridad del equipamiento disponible, una PyME se expone a un grave riesgo que puede comprometer en primera instancia la disponibilidad de la información gestionada por dicho hardware.

En este marco, entre las medidas preventivas a adoptar se pueden enumerar:

- Colocar detectores de incendios o matafuegos y ubicarlos en lo posible lejos de cañerías.

- Disponer de candados o cerraduras en las puertas de acceso, que eviten el acceso no autorizado a sitios. a los que debe acceder solo personal debidamente acreditado. Resguardar adecuadamente las llaves y sus copias.
- Disponer y resguardar el acceso físico a los medios que reguardan las copias de los datos, para las cuales deben utilizarse medios de almacenamiento que cuenten con todas las garantías de fiabilidad física y preservación en el tiempo. Deberán estar ubicados en locaciones remotas para prevenir la pérdida de información valiosa por eventuales problemas de acceso u operación del sitio principal de procesamiento y prevenir fallos de hardware o cualquier otra eventualidad natural o artificial, implementando todas las medidas de protección físicas y ambientales aplicables según la criticidad de la información.
- Adquirir dispositivos UPS- *Uninterruptible Power Supply* (sistema de alimentación ininterrumpida), para evitar posibles fallas y daños de los equipos debidos a cortes de energía o variaciones en la tensión y el cierre ordenado de todos los procesos en ejecución al momento del corte de energía.
- Restringir el acceso a los equipos de comunicaciones solo para personal autorizado.
- Aislar y proteger el cableado tanto eléctrico como de telecomunicaciones, para evitar intercepción, interferencia o daño. Se deberá disponer de canales para cableado estructurado, evitando en lo posible que los cables estén al descubierto.
- Controlar el uso de equipos móviles como laptops tanto fuera como dentro de las propias oficinas con el fin de

evitar robos. Se podrán movilizar solo si existe una autorización previa y por razones justificadas.

- Corroborar que los equipos de hardware que ya no se utilicen sean cuidadosamente descartados para evitar fugas de información.
- Disponer de un programa de mantenimiento preventivo para detectar fallos, disminuir costos de reparaciones y detectar puntos débiles en la instalación. El mantenimiento preventivo ayudará a reducir la falta de disponibilidad que puede generarse por un mantenimiento correctivo.

Se listan a continuación algunas medidas correctivas básicas que puede adoptar la PyME:

- Disponer de un técnico, propio o de un servicio tercerizado, que asegure una rápida reparación y puesta en marcha de los equipos si se produce una falla.
- Restaurar en equipos alternativos copias de backup previamente verificadas, en caso de haberse producido un daño en un equipo principal o en un disco u otro medio de almacenamiento. La comprobación de una copia de backup verifica que esté intacta físicamente para asegurar que todos los archivos contenidos en ella se puedan leer y que se puedan restaurar en caso de necesidad, asegurando así la integridad y disponibilidad de la información.
- Disponer de equipo redundante para su utilización en caso de que el equipo principal sufra desperfectos. De no ser esto posible, tener en claro dónde y en qué condiciones se podrá adquirir equipamiento de reemplazo en caso de ser necesario, si se llegara a presentar una falla importante en dispositivos críticos.

Es importante que la PyME estime una ventana de indisponibilidad que esté dispuesta a asumir, asegurando que no le cause un impacto que pueda comprometer seriamente el negocio. Esta evaluación debe contemplar además de los servidores y los equipos de comunicaciones, la falla en estaciones de trabajo o portátiles, consideradas críticas, durante un periodo determinado de tiempo.

3.2.3 ACCIONES A APLICAR PARA PROTEGER EL SOFTWARE

El software, o los programas informáticos, son uno de los elementos más críticos en una empresa. Debido a la falta de concientización de seguridad de los responsables, es muy común que los programas que componen los activos de la empresa no estén correctamente actualizados y preparados para evitar ataques de código malicioso o posibles pérdidas de información no deseadas, por citar solo algunos de los problemas que podrían presentarse.

> El software debe ser una herramienta para facilitar la actividad en el negocio, pero no puede ser una traba o un problema. El software de gestión empresarial es un elemento crítico y estratégico de un negocio, tanto como los medios de comercialización, producción, logística, etc. Las aplicaciones para la gestión empresarial se han convertido en elementos centrales y críticos de la mayoría de organizaciones actuales y en fuente de ventajas competitivas para aquéllas capaces de interpretarlas adecuadamente. En paralelo, el mercado de las Enterprise Applications crece incesantemente impulsado por fenómenos como el Software Libre, el Software as a Service (SaaS) o el Cloud computing; democratizando el acceso a herramientas y soluciones reservadas, hasta hace poco, a las grandes corporaciones y organizaciones públicas. [16]

Entre las medidas preventivas a adoptar dentro de la PyME se puede mencionar:

- Realizar en forma periódica, particularmente cuando sea requerido por el proveedor del software, las actualizaciones oportunas para prevenir problemas de funcionamiento y de seguridad.
- Instalar software contra código malicioso y mantenerlo actualizado.
- Disponer de software de calidad, en lo posible debidamente certificado por su fabricante, con las correspondientes licencias.
- Resguardar las configuraciones de los equipos, pudiéndose proteger imágenes del sistema que contendrán copias de los programas, la configuración del sistema y su parametrización. Dichas imágenes se deben almacenar de forma pertinente en una ubicación remota y se utilizarán para restaurar los sistemas si el disco duro o el equipo completo presentan fallas que comprometen su funcionamiento.
- Documentar las aplicaciones, aspecto sumamente importante si hubiera que efectuar una reinstalación en caso de emergencia o una modificación en la lógica de los programas o en los parámetros de configuración.
- Registrar la creación, modificación y supresión de usuarios en los sistemas para controlar el acceso a los sistemas críticos.
- Establecer una política de contraseñas fuertes para acceder a la red y a los sistemas.

Se listan a continuación una serie de medidas correctivas básicas a adoptar en una PyME:

- Restaurar copias de backup de imágenes de sistema previamente verificadas. Como ya se mencionó, la

comprobación de una copia de backup verifica que esté intacta física y lógicamente, para asegurar que se pueda leer y restaurar en caso de necesidad, asegurando así la continuidad de las operaciones.

- Verificar periódicamente el software instalado en estaciones de trabajo y suprimir cualquier programa cuya instalación no hubiera sido autorizada, que haya quedado en desuso o que no sea de utilidad para el propósito de la empresa.
- Considerar la posible indisponibilidad de cualquier programa o aplicación local que no sea crítico durante un periodo determinado de horas. Dependiendo de la criticidad y del proceso que maneje el software, se deberán definir ventanas de tiempo, como por ejemplo, que no se pueda prescindir del software que maneja el stock o la facturación durante periodos mayores a 24 horas.
- Implementar el uso de software antivirus que permita realizar análisis preventivos y correctivos. Existen en el mercado varias opciones muy buenas a precios accesibles, así como productos de libre disponibilidad.

3.2.4 ACCIONES A APLICAR PARA PROTEGER LA RED

> Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios. [17]

La red informática es uno de los elementos más sensibles en la infraestructura tecnológica de cualquier organización y, por lo tanto,

también de una PyME. Sin embrago, en general en este tipo de empresas, no existe consciencia sobre lo perjudicial que puede llegar a ser un ataque proveniente del exterior sobre sus redes, así como tampoco se tiene en claro cuál sería la magnitud de los daños que se podrían generar si se llegara a producir un incidente originado internamente que comprometa los servicios de la red. Una red de computadoras es en última instancia, una forma de compartir recursos y es por eso mismo que se puede incrementar el riesgo de accesos no autorizados.

Entre las medidas preventivas a adoptar dentro de la empresa, se podrían destacar las siguientes:

- Instalar una red interna para garantizar que todas las comunicaciones locales y de carácter confidencial no salgan del perímetro de la propia empresa.
- Establecer medidas adecuadas de seguridad para enviar información confidencial a un externo, como el uso de mecanismos criptográficos, existiendo varias opciones de software libre sin costo que sirven para este fin.
- Mantener correctamente instalado y actualizado el software de seguridad de la red, como el firewall y el antivirus de red.
- Establecer políticas de seguridad de acceso a la red.
- Establecer una correcta configuración de seguridad para la red inalámbrica y los dispositivos de comunicaciones que evite el ingreso de terceros no autorizados.

Con relación a las medidas correctivas a adoptar dentro de la empresa:

- Disponer de personal de mantenimiento de la red, propio o tercerizado (personal del proveedor de los servicios de

comunicaciones), lo que asegure una rápida reparación y restablecimiento del servicio.

- Contar con personal propio o tercerizado versado en el mantenimiento y reparación de cableado estructurado, que permitirá reparar en forma expedita algún daño físico a la infraestructura de la red.
- Restaurar copias de respaldo para la instalación y configuración de la red en el caso de haberse producido una pérdida de datos.
- Considerar la posibilidad de contratar un segundo proveedor de Internet, para el caso de que se presenten problemas en el acceso a la web con el proveedor principal.

La empresa podrá considerar la disponibilidad de los servicios de telecomunicaciones (fundamentalmente el acceso a Internet) en forma intermitente durante la jornada de trabajo, con una incidencia no mayor a un número dado de horas/días, de manera de minimizar el impacto sobre la operatoria de la organización.

3.2.5 ACCIONES A APLICAR PARA LA PROTECCIÓN DE LOS DATOS

La información es un elemento necesario para el proceso de toma de decisiones en toda organización y, sobre todo, en las empresas que se proponen satisfacer las necesidades del consumidor y ofrecer un alto nivel de calidad. Las empresas son cada vez más dependientes de la información para mantener sus actividades y por lo tanto, es lógico suponer que aquellas organizaciones que sean capaces de gestionarla adecuadamente a través de los sistemas que la sustentan, se posesionarán mejor ante sus competidores, produciendo mejores ofertas, más competitivas y a la medida de las expectativas de sus clientes.

La necesidad de la PyME de enfocar todo su esfuerzo al sector del mercado al cual dirige su producción de bienes o servicios, requiere que disponga de información actualizada y precisa acerca de dicho ámbito, con el fin de dirigir acertadamente sus acciones para el cumplimiento de sus objetivos y para la creación de valor.

En este contexto, se pueden citar las siguientes medidas preventivas a adoptar en la empresa, para la protección de sus datos:

- Instalar las bases de datos centralizadas, incluyendo la posibilidad de utilizar servicios en la nube, donde se almacene la información importante generada por la empresa para facilitar el almacenamiento, accesibilidad y seguridad de los datos. Asegurarse previamente de la fiabilidad de estas plataformas y de su seguridad, verificando la inclusión de cláusulas contractuales que determinen los niveles de servicio y la disponibilidad y la seguridad de los datos.
- Determinar procedimientos que establezcan las acciones a realizar en caso de pérdida de datos. Entre los detalles a considerar, está la determinación de cuáles van a ser los periodos de tiempo en que se va a mantener el respaldo de la información y qué información se va a respaldar.
- Realizar back ups periódicos de los datos de la PyME, probando siempre que es posible su restauración.

Las medidas correctivas a adoptar dentro de la empresa se listan a continuación:

- Restaurar copias de respaldo en el caso de haberse producido una pérdida de datos.

- Considerar instancias de operación en instalaciones alternativas en caso de que no pueda continuarse con las operaciones en la instalación principal.

Se debe considerar la eventual pérdida de datos públicos, como por ejemplo la información publicada en sitios web a la que no se podría acceder si el sitio es dado de baja o si se encuentra fuera de línea.

3.2.6 ACCIONES A APLICAR PARA PROTEGER AL PERSONAL

De nada sirve tener abundante capital y recursos tecnológicos si no se cuenta con un buen equipo humano de trabajo que logre llevar adelante a la empresa. Lamentablemente, muchas veces esto no es una prioridad en una PyME y se suele dedicar muy poco esfuerzo a la tarea de seleccionar, organizar y capacitar a quienes deben llevar adelante las actividades vinculadas al procesamiento de la información de la empresa.

En cualquier organización el personal con el que se cuente es un factor predominante para la consecución de sus objetivos. Sin embargo, un empleado descontento puede provocar graves daños desde su propio sitio de trabajo, particularmente si hace un uso irresponsable de las tecnologías y pone en riesgo la seguridad de la información.

En efecto, la mayoría de la información estadística señala que muchas de las fallas o ataques informáticos que sufren las empresas tiene un origen interno.

En el caso de una PyME, un ataque desde dentro es menos probable, debido a casi siempre quienes trabajan en la empresa son a la vez sus propios dueños, o son personal contratado que suele desarrollar fuertes lazos de pertenencia, por lo que en consecuencia no realizarán acciones conscientes que provoquen un daño. Sin perjuicio de ello, y como se ha comentado ya con anterioridad, el elemento humano de un PyME suele estar poco concientizado respecto a la

seguridad y la mayoría de las empresas no disponen de una política de respaldo para garantizar la defensa de su información.

En el conjunto de medidas preventivas a adoptar en la empresa, se encuentran:

- Verificar la disponibilidad de referencias personales satisfactorias, la constatación de la honradez y la idoneidad del elemento humano a ser contratado.
- Concientizar a todo el personal sobre la importancia de mantener un adecuado nivel de seguridad de la información en los procesos que se realizan y sobre los riesgos que implica el uso de equipos móviles, ante la eventualidad de su robo y la posible pérdida de información sensible.
- Identificar activos individuales y asignar la responsabilidad de su uso al personal que corresponda, documentando los detalles de la responsabilidad y los controles, garantizando su buen manejo, monitoreo y su devolución cuando la persona deja de pertenecer a la empresa o cambia en su función.
- Establecer una adecuada política de seguridad de información, que sea conocida y entendida por todos los empleados y por terceros que prestan servicios o se vinculan de alguna manera con la información de la organización.
- Procurar la capacitación periódica al personal, especialmente de aquellos que manejan recursos informáticos críticos.

Las medidas correctivas a adoptar en la empresa, por su parte, contempla las siguientes acciones:

- Solicitar la firma de acuerdos de confidencialidad que de alguna forma garanticen el buen manejo de la información

a la que tendrá acceso el personal, los cuales continuarán vigentes aún si el empleado deja de pertenecer a la empresa.

- Proveer y aplicar un proceso disciplinario formal para sancionar a los empleados que hayan infringido cualquier mecanismo de seguridad de la información.

La empresa deberá contemplar la posibilidad de no poder contar con personal tercerizado que por alguna razón ya no pueda asistir a las labores por la que se lo había contratado, debiendo tener en definidas alternativas a considerar en este caso.

CAPITULO IV

4.1 ALCANCE DEL CAPÍTULO

En esta sección se definen una serie de pautas que, a manera de modelo, deben verse reflejadas en una PSI de una PyME, posibilitando que se atiendan debidamente las cuestiones a tener en cuenta en una empresa de este tipo para proteger sus recursos.

Usando esas pautas, se espera mejorar la seguridad de la información de la empresa y facilitar la redacción de una PSI, al presentar en forma simplificada sus contenidos.

A continuación, se describen los principales aspectos a ser considerados, elaborados en base a las buenas prácticas listadas en la ISO/IEC 27002:2013 y analizadas desde la perspectiva de una PyME en el Anexo D de este trabajo final de especialización. Se espera de esta forma simplificar la tarea de los encargados de la seguridad de la información cuando deban encarar la redacción del documento. Se aclara, sin embargo, que cada recomendación debe ser analizada y adaptada a la realidad de la organización en la que se pretenda aplicar este modelo.

4.2 PORQUÉ USAR UN MODELO DE PSI

En la actualidad, la seguridad de la información ha tomado un enorme impulso, debido al sinnúmero de amenazas que aparecen en forma cotidiana y al surgimiento de nuevas plataformas e infraestructuras de procesamiento de información que muchas veces salen al mercado sin las condiciones de seguridad requeridas, es decir, sin la madurez necesaria para ofrecer un funcionamiento libre de fallas.

La realidad contundente es que Internet ha revolucionado la forma en que interactuamos con los demás. En efecto, el aumento de la conectividad hace que un número cada vez mayor de personas esté conectada en un espacio público, proveyendo una plataforma dinámica y creciente que permite que avance la comunicación, la colaboración y la innovación de maneras que nunca hubiéramos podido imaginar

previamente. El universo de las PyME se ha beneficiado de estos avances y se caracteriza por utilizar Internet en forma intensa.

Sin embargo, la creciente conectividad e interdependencia de las plataformas y servicios basados en Internet, trae aparejado un aumento considerable de la exposición a una gran cantidad de actividades y actores relacionados con la delincuencia y la inseguridad. Todos los días aparecen noticias de incidentes y ataques cibernéticos, que se realizan con intención delictiva, y cuya frecuencia y sofisticación están aumentando. Actualmente se entiende que el delito cibernético no reconoce fronteras ni respeta personas o instituciones.

Por lo tanto, se requiere un esfuerzo denodado para abordar la gran cantidad de amenazas informáticas que podrían afectar a la tecnología y a la información. Estos riesgos también acechan a las PyME y en consiguiente, es importante que adopten medidas de protección para minimizar su impacto.

Una PSI particularmente, surge como un instrumento para hacer conocer a los miembros de una organización la importancia y sensibilidad de la información, los servicios críticos que permiten a la empresa desarrollarse en su sector de negocios y el comportamiento esperado en cuanto a su protección. Además, fija los mecanismos que deben adoptar las empresas para salvaguardar sus sistemas y la información que procesan. En el Gráfico N° 2 a continuación, se especifica un resumen de los principales temas que atiende una PSI y sus posibles aristas.

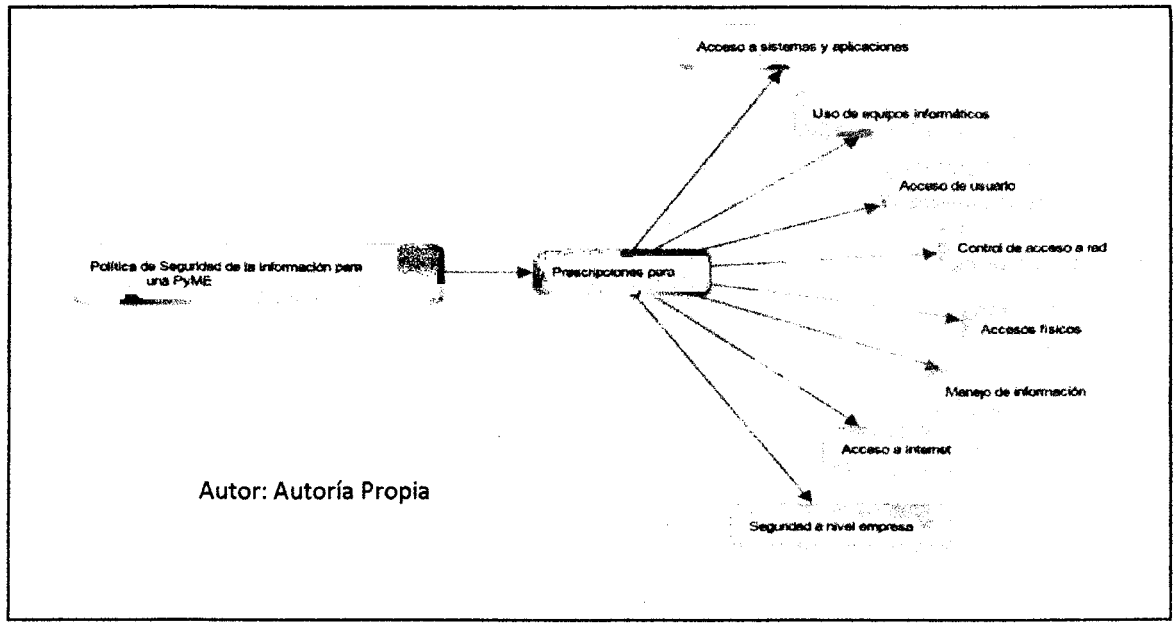


Gráfico N° 2 Políticas de seguridad de la información para PyME

La PSI no se puede considerar solo como una descripción técnica de mecanismos de seguridad, ni como una lista de penalidades que involucre sanciones a conductas de los empleados. Por el contrario, es una descripción de lo que se desea proteger y el porqué de ello, generándose una vía de comunicación entre los superiores dirigida a los empleados respecto al proceder esperado en el tratamiento y la protección de la información de la organización.

En vista de lo mencionado, el desarrollo y la implementación de una política de este tipo requerirán principalmente un alto compromiso de la dirección y de todo el personal, y una serie de destrezas y experiencia técnica para determinar el camino a seguir. Otro aspecto a considerar es la importancia de su actualización, en función del dinámico ambiente que rodea a las organizaciones modernas y al ciberespacio.

Las tecnologías por sí mismas de poco sirven, es lo que la gente hace con ellas lo que marca la diferencia. Una PSI constituye la base de un uso seguro de estas tecnologías en la empresa. Esto aplica a todo tipo de organización, incluyendo a las PyME.

4.3 OBJETIVOS DE LA POLÍTICA

Los objetivos de la PSI son:

- Transmitir el comportamiento esperado por los responsables de la PyME a los empleados, en materia de protección de la información y uso seguro de los recursos informáticos.
- Resguardar la confidencialidad, disponibilidad e integridad de los datos.
- Disminuir los posibles efectos perniciosos de la materialización de amenazas a la seguridad de la información.
- Evitar el uso irresponsable de recursos, que pueda comprometer la seguridad de la información.
- Concientizar a todos los que conforman la empresa y a los que interactúan con ella, si fuera el caso, sobre los riesgos asociados a la inseguridad de la información.

4.4 DISTRIBUCIÓN Y DIFUSIÓN

Una vez avalado y aprobado por los responsables de la PyME, el documento debe ser difundido a todos los empleados de la empresa y a los clientes, intermediarios o proveedores que pudieran estar alcanzados parcial o totalmente por sus contenidos, con la finalidad de que se conozcan el comportamiento esperado y las obligaciones que les competen para el manejo seguro de los activos de información en la PyME.

4.5 ALCANCE Y USO

La PSI debe ser utilizada para gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la empresa. Se aplica en todo el ámbito de la empresa, a sus recursos y a la totalidad de sus procesos, internos y externos. En este contexto, la información que se genera y gestiona en la institución debe ser siempre considerada como un activo, en muchas ocasiones

clave, que debe ser protegido para asegurar el éxito y la continuidad del negocio.

4.6 GLOSARIO DE TÉRMINOS

Backup.- Es la copia de la información como respaldo, que se realiza para hacer frente a posibles eventualidades como fallas eléctricas o electrónicas, robos, ataques cibernéticos, desastres naturales, o cualquier otra situación que pudieran poner en peligro la continuidad del negocio, debiendo ser resguardado en una ubicación geográfica distinta a donde se encuentra la información original.

Comunicación. - Cuando se lleva a cabo la transmisión de la información desde un equipo a cualquier otro. Para que se pueda realizar una transmisión de información, son necesarios tres elementos: el emisor, quien origina la información, el medio de transmisión y el receptor, quien recibe la información.

Confidencialidad. - Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Correo electrónico. - También conocido como "*E-mail*". Es un servicio de red que permite a los usuarios enviar y recibir mensajes electrónicos mediante sistemas de comunicación electrónica. Dependiendo del sistema que se utilice se pueden enviar toda clase de archivos.

Disponibilidad. - Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Estaciones de trabajo. - Es el computador asignado a un usuario de la empresa. Una estación de trabajo también se conoce como PC, equipo o máquina.

Estándar. - Es una norma, regla, patrón o referencia que debe ser seguida por la audiencia para la que fue creada.

Integridad. - Propiedad de la información relativa a su exactitud y completitud.

Id (identificación) de usuario. - Elemento utilizado para que los beneficiarios de acceso a un sistema puedan ser reconocidos. Para ello, el usuario necesita una cuenta, en la mayoría de los casos asociados a una contraseña. Para acceder a un sistema se utiliza una interfaz de usuario.

Malware.- Se trata de un término genérico que agrupa programas informáticos que tiene efectos indeseados o maliciosos, también referido como "código malicioso". Incluye entre otros, virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza para difundirse herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios de almacenamiento extraíbles como dispositivos USB. También se propaga a través de descargas inadvertidas y ataques al software. La mayoría del malware actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fraudes y otras actividades delictivas.

Plan de contingencia. - Es un conjunto de medidas encaminadas a restaurar el funcionamiento normal de una actividad tras la alteración producida por un incidente. Un plan de contingencia tiene carácter reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas. Propone una serie de procedimientos alternativos al funcionamiento normal de una organización, cuando alguna de sus funciones usuales se ve perjudicada por un imprevisto interno o externo.

Red de computadoras. - A nivel más elemental, una red no es más que un conjunto de máquinas (computadoras, impresoras y otros recursos), es decir un medio compartido, junto con una serie de reglas (protocolos) que rigen el acceso a dicho medio.

Usuario. - Entidad que dispone de un conjunto de permisos y de recursos, a los cuales tiene acceso. Es decir, un usuario puede ser

tanto una persona como un dispositivo o una aplicación a la que se le asigna derechos de uso de recursos informáticos.

Nube. - La computación en la nube, conocida también como servicios en la nube es una instancia que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

4.7 PRESCIPCIONES PARA ACCESO DE USUARIOS

Entre los lineamientos para el acceso de usuarios, debe tenerse en cuenta lo siguiente:

- Requerir la firma de una declaración de aceptación de las condiciones de uso del sistema.
- Cancelar las Id de usuario de empleados que ya no trabajen en la empresa, haciendo efectiva dicha cancelación en forma inmediata.
- Verificar la eliminación de Id de usuarios por defecto o prestablecidos.
- Asegurar que se creen Id para nuevos usuarios en forma oportuna, de manera de no obstaculizar su trabajo.
- Solicitar el cambio de contraseñas predeterminadas por el sistema.
- Monitorear la asignación y uso de cuentas de usuarios con privilegios.
- Designar un administrador como único responsable de la asignación de permisos a los usuarios y monitorear su funcionamiento en forma permanente.
- Establecer que la asignación de privilegios a los usuarios sea determinada en base al mínimo acceso que se requiera para la función encargada.

- Documentar y mantener actualizados todos los privilegios asignados a cada usuario.
- Revisar al menos cada 6 meses los permisos y privilegios otorgados a cada usuario.

Sobre los lineamientos para el uso de contraseñas:

- Solicitar a los usuarios que acepten firmar una declaración que establezca su compromiso de mantener secretas sus contraseñas.
- Asegurarse del reemplazo inmediato de las contraseñas temporales asignadas a los usuarios.
- Concientizar a los usuarios sobre la importancia de no anotarlas en sitios inseguros o compartirlas con otros usuarios, así como de otras cuestiones vinculadas a su protección.
- Si se sospecha que una contraseña ha sido comprometida, indicar a los usuarios que deben solicitar su cambio inmediatamente.
- Dependiendo del sistema, establecer que las contraseñas deben tener un mínimo de seis caracteres y ser una mezcla de letras mayúsculas, minúsculas, números y caracteres especiales.
- Requerir el cambio de contraseñas con una frecuencia pre-establecida, que se sugiere sea como máximo cada tres meses.

Respecto a los equipos de los usuarios:

- Propiciar el uso de pantallas de bloqueo de todos los equipos de la organización.
- Requerir que se apaguen los equipos de computación sin uso una vez finalizada la labor diaria, salvo que existan

razones operativas que exijan que permanezcan encendidos.

4.8 PRESCIPCIONES PARA ACCESO A SISTEMAS Y APLICACIONES

Sobre el monitoreo de acceso al sistema, se debe considerar lo siguiente:

- Producir, mantener y revisar periódicamente los registros de eventos que puedan servir para determinar patrones anómalos con efectos negativos sobre la seguridad del sistema.
- Incluir en los registros, datos como ids de usuario, fecha y hora del evento y desde qué terminal se ingresó, entre otros.

Sobre el acceso a las aplicaciones:

- Restringir el número de intentos para acceder a las aplicaciones del sistema y si no procede la autenticación, bloquear el usuario. El valor sugerido debe analizarse en función de cada empresa, sugiriéndose entre 3 y 5 intentos.
- Restringir el acceso de los usuarios a las funcionalidades de la aplicación que no requieren para su función.
- Mostrar algún tipo de advertencia como medida disuasiva cuando se intente acceder en forma no autorizada.
- Asegurar que el personal se encuentre al tanto de la criticidad de la información producida por cada aplicación.
- Asegurar que la información solo pueda ser obtenida por el personal autorizado.

4.9 PRESCIPCIONES PARA EL MANEJO DE INFORMACIÓN

Respecto al manejo de la información, se deben considerar los siguientes aspectos:

- Establecer una capacitación apropiada y actualizaciones regulares para todo el personal, sobre la política de seguridad y los procedimientos de la organización. Dejar evidencia de estas actividades.
- Prohibir a los usuarios el uso de servicios no autorizados, y no permitir que se compartan cuentas o contraseñas entre usuarios.
- Prohibir la guarda de información crítica en las estaciones de trabajo. Utilizar para ello un servidor de archivos con adecuada protección de acceso.
- Establecer que cada usuario será responsable por la estación de trabajo y otros recursos que utiliza.
- Proveer un gabinete con acceso restringido para la información crítica impresa o contenida en medios digitales, exigiendo su debido resguardo.

Respecto a los documentos en papel, se debe considerar lo siguiente:

- Situar en un lugar de acceso restringido y controlado cualquier dispositivo como impresoras o máquinas de fax, que puedan generar duplicados de información confidencial del sistema.
- Verificar periódicamente impresoras, máquinas de fax y áreas adyacentes para asegurarse de que no queden copias desatendidas, las que de encontrarse deben ser destruidas.

- Recoger inmediatamente todos los faxes, impresiones y/o fotocopias que contengan información confidencial para evitar su revelación.
- Disponer de trituradoras de papel de ser posible, o asegurarse de eliminar todos los papeles o documentos que sea necesario destruir, a fin de evitar que un intruso pueda obtener información de la basura. De igual manera, disponer de un adecuado desecho de dispositivos de almacenamiento obsoletos.

Respecto al respaldo de la información o backup:

- Conservar copias de respaldo de los archivos críticos en sitios remotos, manteniendo un registro detallado de dichas copias, y proveer adecuados medios para la protección de su acceso en función de la criticidad de la información que contienen.
- Asegurarse de forma permanente la prueba de los medios de backup, garantizando así la recuperación de información crítica en caso de compromiso o desastre.
- Coordinar la periodicidad de los respaldos, pudiendo ser de tipo mensual, semanal o diario y asegurar que sean llevados a cabo por los responsables asignados a la tarea.

4.10 PRESCRIPCIONES DE SEGURIDAD A NIVEL EMPRESA

Respecto a la competencia y roles de dirección de la PyME:

- Instaurar los roles y responsabilidades respecto a la seguridad de la información para cada uno de los integrantes de la PyME.
- Desarrollar programas de concientización de seguridad de la información.

- Verificar la idoneidad de los controles específicos de seguridad de la información para los activos de información y coordinar su implementación.
- Investigar todo evento o sospecha de ocurrencia de un incidente de seguridad de la información.
- Designar a un responsable que elabore un informe detallado sobre los empleados que infrinjan las políticas de seguridad y determine las sanciones que correspondan.
- Determinar los parámetros y evaluar la clasificación de los activos de información, de acuerdo a su nivel de protección más adecuado.

Sobre la preparación ante desastres que impidan la operación:

- Desarrollar procedimientos a seguir en el caso de que un imprevisto o desastre natural o artificial llegue a afectar a la operatoria de la organización.
- Determinar en forma precisa qué funciones corresponden a cada persona involucrada, considerando además la posibilidad de no poder contar con el personal asignado, y si así lo fuere, determinar sustitutos que puedan suplir las vacantes.
- Realizar simulacros de contingencia de manera anual o dependiendo de las eventualidades que se presenten.
- Realizar programas de difusión y capacitación sobre la importancia del estar prevenidos respecto a la ocurrencia de desastres o de eventos no planificados que impidan continuar con la operación de la organización y conocer los roles y procedimientos a seguir.

4.11 PRESCRIPCIONES PARA EL USO RESPONSABLE DE EQUIPOS INFORMÁTICOS

Es importante considerar el uso correcto de los equipos informáticos con el fin de desarrollar acciones que armonicen con la seguridad de la información en las actividades del negocio. Efectivamente, estos recursos deben ser utilizados siempre de manera adecuada, eficiente y segura.

Sobre el mantenimiento y uso de los equipos informáticos:

- Establecer un relevamiento o inventario de todos los equipos de la PyME, el cual debe permanecer actualizado.
- Realizar un mantenimiento preventivo a todos los equipos que conforman el parque tecnológico de la PyME.
- Llevar un registro de las fallas que ocurrieren en cada equipo y del mantenimiento preventivo.
- Controlar que los equipos informáticos permanezcan en el lugar designado originalmente y que solo sean trasladados mediando la debida autorización.
- Asegurar que las reparaciones sean llevadas a cabo solo por el personal autorizado, propio o contratado para tal efecto.
- Usar el equipo de acuerdo a las recomendaciones del fabricante.
- Si llegara a ser necesario el traslado del equipo para su reparación, asegurar que la información sensible a la empresa se encuentre protegida o sea eliminada, según el caso.
- Controlar las condiciones ambientales dentro de la organización de acuerdo a los requerimientos del fabricante, a fin de asegurar un escenario óptimo para los equipos.

Sobre los equipos inalámbricos:

- Capacitar al personal respecto a los riesgos del uso de tecnología móvil.
- Mantener condiciones de seguridad como instalación de software contra malware y configuraciones seguras.
- Asegurar que equipos de transmisión queden guardados en un sitio seguro para evitar posibles hurtos.
- Evitar el uso de conexiones de comunicación que no hayan sido autorizadas o sean ajenas a la organización.

Sobre el uso de energía eléctrica de respaldo:

- Asegurar la instalación de alimentadores en un número necesario para proporcionar un adecuado suministro eléctrico.
- Usar bancos de energía para todos los equipos informáticos que manejen información crítica, constatando que efectivamente están cumpliendo con su cometido.
- Usar supresores de picos eléctricos o filtros reguladores de tensión que ayuden a evitar daños en los equipos por posibles variaciones de voltaje.

Sobre el cableado eléctrico y de redes:

- Separar el cableado eléctrico del de telecomunicaciones, para evitar interferencias electromagnéticas.
- Procurar que el cableado de redes vaya correctamente guiado a través de canaletas, con la suficiente capacidad para contener nuevos cables que necesiten ser colocados.
- De ser posible, instalar el cableado eléctrico y de redes por vía aérea o subterránea.
- Contar con protección contra incendios, como matafuegos y que su carga se controle periódicamente.

4.12 PRESCRIPCIONES PARA ACCESO FÍSICO RESPONSABLE

Respecto al acceso físico a las instalaciones de la organización:

- Asegurar que siempre exista personal encargado de controlar el acceso y eventualmente acompañar a terceros ajenos a la empresa, previo al ingreso a la zona de procesamiento de información y otras instalaciones críticas.
- Instalar de ser posible, un sistema de cámaras de vigilancia y monitorear las grabaciones.
- Contratar un sistema de vigilancia o control por alarma remota en caso de intrusiones, en días y horarios no laborables.
- Implementar la identificación de todo el personal de la organización a través de elementos tales como credenciales que sean fácilmente reconocibles, de manera de poder alertar en caso de acceso de personal no autorizado.
- Asegurar que el personal de recepción registre los ingresos y salidas de todo el personal a las instalaciones de procesamiento de datos.
- Procurar indicaciones visibles al público para señalar restricciones de acceso.

4.13 PRESCIPCIONES PARA EL CONTROL DE ACCESO A RED

Sobre la utilización de los servicios de red:

- Establecer restricciones a la red, segmentándola de ser posible, si la sensibilidad de la información lo amerita.
- Efectuar una evaluación periódica para constatar su buen estado.

- Si un usuario debe compartir elementos en la con otros, incorporar una clave de acceso y cambiarla periódicamente, documentando los permisos otorgados.

Sobre infecciones de código malicioso:

- Definir el curso de acción a seguir en el caso de que una estación de trabajo sea afectada por software malicioso.
- Constatar que las actualizaciones del sistema operativo y de las aplicaciones de las estaciones de trabajo estén al día.
- Instalar y mantener actualizado software anti malware de reparación.

4.14 PRESCRIPCIONES SOBRE EL ACCESO A INTERNET

Sobre el servicio de Internet:

- Procurar que el uso del servicio de Internet esté dirigido exclusivamente para facilitar la realización de actividades relacionadas con la labor diaria, propiciando un uso racional y apuntando siempre hacia la rentabilidad y el empleo con fines laborales.
- Prohibir la instalación de programas y la descarga de información desde Internet hacia las estaciones de trabajo.
- Usar única y exclusivamente las aplicaciones para navegar provistas en las estaciones de trabajo.
- Permitir el acceso a cualquier sitio de Internet que tenga relación con el quehacer de la empresa, quedando estrictamente prohibido o limitado el ingreso a redes sociales personales, sitios de contenido sexual, terrorismo o contrarios a las buenas costumbres o el buen

gusto y la descarga de elementos sin la debida licencia o permiso.

- Prohibir el uso del servicio de Internet por parte de cualquier persona ajena a la empresa, excepto que exista expresa justificación para tal acceso y el mismo se realice en forma controlada.

Respecto al uso del correo electrónico:

- Controlar que el uso de correo electrónico sea exclusivamente para el envío de información pertinente a la empresa y no como casilla personal.
- Evitar la apertura y el reenvío de correos de dudosa procedencia.
- Al trabajar con información del tipo confidencial, crítica o sensible, tomar recaudos sobre los mecanismos necesarios para asegurarla previo a su envío.
- Concientizar al usuario sobre los riesgos del mal uso del correo electrónico y las implicaciones que traería a la seguridad y reputación de la empresa.
- Tomar precauciones respecto a la revisión de cualquier tipo de archivo adjunto a correos, antes de ser descargado a la estación de trabajo.
- Establecer de ser posible, el uso de encriptación para corroborar la legitimidad y confidencialidad del correo con información importante.

CONCLUSIONES

Como principales conclusiones del presente trabajo final de especialización, se puede afirmar lo siguiente:

- Existe un conocimiento limitado o nulo de estándares y de buenas prácticas en materia de seguridad de la información por parte de los involucrados en la actividad empresarial a escala pequeña y mediana.
- Los responsables de las empresas PyME suelen tener la falsa creencia de que no les puede pasar nada que les impida continuar con sus actividades. Esta percepción no es correcta debido a que en la actualidad cualquier organización, con independencia de su tamaño o actividad, es un objetivo potencial de ataque malicioso. Por otro lado, se han verificado muchos vectores de ataque que aprovechan las vulnerabilidades de organizaciones pequeñas que conforman la cadena de suministros de entidades más grandes, para atacar a éstas últimas.
- Debido a su generalmente escaso presupuesto, las PyME no cuentan con personal especializado en seguridad de la información, ni con un servicio externo que les brinde un asesoramiento adecuado. En este contexto y frente a problemas de seguridad, suelen recurrir a terceros que brindan servicios de soporte informático o a proveedores de equipamiento informático, quienes tampoco suelen conocer lo suficiente sobre cómo asegurar la información. Esto plantea para las PyME una dificultad que de alguna manera se debe soslayar, ya que cualquier compromiso de su información acarreará potencialmente pérdidas económicas, daños en la reputación y en la confianza de los clientes y eventuales sanciones de entidades reguladoras, si fuera el caso.

- A menor tamaño de la empresa, y con la excepción de las empresas dedicadas a la seguridad de la información, suele haber un menor nivel de protección de la información.
- Las deficiencias en la cultura de seguridad en las PyME, ocasionan que los directivos, generalmente los dueños de la entidad, no tenga ningún atisbo de precaución en proteger la información de la empresa.
- Las organizaciones necesitan políticas para cumplir con los requerimientos de seguridad de la información. Si bien las empresas grandes suelen estar sujetas a regulaciones sectoriales, las PyME no suelen verse obligadas a cumplir con ningún tipo de normativa o control en materia de protección de la información. Es precisamente esta falta de formalidad y de control lo que aumenta el nivel de exposición de este tipo de organizaciones, que en general carece de guías o lineamientos a seguir para proteger sus recursos.
- En muchos países de la región y particularmente en Ecuador, hay una falta de oferta de servicios de asesoramiento técnico en seguridad informática para las PyME debido al retraso en adopción de nuevos estándares y a una cultura poco desarrollada de la seguridad de la información. La ausencia de oferta académica en las instituciones de educación superior del país o de inclusión de esta temática en los programas curriculares de las carreras de informática es otro agravante.
- Para que la seguridad de la información sea un hecho, es necesario partir de los riesgos a los que se encuentran expuestos los activos de información, evitando que se materialicen amenazas que puedan tener consecuencias graves para cualquier empresa, con el perjuicio económico que acarrea.
- La elección e implementación de un estándar o buena práctica sobre seguridad de la información en una organización depende exclusivamente de sus necesidades y recursos, pero sobre todo

del compromiso que asuman los directivos de la empresa para implementarlo. Todos los integrantes de la PyME deben estar prevenidos de los graves problemas que conlleva la falta de protección de la información. Sin embargo, son los dueños y máximos responsables de la pequeña o mediana empresa los que deben ser los guías conductores en este camino.

No se consigue asegurar adecuadamente la información con la instalación de un software antimalware en cada computador de la organización, que muchas veces ni siquiera se mantiene actualizado. Su protección va más allá de la compra e implementación de herramientas de tecnología. Implica la adopción de buenas prácticas y procedimientos y la concientización de los empleados. No habrá mucho que hacer si se adquieren los mejores equipos de comunicación con un mecanismo de encriptación fuerte, si la contraseña está anotada en la puerta de la oficina, o si los empleados usan contraseñas robustas, pero no hay conciencia de que hay que cambiarlas cada cierto tiempo y no compartirlas. Todo esto atenta contra la posibilidad de minimizar los riesgos conocidos o de afrontar con mayores garantías las posibles amenazas que pueden impactar sobre la empresa.

Se constituye entonces un verdadero desafío el cambiar la mentalidad de este sector empresarial marcado por el sentido informal o familiar del negocio.

Las políticas de seguridad, complementadas con adecuados procedimientos, se deben considerar como una herramienta que ayude a la PyME a comunicar y concientizar a cada uno de sus integrantes sobre la importancia y criticidad de la información y de las áreas clave que la gestionan, lo cual ayudará a la empresa a desenvolverse de forma saludable y a evitar o mitigar riesgos innecesarios.

Este trabajo de especialización enfoca sus esfuerzos en desmitificar a la seguridad de la información como una materia que debe preocupar en forma exclusiva a las grandes empresas, y que solamente se puede conseguir con muchos recursos y personal

especializado, buscando posicionarse como un punto inicial de referencia.

Las PyME constituyen un amplio mercado que debe ser atendido en sus aspectos vinculados a la seguridad de la información de forma urgente, por la importancia que tiene para el motor productivo de los países de la región y por el nivel de interconexión que muestran en su integración en la cadena productiva de las grandes empresas.

RECOMENDACIONES

Como complemento a lo desarrollado en el presente trabajo de especialización, se exponen a continuación las siguientes recomendaciones para fortalecer la seguridad de la información en las PyMES.

Resulta clave que los directivos de estas empresas sumen conocimientos básicos de seguridad de la información como un adicional a sus habilidades para dirigir el negocio. Debería designarse un responsable interno o como alternativa, contratar un servicio tercerizado que se encargue de impulsar todo lo relacionado con el tema.

En lo que concierne a la implementación de buenas prácticas de seguridad de la información, deben realizarse los mayores esfuerzos en los siguientes aspectos esenciales:

- Identificar los activos críticos de información que posee la PyME.
- Establecer el valor de la información para el negocio y la dificultad de volverla a reconstruir si se destruye, altera o pierde, así como las consecuencias de su divulgación no autorizada y de su falta de disponibilidad cuando se la necesita.
- Determinar claramente quiénes están autorizados para acceder a la información y qué pueden hacer con ella.
- Ser consciente de la ventana de tiempo en la que se puede recuperar y acceder a la información si no está disponible por alguna razón, debido a su pérdida o alteración no autorizada o prevista.

Sobre la implantación de políticas de seguridad, se deben tener en cuenta las siguientes pautas:

- Estar escrita en un lenguaje que sea lo más simple posible, tratando de evitar que por su difícil entendimiento pueda no ser adoptada.
- Basarse en las razones que tiene la empresa para proteger la información.
- No ser restrictiva, de manera que no impida la obtención de los objetivos del negocio.
- Al momento de su redacción y actualización, tomar en cuenta la opinión del personal que está efectuando tareas críticas en la empresa.
- Definir el papel y responsabilidades de los roles involucrados.
- Estar fundamentada en estándares y procedimientos para la seguridad de la información, reconocidos internacionalmente y en el sector en el que se desempeña la PyME.
- Ser apoyada por la dirección de la empresa, ya que no obtener este compromiso pondrá en riesgo su cumplimiento.

Se debe fortalecer la seguridad relacionada a los controles de acceso físico y lógico de usuarios que tengan interacción directa y/o indirecta con los sistemas de información. El mayor porcentaje de incidentes de seguridad que ocurre en las organizaciones, es atribuido generalmente a personal interno, usuarios o a terceros ajenos a la organización que interactúan con ella, quienes podrían actuar de manera no intencional o maliciosa.

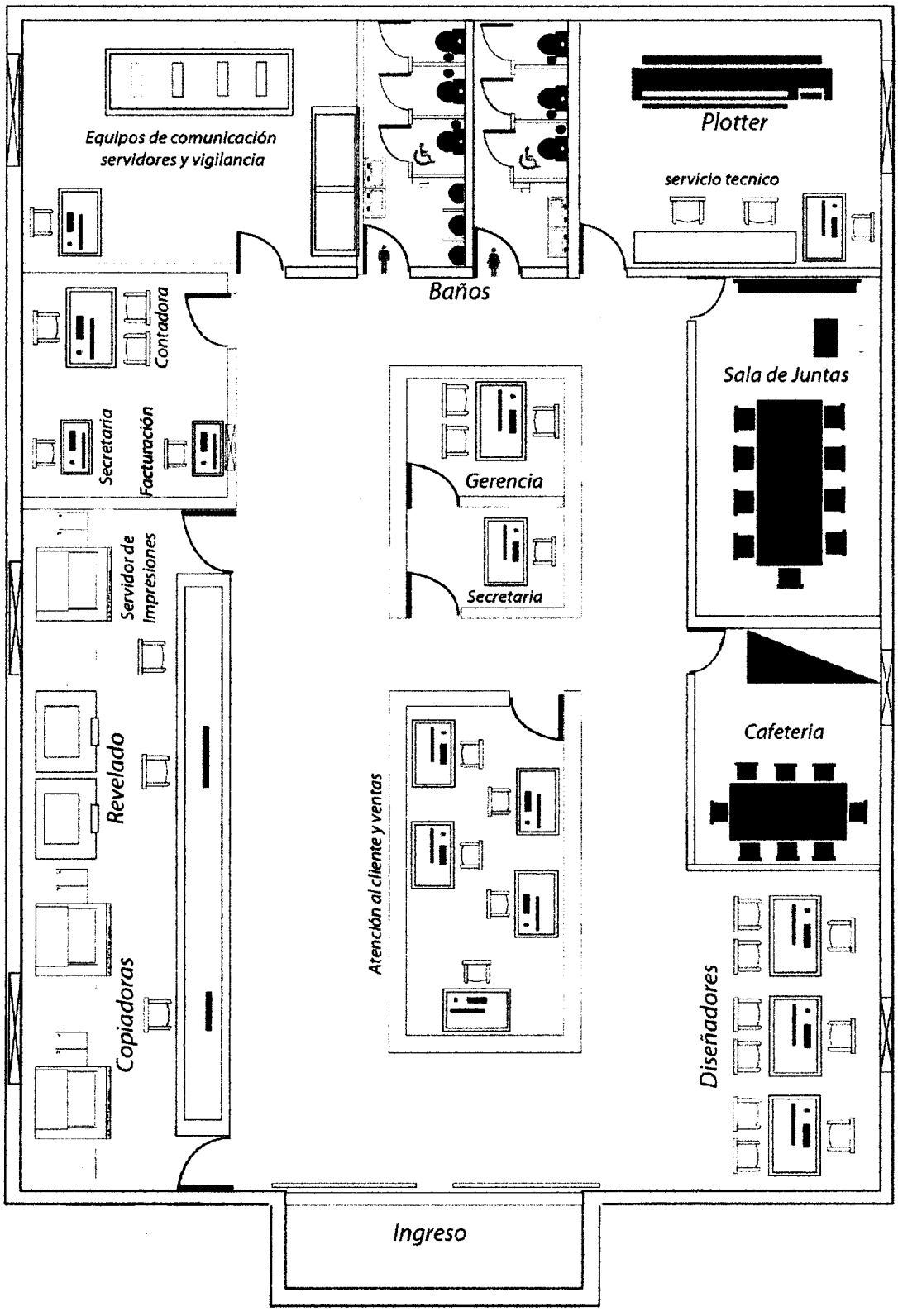
Uno de los principales obstáculos a la hora de implementar controles de seguridad en una organización, es el temor a hacer algo que no se ha hecho antes. En consecuencia, será necesario tener en claro previamente las áreas sobre las que se debe actuar y realizar esta tarea de forma gradual. Si la disponibilidad presupuestaria lo permite,

es recomendable contratar especialistas que auxilien a la PyME, con el fin de establecer el mejor camino a seguir para fortalecer la seguridad de su información.

ANEXOS

1.3 ANEXO A

1.4 A.1 DIAGRAMA DE INSTALACIONES DE PYME MULTISERVICIOS



ANEXO B

B.1 INVENTARIO DE LOS RECURSOS DE HARDWARE DE PYME MULTISERVICIOS

Computadoras personales			
Código	**Ubicación**	**Usuario**	**Funcionalidad**
PC-0001	Gerencia	Gerente	Actividades administrativas
PC-0002	Secretaria	Asistente	Actividades administrativas
PC-0003	Diseño	Diseñador	Diseño gráfico y fotografía
Lap-0004	Diseño	Diseñador	Diseño gráfico y fotografía
Lap-0005	Diseño	Diseñador	Diseño gráfico y fotografía
PC-0006	Técnico	Técnico	Mantenimiento y reparación de pcs
PC-0007	Diseño	Diseñador	Diseño gráfico y fotografía
PC-0008	Técnico	Técnico	Mantenimiento y reparación de pcs
PC-0009	Facturación	Contadora	Actividades administrativas
PC-0010	Ventas	Dependiente	Actividades administrativas
PC-0011	Servidor	Servidor de aplicación de facturación	Actividades administrativas
PC-0012	Servidor	Servidor de impresión	Actividades administrativas
PC-0013	Servidor	Servidor de cámaras de vigilancia	Actividades administrativas
Impresoras multifunción/Plotter			
Código	**Ubicación**	**Usuario**	**Funcionalidad**
Imp-001	Secretaría	Secretaria	Impresión de documentación administrativa
Imp-002	Diseño	Diseñador	Impresión de diseños
Imp-003	Diseño	Diseñador	Impresión de diseños
Imp-004	Diseño	Plotter	Impresión de diseños
Imp-005	Facturación	Contadora	Impresión de documentación administrativa
Imp-006	Técnico	Técnico	Impresión de documentación administrativa
Equipos de comunicaciones y vigilancia			
Código	**Ubicación**	**Usuario**	**Funcionalidad**
Router N/A	Servidor	Uso general	Servicio de Internet, instalado por ISP
Switch-001	Servidor	Uso general	Servicios de red
Switch-002	Servidor	Uso general	Servicios de red
Camara-001	Ventas	Uso general	Servicio de vigilancia

B.2 SOFTWARE INSTALADO EN COMPUTADORES DE PYME MULTISERVICIOS

Multiservicios cuenta con 3 equipos servidores:

- Servidor de aplicación de facturación
  - Windows 8
  - Sistema de facturación Genesis
  - Navegadores web IE y Firefox
  - Microsoft Office
  - Avg Antivirus
- Servidor de impresiones
  - Windows 8
  - Aplicativo Lexmark para impresión
  - Aplicativo Xerox para impresión
  - Aplicativo HP para impresión
  - Navegadores web IE y Firefox
  - Microsoft Office
  - Avg Antivirus
- Servidor de cámaras de vigilancia
  - Windows 8
  - Aplicativo Dlink para cámaras de vigilancia
  - Navegadores web IE y Firefox
  - Avg Antivirus
- 4 máquinas de diseño gráfico con el siguiente software:
  - Windows 8
  - Herramienta de diseño Adobe Illustrator
  - Herramienta de diseño Corel Cad

- Herramienta de retoque fotográfico Adobe Photoshop
- Navegadores web IE y Firefox
- Avg Antivirus

- 2 máquinas para uso de personal técnico
  - Windows 8
  - Navegadores web IE y Firefox
  - Avg Antivirus
- 3 equipos administrativos para secretaría, facturación y ventas
  - Windows 8
  - Sistema de facturación Genesis
  - Navegadores web IE y Firefox
  - Microsoft Office
  - Avg Antivirus

ANEXO C

C.1 CUESTINARIOS EFECTUADOS A PYME MULTISERVICIOS

SEGURIDAD LÓGICA

Nombre:..... Cargo: .....

Departamento: ..... Fecha:.....

Identificación de usuarios

¿El servicio de asistencia técnica informática es brindado por alguien que pertenece a la empresa o fuera de ella?

◯ Pertenece a la empresa ◯ No pertenece a la empresa

◯ No hay personal técnico

¿Para el control de la seguridad qué datos son almacenados en el perfil de usuario?

◯ ID de usuario
◯ Nombre y apellido completo
◯ Puesto de trabajo y departamento de la Institución
◯ Fecha de expiración de la cuenta
◯ No hay idetificación de usuarios

¿El ID del usuario puede repetirse?

SI ◯ No ◯

Mantenimiento

¿Se actualizan, revisan y asignan a los usuarios un grupo determinado con sus respectivos permisos?

SI ◯ NO ◯ No se aplica ◯

¿Cada cuánto tiempo?

◯ 1 a 3 meses ◯ 4 a 6 meses ◯ Cada vez que se requiera

Permisos

La clasificación del acceso a los recursos (datos) está basado por:

◯ Importancia
◯ Los tipos (base de datos, archivos de configuración, datos personales)
◯ Por departamento

¿Quiénes son los encargados de asignar permisos a los usuarios?

◯ Administrador ◯ Usuarios privilegiados ◯ Director

Acciones correlativas a usuarios

¿Los usuarios se identifican en forma única o existen usuarios genéricos que todas las personas usan?

◯ SI ◯ NO ◯ No se aplica

Contraseñas

¿Las contraseñas son creadas?:

◯ Por procesos automáticos (programas de generación de contraseña)
◯ Por los usuarios

¿Cuál es el conjunto de caracteres que se exigen para crear una contraseña?:

◯ Alfa-Numéricos ◯ Numéricos ◯ Caracteres especiales

¿Cuál es el largo mínimo y máximo de caracteres para crear una contraseña?

◯ 1-5 caracteres ◯ 6-8 caracteres ◯ Mas de 8 caracteres

¿En qué periodo de tiempo se cambia la contraseña?

◯ Cada 15 días ◯ Cada Mes ◯ Cuando se lo solicita

Entrenamiento a usuarios

Respecto al manejo de contraseñas por parte de los usuarios, se les enseña a:

◯ No usar contraseñas fáciles de descifrar
◯ No divulgarlas
◯ No guardarlas en lugares donde se puedan encontrar

Limitaciones a los servicios

¿Existen restricciones de servicio en base a:

◯ Usuarios ◯ Aplicaciones ◯ Departamentos

◯ No hay restricciones de ningún

Mecanismos de control de acceso interno

¿Se restringen las interfaces que ven los usuarios, (como el escritorio de Windows) de manera que los usuarios solo vean lo que les está permitido?

◯ SI ◯ NO

Control de acceso externo

¿Existe algún mecanismo de control que supervise el acceso a la información o los sistemas desde el exterior de la oficina?

◯ Gateways o algún equipo de seguridad informática
◯ Acceso de personal contratado, consultores o mantenimiento
◯ Autenticación basada en la identidad del equipo que quiere acceder al sistema y no en la identidad del usuario

¿Existe acceso externo a los datos, desde Internet?

◯ SI ◯ NO

Detección De Intrusos

¿Existe algún tipo de herramienta de monitorización de red para encontrar intrusos?

◯ SI ◯ NO

¿Si se detecta la presencia de algún intruso, sabe que procedimiento debe realizar?

◯ SI ◯ NO

Firma: .....

SEGURIDAD FÍSICA

Nombre: ..... **Cargo:** .....

Departamento: ..... **Fecha:**.....

Control de acceso al Centro de Cómputo

¿Se restringe el acceso al área de información a la gente que no pertenece a esa área?

SI ◯ NO ◯

¿Existen algunos de los siguientes métodos de control de acceso?

◯ Carnets de identificación
◯ Guardias de Seguridad
◯ Circuito cerrado de televisión
◯ Cerraduras o candados
◯ No existe ningún control de acceso al centro de cómputo

Control De Acceso A Equipos

¿Existe alguna contraseña para el acceso a los equipos de computación?

◯ SI ◯ NO

¿Los equipos de cómputo tienen habilitados los puertos USB o la lectora de CD?

◯ SI ◯ NO

¿Mediante algún tipo de software anti virus se controla escanear dispositivos cómo memorias flash o CD's?

◯ SI ◯ NO

¿Se permite desde el *setup* de la máquina el arranque con CD's o memorias usb?

◯ SI ◯ NO

¿Existen entradas no autorizadas en las PC's, como puertos no usados y no deshabilitados?

◯ SI ◯ NO

¿Puede alguien enchufar e instalar una impresora u otro dispositivo en alguna máquina?

◯ SI ◯ NO

¿Se mantienen en los servidores las 24 horas?

◯ SI ◯ NO

Utilidades de soporte

¿Existen, se mantienen y revisan todos estos equipos periódicamente en busca de fallas?

- ◯ Aire acondicionado
- ◯ Luz de emergencia en el centro de cómputo
- ◯ Detectores de humo, agua y calor
- ◯ Matafuegos

¿Se dispone de UPS (Uninterruptible power supply) para mantener funcionando todas las máquinas necesarias para el trabajo diario?

◯ SI ◯ NO

¿Se han probado los UPS trabajando al 100% de necesidad para probar su correcto funcionamiento?

◯ SI ◯ NO

¿Se ha entrenado al personal en la utilización de matafuegos?

◯ SI ◯ NO

¿Los matafuegos se encuentran en lugares visibles y de fácil acceso?

◯ SI ◯ NO

¿Existe algún tipo de control sobre las instalaciones eléctricas o posibles causas de incendio?

◯ SI ◯ NO

¿Hay un dispositivo que evite la sobrecarga de la red eléctrica?

◯ SI ◯ NO

Centro de cómputo:

¿Las instalaciones están ubicadas en pisos elevados (para prevenir inundaciones)?

◯ SI ◯ NO ◯ NO SE APLICA

¿Existe un piso o techo falso para pasar el cableado por debajo de él?

◯ SI ◯ NO

¿Está permitido comer, fumar y beber dentro del centro de cómputo?

SI NO

Cableado

¿Se instaló el cableado estructurado de la red siguiendo algún tipo de norma?

SI NO

¿Se tuvo en cuenta el lugar de los canales de red, de manera que no sean afectados por desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos?

SI NO

Sistemas Móviles

¿Si se usan laptops o PC's portátiles, se tienen en cuenta los diferentes riesgos a los que se someten los datos de la empresa al pasar la información por redes inalámbricas?

SI NO

¿El tipo de cifrado de la red inalámbrica es lo suficientemente fuerte y las contraseñas complejas para evitar algún tipo de infiltración vía wifi?

SI NO

Respaldo de información crítica

¿Con qué frecuencia hacen los respaldos de información?

Diarios Semanales Quincenales No se realiza

Instalación y reparación de Hardware averiado

¿Se contrata un tercero que proporcione los insumos necesarios en caso de emergencia?

SI NO

Si se dispone de más de un establecimiento, ¿en ambos locales existen equipos, que, por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro establecimiento?

SI NO No aplica

¿Hay algún tipo de herramienta de back up automáticos que hagan copias de seguridad?

SI NO No aplica

¿Existen prioridades en las PC's (ej. Se saca respaldo de las máquinas de los Directores)?

SI NO

¿Los backups (respaldos de información importante) se guardan fuera de las instalaciones de la empresa o en internet?

SI NO

¿Si amerita el caso, hay backups de las páginas Web y de sus actualizaciones?

SI NO No se aplica

Firma: .....

Administración de la información y de sus responsables

Nombre: ..... **Cargo:** .....

Fecha: .....

¿Existe algún tipo de normas de seguridad o políticas de seguridad?

◯ SI ◯ NO

¿Existen procedimientos para dar publicidad a las nuevas normas de seguridad?

◯ SI ◯ NO ◯ No aplica

¿Existe algún tipo de política que sirva como base para la planificación, el control y la evaluación de las actividades del área de información?

◯ SI ◯ NO

¿Existe documentación detallada sobre el equipamiento informático? Incluye los siguientes datos:

◯ Distribución física de las instalaciones (identificación de PC´s y equipos, y puestos de trabajo)

◯ Inventario de "hardware" y "software" de base

◯ Información sobre el responsable de un determinado tipo de datos

◯ Ninguna de las anteriores

¿Existe algún responsable de la actualización de los activos de información, como computadores y nuevo software que se instala?

◯ SI ◯ NO

¿Existe algún manual de seguridad para los usuarios?

◯ SI ◯ NO

¿Existe un encargado de los activos de información, como computadores y red informática?

◯ SI ◯ NO

¿Existe en los empleados algún tipo de conciencia sobre los riesgos de no contar con técnicas de seguridad de la información mínimas?

◯ SI ◯ NO

Firma: .....

SEGURIDAD EN LAS COMUNICACIONES

Nombre: ..... **Cargo:** .....

Fecha: .....

Comunicaciones

¿Existe algún tipo de diagrama de red que indique la disposición de los equipos de computación en las instalaciones?

◯ SI ◯ NO

¿Se realizan los controles de acceso adecuados a los servidores que se encuentran conectados a Internet?

◯ SI ◯ NO

Recursos compartidos

¿Se comparten los discos o carpetas de las PC's en la red?

◯ Con permisos a cualquier usuario

◯ Personalizado con sus respectivos permisos a quien necesite

◯ No se comparten

¿Se le permite a cualquier usuario compartir carpetas?

◯ SI ◯ NO

¿Existe algún software para colocar contraseñas a las carpetas compartidas?

◯ SI ◯ NO

¿Quién pone las contraseñas?

◯ El dueño del archivo ◯ El administrador

◯ No se aplica

Configuración de puertos

¿Se deshabilitan los puertos que no son necesarios?

◯ SI ◯ NO

¿Se prueban los puertos de la red?

◯ SI ◯ NO

¿Se hace algún chequeo periódico de la red y sus permisos?

SI NO

Medidas de fiabilidad

¿Existe algún medio opcional de transmisión de datos en caso de que exista alguna contingencia con la red?

SI NO

Mail y chat

Las claves de autenticación de correo de la empresa son de conocimiento de:

Todos los usuarios Un usuario específico

¿Existen direcciones de mail para todos los empleados?

SI NO

¿Se ha programado algún tipo de charla que haga caer en cuenta a los usuarios de abrir correos de remitentes no conocidos y cómo afrontar otros riesgos ligados al uso del correo electrónico y a las redes sociales?

SI NO

¿Se permiten los servicios de chat?

SI NO

¿Los computadores tienen solo cuentas de usuarios secundarios o invitados para evitar la instalación de programas con privilegios de administrador?

SI NO

Privacidad – Firma digital – Encriptación de mails

¿Está expresamente señalado la prohibición del envío de archivos de la empresa u otros documentos confidenciales vía mail?

SI NO

¿Se toman medidas de seguridad especiales cuando el mensaje de salida tiene datos confidenciales?

SI NO

Malware

¿Cuáles de éstas medidas o herramientas existen para evitar la infección de malware?

- Paquetes de software antivirus
- Firewalls
- Creación de un disco de rescate o de emergencia
- Procedimientos para cuando ocurra una infección con virus.
- Back up de datos

¿El antivirus que está instalado en cada PC (incluyendo los servidores) fue obtenido gratis en internet?

SI NO No tiene ningún antivirus instalado

¿Cada cuánto se hace un escaneo total de virus en los computadores de la red?

Semanal Quincenal Nunca

¿Existe algún responsable que se asegure de la instalación de todos los parches de seguridad disponibles del sistema operativo y de los programas usados?

SI NO

¿Hay alguna documentación donde se anote la configuración de las PC´s en la red (Sus números IP, sus placas de red, etc.)?

SI NO

Firma: .....

ANEXO D

D.1 CONTROLES DE LA ISO/IEC 27002:2013 APLICABLES A UNA PYME

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
Políticas de seguridad de la información	Orientación de la dirección en seguridad de la información	Políticas de seguridad de la información	Si	Crear políticas de nivel inferior según la necesidad, persiguiendo la concientización, educación y capacitación para el lector.
		Revisión de las políticas de seguridad de la información	No	El entorno de las PyME no se modifica en cortos o medianos plazos, si bien resultaría conveniente algún tipo de revisión periódica.
Organización de la seguridad de la información	Organización interna	Roles y responsabilidades de la seguridad de la información	Si	Identificar activos de información y asignar responsabilidad sobre cada uno a personal correspondiente, quien se encargará de su cuidado diario. Documentar.
		Segregación de funciones	No	En PyME este control resulta difícil de ejecutar debido a la escasez de personal.
		Contacto con las autoridades	No	Debido a la naturaleza de las PyME, los contactos suelen ser informales.
		Contacto con grupos de interés especial	No	En PyME usualmente no existe personal dedicado a seguridad informática, por lo que este punto no sería de aplicación.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
		Seguridad de la información en la gestión de proyectos	No	En PyME las instancias de gestión de proyectos no se aplican.
	Dispositivos móviles y teletrabajo	Política de dispositivos móviles	Si	Supervisar el uso de dispositivos móviles.
		Teletrabajo	SI	Asegurar condiciones mínimas de seguridad para estaciones de teletrabajo como firewall y antivirus, además de evitar accesos no autorizados a personas ajenas a la empresa.
Seguridad de recursos humanos	Antes del trabajo	Selección	Si	Constatar mediante certificados de antecedentes penales y cartas de recomendación los antecedentes de postulante.
		Términos y condiciones de empleo	Si	Solicitar la firma de acuerdos de confidencialidad, dejando especificado claramente las implicaciones legales en las que se incurriría por su no cumplimiento.
	Durante el empleo	Responsabilidades de la dirección	Si	Dirección debe asegurarse que se cumpla con las políticas de seguridad.
		Concientización, educación y capacitación en seguridad de la información	Si	Motivar y capacitar a empleados sobre los riesgos de la falta de seguridad de la información.
		Proceso disciplinario	Si	Aplicado en términos y condiciones de empleo.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
	Desvinculación o cambio de puesto	Responsabilidades en la desvinculación o cambio de puesto	Si	Notificar la vigencia de los acuerdos de confidencialidad, aún después de que se produzca la renuncia del empleado.
Gestión de activos	Responsabilidad por los activos	Inventario de los activos	No	Este control ya se encuentra cubierto en Roles y Responsabilidades de la Seguridad de la Información.
		Propiedad de los activos	No	Este control ya se encuentra cubierto en Roles y Responsabilidades de la Seguridad de la Información.
		Uso aceptable de los activos	Si	Documentar reglas sobre el buen uso de los activos de información.
		Retorno de activos	Si	Asegurar la devolución de los activos de información una vez concluido el vínculo laboral.
	Clasificación de la información	Clasificación de la información	Si	Cada usuario de los activos de información debe determinar la importancia de la clasificación de información.
		Rotulado de la información	Si	Necesario para preservar el orden.
		Manipulación de activos	No	Muy difícil de implementar en el contexto de una PyME debido a la escasez de recursos.
	Manipulación de medios	Gestión de medios removibles	Si	Necesario para preservar la confidencialidad de cualquier medio que se saque de las instalaciones de la PyME.
		Disposición final de medios	No	Necesario para preservar la confidencialidad de cualquier medio que se saque de las instalaciones de la PyME.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
		Transporte de medios físicos	No	No se aplica para el contexto de una PyME, control más orientado a empresas con grandes volúmenes de información.
Control de accesos	Requisitos del negocio para el control de accesos	Política de control de accesos	Si	Es necesario que haya controles de seguridad mínimos que permitan manejar el acceso a la empresa.
		Acceso a redes y a los servicios de red	No	No aplica, menor volumen de equipos en PyME ocasiona que redes sean más pequeñas y menos segregadas.
	Gestión de accesos del usuario	Alta y baja de registros del usuario	Si	Es necesaria su aplicación ya que debe existir un control sobre la creación de usuarios y la asignación de permisos a dichos usuarios.
		Asignación de accesos del usuario	Si	Se justifica su aplicación por las mismas razones del control anterior.
		Gestión de los derechos de acceso con privilegios	No	Su aplicación dependerá si la PyME cuenta con software que amerite la asignación de este tipo de privilegios a los usuarios que intenten acceder al sistema.
		Gestión de la información secreta para la autenticación de los usuarios	Si	Es necesario que los usuarios tengan en claro la confidencialidad de las credenciales.
		Revisión de los derechos de acceso del usuario	No	Control aplicable si el sistema o sistemas que maneja la PyME establece división de roles para usuarios.
		Remoción o ajuste de los derechos de acceso	Si	Es importante que se eliminen cuentas de usuario que ya no se vayan a usar.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
	Responsabilidades del usuario	Uso de la información secreta para la autenticación	Si	Es necesario que los usuarios tengan en claro la confidencialidad de las credenciales.
	Control de acceso a los sistemas y a las aplicaciones	Restricción de acceso a la información	No	Control aplicado en las políticas de control de acceso. Podría encarecer costos por su aplicación.
		Procedimientos seguros de inicio de sesión	No	Podría encarecer costos por su aplicación.
		Sistemas de gestión de contraseñas	No	Como alternativa se podría implementar un sistema de gestión de contraseñas descargado de la web.
		Uso de programas utilitarios con privilegios	No	Este control granular no aplica para la realidad de una PyME.
		Control de acceso al código fuente de los programas	No	No se aplica a la realidad de las PyME que no cuentan con departamento de desarrollo de software.
Criptografía	Controles criptográficos	Política de uso de los controles criptográficos	No	De acuerdo a la criticidad de la información manipulada correspondería el uso de herramientas de código abierto disponibles en internet.
		Gestión de claves	No	Sugerir la descarga de utilidades para controlar la calidad de contraseñas usadas.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
Protección física y ambiental	Áreas Seguras	Perímetro de seguridad física	Si	Definir área segura donde emplazar área de proceso de información, aisladas del exterior.
		Controles de acceso físico	Si	Asegurar control mínimo de acceso como identificaciones visibles para los empleados.
		Aseguramiento de oficinas, recintos e instalaciones	Si	Definir área segura donde emplazar área de proceso de información, aisladas del exterior.
		Protección contra amenazas externas y ambientales	Si	Garantizar la obtención de asesoría por parte de personal especializado. Por ejemplo: protección contra incendios.
		Trabajo en áreas seguras	Si	Guardar controles de seguridad mínimos en área de procesamiento de información.
		Áreas carga y descarga	No	Este control se podría aplicar de acuerdo a la actividad de cada PyME.
	Equipamiento	Ubicación y protección del equipamiento	Si	Deben existir condiciones mínimas para emplazar y proteger los activos de información usados.
		Elementos de soporte	Si	Asegurar que exista controles sobre las instalaciones de soporte.
		Seguridad del cableado	Si	Instalación segura de cableado de electricidad y telecomunicaciones.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
		Mantenimiento del equipamiento	Si	Debería ser periódico o permanente en el mejor de los casos.
		Retiro de activos	Si	Se debe mantener una bitácora que registre si los equipos, la información o el software ha sido retirado.
		Seguridad del equipamiento y los activos afuera de la organización	No	Comúnmente las PyME no disponen de un parque informático amplio y su labor se reduce a la circunscripción de un sitio único sitio donde concentra sus actividades.
		Disposición final segura o reúso del equipamiento	Si	Constatar que información haya sido correctamente eliminada de equipos obsoletos.
		Equipamiento de usuario que se deja desatendido	Si	Verificar que se haga un bloqueo de equipos si no se los utiliza.
		Política de pantalla y escritorio limpios	Si	Asegurar que no se deje a la vista cualquier tipo de almacenamiento o información en escritorios.
Seguridad de las operaciones	Procedimientos y responsabilidades operativos	Procedimientos operativos documentados	No	Las PyME no cuentan con personal especializado para realizar este tipo de tarea, además de que sus procedimientos no son mayormente complejos.
		Gestión del cambio	No	En general, las PyME no cuentan con procedimientos tan complejos como los que exige este control

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
		Gestión de la capacidad	No	Debido a la escasez de recursos, las exigencias de PyME se solucionan en la medida que se requieren y no se prevén con anterioridad.
		Separación de los entornos de desarrollo, de pruebas y operativo	No	Las PyME no cuentan con recursos necesarios para recrear varios ambientes para el desarrollo de aplicaciones.
	Protección contra código malicioso	Controles contra código malicioso	Si	Se debe coadyuvar con la implementación de software a la detección, prevención y recuperación contra malware, además de implementar procedimientos operativos.
	Resguardo	Resguardo de la información	Si	Implementar plan de copias de seguridad de información crítica. Acceso cifrado para la misma.
	Registro y seguimiento	Registro eventos	No	Este tipo de software requerido para esta tarea tiene licencias muy costosas.
		Protección de la información de los registros	No	No aplicable si no se va a disponer de software de control de registros.
		Registro de administradores y operadores	No	No aplicable si no se va a disponer de software de control de registros.
		Sincronización de relojes	Si	Es necesario que todos los equipos informáticos tengan actualizados al unísono la hora y fecha correspondiente. Necesario para evitar posibles ataques que se aprovechan de este error.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
	Control de software operativo	Instalación de software en los sistemas operativos	Si	Constatar que se instalen programas necesarios y de utilidad para la PyME.
	Gestión de vulnerabilidades técnicas	Control de las vulnerabilidades técnicas	Si	Constatar periódicamente la actualización del software utilizado para las diversas tareas.
		Restricciones a la instalación de software	Si	Constatar que se instalen programas necesarios y de utilidad para la PyME.
	Consideraciones para las auditorias de sistemas de información	Controles de la auditoría de sistemas de información	No	Al no disponer de sistemas informáticos complejos, no es necesaria la implementación de este control.
Seguridad de las comunicaciones	Gestión de la seguridad de la red	Controles de redes	Si	Se debe restringir el acceso a la red para evitar uso no autorizado de la misma.
		Seguridad de los servicios de red	Si	Se debe restringir el acceso a la red para evitar uso no autorizado de la misma.
		Segregación en redes	No	Generalmente los segmentos de red de las PyME son pequeños, y no reviste mayor complejidad su administración.
	Transferencia de información	Políticas y procedimientos de transferencia de información	Si	La confidencialidad es elemental para mantener el secreto de la información de la PyME.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
		Acuerdos de transferencia de información	No	Las líneas de comunicación en una PyME no suelen revestir mayor confusión.
		Mensajería electrónica	Si	Deben existir controles mínimos de protección a la información intercambiada por mensajería electrónica, redes sociales.
		Acuerdos de confidencialidad	Si	Necesario para proteger la confidencialidad de la información.
Adquisición, desarrollo y mantenimiento de los sistemas	Requisitos de seguridad de los sistemas de información	Análisis y especificaciones de los requisitos de seguridad	No	Comúnmente las PyME adquieren software cuyas prestaciones y seguridades han sido probadas. No compran software a medida.
		Aseguramiento de los servicios de aplicaciones en redes públicas	No	Las redes que usan las PyME son internas o de menor complejidad.
		Protección de las transacciones de los servicios de aplicaciones	No	No es necesario contar con una política de este tipo en una PyME debido a que sus sistemas no requieren programación ni comunicaciones complejas.
	Seguridad en los procesos de desarrollo y soporte	Política de desarrollo seguro	No	Es muy poco común que las propias PyME desarrollen sus soluciones de software.
		Procedimientos de control de cambios en los sistemas	No	Es muy poco común que las propias PyME desarrollen sus soluciones de software.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
		Revisiones técnicas de las aplicaciones luego de cambios en la plataforma operativa	No	Es muy poco común que las propias PyME desarrollen sus soluciones de software.
		Restricciones a los cambios en los paquetes de software	No	Es muy poco común que las propias PyME desarrollen sus soluciones de software.
		Principios para la ingeniería segura de los sistemas	No	Es muy poco común que las propias PyME desarrollen sus soluciones de software.
		Entorno seguro de desarrollo	No	Es muy poco común que las propias PyME desarrollen sus soluciones de software.
		Desarrollo provisto por terceras partes	No	Es muy poco común que las propias PyME desarrollen sus soluciones de software.
	Datos para las pruebas	Pruebas de seguridad de los sistemas	Si	Es necesario para probar el software adquirido.
		Pruebas de aceptación del sistema	Si	Necesario para probar nuevo software.
		Protección de los datos para las pruebas	Si	Se debe corroborar que al momento de probar nuevo software se usen datos ofuscados.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
Relaciones con los proveedores	Seguridad de la información en las relaciones con los proveedores	Política de seguridad de la información para las relaciones con los proveedores	No	Las PyME no brindan mayor información a terceras partes o a elementos que estén fuera de la empresa.
		Tratamiento de la seguridad en los acuerdos con los proveedores	No	Las relaciones de las PyME con sus proveedores no tienen un gran nivel de compenetración.
		Cadena de suministros de las tecnologías de la información y las comunicaciones	No	En vista de que las PyME mantienen una relación sin mucha dependencia de sus proveedores no es necesaria la aplicación de este control.
	Gestión de la entrega de servicios por proveedores	Seguimiento y revisión de los servicios prestados por proveedores	Si	Sujeto a la realidad de cada PyME para constatar la prestación de un servicio eficiente de parte del proveedor.
		Gestión del cambio de los servicios prestados por proveedores	No	Salvo que los proveedores de las PyME sean grandes empresas que son más exigentes en la forma en que brindan sus servicios, no es necesario este control.
Gestión de los incidentes de seguridad de la información	Gestión de los incidentes de seguridad de la información y mejoras	Responsabilidades y procedimientos	Si	Se debería implantar un procedimiento básico que sirva como guía en caso de presentarse algún incidente de seguridad.
		Presentación de informes sobre los eventos de seguridad de la información	No	Reuniones informales son el principal medio de difusión en las PyME.
		Presentación de informes sobre las vulnerabilidades de seguridad de la información	Si	Se debe informar sobre alguna anomalía relacionada con los sistemas.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
		Evaluación y decisión sobre los eventos de seguridad de la información	No	Generalmente los eventos de seguridad de la información se manejan de forma muy informal, sin embargo, debería existir consciencia sobre las malas costumbres que provocaron los ataques.
		Respuesta a los incidentes de seguridad de la información	Si	Contar con algún tipo de respuesta respecto a algún incidente de seguridad de la información.
		Aprendiendo de los incidentes de seguridad de la información	Si	Usar la información sobre los incidentes de seguridad de la información para reducir la probabilidad de una nueva ocurrencia.
		Recolección de evidencia	No	Control ambiguo para la realidad de una PyME
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Continuidad de la seguridad de la información	Planificación de la continuidad de la seguridad de la información	No	Las PyME, al no contar con sofisticados sistemas de información y equipos, son fácilmente trasladables.
		Implementación de la continuidad de la seguridad de la información	Si	Toda PyME debería tener un curso de acción mínimo que permita recuperarla en caso de una emergencia informática.
		Verificación, revisión y valoración de la continuidad de la seguridad de la información	No	Control no aplicable a una PyME debido a la carencia de complejidad en sus operaciones.

Dominio	Objetivos de control	Controles	Pertinencia	Observaciones
	Redundancia	Disponibilidad de las instalaciones de procesamiento de la información	Si	Constatar que exista respaldo de la disponibilidad de los sistemas en caso de desastre.
Cumplimiento	Cumplimiento de los requisitos legales y contractuales	Identificación de la legislación aplicable y de los requisitos contractuales	Si	Se hace necesario que la PyME cuente con algún tipo de asesoramiento legal, tercerizado si el presupuesto l permite, para que sea cubierto cualquier vacío sobre normativa de uso de la información que se maneja.
		Derechos de propiedad intelectual	Si	Cumplir con la utilización legal de software de terceros
		Protección de los registros	Si	Constatar la preservación de archivos de registro por cualquier medio, sea este electrónico o no.
		Privacidad y protección de información personal	Si	Mantener reserva sobre la información personal que custodia la PyME.
		Regulación de controles criptográficos	No	La normativa aplicable a una PyME no es tan estricta, no se aplica, en comparación con las grandes empresas.
	Revisión de la seguridad de la información	Revisión independiente de la seguridad de la información	Si	Debería existir el control por oposición dentro de la PyME
		Cumplimiento de las políticas y las normas de seguridad	Si	Se debe constatar la aplicación y cumplimiento correct de las políticas de seguridad de la información.
		Revisión del cumplimiento técnico	Si	Se tiene que tener en cuenta una revisión periódica de los sistemas sobre las normas de seguridad implantadas en una PyME.

BIBLIOGRAFÍA

BIBLIOGRAFÍA ESPECÍFICA

[1] "Ranking empresarial 2016";

http://appscvs.supercias.gob.ec/rankingCias/

Consultada 16/03/2016

[2] [3] "En América Latina el 99% de las empresas son Pymes";

http://www.revistalideres.ec/lideres/america-latina-cifras-empresas-pymes.html

Consultada 18/12/2015

[4] "Proyecto Amparo, Panorama del ciberdelito en Latinoamérica";

http://www.proyectoamparo.net/files/LACNIC-PanoramCiberd-VsFinal-20110701.pdf Consultada 30/01/2016

[5] "Economía digital y seguridad en América Latina y el Caribe";

https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

Consultada 15/03/2016

[6] "Mas del 60% de Pymes de América Latina ha sufrido un ataque informático";

http://www.diariopyme.com/estudio-mas-del-60-de-pymes-de-america-latina-han-sufrido-un-ataque-informatico/prontus_diariopyme/2015-07-09/130902.html

Consultada 15/03/2016

[7] "5 consejos para pymes que quieran incorporar nuevas tecnologías";

https://www.amexcorporate.com.ar/multitaskers/nota.php?id=484&cat=7

Consultada 11/02/2016

[8] "ISO/IEC 27002";

https://es.wikipedia.org/wiki/ISO/IEC_27002

Consultada 13/03/2016

[9] "Informe anual de seguridad 2016 de Cisco";

http://www.cisco.com/c/dam/m/es_mx/offers/assets/pdfs/cisco_2016_asr_012816_es-xl.pdf

Consultada 27/05/2016

[10] "Los diez incidentes de seguridad más caros para una pyme";

http://www.silicon.es/los-10-incidentes-de-seguridad-mas-caros-para-una-pyme-galeria-89973

Consultada 30/05/2016

[11] "Guía de Seguridad ICC para los negocios";

http://www.iccspain.org/wpcontent/uploads/2016/01/ICC_GUIACIBERSEGURIDAD_ESP.pdf

Consultada 30/05/2016

[12] "El impacto económico de los incidentes de seguridad";

http://aunclicdelastic.blogthinkbig.com/sin-duda-es-mejor-prevenir-el-impacto-economico-de-los-incidentes-de-seguridad/

Consultada 30/05/2016

[13] "Desarrollo sostenible y seguro: un marco para las sociedades conectadas resilientes";

https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/

Consultada 01/04/2016

[14] "¿Por qué es imposible la seguridad total?";

http://sg.com.mx/revista/46/por-que-es-imposible-la-seguridad-total#.V08SUfnhDZY

Consultada 01/06/2016

[15] "El hardware, un elemento clave en la gestión de un proyecto de e-commerce";

http://elblogdeecommerce.com/2012/03/08/el-hardware-un-elemento-clave-en-la-gestion-de-un-proyecto-de-e-commerce/

Consultada 04/04/2016

[16] "Beneficios del software abierto para Pymes, autónomos y emprendedores";

http://mqueridiam.tbfnation.com/beneficios-del-software-abierto-para-pymes-autonomos-y-emprendedores/

Consultada 04/04/2016

[17] "Red de computadoras";

https://es.wikipedia.org/wiki/Red_de_computadoras

Consultada 04/04/2016

BIBLIOGRAFIA GENERAL

- **"La importancia de contar con una política de seguridad en la empresa";** http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=7&id_tema=63; Consultada 11/12/2015.

- **"Guía de Seguridad en Informática para PYMES";** http://www.uprm.edu/cde/public_main/slider/files_slider/presentaciones_foro/seguridad_informatica.pdf; Consultada 11/12/2015.

- **"Ramsonware ataca a pequeñas empresas";** http://www.seguridad.unam.mx/noticia/?noti=2502; Consultada 11/12/2015.

- **"Los retos de seguridad para las PYMES";** http://www.enter.co/especiales/enterprise/los-retos-de-seguridad-para-las-pymes/; Consultada 11/12/2015.

- **"Solución integral de seguridad para las pymes mediante un UTM";** http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf; Consultada 15/12/2015.

- **"Plan de seguridad informático";** http://es.slideshare.net/ofebles/plan-de-seguridad-informatica; Consultada 15/12/2015.

- **"Las Pymes marcan el ritmo";** http://redcame.org.ar/adjuntos/suple_pymes_marzo_2015.pdf; Consultada 19/12/2015.

- **"Los 10 errores típicos de una pyme en materia de seguridad";** http://www.securityartwork.es/2013/05/29/los-10-errores-tipicos-de-una-pyme-en-materia-de-seguridad/; Consultada 15/12/2015.

- **"Más del 70% de las pymes sufrió ataques virtuales";** http://garelifabrizi.com/blog/noticias/216-mas-del-70-de-las-pymes-sufrio-ataques-virtuales; Consultada 15/12/2015.

- **"Las pymes serán jugadores clave del futuro";** http://www.lanacion.com.ar/1817784-las-pymes-seran-jugadores-clave-del-futuro; Consultada 15/12/2015.
- **"Incident handling for Smes";** https://www.sans.org/reading-room/whitepapers/incident/incident-handling-smes-small-medium-enterprises-32764; Consultada 15/12/2015.

- **"Evaluación de la seguridad de los sistemas informáticos: Políticas, Estándares y Análisis de Riesgos";** https://qanewsblog.com/2013/04/16/evaluacion-de-la-seguridad-de-los-sistemas-informaticos-politicas-estandares-y-analisis-de-riesgos/; Consultada 15/12/2015.

- **"Analizando factores para el desarrollo de políticas de seguridad";** http://www.welivesecurity.com/la-es/2014/07/18/analizando-factores-desarrollo-de-politicas-de-seguridad/; Consultada 15/12/2015.

- **"Tips para sumar un proyecto de seguridad en las PYMES";** http://www.tecnopymes.com.ar/2015/11/09/tips-para-sumar-un-proyecto-de-seguridad-en-las-pymes/; Consultada 15/12/2015.
- **"En América Latina el 99% de las empresas son pymes";** http://www.revistalideres.ec/lideres/america-latina-cifras-empresas-pymes.html; Consultada 15/12/2015.

- **"Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales";** http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementaci%C3%B3n_SGSDP_ene2014.pdf; Consultada 15/12/2015.

- **"América Latina es "altamente vulnerable" a ciberataques, según estudio";** http://m.eluniverso.com/vida-estilo/2016/03/14/nota/5465745/america-latina-es-altamente-vulnerable-ciberataques-segun; Consultada 15/12/2015.

- **"Estudio: Más del 60% de pymes de América Latina han sufrido un ataque informático";** http://www.diariopyme.com/estudio-mas-del-60-de-pymes-de-america-latina-han-sufrido-un-ataque-informatico/prontus_diariopyme/2013-07-09/130902.html; Consultada 15/12/2015.

- **"Medidas de seguridad en los sistemas informáticos";** http://www.adminso.es/index.php/4._Medidas_de_seguridad_en_los_sistemas_inform%C3%A1ticos; Consultada 15/12/2015.

- **"Informatización en la pequeña y mediana empresa";** http://www.cyta.com.ar/ta0104/articulos/ti/ti.htm; Consultada 15/12/2015.
- **"Introducción a la seguridad Informática- Políticas de seguridad";** http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=4; Consultada 15/12/2015.

- **"Manual de seguridad en redes";** http://es.slideshare.net/Princesadivina/arcert-manual-deseguridadenredesinformaticas; Consultada 15/12/2015.

- **"Seguridad Lógica";** http://www.segu-info.com.ar/logica/seguridadlogica.htm; Consultada 15/12/2015.

- **"Buen uso del correo electrónico corporativo";** http://www.segu-info.com.ar/articulos/35-uso-correo-electronico-corporativo.htm; Consultada 15/12/2015.

- **"Baja, la Seguridad Informática de PyMES";** https://americas.thecisconetwork.com/site/content/lang/es/id/5493; Consultada 15/12/2015.

- **"Informe anual de seguridad de Cisco revela una disminución de seguridad en los defensores y un aumento en el impacto de atacantes industrializados";** https://americas.thecisconetwork.com/site/content/lang/es/id/4901; Consultada 15/12/2015.

- **"¿Cuánto pierden PyMEs o Corp ante fallos de seguridad?";** https://portinos.com/27249/cuanto-pierden-pymes-o-corp-ante-fallos-de-seguridad; Consultada 15/12/2015.

- **"Los daños de reputación de una pyme por una brecha de seguridad pueden ser de 7500 euros";** http://sabemos.es/2016/01/13/los-danos-a-la-reputacion-de-una-pyme-por-una-brecha-de-seguridad-pueden-ser-de-7-500-euros_10530/; Consultada 15/12/2015.

- **"Guía de seguridad ICC para los negocios";** http://www.iccspain.org/wp-content/uploads/2016/01/ICC_GUIA-CIBERSEGURIDAD_ESP.pdf; Consultada 15/12/2015.

- **"Mission Impossible: 4 Reasons Compliance is impossible";** http://www.darkreading.com/risk/mission-impossible-4-reasons-compliance-is-impossible/d/d-id/1139416?piddl_msgorder=asc; Consultada 15/12/2015.

- **"El portal de ISO 27001 en Español GLOSARIO";** http://www.iso27000.es/glosario.html; Consultada 04/04/2016.

- **"El impacto económico de los incidentes de seguridad";** http://aunclicdelastic.blogthinkbig.com/sin-duda-es-mejor-prevenir-el-impacto-economico-de-los-incidentes-de-seguridad/; Consultada 15/12/2015.