Estado de las Pymes a nivel de Seguridad Informática según la Norma ISO27000 para la seguridad de la información Caso: PYMEs en Bogotá (Colombia)

Status of SMEs in terms of Information Security according to the ISO27000 Standard for information security Case: SMEs in Bogota (Colombia)

Peter N. Fierro Castaño

Resumen

En el presente artículo se hablará sobre las Pymes en Colombia. se dará una vista a la historia de las mismas, se estudiará el estado de las pymes de Bogotá a nivel de seguridad de la información teniendo en cuenta los controles que presenta la norma ISO/IEC 27002:2013, estos controles sirven para determinar cómo están las empresas encuestadas en cuanto a nivel de seguridad de la información y tratamiento de los datos.

Palabras clave: Seguridad informática, Ingeniería social, Delitos Informáticos, ISO/IEC 27000, ISO/IEC 27001, información, PYMES.

Abstract

In this article we will talk about Pymes in Colombia. a view will be given to their history, the status of the Pymes in Bogotá will be studied at the level of information security, taking into account the controls presented by ISO / IEC 27002: 2013, these controls are used to determine how they are the companies surveyed regarding the level of information security and data processing.

Keywords: Computer security, social engineering, computer crimes, ISO/IEC 27000, ISO/IEC 27001, information, PYMES.

Recibido / Received: 15 de Noviembre de 2019 Aprobado / Aproved: 20 de Diciembre de 2019
Tipo de artículo / Type of paper: Investigación científica y tecnológica
Afiliación Institucional de los autores / Institutional Affiliation of authors: Corporación Universitaria Minuto de Dios
Autor para comunicaciones / Author communications: peter.fierro@uniminuto.edu
Los autores declaran que no tienen conflicto de interés.

Introducción

Para las empresas de Colombia es muy importante la implementación de estándares que les ayuden a proteger su información, por esto es relevante capacitar al personal de sistemas en cuanto a qué hacer si son víctimas de ataques informáticos y cómo evitarlos. Esa capacitación no debe dirigirse exclusivamente a los empleados del departamento de Sistemas sino a todos en general, ya que cualquier empleado puede ser víctima de un ataque informático el cual pueda llegar a exponer información importante de las organizaciones.

Se debe hacer mucho énfasis en uno de los ataques más comunes y efectivos a nivel de delitos informáticos: la Ingeniería Social, una técnica bastante efectiva que logra grandes índices de efectividad sin que la víctima se dé cuenta de que está dando información valiosa de la empresa donde labora. La Ingeniería Social se puede realizar de manera directa, es decir, mediante el trato personal con la víctima, o indirecta con el uso de la tecnología. La idea es poder saltarse los sistemas de seguridad a través de la información que otorga directamente el empleado o grupos de empleados que manipulan información importante de seguridad en las organizaciones.

"La persona que efectúa este método, trata de engañar a la víctima, buscando entrar en confianza o haciéndose pasar por alguien más para obtener lo que necesita. Teniendo en cuenta que somos muy vulnerables y nos movemos a través de una serie de impulsos irracionales, el que ejecute esta técnica usará comúnmente el teléfono, el internet, el disfraz u otros métodos para engañar fingiendo ser alguien más. En muchos de los casos que he conocido, la persona suplanta a un trabajador de la empresa o a alguien de servicio técnico", dice Emanuel Abraham, hacker ético de Security Solution & Education.

Por esta razón, es importante dar a conocer el estado actual de las Pymes en Bogotá en cuanto a la implementación de la norma ISO 27000, para la seguridad de la información, con el fin de generar conciencia entre las pymes para que implementen estrategias de seguridad y controles, basados en el estándar ISO 2702:2013, y lograr con esto que su activo más importante pueda ser resguardado y protegido de la mejor manera.

Metodo

Se realizó una encuesta online a 29 empresas de diferentes sectores comerciales, presentando el 60% de participación las empresas dedicadas a la Tecnología y Telecomunicaciones. Esta encuesta tiene como fin medir el conocimiento que tienen las pymes de Bogotá, Colombia, sobre la norma ISO 27000, sus variantes y aplicación de la misma.

Para la construcción de esta encuesta se tomó como referencia los controles presentados en la norma ISO 27002:2013, los cuales son de gran importancia ya que sirven para determinar cómo están las empresas encuestadas en cuanto al nivel de seguridad de la información y el tratamiento de los datos.

Para responder esta encuesta se contactó a 29 empleados, los cuales están directamente involucrados en el área de sistemas como son, ingenieros de sistemas, ingenieros de redes y telecomunicaciones, con el fin de dar la mayor veracidad y credibilidad al momento de responder.

Para la construcción de esta encuesta se tomó como referencia los controles presentados en la norma ISO 27002:2013 las cuales son de gran importancia ya que sirve para determinar cómo están las empresas encuestadas en cuanto a nivel de seguridad de la información y tratamiento de los datos.

Resultados

Luego de realizar la encuesta online se procedió a hacer la tabulación de la información obtenida y el análisis correspondiente. La encuesta consta de 21 preguntas que serán presentadas a continuación, (ver Tabla I).

Tabla I. *Encuesta de seguridad de la informacion*

PREGUNTA	SI	NO
¿Conoce la Norma ISO 27000?	13	16
En su planeación anual, ¿dispone de recursos para invertir en la seguridad de la información de su empresa?	9	20
En la empresa donde labora, ¿existe un conjunto de políticas para la seguridad de la información?	18	10

PREGUNTA	SI	NO
En la empresa donde labora, ¿realizan revisiones periódicas de las políticas para la seguridad de la información?	12	17
¿Su empresa cuenta con la certificación de la Norma ISO 27000 0 27001?	9	20
¿Manejan políticas de uso de dispositivos Móviles?	9	20
¿Realizan capacitaciones sobre la importancia que tiene la seguridad de la información en la organización?	7	22
Al momento de firmar su contrato laboral, ¿existe una cláusula de confidencialidad de la información que maneja?	20	9
¿Maneja un control de acceso a las redes y servicios asociados de la organización?	16	13
¿En su organización existe una gestión de información confidencial de autenticación de usuarios?	12	17
En su empresa, ¿Manejan políticas de uso de los controles criptográficos?	10	19
Para acceder a la información de la empresa, ¿manejan procedimientos seguros de inicio de sesión?	18	11
¿Existen controles contra código malicioso?	16	13
¿Realizan copias de seguridad de la información?	21	8
¿Manejan restricciones en la instalación de software?	14	15
¿Realizan auditoría de los sistemas de información?	15	14
¿Implementan mecanismos de seguridad asociados a servicios en red?	18	11
En la empresa, ¿realizan una planificación de la continuidad de la seguridad de la información?	12	17
¿Considera importante aplicar medidas de seguridad de la información sobre la operatividad diaria de la empresa donde labora?	23	6
¿Ha realizado análisis de riesgos sobre las tecnologías de información presentes en su empresa?	10	19

De acuerdo a la respuesta dada por las empresas encuestadas el 55.2% de las empresas desconocen la existencia de la norma ISO 27000. Esto demuestra el nivel de desinformación que se presenta en nuestro país, ocasionando con esto que las pymes de Colombia se enfrenten a diferentes ataques informáticos internos y externos, sin poder actuar adecuadamente para combatirlos.

El 69% de las empresas encuestadas no disponen de recursos para invertir en la seguridad de la información. Esto tiene como resultado empresas que no prestan la atención necesaria en proteger su información y no prevén que en cualquier momento los pueden atacar y al no invertir en el fortalecimiento de su infraestructura física y lógica serán vulnerables a cualquier ataque.

El 58% de las empresas encuestadas no realizan revisiones periódicas de las políticas para la seguridad de la información relacionadas al control de recursos tecnológicos, humanos internos y externos.

El 75.9% de las empresas encuestadas no realizan capacitaciones sobre la importancia que tiene la seguridad de la información en la organización. Por esta razón, los empleados no son conscientes de la importancia que tiene la información que manejan y al no haber interés por parte de los altos mandos ni del personal de sistemas para capacitar a su personal. La información estará siempre disponible para cualquier actor sea interno o externo que quiera sustraer información valiosa de manera ilegal y como los empleados no saben cómo proteger la información se le hará fácil al delincuente informático obtenerla.

El 58.6 % de las empresas encuestadas no realizan un análisis de riesgos sobre las tecnologías de información presentes en su organización. Por esta razón, los empleados no son conscientes de cómo los pueden atacar. Pueden ser atacados a través de un acceso por fuerza bruta, robo de información mediante ingeniería social, sustracción ilegal de la información por los mismos empleados, etc.

Discusión

El objetivo principal de este estudio fue dar a conocer el estado actual de las Pymes en Bogotá en cuanto a la implementación de la norma ISO 27000 para la seguridad de la

información. Dentro de los principales hallazgos encontrados nos damos cuenta que las pymes en Colombia en el caso de Bogotá, está muy por debajo del promedio.

Esto se puede notar en la pregunta número 5 que dice ¿Su empresa cuenta con la certificación de la Norma ISO 27000 0 27001?, para esta pregunta de las 29 pymes encuestadas solo 9 cuentan con la certificación y 20 no la tienen, esto nos da un porcentaje del 31,1 % contra un 69,9%, es algo preocupante porque se nota que las pymes no muestran un interés por tener su información protegida.

Esto nos lleva a un gran interrogante, ¿Las pymes de Bogotá están en la capacidad de proteger su información?, dadas las evidencias recolectadas en el análisis previo, de acuerdo con las respuestas de las 29 empresas encuestadas, vemos que las pymes están por debajo del promedio y que en estos momentos se encuentran vulnerables a cualquier ataque informático y que no cuentan con las herramientas y controles necesarios para proteger su activo más importante, la información.

Conclusiones

Luego de realizar el análisis correspondiente a la encuesta realizada, y entregar los resultados a las 29 empresas entrevistadas, se espera que las pequeñas y medianas empresas de Bogotá implementen la norma ISO 27000 con el fin de proteger su información de cualquier clase de ataque informático. Con el fin de adquirir la experiencia necesaria que les ayude a cumplir esta meta, no solo a nivel de Software y Hardware sino a nivel Humano, en el cual las empresas no tienen en cuenta al momento de realizar una contratación, exponiendo de manera abismal su activo más importante, la información.

De igual forma el semillero de investigación KVM de la Universidad Minuto de Dios, informará a cada empresa encuestada, las diferentes técnicas de delitos informáticos que se pueden presentar y como protegerse de ellos.

Llevar una buena práctica de la norma, así como fomentar la capacitación del personal encargado de mantener la información segura, con el fin de llevar un mejor control de los empleados que manejan la información de la empresa.

La norma ISO 27001 es un estándar Internacional muy importante a nivel de seguridad de la información, por tal razón las empresas de Colombia deben implementarlo, ya que generara un estatus a nivel internacional y ayudara a las organizaciones de nuestro país a mejorar las estadísticas en cuanto a empresas que implementan la Norma ISO 27001, que en este momento estamos muy por debajo de las estadísticas.

Referencias

[1] Sara Gallardo M. (2006). "Pequeñas y medianas empresas, las más desprotegidas". Revista Sistemas: Seguridad Informática: Colombia en la mira.Vol.89. http://www.acis.org.co/index.php?id=855. ACIS

[2] Rodrigo Caldas Lemaitre.(2006). Seguridad informática ¿una política empresarial? Revista Sistemas: Seguridad Informática: Colombia en la mira.Vol.89. http://www.acis.org.co/index.php?id=855. ACIS

[3] Jeimy J. Cano. (2006). Seguridad informática: Colombia en la mira. Revista Sistemas: Seguridad Informática: Colombia en la mira.Vol.89. http://www.acis.org.co/index.php?id=855. ACIS

[4] Jeimy J. Cano. (2006). Inversión y gestión de la seguridad informática. Revista Sistemas: Seguridad Informática: Colombia en la mira.Vol.89. http://www.acis.org.co/index.php?id=855. ACIS

[5] Jorge Ramió Aguirre. (2006). Libro Electrónico de Seguridad Informática y Criptografía. http://www.criptored.upm.es/guiateoria/gt_m001a.htm

[6] Carlos Tori. (2008). Hacking Ético. http://www.etnassoft.com/biblioteca/hacking-etico/

[7] Andrés Ricardo Almanza Junco. (2011). Seguridad Informática en Colombia Tendencias 2010-2011. Revista Sistemas: Ciberseguridad y Ciberterrorismo Encuesta Nacional. Vol. 119. http://www.acis.org.co/index.php?id=1655

[8] Jeimy J. Cano. (2011). Informe Seguridad de la Información en Latinoamérica Tendencias 2011 Revista Sistemas: Ciberseguridad y Ciberterrorismo Encuesta Nacional. Vol. 119. http://www.acis.org.co/index.php?id=1655

[9] Pymes en Colombia. (2015). MiPyme. Reuperado de http://www.businesscol.com/empresarial/pymes/

[10] El Portal ISO 27001 en español. (2015). Norma ISO 27000. http://www.iso27000.es/

[11] UNCOMO. Como calcular el ROI. http://negocios.uncomo.com/articulo/como-calcular-el-roi-79.html

[12] MONOGRÁFICO: Introducción a la seguridad informática. http://recursostic.educacion.es/observatorio/web/ca/software/software general/1040-introduccion-a-la seguridad-informática