¿El concepto de seguridad de la información aplica para las PYMES?

Riveros, Esperanza

Esperanzza.riveros@gmail.com

Universidad Piloto de Colombia

RESUMEN---Paulatinamente las PYMES se involucrarán en el proceso de seguridad de la información, las grandes empresas demandan en mayor proporción sus productos o servicios y toda la información que intercambian deberá conservar los mismos principios de confidencialidad, disponibilidad e integridad, por tal razón es importante que las PYMES adopten las mejores prácticas de seguridad de la información, puede resultar en ventajas competitivas puesto que demuestran su interés por proteger dichos bienes intangibles propios y de terceros.

ABSTRACT— The importance to protect the confidentiality, availability, integrity for the corporate information is a new goal for the PYMES, nowadays, these small, medium enterprises provides technological services for wide financial, government enterprises that for their regulations must accomplish with their laws, statute, etc. These news requirements added with the benefits and hazard of corporate information, SGSI allows PYMES understand the security information like a formal process to assure that the information is safeguarded from malicious people.

ÍNDICE DE TÉRMINOS--- Confidencialidad, Disponibilidad, Integridad, ISO27000, PCI-DSS PYME, SGSI.

I. INTRODUCCIÓN

Este artículo ambientará y sugerirá a las PYMES recomendaciones que les permitirá comprender y actuar frente a los requerimientos de las empresas clientes que exigen evidencias de control sobre la información que intercambian por motivos comerciales.

Iniciando, es importante definir que es una PYME, información y las propiedades de la información que se busca preservar con los sistemas de gestión de información.

II. ¿QUÉ ES UNA PYME?

Se define como **Pyme:** [1] "es el acrónimo de pequeña y mediana empresa. Se trata de la empresa mercantil, industrial o de otro tipo que tiene un número reducido de trabajadores y que registra ingresos moderados".

En Colombia según la Ley para el fomento de la Micro, Pequeña y Mediana Empresa las PYMES se clasifican en: micro, pequeña y mediana empresa donde los activos oscilan entre 501 S.M.L.V (Salarios mínimos legales vigentes) hasta 15.000 S.M.L.V.

De acuerdo con un artículo de la revista DINERO en su edición del 9 de febrero de 2015: "las pymes representan el 99,9 % del total de las empresas en Colombia, cerca de 1,6 millones de unidades empresariales. De ahí la relevancia de conocer las dificultades y desafíos que enfrentan en el panorama económico tanto actual como futuro del país". [2].

III. ¿QUÉ ES INFORMACIÓN?

La información es el grupo de datos codificados que tiene significado y valor para quien la genera, procesa, almacena, transmite, modifica, elimina, entre otras acciones que pueden efectuarse, hoy en día, es un bien intangible que puede generar ventajas competitivas, piense en un nuevo producto que lanzará al mercado a corto o mediano plazo, a pesar de que aún dicho producto no ha sido fabricado, los componentes químicos, fórmulas, propiedades, empaques, costos, proveedores, campañas de mercadeo, toda la información relacionada, ya se encuentra almacenada electrónicamente en un computador, material impreso o incluso almacenada en la nube; se trata de información que usted como PYME ha desarrollado mediante investigación y a la cual le ha asignado recursos económicos y de la cual busca retornar la inversión sumado a las ganancias esperadas, desde este punto de vista la información es el bien o activo más importante de su PYME, ahora bien, como cualquier otro activo físico, usted busca protegerlo y mantenerlo a salvo de manos maliciosas que

puedan afectar su integridad, confidencialidad entre otras, por lo cual adiciona controles que disminuyan el impacto en caso de afectación negativa sobre el activo, allí es cuando toma sentido y cobra valor invertir en un seguro, pero no se trata de los seguros tradicionales, para este ámbito se trata de un sistema de gestión de seguridad de la información, ¿pero qué significa esto? es el medio por el cual se busca preservar las propiedades de la información; confidencialidad, integridad y disponibilidad, a continuación una breve descripción de la confidencialidad: se refiere a que el acceso a dicha información se otorgue únicamente a las personas autorizadas, la integridad se refiere a que dicha información no se modifique o altere y la disponibilidad se refiere a que la información esté disponible en el momento en que las personas autorizadas la requieran acceder, copiar, almacenar, modificar, etc.

A estas propiedades se les denomina la Triada de la información. Véase Fig.1.

Fig.1 Triada de la Información CID. [3]

IV. PROPIEDADES DE LA INFORMACIÓN

¿Estos conceptos que significado tienen para un sistema de seguridad de la información? Son la base fundamental para comprender la naturaleza de las amenazas para que en consecuencia se logre formular contramedidas efectivas que se puedan tecnológica y físicamente aplicar para disminuir el impacto negativo sobre el activo de la información, iniciemos con la confidencialidad.

Las amenazas a la confidencialidad pueden ser:

- Robo de archivos de información.
- Robos de las credenciales y contraseñas.
- Interceptación de la información.
- Ingeniería social.

Las contramedidas son los controles que se instalarían para evitar la pérdida de la confidencialidad, que pueden ser:

- Cifrado de los archivos o cifrado de la conexión, similar a como lo efectuaba Julio César para enviar órdenes a su ejército durante las batallas.
- Clasificar e identificar los usuarios autorizados que deben acceder a la información y al resto de usuarios denegar el acceso.
- Entrenar a los usuarios a identificar indicios de extracción de información confidencial de parte de compañeros o por ingeniería social.

Como segunda propiedad de la información se encuentra la integridad cuyas amenazas son:

- Los conocidos virus.
- Usuarios malintencionados.
- Ransonware.

Las contramedidas disponibles para evitar la pérdida de la integridad pueden ser:

- IPS (Sistema de Detección de Intrusos).
- Antivirus.
- Control de acceso a los aplicativos.
- Filtro de correo, etc.

Finalmente la tercera propiedad la disponibilidad puede verse afectada por las siguientes amenazas:

- Malas condiciones ambientales (fallos de energía).
- Procesos de mantenimientos no controlados.
- Usuarios malintencionados.

Las contramedidas disponibles pueden ser:

- Planes de recuperación de desastres.
- Ambientes de desarrollo y pruebas.
- Uso de firewall, WAF entre otros.

En resumen, entendiendo como actúan las amenazas, se crean o adaptan los controles con los cuales se busca disminuir el riesgo de comprometer la información y todo esto corresponde a un proceso constante que busca asegurar que durante todo el ciclo de vida de la información se mantengan las condiciones

adecuadas, este proceso se llama un sistema de seguridad de la información SGSI.

V. SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

SGSI es un proceso sistémico en el cual se analizan los activos de información, las amenazas y los controles que se pueden implementar para disminuir el riesgo de comprometer la información, es así como la Norma ISO27001 aporta sus recomendaciones para la implementación en aquellas empresas que buscan proteger continuamente su información. Esta norma compila las mejores prácticas de la industria y le permite ampliar su visión respecto a la seguridad de la información, mediante una perspectiva integral de los diferentes actores que intervienen.

Es importante revisar cada uno de los dominios que la norma contempla en su más reciente versión del año 2013.

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Seguridad de los Recursos Humanos.
4. Gestión de Activos.
5. Control de Acceso.
6. Criptografía.
7. Seguridad Física y del Entorno.
8. Seguridad de las Operaciones.
9. Seguridad de las Comunicaciones.
10. Adquisición, desarrollo y mantenimiento de sistemas.
11. Relaciones con los proveedores.
12. Gestión de Incidentes de Seguridad de la Información.
13. Gestión de continuidad del negocio.
14. Cumplimiento.

En la norma ISO 27002:2013 se identifican los posibles 114 controles o contramedidas que la PYME puede implementar de acuerdo a las amenazas identificadas por cada uno de sus activos de información, pero la pregunta es implementando los 114 controles: ¿es posible afirmar que la información está 100% segura?, la respuesta es no; es posible alcanzar una buena aproximación de seguridad pero no garantiza una cobertura total, al igual que sucede con los seguros tradicionales de vivienda o vehículos.

Inicialmente se parte de la premisa que los recursos son finitos por tanto la PYME no buscará implementar 114 de 114 controles, se priorizará y atenderá con la mayor diligencia posible aquellos activos de información calificados con riesgo y criticidad alta para la operación de la PYME.

Aquí es el punto donde se busca un balance en el valor de la información y el valor de protegerla, los mecanismos de control deben guardar un balance rentable para la empresa y no pueden volverse un centro de costo que no aporte valor.

Con el paso de los días los ataques son más sofisticados y buscan atacar el eslabón más débil de la cadena: que es el usuario, normalmente los controles que se ejecutan a los usuarios no incluyen un alto costo pero si un continuo proceso de sensibilización o concienciación, para los delincuentes es más rentable efectuar ataques de ingeniería social que crear procesos elaborados y masivos de ataque, es más factible, rápido y efectivo obtener la información de una fuente confiable, que tiene acceso ilimitado, cuenta con todas las autorizaciones del caso y que no cuenta con mecanismos robustos de defensa.

A plena vista se observa que asegurar la disponibilidad, integridad y confidencialidad de la información no es una tarea sencilla y no corresponde a una receta a seguir al pie de la letra, es importante priorizar y revisar con detalle los procesos, normalmente los atacantes buscan las debilidades en los procesos que son más sencillos de explotar ya que no implica un mayor desgaste de recursos humanos, tecnológicos, bajas posibilidades de ser detectado e identificado, rastros difíciles de seguir, un anonimato ideal, pero al igual que los procesos se busca acceder a los atributos elevados que tienen los usuarios en los sistemas de información y esto se puede efectuar mediante técnicas de ingeniería social que hasta la fecha no cuenta con un hardware o una solución informática que lo detenga, todo depende de la intuición y la destreza de los usuarios, ¿esto es suficiente?.

Definitivamente no, pero ¿cómo llegar a concientizar a los usuarios? Se puede alcanzar mediante campañas de sensibilización concernientes al grado de importancia de la información para la organización en la cual trabaja, es una tarea en la cual se busca demostrar que tal como cada persona cuida su información bancaria, crediticia, personal, ese mismo cuidado

debe trasladarlo y aplicarlo con la información corporativa, es importante ejemplarizar con otras compañías que se han visto afectadas reputacionalmente, financieramente cuando se vulneró la confidencialidad de la información, a modo de ejemplo, en el caso más reciente Ashley Madison ®,un sitio de citas extramaritales por Internet con un total de 42 millones de miembros, Véase Fig.2, en el mes de agosto de 2015 quedó expuesta al público información privada, financiera y de preferencia sexual de 36 millones de miembros a nivel mundial, quienes se vieron extorsionados por delincuentes que solicitaban pagos por no dejar en evidencia sus preferencias sexuales, entre ellos 500,000 colombianos se vieron expuestos por este ciberataque, incidentes de seguridad de la información como estos son los que se buscan prevenir mediante la implementación de sistemas de seguridad de la información. [4].

Fig.2 Ashley Madison. [5]

Como ejemplo un caso nacional, informado el pasado 20 de noviembre de 2015, el CTI capturó a un responsable de hurto por medios electrónicos que operaba en 5 departamentos del país, su modus operandi era ofrecerse a pagar recibos de pago de planilla de seguridad social y facturas de servicios públicos a un costo menor al real, ¿cómo esto es posible? El delincuente recibía el dinero en efectivo y efectuaba los pagos por medios electrónicos, el delincuente había comprometido las credenciales de cuentas bancarias de ciudadanos y empresas, una vez autenticado efectuaba los pagos de las facturas y planillas y se quedaba con el dinero producto del ilícito [6], la pregunta es ¿cómo pudo obtener las credenciales bancarias de los ciudadanos y empresas? Posiblemente lo pudo efectuar como ataques de phishing, malware, ingeniería social, por lo cual nos permite evidenciar que nadie se encuentra exento de que un incidente de este tipo ocurra bien sea como ciudadano o empresa.

Con el contexto de la situación en mente, la idea de proteger la información va tomando importancia, las PYMES son más vulnerables a este tipo de incidentes, porque no invierten en una proporción razonable en tecnología, obviamente enfocan todo su capital al objeto de negocio, pero a medida que crecen asumen retos como atender a clientes corporativos quienes si cuentan con estas medidas de protección de su información y buscan preservar su información en todas sus cadenas de negocios, a modo de ejemplo: actualmente las empresas de mensajería que prestan servicios de entrega de extractos bancarios, tarjetas de crédito a domicilio en grandes, medianas y pequeñas ciudades en el territorio nacional, dichas empresas movilizan a diario información confidencial, financiera de los clientes bancarios que puede ser comprometida fácilmente para efectuar ilícitos, ¿pero cómo puede suceder esto? La respuesta es sencilla, cuando no llegan los extractos financieros, ¿existe un acuse real de recibo de los clientes? La respuesta es: no es necesario, al tener acceso al extracto información como saldos, números de productos, historial de compras o pagos se puede obtener información de los clientes de una manera sencilla, recordemos que los delincuentes buscan los procesos más vulnerables y fáciles de explotar, este tipo de acción no es sofisticada pero su efectividad en la recolección de información es alta.

El anterior ejemplo es un clara muestra en la cual la PYME termina envuelta como superficie de ataque de los incidentes de seguridad en entidades bancarias, este incidente ya fue evidenciado por lo cual se amplió el alcance de las entidades financieras hacia todos los terceros relacionados en los procesos bancarios, que en su gran mayoría se trata de PYMES obligándoles a cumplir con la normas internacionales PCI-DSS (Payment Card Industry Data Security Standards) para los procesos en los cuales intervenía con procesos de tarjetas de crédito, esta norma internacional es regida por un organismo internacional cuyos miembros son Master, VISA, American Express, entre otros, quienes buscan minimizar los fraudes con tarjetas de crédito, razón por la cual se dieron a la tarea de entender los posibles procesos vulnerables y entre ellos encontraron debilidades en el manejo de la información de entidades bancarias y sus proveedores, para nuestro caso las empresas de mensajería, que han tenido que invertir en planes de trabajo para poder cumplir con los requerimientos de dicha norma para continuar trabajando con las instituciones financieras y aperturar nuevos modelos de negocio aprovechando el cumplimiento de dichos requisitos.

VI. IMPLEMENTACIÓN SGSI

Entendiendo la naturaleza de la PYME la pregunta es: ¿Qué tan fácil puede ser implementar dicho sistema de gestión de la seguridad de la información?, el paso inicial es tomar conciencia de lo que se busca con esta implementación y la respuesta no puede ser otra que mantener la información fuera del alcance de terceros, la segunda pregunta es: ¿Cuál es la información que interesa mantener confidencial? Es toda aquella información que es vital para el negocio, que es extremadamente difícil de reconstruir o que se encuentre amparada bajo una ley nacional que lo exija, entre otras, es importante clasificar, priorizar y seleccionar un proceso de negocio a la vez para que la implementación pueda llevarse a feliz término.

Una vez identificada la información o como se citará en adelante: activos de información, es importante clasificar acorde a sus características: pública, privada, confidencial, sensible, de tal manera que los esfuerzos se enfocarán en aquella información clasificada como confidencial y sensible, una vez identificados los activos, se requiere identificar los diferentes procesos corporativos donde dicha información se origina, procesa, almacena, imprime, intercambia, ya que conociendo todos los procesos relacionados se pueden identificar con mayor facilidad las vulnerabilidades y posibles controles compensatorios que se pueden aplicar durante la implementación.

Efectuando el recorrido por la norma ISO27002:2013 por cada uno de sus 35 objetivos de control, en modo preliminar una vez identificados los activos de información se estaría cumpliendo con el requisito del numeral 8 Gestión de Activos en el cual se identifican la responsabilidad, clasificación y manejo de los soportes de almacenamiento.

En el dominio 9 que corresponde a Control de Acceso es importante que efectué un cuadro comparativo donde identifique las diferentes áreas de la PYME y los activos de información y allí consolide que tipos de permisos dicha área requiere sobre la información, como premisa se parte de entregar el menor privilegio, es decir sino requiere acceder a la información, deniegue el acceso, como segundo paso es importante verificar la robustez de las contraseñas de acceso a las diferentes aplicaciones, es importante no hacerle fácil el trabajo a los delincuentes, usted no le pondría una cerradura universal a la caja fuerte donde guarda su dinero, este consejo aplica también para las contraseñas.

En el dominio 10 que corresponde Cifrado se busca validar si la información almacenada e intercambiada requiere técnicas de cifrado por su alto grado de confidencialidad como por ejemplo: números de tarjeta de crédito regulados fuertemente por la norma PCI-DSS. En el mercado existe numerosas herramientas gratuitas de cifrado de archivos como GnuPGP® que le permitirá cifrar los archivos seleccionados y así almacenar cifrados los archivos y solo cuando se requiere acceder se aplica el proceso de descifrado con la misma herramienta y la llave de cifrado especifica al proceso.

En el dominio 11 que corresponde a Seguridad Ambiental y Física se busca asignar controles de acceso perimetral a aquellos sitios donde se almacena, procesa información confidencial, es el conjunto de barreras físicas que se disponen para que quienes necesitan ingresar lo efectúen de manera controlada y generando puntos de trazabilidad, el restante universo de usuarios físicamente se les restringe el acceso a dichas instalaciones.

Este dominio incluye la seguridad de los equipos de cómputo dentro y fuera de las instalaciones de la PYME, si cuenta con equipos portátiles se aconseja el cifrado de discos, en caso de que sus portátiles fuesen hurtados, los delincuentes no tendrían acceso a la información confidencial.

En este dominio también se recomienda las políticas de escritorio limpio y sesión desatendida, pequeñas acciones que los usuarios pueden efectuar sin invertir en una gran infraestructura, el objetivo es: que no se conserven documentos impresos con información confidencial sobre el escritorio durante largos periodos sin supervisión del responsable, no se puede tener una trazabilidad de quien pudo haberlos leído, copiado, adulterado, eliminado entre otros, la sesión desatendida se refiere a evitar el acceso de personas diferentes al usuario que puedan consultar, ingresar, eliminar información abusando de los privilegios otorgados previamente a otro usuario, el usuario debe comprender que esto es una práctica similar a la suplantación y en el cual se puede ver involucrado si se llega a llevar a cabo una investigación por algún delito informático que en Colombia ya se encuentra regulado por la Ley 527 de 1999.

En el dominio 12 de Seguridad Operativa incluye las acciones que debe seguir el administrador de sistemas respecto a código malicioso, análisis de vulnerabilidades, copias de seguridad, registros de actividades sobre los sistemas operativos de los servidores de aplicaciones entre otros, como un tema específico para el análisis de vulnerabilidades la PYME se puede apoyar en el

uso de herramientas gratuitas como Retina® u Open Vas®.

En el dominio 13 que corresponde a seguridad en las telecomunicaciones, los equipos de red deben configurarse acorde a requerimientos estándar de seguridad estas se denominan plantillas que el fabricante sugiere y comparte a sus clientes para que la configuración de dichos equipos no sea insegura y susceptible a accesos u operaciones no autorizadas.

Este dominio incluye el intercambio de información con terceros es aquí donde se estipulan los procedimientos y herramientas mediante las cuales se intercambia información de manera segura con terceros, como por ejemplo si se utiliza el correo corporativo adjuntando únicamente documentos cifrados, conexiones FTPS o SFTP, se prohíbe el uso de herramientas de almacenamiento público como Google Drive® o Dropbox®, entre otras.

En el dominio 17 la importancia de contar con planes de continuidad de negocio, infraestructura tecnológica redundante, que en eventos de catástrofes naturales o ambientales permitirán a la PYME continuar operando sin interrupción y con tiempos de recuperación aceptables para su operación.

VII. CONCLUSIONES

La implementación de un sistema de gestión de seguridad de la información SGSI no se encuentra supeditado al tamaño de la empresa, se considera que dicha implementación es una recopilación de las mejores prácticas de la industria que les sugiere a las empresas que acciones tomar de una forma holística cuando se trata de proteger la confidencialidad, integridad, disponibilidad de la información corporativa.

Es fundamental entender todo el proceso de generación, procesamiento, almacenamiento, transmisión, eliminación de la información, para poder enfocar con mejor precisión los controles requeridos para preservar la información, el objetivo es proteger sin sacrificar la productividad de la PYME.

Es importante indicar que la mejor práctica es empezar paulatinamente dicha implementación por procesos, recordando el principio de divide y vencerás, iniciar con un proceso productivo a la vez permite lograr el objetivo y conseguir mejores resultados, permite retroalimentar los demás procesos con las lecciones aprendidas internas mejorando en tiempo y efectividad de los controles compensatorios aplicados.

Atreverse a implementar nuevas prácticas llevará a que las PYMES puedan ser más competitivas, responsables y conscientes de la importancia de la información interna y de los terceros que depositan sus secretos comerciales.

REFERENCIAS

[1] Sitio web. Autor no especificado. (Año, mes no disponible). Título. Definición de pyme - Qué es, Significado y Concepto. Disponible: http://definicion.de/pyme/#ixzz3sFpokWh7

[2] Revista DINERO. Autor no especificado. (2015,02) Título. ¿Por qué fracasan las pymes en Colombia? Disponible: http://www.dinero.com/economia/articulo/pymes-colombia/212958

[3] Trabajo fin de grado. González, Mario. (2014,05). Título: Estudio de mecanismos de autenticación basados en contraseñas visuales en dispositivos móviles Android. Disponible: https://repositorio.uam.es/bitstream/handle/10486/660995/gonzalez_nahon_mario_tfg.pdf?sequence=1

[4] Periódico EL TIEMPO. José García y Camilo Peña. (2015,08) Título: Estos son los datos de Colombia en el 'portal infiel' filtrado. Disponible: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/ashley-madison-estos-son-los-datos-de-colombia-en-el-portal-infiel-filtrado/16273478

[5] Sitio web. Autor no especificado. (2001-2015). Disponible: https://www.ashleymadison.com/?c=20&lang=es_US&age_gate=0&utm_source=google&utm_medium=cpc&utm_term=%2Bashley+%2Bmadison&utm_content=b&utm_campaign=Ashley+Madison+-+CO+-+Brand&utm_logged=1

[6] Sitio web. Autor no especificado. (2015,11). Título: CTI captura a una persona por hurto informático en 5 departamentos del país Disponible: http://www.fiscalia.gov.co/colombia/noticias/cti-captura-a-una-persona-por-hurto-informatico-en-5-departamentos-del-pais/