Universidad de Buenos Aires

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

Maestría en Seguridad Informática

TESIS DE MAESTRÍA

TÍTULO:

Gestión de incidentes de Seguridad Informática de las PyMe desde la perspectiva de un CSIRT

Autor:

Miguel Eduardo Álvarez Espinoza

Directora: Mg. Patricia Prandini

Abril de 2017

Cohorte 2017

DECLARACIÓN JURADA DEL ORIGEN DE LOS CONTENIDOS

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de tesis 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

Un CSIRT (*Computer Security Incident Response Team* o Equipo de Respuesta a Incidentes de Seguridad) es una entidad especializada que asiste a organizaciones públicas y privadas frente a la ocurrencia de incidentes que pueden afectar su información y los activos informáticos utilizados para gestionarla. De este modo, actúa como un equipo especializado, brindando servicios proactivos y reactivos que representan un importante valor agregado para las entidades afectadas por las amenazas que perturban al ciberespacio. Estas amenazas tienen como blanco a todo tipo de organizaciones, sin importar tamaño, especialidad o ubicación geográfica. El sector conformado por pequeñas y medianas empresas (PyME) por otro lado, no dispone generalmente de una organización adecuada para gestionar su seguridad, carece de un nivel de madurez y de recursos económicos para solventar una estructura defensiva o para contratar personal especializado; y no es generalmente consciente de la necesidad de invertir en la protección de la información.

La creación de un CSIRT cuyos servicios estén destinados al sector PyME podría significar entonces un aporte importante para la protección de los recursos de las entidades de este sector. En esta línea, el presente trabajo final de Maestría propone un modelo de CSIRT PyME acorde con sus características, recursos y necesidades, como una propuesta destinada a fortalecer la seguridad de la información en este importante sector económico.

PALABRAS CLAVE

- PyME
- CSIRT
- Seguridad de la información
- Incidentes de seguridad

ÍNDICE

DEDICATORIA

Quiero expresar mi profundo agradecimiento a la Mg. Patricia Prandini, sin cuya invalorable tutoría, paciencia y conocimientos no hubiera podido realizar la entrega de este trabajo final de maestría.

A Jessica y Mariángeles, por ser ahora mi fuente de motivación e inspiración para ser cada día un mejor profesional; y así poder luchar para que la vida nos depare un futuro mejor.

A mis padres por su eterno apoyo, mis mejores aliados y confidentes; sus palabras de aliento y soporte no me dejaron decaer en ningún momento.

A mis abuelos, tíos y primos; amigos y compañeros en Ecuador y Buenos Aires, por el gran cariño que me supieron brindar mientras residí y cursé mis estudios en Argentina.

Y a Dios especialmente, por haberme acompañado y guiado a lo largo de mi carrera; por ser mi fortaleza en momentos de debilidad y por brindarme una vida llena de aprendizaje y nuevas experiencias.

INTRODUCCIÓN

Nos encontramos en una era de continuo y rápido desarrollo, uso y difusión de nuevas tecnologías, las cuales sin que nos demos cuenta, han logrado ocupar un importantísimo papel en la cotidianidad de nuestras sociedades.

Tenemos la certeza de que esta tendencia ha permitido explotar, como nunca antes, la creatividad y el conocimiento de los seres humanos, abriendo un abanico de posibilidades de innovación casi ilimitadas, acortando distancias y haciendo de este mundo un lugar cada vez más conectado.

Pero también es cierto que el desmedido uso y abuso de dichas tecnologías y el incremento de las amenazas informáticas se presenta como el gran desafío que los profesionales de la seguridad de la información y las organizaciones de todo tipo deben enfrentar.

Este trabajo final de Maestría tiene por objetivo principal explorar la posibilidad de tratar la seguridad de la información de pequeñas y medianas empresas desde la visión un CSIRT, ente que, entre otras actividades, se encarga de prevenir, responder y alertar sobre cualquier daño eventual ocasionado por la explotación de una vulnerabilidad, colaborando con la entidad afectada para una recuperación rápida de los servicios impactados. En su desarrollo, se determinarán los servicios que un CSIRT brinda e identificarán los más adecuados para el contexto de las PyME.

El presente trabajo final de Maestría se desarrolla en cuatro capítulos de la siguiente manera:

El Capítulo I presenta la definición y la caracterización de una PyME y los principales aspectos que las exponen a mayores riesgos de sufrir ataques informáticos respecto a las grandes empresas.

En el Capítulo II se realiza una introducción a un CSIRT como tal, es decir, cuáles son los servicios que brinda, los problemas que soluciona, cómo se estructura y cuáles son los roles con los que cuenta.

Se expone también un relevamiento de CSIRT´s que ofrecen servicios para PyME a nivel mundial y sus principales características.

En el Capítulo III se discuten cuáles son los principales obstáculos para el desarrollo de un CSIRT PyME, planteándose varias hipótesis al respecto. Se expone adicionalmente una breve descripción de el por qué sería válida la gestión de emergencias informáticas de las PyME a través de un CSIRT especializado.

Finalmente, en el Capítulo IV y en base a lo expuesto en Capítulo III, se presenta un listado con los beneficios y los riesgos que conlleva la creación de un CSIRT PyME, una selección de cuáles serían los servicios más adecuados (tomando en cuenta las limitaciones de las pequeñas y medianas empresas) y la mención de sus respectivas políticas para su constitución. También se expone un presupuesto probable para el arranque del CSIRT-PyME considerando diversos aspectos para su puesta en marcha.

Adicionalmente a este documento se presentan varios anexos, entre los que se destacan el ANEXO A con un cronograma tentativo de todas las actividades pertinentes para el arranque del CSIRT PyME. El ANEXO B que es un ejemplo de política de seguridad informática (PSI) orientado a todo interesado en brindar seguridad básica a una PyME y el ANEXO C, una descripción de los servicios del CSIRT PyME de acuerdo a la norma *Request for Comments* (RFC) 2350 *Expectations for Computer Security Incident Response* emitido por el *Internet Engineering Task Force*, cuyo propósito es expresar por escrito y en un formato estandarizado información básica sobre el CSIRT PyME.

El trabajo final de Maestría termina con las principales conclusiones a las que se arriba a partir de su desarrollo y una serie de recomendaciones al respecto.

Se aclara que una posible solución frente a la falta de preparación del sector PyME, para enfrentar posibles incidentes o fallas de seguridad, es que alguno de los CSIRT existentes extienda el alcance de su comunidad objetivo para abarcar a las pequeñas y

medianas empresas. No obstante, varios de los aspectos analizados y de las soluciones propuestas en este trabajo podrían ser de utilidad en el caso de que se optara por la creación de un CSIRT dedicado exclusivamente a las PyME.

CAPITULO I

1.1 DEFINICION Y CARACTERIZACIÓN DE UNA PYME

Una PyME (acrónimo de pequeña y mediana empresa) es un tipo de organización de dimensiones y personal limitado, que se define principalmente por contar con un nivel de recursos y posibilidades mucho más reducidas que las de las grandes empresas. El término se aplica además a las empresas que generan una determinada cantidad de ingresos anuales, por lo cual todas aquellas que sobrepasen el límite o parámetro establecido (que varía de una región a otra) dejan de ser consideradas como tales.

> La definición de pyme varía según el país. En Argentina, por ejemplo, las empresas se clasifican de acuerdo a sus ventas anuales y a su rubro (una pyme industrial puede tener un volumen de facturación que, en otro sector económico, la ubicaría entre las de mayor volumen). En otros países, el concepto de pyme se asocia a la cantidad de empleados. Entre 1 y 10 empleados, se habla de microempresa; entre 11 y 50, de pyme. Dichas cifras, de todas maneras, pueden variar de acuerdo a la región." [1]

Categoría de empresa	Efectivos: Unidades de trabajo anual (UTA)	Volumen de negocios anual o	Balance general anual
Medianas	< 250	≤ 50 millones EUR o	≤ 43 millones EUR
Pequeñas	< 50	≤ 10 millones EUR o	≤ 10 millones EUR
Microempresas	< 10	≤ 2 millones EUR o	≤ 2 millones EUR

Cuadro N° 1 Umbrales para la definición de una PyME según la Unión Europea [2]

Existe una amplia coincidencia entre los especialistas en que el desarrollo de las empresas pequeñas y medianas PYME es provechoso, tanto desde el punto de vista económico como social. Las PYME absorben una parte importante de población económicamente activa y generan un porcentaje significativo de la producción, contribuyendo a mejorar los índices micro y macro económicos de una nación.

Las empresas de este tipo presentan varias ventajas, entre las que se cuentan:

- Son más dúctiles que las empresas más formales en el manejo de sus procesos internos.
- Dinamizan la economía local y nacional, y suelen ser parte de las cadenas de proveedores de las grandes empresas.
- Comúnmente logran vínculos más sólidos con sus clientes.
- Gracias a la mayor sencillez de su infraestructura, les es más fácil cambiar de nicho de mercado (el espacio donde se encuentran los potenciales proveedores y usuarios o consumidores de un servicio o producto).
- Los puestos de trabajo son más amplios, menos estrictos y los trabajadores sienten que son parte importante en la toma de decisiones de la empresa
- El mayor nivel de conocimiento específico, que se da gracias a la cercanía de los integrantes con el día a día de la empresa, puede convertirse en una importante ventaja.
- El tiempo que requiere la toma de decisiones estratégicas puede ser considerablemente menor, dado que los procesos de gestión resultan menos complejos.

- Presentan un enfoque mucho más práctico y sencillo de administrar, más orientado a las necesidades y demandas de los clientes, lo que les permite adoptar sobre la marcha importantes modificaciones a nivel estructural.
- Aceptan rápidamente nuevas metodologías para encarar los desafíos que se presentan a cada paso.

Entre sus principales desventajas están:

- Dado que se mueven por procesos informales fácilmente mutables, no cuentan con lineamientos específicos; por lo que experimentan constantes cambios y evoluciones.
- No gozan de un importante respaldo financiero y tienen bajo acceso a líneas de crédito, lo que les impide embarcarse en negocios de gran envergadura y crecer.
- Requieren de una constante revisión de su estructura, dado que su naturaleza adaptable puede convertirse en la razón de su disolución a causa de la pérdida del control organizativo.
- Dado que generalmente tienen planillas pequeñas de personal, la mayor cercanía entre los trabajadores puede ser negativa, al proyectar posibles problemas personales en la empresa. Muchas PyME poseen inclusive una estructura familiar donde dueños y empleados tienen algún nivel de parentezco.
- Suelen carecer de recursos y conocimientos suficientes para publicitar sus productos, por lo que la empresa puede pasar desapercibida ante los consumidores. [3]

A pesar de estas desventajas, y como ya se mencionó, en la mayoría de las economías del mundo las PyME son imprescindibles para el desarrollo económico y social, ya que generan puestos de trabajo y oportunidades de negocio de distinta naturaleza en diferentes

estratos. Tienen una presencia importante en el escenario económico de una nación, lo que demanda la necesidad de que desarrollen esquemas de operación estratégicos, acordes al entorno global y competitivo en que se vive actualmente.

En Latinoamérica particularmente, son varios los países de la región en los que las PyME son la base del crecimiento de sus PBI (Producto Bruto Interno).

> "Las pequeñas y medianas empresas (pymes) son vitales para la economía ecuatoriana. El 65% de los empleos son generados por pymes, las cuales aportaron con un 15% del PIB el año pasado y unas 1.500 exportan en la actualidad. Estas empresas se encuentran en segmentos que van desde el comercio, la agricultura y las industrias manufactureras, hasta el transporte, los servicios, entre otros. Además, hasta el 2017 se contabilizaban cerca de 838 000 pymes, según el directorio de empresas del Instituto Nacional de Estadísticas y Censos. Estos datos confirman el peso que las pymes tienen como motor productivo del país, pero este sector también enfrenta una serie de desafíos." [4]

1.2 RIESGOS DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LAS PYME

Con la dinámica del mercado y el crecimiento de los estándares mundiales de calidad, las PyME deberían estar en condiciones de implementar cambios rápidamente. En el mismo sentido, puede decirse que ha aumentado la presión sobre estas empresas para adaptarse y cumplir con nuevas exigencias, siendo la tecnología un medio para lograr este objetivo.

El reto y principal tarea consiste en que las PyME, con escasos recursos económicos, adopten de manera eficiente herramientas informáticas como una oportunidad de desarrollo, ampliación y diversificación de su operatoria en respuesta al mercado en permanente transformación; cumpliendo a su vez con mínimos estándares de calidad en la entrega de sus productos y servicios.

> La entrada de las Pymes al mundo digital es el siguiente paso evolutivo de los negocios. Amenaza y oportunidad al mismo tiempo: quienes se preparen y adapten a la cuarta revolución industrial serán quienes puedan competir y despuntar. Para lograrlo se debe ser cauteloso: cada vez más Pymes almacenan sus datos en formato digital, pero pocas estiman tener "una protección actualizada completamente en funcionamiento". [5]

Las tecnologías de la información son un instrumento de invaluable soporte y la democratización de su difusión y uso está en un pináculo histórico nunca antes visto. Si una PyME quiere ser exitosa y expandirse, deberá procurar sacar el mayor provecho posible a dichas tecnologías, lo cual se traducirá en un aumento de la productividad como resultado de la mejora de procesos y la creación de valor para clientes y empleados de la organización, al tiempo de incrementar su alcance geográfico y su cartera de clientes.

En la actualidad, sin embargo, son comunes las noticias que alertan sobre incidentes informáticos; dejando en evidencia los peligros que la tecnología acarrea, como, por ejemplo, los ciberataques a servidores o el robo de datos. El sector PyME también es blanco de este tipo de actividad maliciosa.

> "Según la Encuesta de riesgos de la seguridad corporativa, realizada por Kaspersky Lab en 2016, el 62% de las pymes en Argentina sufrió de dos a cinco incidentes separados de pérdida de datos en un año." [6]

A medida que las grandes empresas aumentan y adquieren herramientas de defensa más sofisticadas, los atacantes informáticos comienzan a dirigir sus esfuerzos hacia otros sectores más vulnerables, como las empresas PyME.

> "Hace unos años, los empresarios locales creían que los delincuentes informáticos tenían en su mira sólo a Estados Unidos y Europa. Pero la situación cambió. Brasil, por ejemplo, ocupa el noveno puesto a nivel mundial en el ranking de víctimas de ciberataques. Aunque la Argentina aún tiene un porcentaje bastante bajo dentro de la región, los especialistas advierten que esto podría revertirse en poco tiempo y, además, reconocen que muchos ataques se desconocen, porque no son denunciados por las pymes." [7]

A continuación, se presenta una lista de algunas de las vulnerabilidades más importantes que muestran las empresas PyME. Muchas de ellas impactan también en organizaciones de mayor dimensión, pero sus consecuencias suelen ser más devastadoras en para para protegerse:

- Falta de consciencia sobre las amenazas informáticas.
- Recursos insuficientes.
- Software ilegal o sin licencia.
- BYOD.
- Ausencia de respaldo de información crítica.
- Profesionales no calificados.
- Desconocimiento de la dirección sobre los riesgos de las TI.
- Ausencia de previsiones para evitar el robo de datos y recursos para su procesamiento.

1.2.1 FALTA DE CONSCIENCIA SOBRE LAS AMENAZAS INFORMATICAS

En general, en el tipo de empresas bajo estudio, no existe una correcta apreciación de todos los integrantes que la conforman sobre lo perjudicial que puede llegar a ser un ataque proveniente del exterior a la compañía, ni tienen idea de los procesos ni de la información crítica con la que se cuenta y cómo protegerla. Tampoco se tiene claro cuál sería la magnitud de los daños que se podrían generar si se llegara a producir un incidente originado internamente o un ataque perpetrado por algún colaborador de la misma empresa, que comprometa los servicios informáticos.

Los responsables de las PyME suelen suponer que, por tener un volumen de negocio menor; la información que manejan carece de valor para los atacantes informáticos. Sin embargo, para estos delincuentes no hay diferencia entre una empresa grande o pequeña.

Si una PyME maneja datos o transacciones de sus clientes, por ejemplo, pagos y números de tarjetas de crédito o débito, entonces ya tiene un recurso valioso que será apetecido por manos malhechoras, y que además es información que es altamente cotizada en el mercado ilegal.

> "La gestión de la información a través de las nuevas tecnologías está aportando un gran valor a las pymes. Proteger toda esa información genera confianza en clientes, proveedores y colaboradores. Tener la ciberseguridad como uno de los valores de tu empresa es un elemento que la diferencia de la competencia, pero ocurre que las pymes toman conciencia del peligro «cuando ya han sufrido un ataque». Al menos hasta hace poco, porque van reconociendo los riesgos." [8]

Cualquier negocio, por muy pequeño que sea, debe establecer medidas de seguridad razonables, que empiecen necesariamente por mejorar la cultura y el conocimiento en seguridad informática.

> "Las pymes piensan que no son objetivos de los hackers, pero la realidad es que normalmente estos no son personas atacando ordenadores, sino máquinas atacando a máquinas; es totalmente indiscriminado. Además, con cientos de miles de sistemas, ¿por qué ir al que está protegido?" [9]

En cuanto a los atentados generados por sus propios empleados, las PyME, particularmente, son el segmento empresarial que se muestra más significativamente despreocupado por las actividades que realizan sus integrantes.

> Según el Informe Riesgos de Seguridad TI de 2016 de Kaspersky Lab, una plantilla desinformada o descuidada, que hace uso de los recursos de TI de manera inapropiada, puede poner en peligro la protección de una organización. De hecho, puede afectar a cualquier negocio de cualquier tamaño. Según la encuesta, las acciones de los empleados se encuentran entre los tres principales desafíos de seguridad que hacen a

> las empresas más vulnerables. Más de la mitad de los negocios (61%) que han experimentado un incidente de ciberseguridad en 2016 ha admitido que el comportamiento descuidado y la desinformación de los trabajadores han contribuido a ello. [10]

Es evidente que el factor humano es el elemento más sensible y los atacantes están continuamente perfeccionando sus técnicas para tratar de persuadir a incautos usuarios. Día a día llegan a buzones de correo importantes cantidades de notificaciones engañosas de pagos atrasados, compras canceladas u donaciones de dinero. Tomar por sorpresa suele ser la artimaña más comúnmente usada, y quizás una de las más eficaces. Lo que ocurre posteriormente va por añadidura, el iluso accede a enlaces que solicitan información personal o del negocio.

1.2.2 RECURSOS INSUFICIENTES

Habitualmente se considera que el nivel de desarrollo tecnológico de las PyME es bajo. Los escasos recursos económicos con los que cuenta son la limitante a la hora de contar con tecnología en hardware o software que soporte las actividades informáticas de una manera segura y eficiente. Por otro lado, y de igual forma que las empresas grandes, también las pequeñas y medianas se enfrentan al desafío de gestionar un escenario tecnológico que evoluciona permanentemente a la par de los riesgos que las amenazan.

> “El acceso a recursos financieros por parte de las PYMEs se ve limitado en diversos frentes. Las PYMEs no tienen acceso a recursos del mercado de capitales, cuyo desarrollo es todavía limitado y concentrado en empresas grandes. Pero muchas de las empresas tampoco disponen de acceso al mercado de crédito o, si lo tienen, enfrentan condiciones de costo y oportunidad relativamente elevados.” [11]

Si un ataque, por ejemplo, a través de un programa malicioso llega a afectar la continuidad de sus operaciones, podría quizás hasta acabar con su negocio y, por tanto, sería más alta la pérdida que la inversión necesaria para implementar mecanismos para evitarlo. Por ello, es importante la implantación temprana de acciones o medidas proactivas, sin que necesariamente se tenga que hablar de grandes inversiones, para proteger la información crítica.

Como se conoce en el argot popular, más vale prevenir que lamentar; y siempre será más económico hacer una inversión preventiva que una reactiva.

1.2.3 SOFTWARE ILEGAL O SIN LICENCIA.

La instalación y uso de programas gratuitos de dudosa procedencia o sin licencia es otra de las causas por las que las PyME sufren ciberataques. Es habitual que, por ahorrar algo de dinero, no se tome en cuenta el cuidado necesario en comprobar la reputación tanto de las aplicaciones descargadas o compradas, como de las fuentes y enlaces desde donde se obtienen.

Sistemas operativos y programas sin licencias son altamente proclives a no contar con todas sus prestaciones activas, incluyendo las actualizaciones; las cuales además de mejorar el desempeño de los programas, adicionan componentes de seguridad, útiles para aumentar su inviolabilidad.

> Al utilizarse software sin licencia, las probabilidades de encontrarse con software malicioso son altas. Y el costo de lidiar con esto puede ser abrumador. A modo de ejemplo, solo en el 2017, las empresas tuvieron que afrontar un gasto de $400 mil millones en ciberataques. Cuanto mayor sea la tasa de software de PC sin licencia, mayor será la probabilidad de que los usuarios experimenten malware potencialmente debilitante. [12]

Ataques como el del *ramsonware* WannaCry en mayo de 2017, dejan en evidencia la necesidad de poder contar con sistemas operativos licenciados y con sus actualizaciones activas y al día.

> Los ataques ransomware de la variedad WannaCry (en inglés *WannaCry ransomware attack o Wanna Cry Doble Pulsar Attack*), son ataques informáticos que usan el criptogusano conocido como WannaCry (también denominado WannaCrypt, WanaCrypt0r 2.0, Wanna Decryptor) dirigidos al sistema operativo Windows de Microsoft. Durante el ataque, los datos de la víctima son encriptados, y se solicita un rescate económico pagado con la criptomoneda Bitcoin, para permitir el acceso a los datos.
>
> Los ataques ransomware presuntamente infectan un ordenador cuándo un usuario abre un email phishing. Una vez instalado, WannaCry utiliza el exploit conocido como EternalBlue, desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA), para extenderse a través de redes locales y anfitriones remotos que no hayan recibido actualizaciones de sistema operativo más reciente, y de esta manera infecta directamente cualquier sistema expuesto. [13]

1.2.4 BYOD

Una de las tendencias a tomar en cuenta, y que mayores problemas están trayendo a las PyME, es la política del BYOD *(bring your own device)*, que se traduce como “traer tu propio dispositivo”, una corriente que en los últimos tiempos ha ganado auge, y que sin duda ha ocasionado una alta probabilidad de complicaciones a este tipo de empresas. Esta tendencia se caracteriza por el hecho de permitir a los empleados la incorporación de sus dispositivos móviles personales (portátiles, teléfonos inteligentes y tabletas) a las redes corporativas desde su casa, la propia oficina o cualquier otro lugar, aceptando su uso compartido, tanto para las tareas profesionales de uso corporativo como para las personales.

Varios casos famosos a nivel mundial de robo de datos personales han dado la alerta sobre la vulnerabilidad de los dispositivos móviles como teléfonos y tabletas. Estos dispositivos no se encuentran libres de vulnerabilidades y la falta de previsión allana el camino a los criminales. Todos estos terminales tienen que contar con medidas de seguridad básicas, ya que hoy en día, son una herramienta más de trabajo.

> "Las pequeñas y medianas empresas están utilizando entre 100 y 1000 dispositivos tecnológicos, incluyendo computadoras de escritorio, laptops, teléfonos inteligentes y tablets. Y con todos estos equipos las compañías sufren amenazas en seguridad tecnológica. Entre las mayores causas de violaciones de datos se encuentran los virus, troyanos, exploits (fragmento de software utilizado con el fin de aprovechar la vulnerabilidad de seguridad de un sistema) y la pérdida de información por medio del malware móvil, ransomware y phishing" [14]

1.2.5 AUSENCIA DE RESPALDO DE INFORMACIÓN CRÍTICA

Lo que ocurre en la vida cotidiana es que muy pocos se interesan en respaldar información hasta que ocurre alguna desgracia de grandes proporciones. Calamidades que van desde la avería imprevista del servidor que almacenaba la información de pagos de clientes, un terremoto que afecta al edificio donde se encuentra la oficina, un incendio o el robo de un computador portátil son ejemplos válidos. Las PyME no toman como prioridad un plan de respaldo de datos continuo y fiable, ya sea porque no saben cómo hacerlo, porque creen que es una operación compleja o porque piensan que es una pérdida de tiempo.

En la actualidad casi toda la información se encuentra en formato digital y es ineludible darle respaldo, especialmente a los datos que son considerados indispensables o críticos. Nada ni nadie está exento de sufrir algún desastre natural o provocado por el hombre, que le impida

acceder a los datos de su actividad o a las instalaciones dónde los procesa.

1.2.6 PROFESIONALES NO CALIFICADOS

En las PyME prácticamente cualquier persona puede desempeñar varios roles, dejando un amplio margen de acción a la improvisación ante la ausencia de personal especializado. De igual manera que respecto a otros riesgos que las afectan, la falta de recursos económicos frena la contratación de personal fijo o de servicios tercerizados adecuado para brindar soporte a las tareas que respalden una correcta gestión de los datos y su debida protección.

> "En pequeños negocios sin un personal TI adecuado es muy común ver cómo muchos trabajadores implementan por sí mismos seguridad en sus puestos de trabajo, por ejemplo, instalando soluciones antimalware gratuitas con funcionalidades limitadas. Esto plantea riesgos importantes para las empresas, pues un único descuido de un empleado puede afectar a todos los datos que hay en una organización – lo que supone pérdidas instantáneas de datos de clientes y dinero. Las compañías deben implementar soluciones de seguridad diseñadas específicamente para pequeñas y medianas empresas con protección para que cualquier administrador TI, incluso con pocos conocimientos tecnológicos, pueda mantenerlas fácilmente desde cualquier lugar" [15]

En un escenario ideal, es necesario contar con recursos humanos con conocimientos en materia de seguridad informática que se encargue de gestionar la seguridad de la información, aplicando algún medidas que guíen a la PyME en la implementación de la seguridad de su información.

1.2.7 DESCONOCIMIENTO DE LA DIRECCIÓN SOBRE LOS RIESGOS DE LAS TI

Por su naturaleza informal, las PyME suelen ser dirigidas por personas que no cuentan con una adecuada preparación en gestión empresarial. Arrancan como negocios personales o familiares, con un

desarrollo más extenso en el tiempo y con curvas más moderadas de crecimiento, tratando de cubrir una necesidad existente en un mercado local.

Generalmente en estas empresas todo se realiza con el visto bueno de un número muy limitado de personas, que piensan que pueden resolver temas de diversa índole por su propia cuenta, confiando únicamente en su propia capacidad de resolución.

Dada la importancia del control informático, el gerente, dueño o responsable debe ser consciente de que en la mayoría de los casos, no tienen ni el tiempo para realizar una adecuada gestión ni los conocimientos requeridos para una adecuada protección de la información; y partiendo del hecho de que bastaría solamente un incidente que logre comprometer la seguridad de la información para paralizar o acaso, sacar del negocio a una PyME, se deja en claro entonces el riesgo que corren estas organizaciones en las manos de una o varias personas sin la destreza necesaria.

1.2.8 AUSENCIA DE PREVISIONES PARA EVITAR EL ROBO DE DATOS Y RECURSOS PARA SU PROCESAMIENTO

El robo de información se ha convertido en una de las grandes amenazas que afectan a las empresas. Fugas de información ejecutadas por personal propio a través de medios magnéticos, micrófonos, puertos USB no bloqueados o sesiones que no son debidamente bloqueadas, ataques provenientes del exterior ejecutados por delincuentes cibernéticos, dejan a las PyME en situación de indefensión y permiten filtraciones o el acceso de personas no autorizadas a datos sensibles.

> Las empresas manejan una gran cantidad de información que puede ser sustraída con fines delictivos. Sin embargo, son muchas las que consideran que no corren ningún riesgo al no protegerla. "Una de las razones de esta falta de concienciación de seguridad por parte de las pequeñas empresas es la creencia de que los cibercriminales no malgastan su tiempo atacando negocios pequeños. No obstante, algunos ciberdelincuentes comunes prefieren enfocarse en ellas

> precisamente porque no están debidamente protegidas, llevando a cabo robos de menor cuantía, pero mucho más fáciles de perpetrar. [16]

El sector de la PyME debe ser cuidadoso y consciente de la importancia de salvaguardar los datos personales, así como la información de su operatoria.

Muchas PyME rebosan de ideas y de mucho entusiasmo para llevar adelante su actividad, sin embargo, carecen de un plan de continuidad para que su proyecto prevalezca en el tiempo. Es inexcusable que se realice una evaluación de los peligros a los que podrían estar expuestas, ya que, al protegerse debidamente generarán confianza, lo cual las ayudará a conseguir sus objetivos a corto, mediano y largo plazo.

Es tarea de las PyME resguardar a conciencia sus datos y los de sus empleados, negocio, productos y colaboradores externos frente a toda especie de amenazas que puedan afectar su inversión, pudiendo así ayudar a garantizar el éxito y la supervivencia de su empresa.

CAPÍTULO II

2.1 CSIRT

2.1.1 SIGNIFICADO Y DEFINICIÓN

CSIRT son las siglas de la expresión en inglés "*Computer Security Incident Response Team",* lo que en español se traduce como "Equipo de Respuesta a Incidentes de Seguridad Informática".

> Se usan diferentes abreviaturas para el mismo tipo de equipos:
>
> CERT (Computer Emergency Response Team, equipo de respuesta a emergencias informáticas)
>
> IRT (Incident Response Team, equipo de respuesta a incidentes)
>
> CIRT (Computer Incident Response Team, equipo de respuesta a incidentes informáticos)
>
> SERT (Security Emergency Response Team, equipo de respuesta a emergencias de seguridad) [17]

De estos, los acrónimos más requeridos para nombrar a estos equipos son CSIRT y CERT. El término CSIRT es mayoritariamente usado en Europa y es equivalente al término protegido CERT, registrado por la Universidad Carnegie Mellon en Estados Unidos, el cual requiere su autorización para su uso.

Un CSIRT es un grupo de expertos que sirve a una comunidad objetivo[1], el cual es responsable del desarrollo de medidas preventivas, reactivas y de gestión ante incidencias de seguridad en los sistemas de información. En el desarrollo de su actividad, entre otras opciones, se analiza el estado de seguridad global de redes y computadoras, se proporcionan servicios de respuesta ante incidentes a víctimas de ataques en la red, se publican alertas relativas a amenazas y

[1] Se define como comunidad objetivo al conjunto de clientes o usuarios, con características, intereses u objetivos similares, a los cuales el CSIRT brinda sus servicios. Es necesario que se conozcan las necesidades del grupo atendido, tener clara la propia estrategia de comunicación y determinar cuáles son los canales de comunicación más adecuados para transmitir información al grupo y para recolectar aquella que sea de interés para quienes reciben los servicios.

vulnerabilidades y se ofrece información que ayuda a mejorar la seguridad de estos sistemas. El primer CERT fue creado en 1988 en respuesta al incidente del gusano Morris. [18]

2.1.2 HISTORIA DE LOS CSIRT

La historia de los CSIRT comienza a finales de la década de los ochenta. Surgieron como una iniciativa organizada para poder hacer frente al surgimiento de amenazas informáticas en ambientes distribuidos.

> El culpable fue Robert Tappan Morris, un estudiante de 23 años hijo de Robert Morris, un criptógrafo de la NSA que había sido uno de los padres del Unix. Morris hijo aplicó la ciencia de su padre para crear un programa capaz de reproducirse a sí mismo a través de las redes y esconderse después. Había creado el primer gusano informático que se difundiría por internet, una de las mayores pesadillas de los administradores de sistemas desde entonces. [19]
>
> El gusano Morris fue el primer ejemplar de malware auto replicable que afectó a Internet (entonces ARPANET). El 2 de noviembre de 1988, aproximadamente 6000 de los 60.000 servidores conectados a la red fueron infectados por este gusano informático, lo que motivó que la DARPA (*Defence Advanced Research Projects Agency*, Agencia de Investigación de Proyectos Avanzados de Defensa) creara el primer CSIRT: el CERT Coordination Center (CERT/CC3), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania) en réplica a las necesidades expuestas durante el incidente, que finalmente terminó actuando como una alarma: de repente todo el mundo se dio cuenta de que existía una gran necesidad de cooperación y coordinación entre administradores de sistemas y gestores de TI para enfrentarse a este tipo de casos. Por ser el tiempo un factor decisivo, se tenía que establecer un enfoque más organizado y estructural de la gestión de los incidentes relacionados con la seguridad de las TI. [20]

Hoy existen más de 380 CERT de carácter gubernamental, comercial o educativos en todo el mundo englobados dentro de la red FIRST *Forum of Incident Response and Security Teams* (Forum de Equipos de Seguridad y Respuesta de Incidentes), si bien se han

desarrollado otros grupos que no integran esta organización. Desde 1990 cuando se fundó, FIRST (cuyo sitio web es https://www.first.org/) intenta fomentar la cooperación y la coordinación en la prevención de incidentes entre sus miembros, lo cual han generado un flujo permanente de información de seguridad relacionado con los ataques e incidentes, incluyendo el manejo de vulnerabilidades que afectan a millones de sistemas y redes en todo el mundo. El propósito de FIRST es estimular una reacción rápida a los acontecimientos y promover la distribución de información entre sus miembros, generando una red global de confianza.

2.1.3 DEFINICIÓN DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Un incidente de seguridad es a rasgos generales, cualquier tipo de acción, intencional o no, que busque comprometer la confidencialidad, disponibilidad y/o integridad de la información de una organización o de una persona. Otra definición mas elaborada es la que sigue:

> Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Seguridad de la Información [21]

2.2 OBJETIVOS A CUMPLIR

La razón principal para constituir un CSIRT es la necesidad de atender a una comunidad objetivo para asistirla en la resolución de problemas e incidentes de seguridad informática, a través de profesionales experimentados y dedicados específicamente a la gestión de incidentes.

Otra meta no menos importante, busca elevar el nivel de conocimientos en los usuarios que atiende sobre la importancia de la

seguridad de las tecnologías de la información, implantando una cultura de sensibilización y promoviendo la adopción temprana de medidas proactivas y preventivas

Internet está repleto de atacantes y delincuentes que buscan acceder a la información que poseen las empresas, cualquiera sea su tamaño y finalidad. La información es un activo de gran valor que tratan de obtener con el fin de conseguir alguna ganancia económica, sobresalir como expertos en romper la seguridad de los sistemas, dar a conocer un mensaje político o simplemente para dañar la reputación de la empresa atacada. Se necesita, por tanto, montar mecanismos de defensa y alerta temprana que restrinjan este tipo de acciones y minimicen su impacto.

Un CSIRT procura ofrecer cursos de operación para responder a amenazas e incidentes informáticos en una escala local, nacional o internacional, integrando esfuerzos con otros CSIRT y tratando de ofrecer una respuesta expedita al grupo de clientes atendidos. El tiempo de respuesta es trascendental para un CSIRT efectivo. Una respuesta rápida puede minimizar el daño en el hardware y software de una organización causado por un incidente concreto.

El CSIRT coordinará los pasos a seguir para una recuperación vertiginosa y eficiente de los servicios que se hayan visto afectados, de manera que la organización pueda reanudar su rutina en el menor tiempo y con el menor impacto posible.

Además, buscará que el origen y la solución de dichos eventos sirvan para la implementación de acciones para casos similares que pudieran presentarse en un futuro, propiciando la creación de una base de conocimientos que ayude a registrar las lecciones aprendidas de estos sucesos con el propósito de que no se repitan, y si esto llegara a acontecer, que se pueda contar con las posibles y rápidas soluciones.

Para cumplir con estas metas, los CSIRT comparten información sobre incidentes de seguridad con otros equipos de similar naturaleza,

con el fin de alertar sobre los mismos e intentar mitigar el impacto de nuevas amenazas, vulnerabilidades o ataques.

2.3 TIPOS DE CSIRT

Existen varios criterios para clasificar a un CSIRT. De acuerdo a la comunidad objetivo que atienden, es decir identificando posibles sectores beneficiarios, se pueden identificar los siguientes:

- CSIRT del sector académico.
- CSIRT comercial para una o varias compañías.
- CSIRT del sector de infraestructuras críticas de información, conocidas con la sigla CIP/CIIP.
- CSIRT del sector público.
- CSIRT interno.
- CSIRT del sector militar.
- CSIRT nacional.
- CSIRT del sector PYME.
- CSIRT de soporte.

De acuerdo al Manual Básico de Gestión de Incidentes de Seguridad Informática del Proyecto Amparo [22], otra manera de clasificar a los CSIRT viene dada por el tipo de modelo organizacional a adoptar, con lo que se tendría la siguiente categorización:

- Equipo de respuesta a incidentes centralizado: existe un único equipo de respuesta a incidentes que se encarga del manejo de todos los incidentes. Apto para aquellas organizaciones grandes cuya infraestructura tecnológica no esté en sitios geográficamente distantes. El centro de respuesta centralizado es el único punto de contacto en

toda la organización para la respuesta a incidentes y reportes de vulnerabilidades.

- Equipo de respuesta a incidentes distribuido: En una organización se cuenta con varios equipos de respuesta a incidentes. Se crean o definen para responder incidentes específicos y suelen actuar de forma coordinada.

Adicionalmente existe una tipificación de acuerdo a la estructura organizacional:

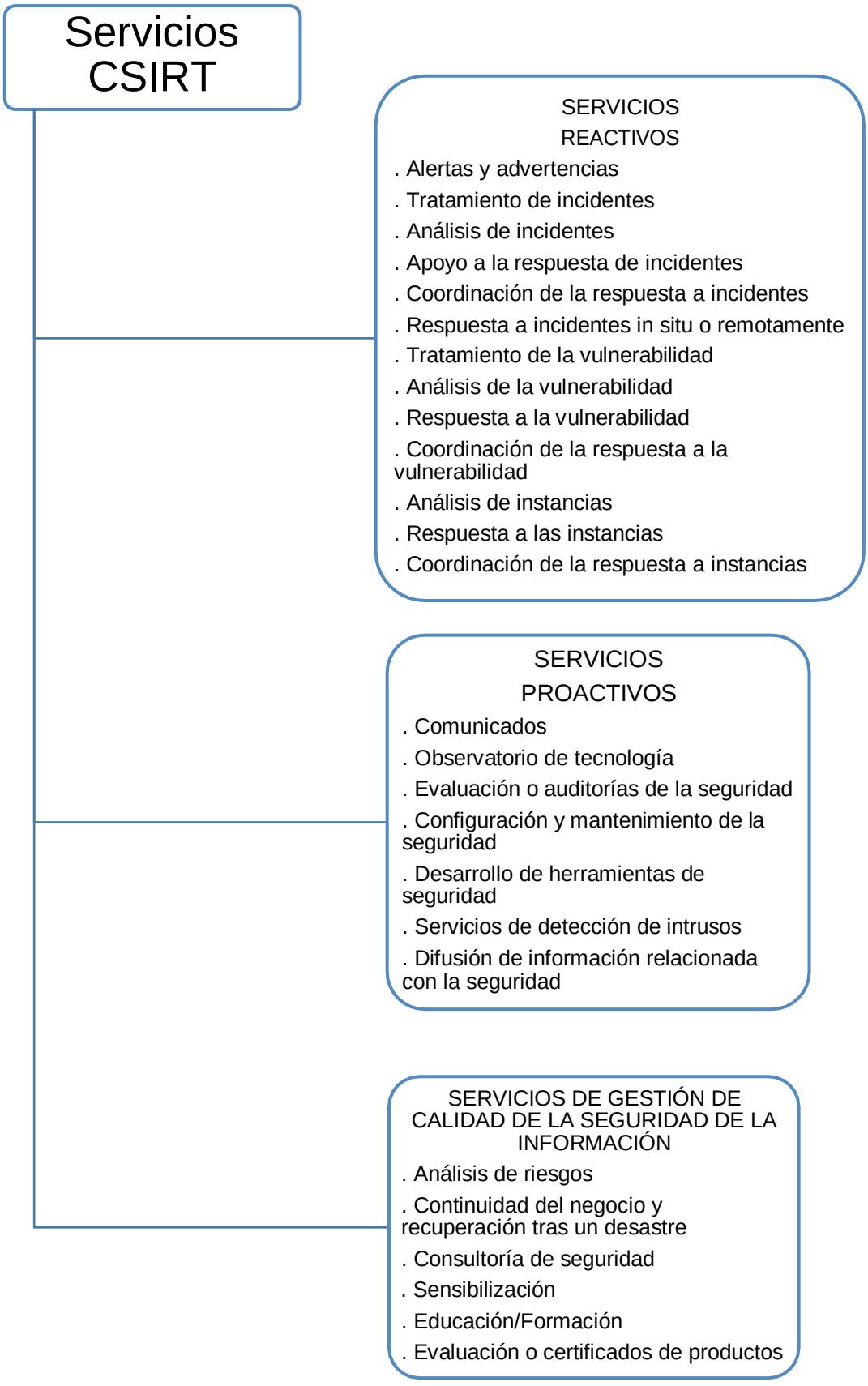
- Modelo funcional: Las actividades se agrupan por funciones comunes desde la base hasta la cima de la organización
- Modelo basado en el producto: Se organiza de acuerdo a lo que se produce ya sean bienes o servicios, similar al modelo de divisiones en las grandes compañías.
- Modelo basado en los clientes: El cliente es el eje central, los clientes en cada conjunto tienen problemas y necesidades comunes que pueden ser resueltos teniendo especialistas departamentales para cada uno.
- Modelo híbrido: Agrupa varias características más destacadas de los modelos anteriormente descritos. De acuerdo a la necesitad, un CSIRT puede requerir un enfoque basado en productos y funciones.
- Modelo matricial: Comparte flexiblemente los recursos humanos entre productos. Adaptado para tomar decisiones complejas y cambios frecuentes en un entorno inestable.

2.4 SERVICIOS QUE PROPORCIONA UN CSIRT

Dentro de las actividades que un CSIRT puede brindar se pueden distinguir tres grandes grupos:

- Servicios reactivos: Centrados a responder y tratar los incidentes y reducir el impacto que pueda presentarse.
- Servicios proactivos: Se enfocan en la prevención mediante la mejora en la infraestructura y los procesos de seguridad de la comunidad objetivo a ser atendida antes de que se produzcan o detecten incidentes. Sus objetivos son claros: evitar los incidentes y reducir el riesgo y su alcance en el caso de que llegaran a presentarse.
- Servicios de gestión de calidad de la seguridad de la información: Los servicios de esta categoría no son propios del tratamiento de incidentes ni de los CSIRT. Son servicios diseñados para mejorar la seguridad general de una organización. Merced a la experiencia adquirida con la prestación de los servicios reactivos y proactivos, un CSIRT puede aportar a esos servicios de gestión de la calidad perspectivas únicas de las que en caso contrario no dispondrían.

A continuación se presenta un cuadro obtenido del Manual “Cómo crear un CSIRT paso a paso” **[23]** que condensa todos los servicios previstos por un CSIRT. Una de las tareas más importantes que tiene un CSIRT es definir los servicios a ofrecer, según la necesidad requerida y de acuerdo a los recursos disponibles de los integrantes de la comunidad objetivo.



Cuadro N° 2 Servicios de un CSIRT

Como se indica, un CSIRT puede ofrecer servicios proactivos, reactivos o de gestión de calidad de seguridad de la información, compartir su accionar con otros equipos de respuesta a incidentes o tercerizar algunos servicios. Sin embargo, si solo se centrara en responder a incidentes (servicios reactivos), también se lo puede considerar como un CSIRT, siendo este el servicio que hace a la esencia de un equipo de esta naturaleza.

Un CSIRT podría arrancar su actividad ofreciendo servicios de este tipo, y si se estimara conveniente, en lo posterior podrá ir incorporando los demás.

2.5 BENEFICIOS DE LA IMPLEMENTACIÓN DE UN CSIRT

Un CSIRT ofrece a la comunidad objetivo mecanismos que permitan una respuesta ágil a un incidente de seguridad informática y la recuperación del daño causado en el menor tiempo posible, con el correspondiente restablecimiento del servicio afectado. Comparte información con otros equipos de respuesta a incidentes con el fin de brindar alertas e intercambiar experiencias y conocimientos, fomentando procedimientos comunes para responder a incidentes de seguridad y formar personal especializado.

De acuerdo al Manual Básico de Gestión de Incidentes de Seguridad Informática del Proyecto Amparo [24] a continuación, se listan algunos de los beneficios más comunes que se obtiene al implementar un CSIRT:

- Se conforma como un punto de contacto confiable dentro de la comunidad para el manejo de incidentes de seguridad informática.
- Se promueve el uso de infraestructura tecnológica basada en buenas prácticas para la adecuada coordinación de la respuesta a incidentes de seguridad informática.

- Se cuenta con un punto especializado para la protección de las distintas actividades informáticas de los integrantes que conforman su comunidad objetivo.
- Se difunde información sobre vulnerabilidades y recomendaciones para la su mitigación.
- Se proveen servicios de publicación de información eficaz con la finalidad de fortalecer una cultura de seguridad informática.
- Se comparten experiencias con equipos similares y proveedores de servicios de seguridad informática, lo que facilita el establecimiento de mejores estrategias para el manejo de incidentes de seguridad informática.
- Se asiste a otras instituciones que lo requieran para desarrollar capacidades propias para el manejo de incidentes y se implantan buenas prácticas de seguridad informática.
- Se cuenta con un equipo de personal especializado, en constante actualización para brindar servicios de seguridad informático con un alto nivel de eficacia y eficiencia a los distintos requerimientos que la comunidad demande de su respectivo CSIRT.
- Se promueve y desarrolla material de concientización, educación y entrenamiento en temas de seguridad informática.

Un CSIRT debería enfocar un gran esfuerzo a tareas más proactivas y no tanto a las de carácter reactivo, excepto aquellas que constituyen su función esencial. Es importante que conozcan riesgos y ejecuten procesos de prevención y aseguramiento, permitiendo la reducción de los efectos de fallas y ataques informáticos en la comunidad objetivo.

2.6 RELEVAMIENTO DE EQUIPOS CSIRT EN ARGENTINA Y ECUADOR

De acuerdo a la información que consta en el FIRST, los únicos equipos CSIRT registrados en la Argentina y Ecuador son:

- CSIRTBANELCO, https://csirt.banelco.com @BanelcoCSIRT, que provee monitoreo para la detección de amenazas, respuesta a incidentes e intercambio de información a los bancos que integran la red BANELCO, la cual dispone de cajeros automáticos en Argentina y brinda otros servicios relacionados al manejo de dinero, como tarjetas de débito, transferencias electrónicas, servicios de pago, etc. [25]
- ICIC-CERT, http://www.icic.gob.ar/, del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, de carácter gubernamental. Este Programa tiene por objetivo impulsar la creación y adopción de un marco regulatorio específico que propicia la identificación y protección de las infraestructuras estratégicas y críticas del sector gubernamental, los organismos interjurisdiccionales y las organizaciones civiles y las entidades del sector privado que así lo requieran.
- BA-CSIRT https://www.ba-csirt.gob.ar/, centro de respuesta a incidentes de la Ciudad Autónoma de Buenos aires, se dedica a asistir y concientizar a los ciudadanos y a los organismos públicos de dicha ciudad, en todo lo relacionado a la seguridad de la información.
- CSIRT-CEDIA, https://www.cedia.edu.ec, Centro de respuesta a Incidentes informáticos de la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia, impulsada por la asociación de universidades, institutos y otras instituciones educativas locales.

- EcuCERT, http://www.ecucert.gob.ec, Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones, ente financiado con fondos estatales que busca contribuir a la seguridad de las redes de telecomunicaciones en Ecuador.

Adicionalmente en Argentina existen otros CSIRT, que se listan a continuación:

- CERTUNLP http://www.cespi.unlp.edu.ar/, el Centro de Respuestas de Incidentes académico de la Universidad Nacional de La Plata (UNLP). Previene, detecta, gestiona, mitiga e investiga problemas e incidentes de seguridad, coordinando acciones para la protección de los usuarios y los servicios de la UNLP.
- Equipo de Respuesta frente a Incidencias de Seguridad Informática de la Provincia de Buenos Aires, http://www.ciberseguridad.gba.gov.ar/, constituido mediante resolución 251/2017 del Secretario General de la Gobernación.
- Red Link, Servicio de CSIRT, https://www.redlink.com.ar/servicio_csirt.html, brinda soporte a Bancos que integran la Red LINK y proporciona asesoramiento en la prevención y neutralización de ataques web.

Respecto a iniciativas CSIRT para PyME, no se registra ninguna en Argentina o Ecuador.

2.7 CSIRTS PARA PYME

A nivel internacional, solo puede identificarse una iniciativa de equipos de respuesta a incidentes para PyME en los países de habla

hispana, la de INCIBE (Instituto Nacional de Ciberseguridad de España).

Este Instituto fundado en 2006 cambió su denominación en 2014, siendo previamente conocido como Instituto Nacional de Tecnologías de la Comunicación (INTECO). Es un ente estatal referente para el desarrollo de la ciberseguridad que brinda servicios a empresas y profesionales, expertos en ciberseguridad y ciudadanía en general y que hace foco especial en las pequeñas y medianas empresas desde la sección “Protege tu empresa” de su página web https://www.incibe.es/

Considerado las limitaciones que las PyME tienen en cuanto a recursos y conocimientos y, por otro lado, su importante rol en las economías regionales y en las cadenas productivas de las grandes empresas, resulta llamativo que ningún país latinoamericano haya generado una iniciativa como la de INCIBE, por lo que podría considerarse como un factor de alto riesgo.

En efecto, varias PyME también forman parte de encadenamientos productivos con empresas mas grandes, provisionandoles servicios especializados. En 2014 la tienda minorista Target, una de las mas grandes cadenas en los Estados Unidos, sufrió las devastadoras consecuencias de un ciber ataque a sus sistemas perpetrado a través de una de sus proveedoras de servicios de refrigeración. A continuación, la siguiente cita describe lo ocurrido.

> Una empresa de sistemas de aire acondicionado que es proveedora de Target fue víctima de una "sofisticada operación de ciberataque" que pudo haber permitido a los hackers infiltrarse en los sistemas informáticos de la segunda cadena minorista más grande de Estados Unidos y robar millones de números de tarjetas de crédito y débito.
>
> Fazio Mechanical Services Inc., con sede en Sharpsburg, Pensilvania, emitió un comunicado el viernes después de que blogueros expertos en seguridad informática la identificaran como el tercero a través del cual piratas informáticos ingresaron a los sistemas de Target.
>
> La cadena de tiendas ha dicho que al parecer los hackers ingresaron en un principio a su extensa red informática a través de uno de sus

proveedores. Una vez dentro, los malhechores se movieron por las redes de Target y al final instalaron software malicioso en el sistema de punto de venta de la empresa.

Los expertos creen que la serie de infiltraciones dio a los intrusos acceso a unos 40 millones de números de tarjetas de crédito y débito, además de información personal de otras 70 millones de personas.[26]

En el próximo capítulo se explorarán algunos posibles motivos para la falta de desarrollo de un CSIRT para este tipo de empresas.

CAPITULO III

3.1 DIFICULTADES PARA LA IMPLEMENTACIÓN DE UN CSIRT PYME

Como ya se explicó, las PyME presentan una serie de particularidades, entre las que cabe mencionar:

- Escasez de presupuesto: como su principal limitante a la hora de invertir.
- Infraestructura sub desarrollada: no cuentan con recursos suficientes para implementar mejores técnicas para sus procesos.
- Propiedad: son empresas independientes y su gestión comúnmente suele estar unida a una sola persona o familia. Esto particularmente, es un signo identificatorio del carácter informal de estos emprendimientos.
- Estructura interna: que suele nacer y mantenerse simple, con una escasa segmentación de funciones y organización.
- Posicionamiento: carecen de una posición dominante en el mercado.

El buen funcionamiento, e incluso la supervivencia de una PyME, dependen en gran medida de su adaptación al medio en el que desarrolla su actividad, es decir al mercado en el que busca operar y los cambios que atraviesa. La tendencia actual para todo emprendimiento de cualquier tipo es incorporar tecnologías para gestionar su información, por lo que, en estas empresas, inmersas en un entorno tecnológico en constante cambio y con niveles incrementales de dependencia hacia ellas, la ciberseguridad debería empezar a considerarse un tema de importancia para la supervivencia de la entidad.

Los sistemas de información facilitan todos los procesos de cualquier organización empresarial: comunicación interna, relación con los proveedores, logística, producción, marketing, atención al cliente, selección y formación de personal, internacionalización, innovación, etc. Las PyME que no han nacido digitales se ven obligadas a evolucionar, por sus clientes o por la competencia, motivadas por la necesidad de supervivencia.

Sin embargo, como se vio, existen escasas iniciativas a la fecha que permitan fortalecer la seguridad de la información en las PyME, siendo una posibilidad la creación de un CSIRT para estos emprendimientos en Ecuador o Argentina.

Esto lleva a plantear las hipótesis que siguen como posibles justificativos para la inexistencia a la fecha de un CSIRT PYME.

3.1.1 SUBESTIMACIÓN DE LAS PYME DE LA IMPORTANCIA DE SU INFORMACION

Uno de los problemas evidentes en nuestras sociedades es la falta de desarrollo de una cultura de seguridad de la información, lo cual no es una meta fácil de alcanzar ya que se requieren plazos amplios y acciones continuas.

Este proceso de construcción requiere que las personas y las organizaciones interioricen en sus quehaceres diarios una manera de trabajar que avale que es indispensable atender los aspectos vinculados a la seguridad de los datos y un uso responsable de los recursos informáticos. Sin embargo, la gran mayoría de las PyME parece ignorar la importancia de asegurar sus recursos de información.

> Según un reciente estudio de los consumidores realizado por Kaspersky Lab y B2B International, la falta de conocimiento en seguridad informática sigue siendo una realidad preocupante para las empresas de todo el mundo. La investigación descubrió que solo una décima parte (12%) de los empleados encuestados son plenamente conscientes de las políticas y normas de seguridad de TI establecidas en las organizaciones para las que trabajan. Esto, combinado con el hecho de

> que la mitad (49%) de los empleados considera que la protección contra las amenazas cibernéticas es unaresponsabilidad compartida, presenta desafíos adicionales cuando se trata de establecer el marco de ciberseguridad correcto. [27]

Muchas PyMe optan por asignar los escasos recursos con lo que cuentan a otras actividades y no a contar con medios elementales para estar protegido, como por ejemplo ser asesorados por personal dedicado exclusivamente a la seguridad de la información o capacitar a los empleados sobre buenas prácticas.

3.1.2 ESCASEZ DE RECURSOS

El ambiente de las PyME siempre va a estar condicionado por la falta de recursos financieros como una de sus debilidades más marcadas. Hay limitadas posibilidades de obtener capitales, aferrándose únicamente a sobrevivir de recursos propios o mediante créditos que luego hay que afrontar. Si para las grandes compañías es un reto destinar recursos fijos proteger su información, resulta mucho más complicado para una PyME destinar fondos para obtener un bien intangible, porque, de hecho, es más complejo medir y demostrar el beneficio que se obtiene por medidas que buscan prevenir daños antes que acontezcan o a mitigar riesgos antes de que se materialicen.

El problema es que, si bien se puede calcular el costo total de la inversión en seguridad de la información, los ingresos se suelen medir como el ahorro de costos ante un incidente que comprometa los datos y los recursos utilizados para procesarlos.

Hoy la información es en muchos casos, la materia prima de la organización. Tener información significa poder tomar decisiones con mayor seguridad y rapidez. Por tanto, asegurar que esta información esté disponible en todo momento, sólo para las personas autorizadas y además que sea fiable, es primario para la supervivencia y el progreso de cualquier entidad, incluyendo las PyME. Por lo tanto, también para este tipo de empresas, la seguridad de la información no debería considerarse un gasto, sino una inversión.

3.1.3 FALTA DE PERSONAL DE SEGURIDAD INFORMÁTICA CAPACITADO

Al no existir una oferta suficiente de personal capacitado en seguridad de la información que comprenda las ventajas de cumplir con buenas prácticas y sea consiente de los riesgos que conlleva estar conectado a internet, mucho menos se van a entender las funciones que tiene un equipo de respuesta a incidentes de seguridad informática y los beneficios que representa acceder a sus servicios. Las PyME por si solas no pueden darse el lujo de contar con esta clase de profesionales en sus nóminas, lo que muchas veces las lleva a asesorarse con gente sin preparación. Por otro lado, el limitado número de especialistas que existe, se siente atraído y es mayoritariamente absorbido por grandes empresas con áreas específicas, presupuestos e infraestructuras dedicadas exclusivamente al trabajo de salvaguardar la información. Estas empresas cuentan además con más recursos para solventar los salarios que demandan profesionales de este tipo.

3.1.4 FALTA DE CAMPAÑAS DE CONCIENTIZACIÓN SOBRE SEGURIDAD DE LA INFORMACIÓN

Partir desde una escala macro, con el impulso y la sociabilización de campañas regionales, nacionales y locales de prevención de incidentes de seguridad informática por parte de organizaciones estatales o privadas, puede favorecer la desmitificación o la eliminación del enigma que muchas veces acompaña a la seguridad de la información, permitiendo de esta forma y de manera colateral, favorecer la creación de nuevos entes más especializados como un CSIRT PyME, dedicados a llevar adelante propuestas válidas para este objetivo en específico. A excepción de las noticias del día sobre el último incidente de seguridad informática que provocó pérdidas económicas o bloqueó las actividades de una o varias empresas en algún lugar del mundo y las recomendaciones de algún especialista sobre cómo prevenir ser víctima de esta amenaza, es muy

escueto o nulo el esfuerzo que se realiza para generar campañas de este tipo en Ecuador y en otros países de la región.

3.2 IMPORTANCIA DE LA GESTIÓN DE LOS INCIDENTES DE SEGURIDAD INFORMÁTICA EN LAS PYME A TRAVÉS DE UN CSIRT

Todo emprendimiento empresarial por muy pequeño que sea, debe tener entre sus objetivos la implementación de medidas que favorezcan la cultura y conocimiento en seguridad de la información. Además, se deben adoptar medidas que permitan saber qué hacer cuando se presenta un evento que comprometa su actividad.

La gestión de los incidentes informáticos es un aspecto necesario para lograr el mejoramiento continuo de una empresa pequeña o mediana que como se explicó, son también blanco de incidentes de seguridad. Sin embargo, una gran mayoría no lo realiza; principalmente por subestimar la importancia de la información que manejan y por la escasez de recursos.

> El ecosistema de pymes dispone, por lo general, de medios reducidos y no puede dedicar tiempo y esfuerzos a esta tarea. Se recomienda que cuenten con la figura de responsable de seguridad de información (CISO, por sus siglas en inglés) pero una pyme no puede invertir en una figura así. No es necesaria una gran inversión para estar protegido. A veces, una auditoria pequeña les puede dar unos pasos a seguir y le pueden bastar. No todas las empresas tienen las mismas necesidades. [28]

En el mismo sentido, debería ser materia de preocupación para las grandes empresas (que tienen empresas más pequeñas como proveedores), para las entidades de gobierno (con competencias en materia de PyME) y de la comunidad en general, que existan iniciativas que integren a este sector en planes nacionales de prevención de incidentes informáticos.

Dado este escenario, sería entonces recomendable que un equipo de respuesta a incidentes de seguridad CSIRT especializado

pudiera tener un rol protagónico al momento de tratar de mejorar la seguridad de la información y servir como una guía en una comunidad PyME.

Al centrar la prevención, la gestión y la respuesta a ataques masivos o dirigidos y la concientización en un único ente técnico, las PyME tendrían una nueva arma que esgrimir para mejorar su gestión y la calidad de sus productos y servicios. Con relación al problema de la escasez de fondos, el capítulo 4 de este trabajo de especialización presenta varias propuestas para el financiamiento de un CSIRT PyME, permitiendo a las PyME disponer de estos servicios a un costo razonable.

Es una utopía pensar que, desde una única organización, y mucho menos, desde una PyME, se podrán soslayar todas las amenazas posibles. En consecuencia, la razón de la materialización de un CSIRT PyME se fundamenta primordialmente, en que sería una entidad enfocada en conocer la realidad de estos emprendimientos, que comprende las limitantes de este sector empresarial pero que se encuentra preparada para desarrollar un conjunto de medidas preventivas y correctivas convenientes a cada circunstancia, y que tratará de orientar a las PyME para mitigar los posibles efectos negativos de las amenazas.

En el próximo capítulo se presenta una propuesta de desarrollo de un CSIRT para PyME.

CAPITULO IV

4.1 CSIRT PARA PYME

Como ya se expresó en capítulos anteriores, las características de las empresas que conforman el sector PyME muestran que es prácticamente imposible que las organizaciones clasificadas en este segmento puedan implementar de forma individual las funciones de un CSIRT. Surge, por tanto, la necesidad de asociar esfuerzos y tratar de ofrecer los servicios de un único CSIRT a varias PyME.

El presente trabajo se focalizará en la implementación de un CSIRT para empresas PyME en Ecuador, que se constituya en un eslabón más en la cadena de protección orientada expresamente a las organizaciones de este segmento. Se formaría como una entidad especializada en relevar las necesidades de empresas pequeñas y medianas con presupuestos limitados, para poder desplegar mayor cobertura de seguridad de su información y ofrecer respuestas acordes con esta demanda.

4.2 FUNDAMENTACIÓN DE UN CSIRT PYME

Se presenta a continuación un cuadro que muestra los beneficios y los riesgos asociados al desarrollo de un CSIRT PyME, como una herramienta para dilucidar oportunidades y debilidades del proyecto, a partir de las necesidades de la comunidad objetivo a atender.

Beneficios y riesgos en el desarrollo de un CSIRT	
Beneficios	▪ Proveer a las PyME de personal técnico especializado, certificado y entrenado que estas empresas no pueden cubrir dentro de sus limitadas nóminas de personal. ▪ Brindar a las organizaciones del sector capacidades y herramientas para responder en forma adecuada a la ocurrencia de incidentes de seguridad informática que afecten real o potencialmente sus servicios. ▪ Respaldar a la comunidad empresarial PyME que representa la mayor fuerza laboral en el país, fortaleciendo este sector empresarial. ▪ Disminuir las pérdidas económicas por incidentes informáticos y ataques en las PyME.
Riesgos	▪ Falta de experiencia en la atención a un sector muy limitado de recursos. ▪ Demanda limitada de los servicios y escaso apoyo a su desarrollo, por la falta de prioridad que dan las PyME a la protección de su información. ▪ Escasez de personal especializado que pueda ser parte del Csirt PyME. ▪ Soporte financiero limitado de las PyME.

Cuadro N° 3 Beneficios y riesgos en el desarrollo de un Csirt PyME

4.3 ORGANIZACIÓN PATROCINADORA

Para la creación del CSIRT PyME, se hace pertinente contar con el respaldo de una entidad especializada y conocida que sea referente en este sector.

> El CSIRT PyME no nace espontáneamente, sino que está promovido por una organización, pública o privada, que ha detectado la necesidad de proveer a una determinada comunidad de la capacidad de respuesta ante incidentes de seguridad informática. Esta organización es la que se denomina Organización patrocinadora. [29]

Se pretende entonces proponer la iniciativa de creación del CSIRT PyME a la Cámara de la Pequeña y Mediana Empresa (https://www.capeipi.org.ec/), agrupación constituida por los sectores productivos de las PyME del Ecuador, en cuanto a la representación gremial y prestación de servicios empresariales a sus socios.

CAPEIPI es un ente acreditado por las PyME, que podría brindar información sobre sus afiliados para que en lo posterior se pueda poner a disposición de estos últimos los servicios que el CSIRT PyME ofrezca. En retribución, CAPEIPI podrá ser reconocida como una entidad que refuerza su valor social mostrando preocupación por la protección de la información de las entidades que agrupa, así como apoyo a actividades y desarrollo de servicios innovadores de calidad, adecuado a las necesidades del sector.

4.4 AREA DE INFLUENCIA

Se propone un CISRT con alcance local, que abarque el universo de las PyME de la ciudad de Quito, Ecuador. Brindará apoyo para la prevención y rápida detección, identificación, manejo y recuperación frente a incidentes, buscando identificar las amenazas a la seguridad de información de las entidades que integran este segmento del mercado en la mencionada localización geográfica.

A su vez, estará abierto a brindar eventualmente apoyo técnico y proporcionará información especializada a otros CSIRT, a las fuerzas de la ley y a la sociedad en general sobre temas relacionados con incidentes informáticos, siempre con la mayor responsabilidad y control en el manejo que este tipo de información requiere, respetando la privacidad de los datos.

4.5 POSIBLES FUENTES DE FINANCIAMIENTO

Existen varias formas posibles de financiamiento para el CSIRT PyME, a saber:

- Mediante el pago de un canon por parte de las PyMES que integran la comunidad a atender.
- A través de subvenciones del Estado.
- Mediante los aportes de grandes empresas, cuyas cadenas de suministro están integradas por las PyME a atender o de organizaciones no gubernamentales sin fines de lucro, que pudieran estar interesadas en el fortalecimiento de la seguridad en el sector.
- Mediante la oferta de parte de sus servicios a la sociedad en general, a empresas de todo tipo o a organismos públicos, que se encuentren en mejores condiciones que las PyME para afrontar el pago.

Se puede contemplar la opción del financiamiento a través de un modelo mixto, con participación conjunta de varias de las fuentes mencionadas, lo que permitirá dar mayor estabilidad al inicio de las operaciones del CSIRT PyME y el sostenimiento en el tiempo de los servicios ofrecidos. En la medida que vaya creciendo la demanda de estos servicios y madurando sus procesos, podrá entonces buscar nuevas formas de financiamiento futuro que le permita extender sus actividades.

4.5.1 CANON DE LAS PROPIAS PYMES ATENDIDAS

El CSIRT PyME podría financiarse mediante el pago de un canon anual, semestral, trimestral o mensual de todas las empresas que constituyen la comunidad objetivo. La suscripción incluiría la prestación de servicios básicos proactivos como alertas y charlas de concientización, difusión de información relacionada con la seguridad y servicios reactivos, así como la respuesta a incidentes en las instalaciones de la entidad o vía remota, aplicables cuando se presente una emergencia informática.

Otros servicios no considerados en el canon básico, como auditorias o evaluaciones de la seguridad de la información, se podrían abonar adicionalmente.

Como ventajas para este tipo de financiamiento se podría citar su recaudación más sencilla, ya que el canon podría ser incluido en la cuota mensual del asociado de la PyME a la Cámara CAPEIPI.

4.5.2 SUBVENCIONES PÚBLICAS

Otra vía que merece la pena considerar es la de pedir una subvención al Estado, es decir que directamente un área del gobierno con competencias en el sector destine parte de su financiamiento a desarrollar las funciones de un CSIRT. Efectivamente, en la actualidad son muchos los países que disponen de fondos públicos para proyectos de seguridad de las TI. Esta posible fuente de financiamiento se justificaría por el hecho de que se estaría ofreciendo fomentar una actividad de utilidad pública.

4.5.3 SUBVENCIONES DE EMPRESAS PRIVADAS

Como ya se indicó, es común que empresas PyME sean proveedoras de empresas grandes. En consiguiente, podría ser de interés para estas últimas, que la gran inversión que realizan para obtener seguridad informática no se ponga en peligro por no poder controlar el posible vector de ataque que se generaría a través de una

PyME mal protegida en su tecnología, que accede, por ejemplo, a su intranet. Se contempla la posibilidad entonces de que las grandes empresas puedan interesarse en financiar la creación de un CSIRT para atender el segmento PyME.

Por otro lado, también existe la opción de poder presentar la creación del CSIRT PyME a alguna organización sin fines de lucro que se interese en el tema de la seguridad informática.

4.5.4 OFERTA DE SERVICIOS A OTRAS ENTIDADES NO PERTENECIENTES AL SECTOR

Una posible fuente de financiamiento podría provenir de la prestación de actividades especializadas, como cursos de capacitación en temas específicos o revisiones de seguridad y auditorías, a instituciones privadas o públicas que requieran ayuda para mejorar su seguridad informática.

Se podrán definir tablas de tarifas que especifiquen los servicios a brindar, con las condiciones pertinentes.

De este modo se aprovecharía el personal del CSIRT, con experiencia y conocimientos en ciberseguridad, para generar ingresos para sostener los servicios ofrecidos a las PyME.

4.6 SOCIABILIZACIÓN DE LOS SERVICIOS DEL CSIRT PYME EN SU COMUNIDAD OBJETIVO

Para poder hacerse de un lugar en un mercado reacio a contratar asistencia externa como el de las PyME, por ignorancia o por sus limitados recursos, el CSIRT debe labrarse una buena imagen, la que le servirá como herramienta para lograr protagonismo en ese ambiente y captar más interesados en su actividad.

En este proceso es importante que el CSIRT consolide su identidad, o sea identifique los servicios que brindará a través de su comportamiento y comunicación. Esto se constituirá en uno de los

pilares que dará soporte a su transformación en un punto de confianza de sus clientes, central a su imagen.

En consecuencia, es necesario que la comunidad a atender conozca la razón de ser del CSIRT PyME. Para ello, debe contar con personal calificado y estándares definidos y conocidos para atención de incidentes, a fin de responder eficientemente las solicitudes de soporte que se le requieran.

Por otro lado, es importante que las empresas PyME distingan el compromiso del CSIRT en la defensa de sus activos de información y en el manejo de situaciones comprometedoras.

Para difundir los servicios del CSIRT PyME, se plantea entonces realizar las siguientes actividades:

- Promoción en redes sociales.
- Charlas de concientización.
- Difusión de material preventivo.

Debe tenerse en cuenta que ganar la confianza de la comunidad objetivo es uno de los retos más complicados de superar, por lo que se necesitará mucho trabajo y sumar experiencia para cumplir con las expectativas de los clientes y lograr su fidelización.

4.7 DECLARACIÓN DE SERVICIOS DE CSIRT PYME

La declaración de servicios se constituye en una explicación sucinta de los servicios que ofrece a la comunidad atendida y que permite comunicar en forma estandarizada y con claridad la existencia y función del nuevo CSIRT.

A tal fin se propone el siguiente texto:

“El CSIRT PyME brinda información y asistencia a la comunidad PyME con el fin de proveer de planes proactivos destinados a reducir el riesgo de sufrir de incidentes de seguridad informática, así como ofrecer servicios reactivos para responder a tales incidentes cuando se produzcan.”

En una sección posterior se realiza una enumeración y explicación de los servicios provistos por el CSIRT PyME.

4.8 OBJETIVOS ESTRATÉGICOS

Los objetivos estratégicos son los fines o metas desarrollados a alto nivel, y que una organización pretende alcanzar a largo plazo.

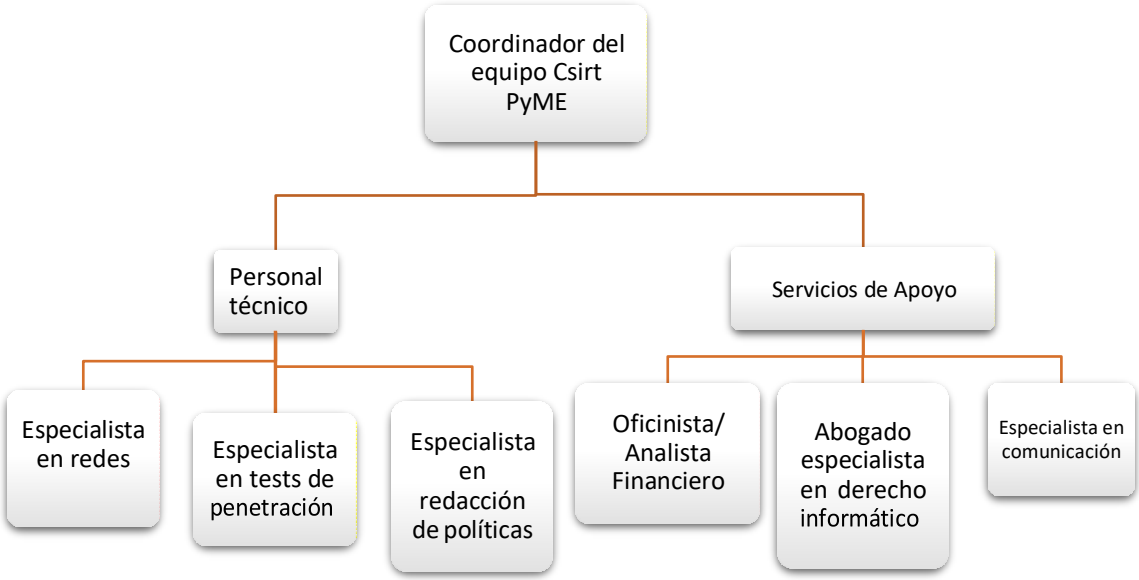
Para los objetivos estratégicos para el CSIRT PyME se proponen los siguientes:

- Ofrecer soporte para la mejora de la seguridad de la información en las PyME y crear conciencia en la comunidad objetivo.
- Afianzarse con un nombre propio, como base en la credibilidad de la propia comunidad objetivo.
- Lograr la excelencia operacional y ser un ente referente en su ámbito.
- Brindar una correcta y metodológica respuesta a incidentes que afecten la información.
- Ser una entidad autosustentable financieramente.

Sobre la base de estos objetivos estratégicos, el CSIRT PyME deberá desarrollar sus planes operativos y sus procesos.

4.9 DEFINICION DE ROLES EN EL CSIRT PYME

La conformación del CSIRT PyME debe involucrar inicialmente un responsable principal, de quien dependerán dos áreas destinadas a cubrir las funciones pertinentes de seguridad de la información y las actividades de soporte vinculadas. El siguiente cuadro muestra el organigrama propuesto y a continuación se detallan los roles.



Cuadro N° 4 Estructura CSIRT PyME

4.9.1 COORDINADOR DE EQUIPO DEL CSIRT PYME

El coordinador de equipo del CSIRT será responsable de las actividades del CSIRT PYME y de la supervisión de sus acciones. Su función principal será el planeamiento, coordinación, gestión y monitoreo de las tareas del CSIRT.

Dentro de las características técnicas deseables de un coordinador, se pueden mencionar las siguientes:

- Formación en tecnologías de información o en carreras afines.
- Conocimiento de sistemas operativos a nivel de usuario avanzado y a nivel administrador, redes, programación y normativa informática.
- Estar actualizado respecto a los avances tecnológicos y sus vulnerabilidades.
- Experiencia en técnicas de intrusión.
- Conocimiento de los diferentes tipos de ataques mediante códigos maliciosos.

- Conocimientos de legislación informática.
- Conocimiento de herramientas de seguridad como scanners, firewalls y sistemas de detección de intrusos.
- Conocimiento de criptografía o informática forense.
- Experiencia participando en procesos de auditoria de seguridad de información.
- 5 años de experiencia en posiciones similares o cargos relacionados con la actividad.
- Dominio de inglés técnico.

Como habilidades personales se requerirán las siguientes particularidades:

- Atención focalizada, que se mantenga por largos periodos de tiempo. Concentración.
- Capacidad de reflexión, análisis y de síntesis. Habilidad para pensar creativamente. Habilidad para la toma de decisiones.
- Habilidad para organizar información de corto y de largo plazo.
- Habilidad para expresarse. Habilidad para comunicarse con personas no expertas y expertas en el área.
- Habilidad para potenciar a subalternos. Habilidad para trabajar en equipos reales y virtuales. Capacidad de mando, liderazgo y motivación. [30]

Es importante destacar que tendrá la responsabilidad de actuar como enlace entre el CSIRT y los propietarios de las PyME y sus responsables informáticos, si los hubiera. También es el punto de contacto en materia de respuesta a incidentes para interactuar con entidades externas, como otros equipos de respuesta a incidentes

estatales o privados, nacionales o internacionales, tales como la Policía, los entes de control, etc.

4.9.2 PERSONAL TÉCNICO DEL CSIRT PYME

Será deseable que los expertos que se encargan de desarrollar la respuesta a incidentes de seguridad informática cumplan con los siguientes requerimientos técnicos:

- Formación en informática o en carreras afines.
- Conocimiento de la seguridad informática en profundidad.
- Experiencia en manejo de sistemas operativos y redes como operador y como administrador.
- Conocimiento de vulnerabilidades en sistemas y redes.
- Comprender la metodología de los diferentes tipos de ataques de código malicioso.
- Experticia en técnicas de intrusión.
- Capacidad de análisis de incidentes y su manejo.
- Comprensión del inglés técnico.

Como habilidades personales, se requerirá que maneje las siguientes destrezas:

- Flexibilidad, creatividad y espíritu de equipo.
- Capacidad de análisis.
- Habilidades de comunicación para interactuar con las PyME atendidas a fin de hablar de temas técnicos de una manera sencilla.
- Confidencialidad y capacidad de trabajo sistemático.
- Buenas aptitudes organizativas.
- Resistencia al estrés.
- Facilidad para escribir informes técnicos.

- Mente abierta y voluntad de aprender.
- Un año de experiencia en puestos similares o afines a la actividad requerida.

El CSIRT PyME debe contar con personal que domine la administración de redes, exámenes de penetración, redacción de políticas y legislación informática sobre delitos.

> Cada miembro del personal debe ser hábil para resolver problemas y eso regularmente se logra a través de la experiencia y la transferencia de conocimiento. No todos los miembros del personal deben ser expertos en cada tema, pero sí es conveniente que para cada área de las mencionadas haya al menos una persona con las habilidades suficientes para proporcionar apoyo en algún incidente crítico que involucre su área.
>
> Para el desarrollo de habilidades y conocimientos del personal, también puede acudirse al intercambio con expertos de otras entidades y promover la retroalimentación e intercambio de conocimientos con esas entidades [31]

Sería interesante entonces contar con personal versado en los aspectos claves del CSIRT PyME, que además puedan servir de guía a los menos preparados para que puedan ponerse a tono con todas las tareas

Dentro de los roles requeridos en el equipo técnico del CSIRT PyME se puede referir los siguientes especialistas:

- Especialista en redes: Analiza, prueba, identifica y resuelven problemas y evalúa sistemas de red existentes, tales como red de área local (LAN), red de área amplia (WAN), internet o un segmento de un sistema de red.

- Especialista en test de penetración: Realiza exámenes de penetración conocidos como “pentest”. Un examen de penetración consiste en simular una ofensiva a un sistema informático, una red o un sitio web, con la intención de encontrar debilidades que podrían comprometer su seguridad, su funcionalidad y datos.
- Especialista en redacción de políticas: Encargado del diseño, formulación y elaboración de documentos que reflejen planes estratégicos orientados a mejorar la seguridad de la información. Se encarga además de realizar actividades de sensibilización y evaluación como método de prevención y de redactar políticas y procedimientos de seguridad.

4.9.3 SERVICIOS DE APOYO

Adicionalmente al equipo del CSIRT principal, sería deseable que se contara con personal que brinde soporte a los roles principales. Entre ellos se puede citar personal administrativo, abogados, desarrolladores web, redactores técnicos, encargados de relaciones públicas son ejemplos de este tipo de roles. Estas actividades pueden ser subcontratadas o provistas externamente. Se destacan especialmente:

- Abogado especialista en derecho informático: Se trata de un especialista en leyes, que tendrá específica atención a legislación correspondiente a delitos informáticos y derechos de usuarios, tanto a nivel nacional como internacional.

- Oficinista/ analista financiero: Brinda asistencia en las actividades secretariales desarrolladas en la oficina y de control financiero del CSIRT PyME. Entre ellas se pueden citar la elaboración de presupuestos, recepción de reportes de incidentes de seguridad, chequeo, clasificación, distribución, y archivado de documentos, etc.
- Especialista en comunicación: Su intervención será valorada al momento de posicionar la imagen del CSIRT en el mercado y posteriormente, para difundir los resultados de las intervenciones del CSIRT PyME.

4.10 CATÁLOGO DE SERVICIOS DE UN CSIRT PYME

A continuación, se listan los servicios que más atañen a la realidad y al ámbito de las PyME.

Servicios reactivos	Servicios proactivos	Servicios de gestión de calidad de la seguridad de la información
• Tratamiento y análisis de incidentes. • Respuesta a incidentes in situ o remotamente. • Identificación de vulnerabilidades.	• Alertas y advertencias. • Comunicados. • Evaluación / auditorías de seguridad	• Continuidad del negocio y recuperación tras un desastre • Consultoría de seguridad. • Educación y formación.

Cuadro N° 5 Resumen de los servicios de un Csirt PyME

4.10.1 SERVICIOS REACTIVOS

Son aquellos que constituyen el punto neural de la actividad de un CSIRT y se llevan a cabo ante la ocurrencia de un evento de seguridad.

Un ejemplo común que se utiliza para entender el rol de un CSIRT en este aspecto, es el que tiene que ver con su comparación con un cuerpo de bomberos cuando este responde a una emergencia por un incendio. La labor del CSIRT PyME será equivalente en el ámbito informático, tratando de responder y gestionar el incidente informático y luego investigar las razones por las que se produjo, a fin de evitar que se repita.

. A continuación, se proponen una serie de servicios reactivos que serían más adecuados para la comunidad PyME.

4.10.1.1 TRATAMIENTO Y ANALISIS DE INCIDENTES

Recibir y analizar posibles eventos de seguridad son las tareas que corresponden a este servicio. Se contemplan actividades como buscar intrusos y filtrar tráfico de red para identificar qué ocurrió y por qué.

Será necesario examinar todas las pruebas que rodearon al incidente, a través de técnicas como las que ofrece la informática forense destinadas a garantizar que la evidencia obtenida sea fiable y proba.

Como labor adicional se podría requerir el rastreo o seguimiento de las acciones del intruso, reconociendo la metodología que siguió para poder acceder sin autorización a la red, sistema vulnerado o a cualquier otro tipo de ataque, si bien corresponde a los cuerpos judiciales y policiales perseguir al potencial ciberdelincuente.

4.10.1.2 RESPUESTA A INCIDENTES IN SITU O REMOTAMENTE

El CSIRT PyME podrá prestar asistencia en el domicilio del afectado, a fin de poder brindar soporte de primera mano al cliente atendido, permitiendo que pueda recuperarse del incidente. En el mismo sentido, se brinda la posibilidad de asistir a los perjudicados mediante vías de comunicación alternativas basadas en conexiones seguras a través de programas que permiten la comunicación remota. La asistencia remota o soporte remoto tiene la ventaja de la inmediatez y de no comprometer recursos del CSIRT por temas de traslado.

4.10.1.3 IDENTIFICACIÓN DE VULNERABILIDADES

Esta actividad engloba las tareas que deriven en averiguar mediante estudios técnicos, los puntos débiles del hardware y software afectado y cómo pudieron ser explotados por los atacantes. Una vez hecho el diagnóstico, se establecerá la solución más rápida y eficiente que permita subsanar el vacío en la defensa del sistema o equipo informático y restablecer la operatividad de los servicios afectados. Luego se procederá a notificar a terceros, entre los que se encuentran la comunidad PyME, proveedores, otros CSIRT y organismos competentes como la Policía o la Justicia.

4.10.2 SERVICIOS PROACTIVOS

En esta categoría se engloban cada una de las actividades que buscan prevenir incidentes y fortalecer la seguridad en la comunidad objetivo, fortaleciendo sus activos de información. Son buenas prácticas que buscarán reducir el número de incidentes en el futuro.

4.10.2.1 ALERTAS Y ADVERTENCIAS

Este servicio incluye la difusión de información a toda la comunidad atendida por el CSIRT PyME, que explica el ataque o alerta sobre un tipo de incidente o vulnerabilidad y da aviso sobre cualquier

amenaza específica. Además, brinda recomendaciones para prevenir el incidente y fortalecer los posibles dispositivos afectados.

El aviso se brinda con el afán de que toda la comunidad pueda poner sus sistemas e información a buen recaudo. Se pueden originar en el mismo CSIRT PyME o tratarse de alertas brindadas por otras fuentes como, por ejemplo:

- Otros CSIRT privados, públicos, nacionales o internacionales.
- Empresas del sector.
- Medios de prensa en general.
- Organismos de investigación.
- Entidades académicas.
- Sitios web dedicados a seguridad informática.

La información será sociabilizada a través de grupos de listas de correo y las redes sociales más comunes para tratar de lograr el mayor el impacto en la trasmisión, considerando que la posible amenaza y sus efectos se puede propagar en tiempos relativamente cortos.

4.10.2.2 COMUNICADOS

Son documentos informativos como afiches, folletos, boletines, sitios web u otros recursos informativos que serán redactados en un lenguaje amigable y entendible a personas con quizás escasos conocimientos de informática.

Estos informes, que pueden ser propios o de terceros, facilitarán a la PyME atendida mecanismos para hacer contacto con el CSIRT.

4.10.2.3 EVALUACIÓN/ AUDITORIA DE SEGURIDAD

Un CSIRT PyME también puede brindar este tipo de servicio, que busca revisar el estado de la seguridad, si se han establecido

mecanismos preventivos y correctivos y si estos han sido adecuadamente implementados y funcionan de la manera esperada.

Las auditorias deben llevarse a cabo en base a las mejores prácticas para proteger los activos de información y pueden incluir escaneos que permitan detectar vulnerabilidades provocadas por malware y pruebas de penetración a los sistemas que manejan las PyME.

Las tareas que se podrían ejecutar en este servicio serían las siguientes:

- Revisión de la infraestructura: Para certificar las políticas, mejores prácticas y las configuraciones estándar, revisando el hardware, software, redes, enrutadores, firewall, servidores, etc. y generando recomendaciones para la correcta instalación y configuración de los recursos relacionados con la infraestructura tecnológica.
- Revisión de las mejores prácticas: Con el objeto de determinar si las prácticas de seguridad (si las hay) se adaptan a las políticas establecidas y definidas por la organización y brindar recomendaciones.
- Escaneo de vulnerabilidades: Uso de detectores de vulnerabilidades o malware para determinar qué sistemas y redes son vulnerables, además del monitoreo, detección y prevención de posibles intrusos.
- Test de penetración: Como ya se explicó, busca comprobar la seguridad de la información de una entidad a través de un ataque deliberado y autorizado a sus sistemas y redes.

4.10.3 GESTION DE LA CALIDAD DE LA SEGURIDAD DE LA INFORMACION

En esta categoría se encuentran aquellos servicios generalmente no técnicos, que son preventivos en su naturaleza. Surgen de la retroalimentación obtenida por el tratamiento de

incidentes, tomando en cuenta la información recopilada a través del contacto con los miembros y de otros actores y las lecciones aprendidas.

4.10.3.1 EDUCACION Y ENTRENAMIENTO

El CSIRT PyME podrá brindar este servicio a fin de procurar mayor sensibilización a su comunidad atendida sobre la criticidad de mantener una actitud responsable de protección de la información. Las amenazas y ataques informáticos van cambiando con el tiempo, por lo que es necesario que la educación sobre seguridad informática se arraigue en el pensamiento de todos integrantes de las PyME. Herramientas como los seminarios, charlas, talleres, cursos y tutoriales accesibles para todos los involucrados deben ser considerados instrumentos valiosos que permitan diseminar las buenas prácticas y metodologías que contribuirán a mitigar riesgos, protegiendo así a la información frente a incidentes que puedan afectarla.

Como parte del entrenamiento y sensibilización que el CSIRT PYME recomienda, un posible punto de partida sería brindar a toda la comunidad PyME a manera de introducción a la seguridad informática, un modelo de Política de Seguridad Informática para una Pequeña o Mediana Empresa, que se incluye como ANEXO B de este trabajo de investigación, orientada a cualquier usuario de activos de información que esté interesado en aprender a protegerlos.

4.10.3.2 CONTINUIDAD DEL NEGOCIO Y RECUPERACION TRAS UN ATAQUE

Debido a la multiplicación de incidentes que comprometen la seguridad informática con consecuencias desastrosas para las víctimas, el CSIRT PyME brindará pautas que permitan respaldar y recuperar información crítica y los sistemas que la manejan, con el

propósito de poder continuar su actividad cotidiana luego de eventos relacionados con ataques o fallas masivas.

4.10.3.3 CONSULTORÍA DE SEGURIDAD

El CSIRT PyME brindará recomendaciones a su comunidad objetivo respecto a las mejores prestaciones y controles más efectivos de seguridad de la información, de todo lo relacionado a la protección de la información y su manejo seguro, desde la adquisición de nuevas plataformas de hardware y software hasta su instalación, configuración y prueba.

4.11 RESUMEN DE OFERTA DE SERVICIOS CSIRT PYME

Todas las PyME que estén interesadas en contar con uno o varios de los servicios del CSIRT deberán estar matriculadas por medio de una membresía que será renovada anualmente, en la que se le solicitará la registración de todos sus datos y medios de contacto, incluyendo la nominación de una o varias personas como enlaces. A partir de esta membresía, se habilita a la PyME a acceder a los servicios descriptos previamente.

En una etapa inicial e incluida en la cuota, se tiene prevista la provisión de un abanico básico de prestaciones, además de otros servicios con costo adicional, sujetos a disponibilidad del CSIRT PyME. A medida que el modelo de negocio del CSIRT avance, y una vez se haya establecido el CSIRT PyME como marca, se contempla brindar otros beneficios que serán tarifados de acuerdo a su complejidad.

A continuación, se resumen los servicios considerados en la etapa inicial:

SERVICIOS PROACTIVOS	PERIODICIDAD/TARIFA
Alertas y advertencias	Permanente
Comunicados	Permanente
Evaluación/Auditoría de Seguridad	A demanda, servicio tarifado, sujeto a análisis y a disponibilidad de recursos

Cuadro N° 6 Cartilla de servicios proactivos

SERVICIOS REACTIVOS	PERIODICIDAD/TARIFA
Tratamiento y análisis de incidentes	Permanente, previo análisis y sujeto a disponibilidad de recursos. Requerimiento adicional será tarifado.
Respuesta a incidentes in situ o remotamente	Respuesta remota permanente. Respuesta in situ 1 vez al año, previo análisis y sujeto a disponibilidad de recursos. Requerimiento adicional será tarifado.
Identificación de vulnerabilidades	1 vez al año, previo análisis y sujeto a disponibilidad de recursos. Requerimiento adicional será tarifado.

Cuadro N° 7 Cartilla de servicios reactivos

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	PERIODICIDAD/TARIFA
Continuidad del negocio y recuperación tras un desastre	Servicio tarifado, previo análisis y sujeto a disponibilidad de recursos.
Consultoría de seguridad	1 vez al año, previo análisis y sujeto a disponibilidad de recursos. Requerimiento adicional será tarifado.
Educación y entrenamiento	1 vez al año se brindarán charlas preventivas. Sujeto a condiciones. Requerimientos adicionales serán tarifados.

Cuadro N° 8 Cartilla de servicios de Gestión de la Seguridad de la Información

4.12 NOTIFICACIÓN DE INCIDENTES AL CSIRT PYME

Para realizar el reporte de incidentes se deberán utilizar los canales de comunicación definidos por el CSIRT PyME, para su posterior registro de casos en una base de datos de gestión de incidentes que contendrá:

- Identidad del informante.
- Fecha y hora de la comunicación y medio utilizado.
- Miembro de la comunidad PyME que notifica.
- Sistemas/Información afectada.
- Descripción de la situación notificada.
- Calificación del incidente (Grave, media, leve, o categorización similar)
- Seguimiento del caso y medidas adoptadas
- Cierre del caso

4.13 POLITICAS DEL CSIRT PYME

Es necesario que un CSIRT PyME cuente con políticas internas relativas a sus propios servicios, como un elemento imprescindible para organizar los procesos y mostrar transparencia interna y hacia la comunidad y terceros involucrados.

Estas políticas constituirán una guía de las actividades que están permitidas y aquellas que se prohíben, creando un marco normativo que determine la postura del CSIRT PyME hacia la protección de los activos propios y de la información relativa a los datos de los incidentes ocurridos en la comunidad objetivo.

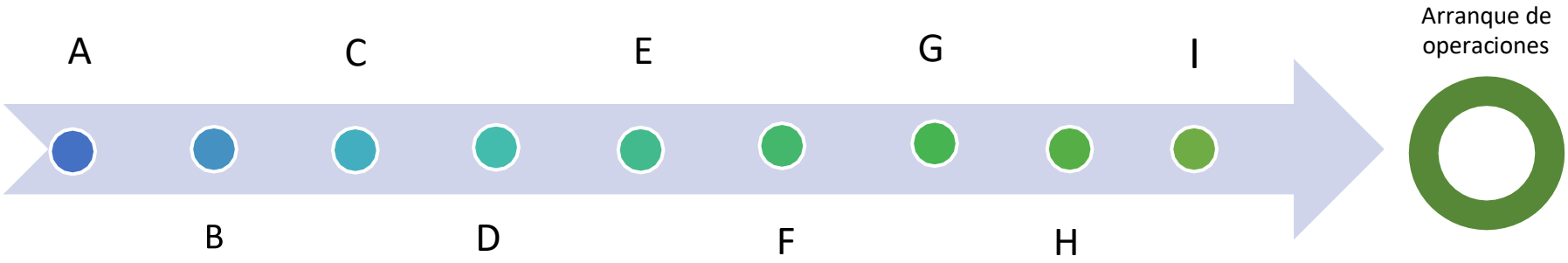
El siguiente cuadro muestra algunas de las políticas que el CSIRT PyME deberá desarrollar, vinculándolos a los servicios expuestos en la sección anterior.

Servicios y políticas de un Csirt PyME		
Tipo de Servicio	Servicio	Política
Servicios reactivos	Tratamiento y análisis de incidentes Respuesta a incidentes in-situ o remotamente	Política de tratamiento y respuesta a incidentes, incluyendo aspectos de confidencialidad
	Identificación de vulnerabilidades	Política de gestión de vulnerabilidades
Servicios proactivos	Alertas y advertencias	Política de notificación de incidentes
	Comunicados	Política de comunicación
	Evaluación/Auditorías de Seguridad	Política de revisión del estado general de la seguridad en PyMEs
Servicios de gestión de calidad de la seguridad de la información	Continuidad del negocio y recuperación tras un desastre	Política de resiliencia
	Consultoría de seguridad	Política de vinculación con miembros de la comunidad atendida para la provisión de servicios de consultoría
	Educación y formación	Política de entrenamiento y capacitación

Cuadro N° 9 Políticas de los servicios de un Csirt PyME

4.14 ACTIVIDADES PARA LA EJECUCIÓN Y PUESTA EN MARCHA DEL CSIRT PYME

Las actividades a desarrollar para la etapa de arranque del CSIRT PyME serán las siguientes (revisar ANEXO A para detalles de tiempos de ejecución). Se considera la posibilidad de poder desarrollar varias de estas actividades en paralelo, y de acuerdo a disponibilidad de recurso humano,



Cuadro N° 10 Etapas de la ejecución y puesta en marcha del Csirt PyME

- A: Conseguir habilitación para la creación del Csirt PyME
- B: Conseguir instalaciones para oficinas
- C: Contratar recursos humanos
- D: Capacitación de recursos humanos
- E: Adquisición de infraestructura de tecnología
- F: Implementación de infraestructura de tecnología
- G: Definición de políticas, procesos y procedimientos
- H: Definición de plan de comunicación
- I: Ejecución de plan de comunicación y difusión

4.15 INDICADORES CSIRT PYME

A continuación, se presenta un resumen con indicadores o métricas orientados a medir el desempeño del CSIRT PyME. Estos indicadores constituyen una herramienta que permitirá conocer su evolución en el tiempo y estudiar tendencias respecto a la relevancia de sus servicios, como instrumento de valoración en los procesos de evaluación y de toma de decisiones.

PERSPECTIVA	OBJETIVOS ESTRATÉGICOS	INDICADOR	METAS		UNIVERSO
			AÑO 1	AÑO 2	
Seguridad de la Información	Dar soporte a la comunidad PyME objetivo para mejorar los niveles de seguridad de la información	Cantidad de PyME cubiertas	90	120	1100[2]
		Número mínimo incidentes tratados	20	30	Total de incidentes atendidos por año
		Porcentaje de usuarios que declararon satisfacción	60%	70%	Total de usuarios encuestados
Económica	Transformarse en una entidad económicamente sustentable	Erogaciones vs. Punto de Equilibrio (P.E.)	Erogaciones <= P.E.	Erogaciones <= P.E.	Total de erogaciones
Aprendizaje interno	Mejorar la atención brindada	Tiempo promedio de demora en la asistencia a usuarios en días hábiles de semana.	3 horas	2 horas	Total de incidentes reportados
	Incrementar especialistas en el CSIRT PyME	Cantidad de especialistas	6	8	Total de personal dependiente del CSIRT PyME

Cuadro N° 11 Indicadores del CSIRT PYME

[2] Número de empresas PyME asociadas a la Cámara de la Pequeña y Mediana Empresa de Pichincha, CAPEIPE

4.16 PRESUPUESTO PRELIMINAR DE INVERSIÓN PARA EL CSIRT PYME

A continuación, se muestra un detalle del posible presupuesto para el mercado ecuatoriano y de acuerdo a valores de ese país, a ser considerado para la puesta en marcha del CSIRT PyME.

Elemento	Unidades	Frecuencia Anual	Costo Unitario/Mensual	Total (en dólares)
Presupuesto de Inversión Inicial				
Inversión en Tecnología				
Hardware	1	1	5000,00	5000,00
Software	1	1	5000,00	5000,00
Desarrollo web	1	1	500,00	500,00
Total inversión en tecnología				10500,00
Bienes muebles	1	1	3000,00	3000,00
Total Presupuesto de Inversión Inicial				**13500,00**
Presupuesto de funcionamiento				
Salarios				
Coordinador del equipo CSIRT PyME	1	12	1000,00	12000,00
Especialista en redes	1	48[3]	200,00	9600,00
Especialista en test de penetración	1	48	200,00	9600,00
Especialista en redacción de políticas	1	12	200	2400,00
Oficinista/ Analista Financiero	1	12	500	6000,00
Abogado especialista en derecho informático	1	6	300	1800,00
Especialista en comunicación	1	2	500	1000
Total costo de salarios				42400,00

Cuadro N° 12 Presupuesto de Inversión para CSIRT PyME

[3] Especialista en redes, comunicación, test de penetración y abogado reciben pago correspondiente por cada evento atendido.

Elemento	Unidades	Frecuencia Anual	Costo Unitario/Mensual	Total* (*en dólares)
Operación				
Logística para talleres de capacitación	1	4	200,00	800,00
Impresión de material informativo (folletería, posters, tarjetas, etc.)	1	1	1000,00	1000,00
Total costos operativos				1800,00
Total presupuesto de funcionamiento para el primer año				**44200,00**
Presupuesto de Ventas				
Presupuesto de ventas para asociados y no asociados al Csirt PyME, incluyendo traslados, viáticos, etc.				
Respuesta a incidentes in situ o remotamente	1	24	200,00	4800,00
Evaluación/Auditorias de Seguridad	1	24	150,00	3600,00
Educación y entrenamiento	1	30	200,00	6000,00
Total presupuesto de ventas para el primer año				**14400,00**

Cuadro N° 12 Presupuesto de Inversión para CSIRT PyME

CONCLUSIONES

Como principales conclusiones del presente trabajo final de maestría, es posible afirmar lo siguiente:

- Los equipos de respuesta a incidentes de seguridad o CSIRT son estructuras concebidas para proteger a las organizaciones frente a las amenazas que puedan afectar la confiabilidad, disponibilidad e integridad de su información. Sin embargo, por su envergadura y naturaleza, no es viable para una PyME implementar un equipo de respuesta a incidentes dentro de la propia organización. Por lo tanto, aparece la posibilidad de crear un CSIRT que atienda a las entidades que conforman el sector PyME, respondiendo a las características, necesidades y requerimientos propios de este tipo de empresas.
- Escasos recursos económicos marcan el desenvolvimiento de las empresas PyME, por lo tanto, tienen serias dificultades para acceder a personal especializado en seguridad de la información y/o a servicios externos que les brinden un asesoramiento adecuado. Frente a problemas de seguridad que atentan contra sus datos, suelen buscar a terceros que ofrecen servicios de soporte informático, que no suelen tener conocimientos sobre cómo proteger su información y los recursos utilizados para gestionarla. Esto plantea para las PyME un gran problema que debe ser tratado, ya que desarrollar su actividad sin ninguna protección significa que fácilmente se deja la puerta abierta a la potencial concreción de ataques o fallas que podrían haberse evitado, lo que posteriormente podría traducirse en pérdidas económicas y daños en su reputación e imagen e inclusive, su propia supervivencia. Esto se ve agravado por el hecho de que muchas PyME forman parte de

encadenamientos productivos que incluyen relaciones con empresas más grandes, que también podrían verse afectadas si las primeras son atacadas.

- En Ecuador no existe ningún tipo de actividad pública o privada que atienda cuestiones vinculadas a la seguridad de la información de las PyME, y mucho menos un centro especializado que se encargue de brindar recomendaciones y de asistencia sobre cómo proteger sus activos de información frente a las amenazas cibernéticas que podrían afectarlos. Esta es una realidad que afecta a muchos países de la región y del mundo.
- Uno de los principales escollos para el impulso de la creación del CSIRT PyME es conseguir el financiamiento, por el escaso poder adquisitivo de estas entidades y la baja conciencia de la importancia de la seguridad que existe en el sector.
- La creación, implementación y puesta en marcha del CSIRT PyME requerirá una cuidadosa planificación, además de la correspondiente disponibilidad de los recursos necesarios para llevar adelante la prestación de sus servicios, todo esto con el fin de cumplir con la dura pero fundamental labor, de cambiar la mentalidad de un sector empresarial muy marcado por la informalidad y el sentido familiar del negocio, para el que la seguridad de la información es un tema que dista de encontrarse en agenda.

En este trabajo de maestría se ha buscado establecer las cuestiones básicas a impulsar para la constitución de un equipo de respuesta a incidentes informáticos para el sector PyME, incluyendo una propuesta de alternativas para generar los recursos y los servicios más adecuados que se podrían prestar de acuerdo a las necesidades de dicho sector.

Las PyME constituyen un variado pero importante mercado en la mayoría de los países, por su papel preponderante en el desarrollo de las economías locales y regionales y su capacidad de empleo para amplios sectores de la población. Como muchos otros sectores, a lo largo estos últimos años, la mayoría de las entidades que lo conforman han ido incorporando herramientas tecnológicas para el desarrollo de su actividad. Por lo tanto, este sector requiere una urgente atención de los aspectos vinculados a la seguridad de la información, protegiendo de este modo no solo a las PyME sino a sus clientes, empleados y a otras empresas de mayor tamaño, a quienes proveen servicios. El desarrollo de un CSIRT PyME podría ser un valioso aporte para el logro de un sector más protegido, aportando de este modo valor a la economía de un país como Ecuador.

RECOMENDACIONES

Como complemento a lo desarrollado en el presente trabajo de maestría, se exponen a continuación las siguientes recomendaciones:

- Sensibilizar a los entes gubernamentales y privados del Ecuador con competencias en el sector PyME o capacidad de incidir en la problemática de seguridad de la información, sobre la necesidad de generar acciones inmediatas para la creación de estructuras organizativas de coordinación y respuesta a incidentes destinadas al mercado de dicho sector.
- Exponer en la comunidad de la pequeña y la mediana empresa las ventajas que el CSIRT PyME puede brindar para cumplir con sus objetivos, y hacer notar la importancia que conlleva la creación de un equipo especializado presto a brindar asistencia con conocimientos, experiencia y un conjunto de acciones para una mejor respuesta frente a incidentes de seguridad informática.
- Proponer una política local que impulse, en los niveles académico y ciudadano, programas de capacitación; con el fin de instruir a todos los actores sobre los riesgos y las consecuencias generadas frente a incidentes de seguridad reales o potenciales.
- Será clave también la prestancia y la habilidad del personal del CSIRT PyME para lidiar con la dificultad de interactuar con usuarios de la comunidad objetivo que no cuentan con conocimientos de informática. Comprender su preocupación y saber cómo prepararlos para la adopción de medidas de protección frente a la inevitabilidad de la falla y de la ocurrencia de incidentes informáticos, será crucial para abordar la situación.

- En el caso de que la asignación presupuestaria lo limite; planificar un CSIRT PyME con personal con asignación de tiempo parcial en una etapa inicial, contemplando también un esquema de asesorías o consultorías bajo demanda como alternativa para abaratar costos y habilitar un desarrollo paulatino pero constante hacia el establecimiento de un Equipo de Gestión de Incidentes estable y eficiente para las necesidades del sector.

ANEXOS

ANEXO A

A.1 CRONOGRAMA DE EJECUCIÓN Y PUESTA EN MARCHA DEL CSIRT PYME

	Actividad	Duración	Inicio	Fin	Actividad previa
1	Conseguir permisos para la creación del Csirt PyME	60 días	2-01-2019	1-03-2019	
2	Conseguir instalaciones para las oficinas	20 días	2-03-2019	22-03-2019	1
3	Contratar recursos humanos	40 días	1-04-2019	10-05-2019	2
4	Capacitación de recursos humanos	60 días	15-05-2019	15-06-2019	3
5	Adquirir estructura de tecnología	40 días	16-06-2019	31-07-2019	4
6	Implementación de la infraestructura de tecnología	15 días	01-08-2019	16-08-2019	5
7	Definición de políticas, procesos y procedimientos	20 días	16-06-2019	5-07-2019	3
8	Definición de plan de comunicación	15 días	01-0-2019	15-08-2019	4
9	Ejecución de plan de comunicación y difusión	15 días	2-03-2019	17-03-2019	1
10	Arranque de operaciones	0 días	17-08-2019		6-7-9

ANEXO B

B.1 MODELO DE POLÍTICA DE SEGURIDAD INFORMÁTICA PARA UNA PEQUEÑA O MEDIANA EMPRESA

En este apartado se definen una serie de pautas que, a manera de modelo, deben verse reflejadas en una Política de Seguridad Informática (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. 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.

- 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.

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.

- 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.

- 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.

- 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.

- 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.

- 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.
- PRESCRIPCIONES 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.

- 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.

- 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.
- 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.

- 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.

- <u>PRESCRIPCIONES PARA EL CONTROL DE ACCESO A RED</u>

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.

- 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.

ANEXO C

C.1 DESCRIPCIÓN DE LOS SERVICIOS DEL CSIRT-PYME, DE ACUERDO A LA NORMA REQUEST FOR COMMENTS (RFC) 2350

1. Información del Documento
   1.1 Fecha de la última actualización
   1.2 Ubicación del Documento
2. Información de Contacto
   2.1 Nombre del Equipo
   2.2 Dirección
   2.3 Zona Horaria
   2.4 Número de Teléfono
   2.5 Dirección de Correo Electrónico
   2.6 Miembros del Equipo
   2.7 Más Información
   2.8 Horario de Atención
   2.9 Puntos de contacto para clientes
3. Constitución
   3.1. Misión
   3.2. Comunidad a la que brinda servicios
   3.3. Patrocinio / Afiliación
4. Políticas
   4.1 Políticas ofrecidas por el CSIRT PyME
5. Servicios
   5.1 Servicios reactivos
   5.2 Servicios proactivos

5.3 Servicios de gestión de la seguridad de la información

6. Formas de notificación de incidentes

7. Disclaimer

1. Información del Documento

1.1 Fecha de la última actualización: 01 de octubre de 2018

1.2 Ubicación del Documento: La versión actual del documento está disponible en el sitio web del CSIRT PYME http://csirt.capeipi.org.ec/rfc2350

2. Información de Contacto

2.1. Nombre del Equipo: CSIRT PYME, Equipo de Respuesta a Incidentes de Seguridad Informática de la Cámara de la Pequeña y Mediana Empresa de Pichincha

2.2. Dirección

Cámara de la Pequeña y Mediana Empresa de Pichincha, CSIRT PYME

Av. Amazonas N34-332 y Atahualpa, Quito-Ecuador

2.3. Zona Horaria: UTC-GMT -5

2.4. Número de Teléfono: (593) (02) 2 55555 – ext. 1111

2.5 Dirección de Correo Electrónico: csirt@capeipi.org.ec

2.6. Miembros del Equipo

Ing. Juan Pérez

Ing. Antonio Valencia

2.7 Más Información

Información general acerca del CSIRT PYME, recomendaciones de seguridad y más puede encontrarla en http://csirt.capeipi.org.ec

2.8 Horario de Atención: De lunes a viernes de 8:00 – 13:00 y de 15:30 – 18:30.

2.9 Puntos de contacto para clientes

La comunicación entre el Equipo CSIRT PYME y los miembros de la CAPEIPI para el reporte de incidentes, se lo realiza a través del Área de Mesa de Servicios, ext. 3333.

Para comunicarse con el CSIRT PYME acerca de información de vulnerabilidades o alertas de seguridad, puede utilizar medios como correo electrónico o teléfono.

3. Constitución

3.1. Misión

“Brindar asistencia en la provisión de servicios proactivos para reducir el riesgo de sufrir de incidentes de seguridad informática en las empresas PyME, así como ofrecer otros servicios vinculados a la

gestión, prevención, detección, preparación y respuesta ante las eventualidades que se produzcan.”

3.2. Comunidad a la que brinda servicios

Todas las empresas asociadas a la Cámara de la Pequeña y Mediana Empresa de Pichincha que se encuentren al día en el pago de sus cuotas mensuales.

3.3. Patrocinio / Afiliación

El Equipo CSIRT PYME es patrocinado por la Cámara de la Pequeña y Mediana Empresa de Pichincha.

4. Políticas

4.1. Políticas ofrecidas por el CSIRT PyME

- Política de tratamiento y respuesta a incidentes
- Política de gestión de vulnerabilidades
- Política de notificación de incidentes
- Política de comunicación
- Política con lineamientos para la revisión de estado general de la seguridad en PyMEs
- Política de resiliencia
- Política de gestión de la seguridad en nuevas tecnologías
- Política de entrenamiento y capacitación

5. Servicios

5.1. Servicios reactivos

El equipo CSIRT PYME ayudará en las tareas relacionadas con el manejo y repuesta a incidentes de acuerdo las metodologías realizadas para el manejo de los mismos. CSIRT PYME proporcionará asistencia en el manejo de incidentes con respecto a:

- Tratamiento y análisis de incidentes
- Respuesta a incidentes in-situ o remotamente
- Respuesta a la vulnerabilidad

5.2. Servicios proactivos

Los servicios proactivos que se brindarán en el Equipo CSIRT PYME son:

- Alertas y advertencias
- Comunicados
- Evaluación/Auditorías de Seguridad

5.3. Servicios de gestión de la seguridad de la información

Los servicios que brindará el equipo CSIRT PyME son:

- Continuidad del negocio y recuperación tras un desastre
- Consultoría de seguridad
- Educación y formación

6. Formas de notificación de incidentes

Para realizar el reporte de incidentes debe utilizar los canales de comunicación puestos a disposición por el equipo del CSIRT PYME en su sitio web.

7. Disclaimer

El Equipo CSIRT PYME no se responsabiliza por el mal uso que se dé a la información aquí contenida.

BIBLIOGRAFÍA

BIBLIOGRAFÍA ESPECÍFICA

[1] "Definición de Pyme";

http:// http://definicion.de/pyme/

Consultada 10/06/2017

[2] "Guía del usuario sobre la definición del concepto de pyme";

http://www.ipyme.org/es-ES/DatosPublicaciones/Documents/Guia-usuario-Definicion-PYME.pdf

Consultada 10/02/2018

[3] "¿Cuáles son las ventajas y desventajas de las PYMES?";

https://www.pyme.es/ventajas-y-desventajas-de-las-pymes/

Consultada 10/06/2017

[4] "Lasso y Moreno coinciden en reducir los trámites para ayudar a las pymes"

http://www.elcomercio.com/actualidad/leninmoreno-guillermolasso-propuestas-tramites-pymes.html

Consultada 04/02/2017

[5] "Los principales riesgos de una Pyme";

https://www.forbes.com.mx/los-principales-riesgos-de-una-pyme/

Consultada 11/06/2017

[6] [7] "Ciberataques: las pymes también están en peligro";

http://www.lanacion.com.ar/1980567-ciberataques-las-pymes-tambien-estan-en-peligro

Consultada 11/06/2017

[8] "Pymes, el objetivo más vulnerable para los ciberdelincuentes: 70.000 ataques en 2016";

http://www.abc.es/economia/abci-pymes-objetivo-mas-vulnerable-para-ciberdelincuentes-70000-ataques-2016-201605302128_noticia.html

Consultada 11/06/2017

[9] [28] "La débil apuesta de las pymes por la seguridad informática";

https://retina.elpais.com/retina/2017/06/01/tendencias/1496307759_889133.html

Consultada 11/06/2017

[10] "Las pymes subestiman el peligro de las acciones TI irresponsables de los empleados";

http://haycanal.com/noticias/10222/las-pymes-subestiman-el-peligro-de-las-acciones-ti-irresponsables-de-los-empleados

Consultada 13/04/2017

[11] "El financiamiento de la pequeña y mediana empresa en Costa Rica: análisis del comportamiento reciente y propuestas de reforma";

http://www.cepal.org/es/publicaciones/5283-financiamiento-la-pequena-mediana-empresa-costa-rica-analisis-comportamiento

Consultada 12/07/2017

[12] "¿A cuánto asciende el software ilegal en Argentina?";

http://www.tecnopymes.com.ar/2017/02/22/a-cuanto-asciende-el-software-ilegal-en-argentina/

Consultada 18/10/2017

[13] "Ataques ransomware WannaCry";

https://www.wikiwand.com/es/Ataques_ransomware_WannaCry Consultada 02/09/2017

[14] "Ciberataques: las pymes también están en peligro";

http://www.lanacion.com.ar/1980567-ciberataques-las-pymes-tambien-estan-en-peligro

Consultada 14/10/2017

[15] "Las pymes subestiman el peligro de las acciones TI irresponsables de los empleados";

http://haycanal.com/noticias/10222/las-pymes-subestiman-el-peligro-de-las-acciones-ti-irresponsables-de-los-empleados

Consultada 22/03/2018

[16] "Las pymes, un paraíso para el 'malware'";

https://www.elconfidencial.com/tecnologia/2017-04-15/seguridad-internet-pymes-malware_759154/Consultada 22/03/2018

[17] "Como crear un CSIRT paso a paso"

https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

Consultada 20/02/2017

[18] "Equipo de Respuesta ante Emergencias Informáticas";

https://www.wikiwand.com/es/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas

Consultada 24/06/2017

[19] "Los vigilantes de las redes";

http://www.elperiodico.com/es/sociedad/20170709/vigilantes-redes-labora-cert-csirt-6152855

Consultada 24/06/2017

[20] "Gusano Morris"

https://www.wikiwand.com/es/Gusano_Morris

Consultada 24/06/2017

[21] "Reporte de Incidentes"

http://www.seguridadinformatica.unlu.edu.ar/?q=node/4

Consultada 20/10/2017

[22] [24] [31] "Manual básico de gestión de incidentes de seguridad informática"

http://www.proyectoamparo.net/es/manuales

Consultada 24/06/2017

[23] "Como crear un CSIRT paso a paso"

https://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjrt-rh_ezRAhVCkJAKHUJJCpYQFggqMAE&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fcsirt-setting-up-guide-in-spanish%2Fat_download%2FfullReport&usg=AFQjCNGhtU_YnhaU2ubjs58DhCcKTKL4dA&sig2=JOzLQJvShQbnEVoYjObpXg&bvm=bv.145822982,d.Y2I

Consultada 20/10/2017

[25] "Banelco"

https://www.wikiwand.com/es/Banelco

Consultada 17/09/2017

[26] "Proveedor de Target confirma ciberataque"

https://www.wikiwand.com/es/Banelco

Consultada 17/09/2017

[27] "La falta de conocimiento en seguridad informática pone en riesgo a las empresas"

https://latam.kaspersky.com/about/press-releases/2018_la-falta-de-conocimiento-en-seguridad-informatica-pone-en-riesgo-a-las-empresas

Consultada 17/08/2017

[29] "GUÍA DE CREACIÓN DE UN CERT / CSIRT"

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf

Consultada 24/06/2017

[30] "Perfil del Oficial de Seguridad Informática"

http://www.cudi.edu.mx/rfc/drafts/draft4.pdf

Consultada 24/06/2017

BIBLIOGRAFIA GENERAL

- **“Guía de Seguridad en Informática para PYMES”;** http://www.uprm.edu/cde/public_main/slider/files_slider/presentaciones_foro/seguridad_informatica.pdf; Consultada 11/12/2017.

- **“Por qué la privacidad en internet es importante para quienes no tienen nada que ocultar”;** https://www.infobae.com/america/tecno/2018/04/04/por-que-la-privacidad-en-internet-es-importante-para-quienes-no-tienen-nada-que-ocultar/?outputType=amp-type& twitter_impression=true; Consultada 4/04/2017.

- **“Los retos de seguridad para las PYMES”;** http://www.enter.co/especiales/enterprise/los-retos-de-seguridad-para-las-pymes/; Consultada 11/12/2017.

- **“Solución integral de seguridad para las pymes mediante un UTM”;** http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf; Consultada 15/12/2017.

- **“Plan de seguridad informático”;** http://es.slideshare.net/ofebles/plan-de-seguridad-informatica; Consultada 15/12/2017.

- **“Las Pymes marcan el ritmo”;** http://redcame.org.ar/adjuntos/suple_pymes_marzo_2017.pdf; Consultada 19/12/2017.

- **“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 15/12/2017.

- **“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 15/12/2017.
- **“Las pymes serán jugadores clave del futuro”;** http://www.lanacion.com.ar/1817784-las-pymes-seran-jugadores-clave-del-futuro; Consultada 15/12/2017.

- **“Incident handling for Smes”;** https://www.sans.org/reading-room/whitepapers/incident/incident-handling-smes-small-medium-enterprises-32764; Consultada 15/12/2017.

- **“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 15/12/2017.

- **“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 15/12/2017.

- **“Tips para sumar un proyecto de seguridad en las PYMES”;** http://www.tecnopymes.com.ar/2017/11/09/tips-para-sumar-un-proyecto-de-seguridad-en-las-pymes/; Consultada 15/12/2017.
- **“En América Latina el 99% de las empresas son pymes”;** http://www.revistalideres.ec/lideres/america-latina-cifras-empresas-pymes.html; Consultada 15/12/2017.

- **“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 15/12/2017.

- **“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 15/12/2017.

- **“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 15/12/2017.

- **“Medidas de seguridad en los sistemas informáticos”;** http://www.adminso.es/index.php/4._Medidas_de_seguridad_en_los_sistemas_inform%C3%A1ticos; Consultada 15/12/2017.

- **“Informatización en la pequeña y mediana empresa”;** http://www.cyta.com.ar/ta0104/articulos/ti/ti.htm; Consultada 15/12/2017.
- **“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 15/12/2017.

- **“Manual de seguridad en redes”;** http://es.slideshare.net/Princesadivina/arcert-manual-deseguridadenredesinformaticas; Consultada 15/12/2017.

- **“Seguridad Lógica”;** http://www.segu-info.com.ar/logica/seguridadlogica.htm; Consultada 15/12/2017.

- **“Buen uso del correo electrónico corporativo”;** http://www.segu-info.com.ar/articulos/35-uso-correo-electronico-corporativo.htm; Consultada 15/12/2017.

- **“Baja, la Seguridad Informática de PyMES”;** https://americas.thecisconetwork.com/site/content/lang/es/id/5493; Consultada 15/12/2017.

- **“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 15/12/2017.

- **“¿Cuánto pierden PyMEs o Corp ante fallos de seguridad?”;** https://portinos.com/27249/cuanto-pierden-pymes-o-corp-ante-fallos-de-seguridad; Consultada 15/12/2017.

- **“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 15/12/2017.

- **“Guía de seguridad ICC para los negocios”;** http://www.iccspain.org/wp-content/uploads/2016/01/ICC_GUIA-CIBERSEGURIDAD_ESP.pdf; Consultada 15/12/2017.

- **“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 15/12/2017.

- **“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 15/12/2017.