Universidad Latinoamericana de Ciencia y Tecnología

Desarrollo de Software

¿Que posibilidades de colocación tienen los profesionales de seguridad informática en Costa Rica?

Félix Sandoval Vargas 1-1193-0533

IICO 2012

Resumen

En Costa Rica la brecha tecnológica ha venido en disminución gracias a que las personas con el tiempo han ido adquiriendo mas posibilidades de acceder a internet y con ello ha aumentado el riesgo de estafas vía internet así como también han aparecido nuevas posibilidades de empleo. En este estudio se analiza la posibilidad de colocación que tienen los profesionales en seguridad informática en PYMES, se hace un análisis de la realidad mundial y de la realidad costarricense.

Abstract

In Costa Rica the technology gap has been declining due to people over time have gained more likely to access the internet and this has increased the risk of scams via the internet and also there are new employment opportunities. This study examines the possibility of placement with the computer security professionals in SMEs, is an analysis of the global reality and the reality of Costa Rica.

Introducción

El mundo a evolucionado drásticamente desde la aparición de las computadoras, las cuales han traído muchos beneficios, sin embargo con ellas también han nacido peligros para los usuarios de la red, estas amenazas navegan de forma silenciosa entre los bytes de la telaraña de servidores y computadoras poniendo en jaque tanto a empresas como a personas.

Es claro que en cuanto a ataques informáticos ya contamos con una larga historia de anécdotas gracias a Anonymus, se pueden mencionar los ataques constantes a los servidores de Sony que estuvieron abajo durante casi un mes y donde se especulaba se robaron información confidencial, es bueno anotar que este ataque le costó la cabeza al jefe de seguridad informática de Sony.

También se pueden agregar a la lista de cyber-atentados los últimos ataques de denegación de servicio a la casa blanca, el FBI, Universal Music en donde el desencadenante fue el cese de operaciones del sitio web de MEGAUPLOAD y el resultado fue una semana de ataques continuos a esas entidades en lo que se apostó a llamar la WORLD WAR WEB, y es allí a donde precisamente vamos como seres humanos en nuestro continuo ímpetu por utilizar todo lo bueno que conocemos para fines no tan buenos.

El sin fin de amenazas a manos de movimientos organizados ha desencadenado en una nueva rama laboral donde los profesionales usan sus conocimientos para hacer de las redes un lugar seguro, o por lo menos intentar mantener nuestros datos personales lo mas alejados de personas sin escrúpulos que poseen el suficiente conocimiento para hacer de nuestros días un verdadero calvario.

Dentro del un plano costarricense se puede ejemplificar del peligro que asecha en la red citando al diario La República del 18 de marzo del 2002 en donde Jhonny Castro menciona que "*las perdidas por infecciones de virus informáticos pudieron haber llegado a más de $23 millones en el mercado nacional" , además* también se menciona que varias compañías como Bysupport, Computer Associates, Sidif abrieron oficinas en el país ya que en él vieron opciones de desarrollo debido a que muchas empresas no tienen presupuesto para la seguridad informática, ni siquiera poseen un oficial a cargo y por ello vieron al país como uno de los mercados mas fuertes, así Espinoza dice que en el 2008 la cuota del mercado en seguridad alcanzó los 13 mil millones de dólares americanos, reflejando un crecimiento del 18,6% con respecto al 2007 según el documento elaborado por el PROSIC.

Con la información anterior pregúntese ¿Que pasaría si en Costa Rica alguien decidiera hurgar en los servidores del gobierno costarricense? ¿Hay profesionales que puedan evitar estas intrusiones? **¿Que posibilidades de desarrollo y colocación tienen los profesionales en seguridad informática en Costa Rica?** es la pregunta que este trabajo responde.

Referencias Bibliográficas

Anonymous desencadenó un ataque mediante DdoS (denegacion de servicio), en respuesta al cierre del sitio Megaupload, un hackeo masivo contra diversas webs gubernamentales y de la industria discográfica norteamericana. Con más de 27.000 computadoras implicadas y cerca de 10.000 personas tras ellos, se trata del mayor ataque informático que se conoce a hoy, por encima incluso del registrado tras la clausura de WikiLeaks. Los afectados fueron los sitios del Departamento de justicia, de la oficina federal de Copyright, el FBI, y la Sociedad General de Autores y Editores (SGAE) (Pascual, 2012).

Son cada vez más sofisticadas las tecnologías que utilizan los delincuentes por la Red (phishing, scam, pharming, troyanos bancarios, inteligencia social, chat in the middle, keyloggers...). En el quinto Informe de Fraude Online y Cibercirmen de S21sec, la compañía española informaba de que, durante 2009, detectaron y solucionaron un total de 2.534 incidentes de phishing, códigos maliciosos, redirectores y otras actividades calificadas de fraude online, dirigidas a entidades en España. Según la firma, el phishing continua siendo una de las principales preocupaciones de las empresas, ya que supuso el 63 por ciento del total de incidentes en 2009, y se mantiene respecto al año anterior (62 por ciento) (Oriol, 2012).

Por otra parte, una encuesta realizada en el 2006 en Brasil, Chile, Colombia y México, por Websense reveló que la mayoría de las empresas confían erradamente en los sistemas de seguridad informática que poseen y no realizan acciones proactivas para detectar nuevos peligros en Internet, la mayoría de los directores de tecnología de la información piensan que los sistemas contra virus y espías informáticos con que cuentan protegen sus redes y equipos y Al menos el 86% de los encargados informáticos cree que pueden evitar el espionaje informático con una solución spyware, así el 95% confía en el antivirus esta firma alertó que las compañías carecen de sistemas proactivos, entendiendo por estos, políticas, mecanismos y herramientas de seguridad informática que detecten y puedan bloquear nuevas amenazas difundidas en Internet. El mayor riesgo proviene de las posibilidades que tienen los empleados de las compañías para navegar en Internet - una hora al día en promedio- en sitios no relacionados con sus funciones laborales.

De casi 28 millones de computadoras analizadas por McAfee en diferentes países del mundo, un 17% no tiene protección contra programas maliciosos y aún así son utilizadas para navegar por Internet. Este es uno de los hallazgos del estudio, que mostró que si bien un 83% de los dueños tienen su equipo con protección básica , muchos están utilizando software con licencias expiradas. El reporte también reveló que los consumidores opinan que un 27% de sus archivos serían imposibles de recuperar y que su valor sería de unos $10.014 (Ruiz, 2012).

La Asociación de Control del Fraude (CFCA), realizó una encuesta en 16 países, a diferentes compañías, un 80% de estas compañías indicó, que las pérdidas que ellas tenían por fraude habían incrementado y el 45% manifestó que habían visto incrementar el fraude dentro de las mismas compañías. Entonces se observa que estos ataques, no solo proviene desde el exterior, sino que dentro de nuestra compañía podemos enfrentar este tipo de situación (Prosic - Blanco, 2011), además recientemente salió una publicación que señala que el 20 o 25% de los ataques de seguridad son producidos desde adentro, de esos casos, la mitad son intencionales, la otra mitad son por ignorancia, entonces es importante mitigar ese 25%, tal vez mitigarla con información, con educación, para concientizar (Prosic- Espinoza, 2011).

En Costa Rica la seguridad informática, aunque aparece con bastante frecuencia en la cotidianidad de las personas y las organizaciones que enfrentan situaciones concretas de ataques informáticos, no ha sido abordada de manera integral ni ha constituido materia de atención explícita por parte de una población y de una institucionalidad que cada vez con mayor frecuencia e intensidad emplea las tecnologías de la información y la comunicación (Prosic - Villasuso, 2011) que estaban desprotegida, incluso no se ha pensado en asignar un presupuesto para que las oficinas brinden seguridad cibernética a las entidades estatales (Prosic - Gamboa, 2011).

El mercado laboral en informática creció al punto que en el 2007 el financiero informó que Costa Rica requería duplicar el numero de graduados, de tal forma que el país requería más de 3000 nuevos informáticos, para responder al aumento de los negocios en el mercado de software, además del estado, agroindustria, comercio y banca, así según Conare para el 2007 se graduaban 1600 profesionales por año (Cordero, 2007).

En 1996 se abrió la Unidad de Delitos Informáticos del Organismo de Investigación Judicial, a partir del cual y hasta el año 2001, habían recibido alrededor de 300 casos, un promedio de 60 ilícitos cada año, según informa Solano (2001) en un

artículo publicado en el periódico La Nación del 1 de junio de 2001. De acuerdo con Lewis (2006), en el año 2004 se reportaron 134 denuncias y en el 2005, 142 denuncias. Lo que muestra una tendencia de aumento en este tipo de delitos (Chen, 2011).

El Ministerio de Ciencia y Tecnología (Micit) había anunciado la creación del Consejo Nacional de Respuesta a Incidentes de la Seguridad Informática (Crisec-cr), que sería la organización "orientada a la implementación de medidas preventivas contra la amenaza a la seguridad cibernética que pueden afectar las tecnologías de información y comunicación del país", en palabras de la entonces ministra del ramo, Eugenia Flores (Fonseca, 2011).

Para esto se han creado diferentes mecanismos e instrumentos destinados a proteger la información como las técnicas de encriptación, técnicas de identificación computarizada, certificados digitales, autoridades certificadoras, firma digital El uso murallas y claves de accesos. Utilización de software que filtran información no deseada. Utilización de licencias de programas, o registro de ellas. Implementar a nivel organizativo y administrativo, protocolos de actuación de seguridad, auditorías, y otros mecanismos en los centros de almacenamiento y procesamiento de datos para proteger los sistemas de información de accesos no autorizados, daños fortuitos y otros (Chen, 2011) .

Existen tres tipos básicos de amenazas: revelación de información, denegación de servicio, o repudio y corrupción de la integridad de los recursos (Amoroso, 1994). el secuestro del control y la suplantación (Prosic- Barrantes, 2011), Para descubrir las posibles vulnerabilidades de los sistemas, diversas empresas e instituciones recurren a firmas externas que tienen avanzados laboratorios y aplican metodologías como lo que se denomina hackeo ético. Estas brindan confidencialidad y tienen el conocimiento y la experiencia necesaria para recomendar qué hacer ante las debilidades (Cordero, 2007).

De acuerdo con los resultados de una encuesta sobre Seguridad y Almacenamiento en las PyMEs realizada por Symantec en 2009, aproximadamente una de cada tres pequeñas y medianas empresas en América Latina ha enfrentado una brecha de seguridad en los últimos doce meses, lo que significa que información importante o confidencial de la compañía se perdió, ha sido robada o consultada sin autorización. En gran medida, estas brechas se deben principalmente a gallas *(sic)* en el sistema, el robo o pérdida de medios de almacenamiento y de medios portátiles como laptops, smartphones o PDAs, las tres principales preocupaciones en materia de seguridad que enfrentan las PyMEs en la región son los virus (77 por ciento), las fugas de datos

(73 por ciento), y el control y la protección de dispositivos portátiles que se conectan a la red de forma remota (72 por ciento). Es decir, las pequeñas y medianas empresas de América Latina parecen estar conscientes de la importancia de la seguridad para sus organizaciones, pero más de la mitad no ha implementado alguna solución de protección de endpoints que les permita proteger sus datos confidenciales contra los distintos riesgos para evitar fugas de datos, aunque las PyMEs entienden los riesgos de seguridad que enfrentan, una cantidad sorprendente de estas empresas en América Latina no cuenta con prácticas elementales de seguridad. De hecho, un 29 por ciento de las pequeñas y medianas empresas encuestadas en la región no tienen la protección más básica – un antivirus. Además, como lo muestra, un 36 por ciento no tiene instalada una solución antispam y 52 por ciento no ha implementado una solución de protección de endpoints (software que protege equipos portátiles, de escritorio y servidores contra malware (prosic Severino, 2011).

Método

El propósito de esta investigación es demostrar si existe en Costa Rica una posibilidad de colocación laboral para los profesionales en seguridad informática por esto se plantea la siguiente pregunta *¿Que posibilidad de colocación tienen los profesionales en seguridad informática en Costa Rica?* Se procede a hacer la búsqueda de la información bibliográfica con el fin de generar temas que sirvan para debatir, durante el proceso de investigación no se encuentra información referente al estado del mercado laboral de estos profesionales en el país, si embargo con la información que se obtiene de los medios se plantean las preguntas y se construye un cuestionario de 8 preguntas.

El cuestionario se aloja en el sitio web de encuestas survey monkey y mediante el siguiente enlace se accede http://www.surveymonkey.com/s/XNPM7FF , el enlace es distribuido vía email a unas 50 personas que laboran y ocupan un puesto de gerencia en pequeñas y medianas empresas (PYMES). El cuestionario cuenta con una breve introducción en la que se describen los objetivos y los motivos de estudios ademas se dan las instrucciones para responder la encuesta, las preguntas son de respuesta única, y en otros casos de respuesta múltiple para facilitar la recolección los datos, es totalmente anónima y se estima que pueda ser contestada en menos de 10 minutos.

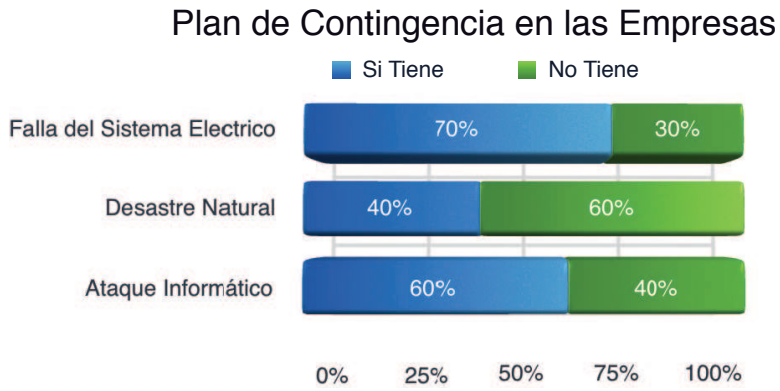
La información suministrada por las personas participantes en el estudio es tratada mediante las herramientas de manejo de datos que ofrece surveymonkey.com para ahorrar tiempo y evitar atrasos, las tablas de datos son descargadas en archivos para Numbers en IOS y los datos son representados en forma gráfica para su fácil comprensión.

La selección de la muestra es a conveniencia y para cumplir con los requisitos del mismo se distribuye entre las empresas con el propósito de que al menos 50 empresas participen de una población total de 62,909 según datos de la caja costarricense del seguro social publicadas en el financiero para lo que se obtiene un margen de error del 6% y se utilizó una confiabilidad del 95% según la herramienta web ncalculators la cual se puede acceder mediante el sigue piense enlace http://es.ncalculators.com/statistics/margin-of-error-calculadora.html

La mayor parte de las empresas encuestados tiene mas de 11 años en el sector de servicios, un 40% de las empresas tienen de 6 a 10 años finalmente un 5% son empresas de menos de 5 años, el 70% de las empresas participantes pertenece al sector de servicios, 20% al sector comercial y un 10% al industrial.

Resultados

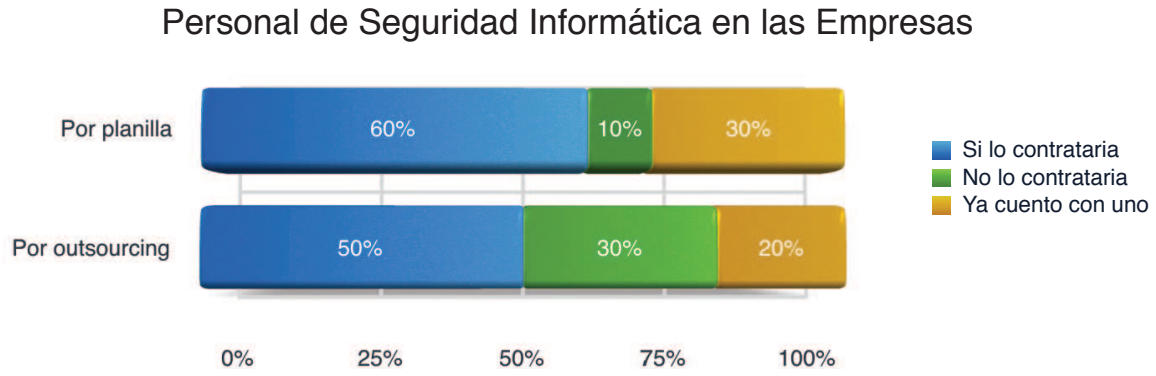
El propósito del gráfico 1 es conocer si las empresas entrevistadas cuentan con un plan de contingencia en caso de recibir un ataque informático, como se puede observar cerca del 60% (30 empresas) aseguran tener un plan de contingencia en cambio un 40% (20 empresas) dice no contar con el plan.



	Si	%	No	%
Falla del Sistema Eléctrico	35	70%	15	30%
Desastre Natural	20	40%	30	60%
Ataque Informático	30	60%	20	40%

Gráfico 1. Fuente Propia

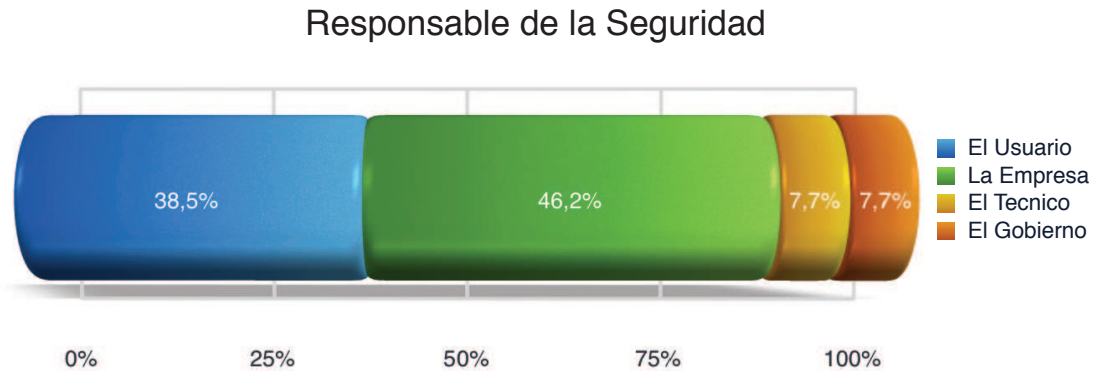
En el gráfico 2 se evalúan las posibilidades que tienen los profesionales en informática de incorporarse a una pequeña o mediana empresa, un 60% de las empresas contrataría a un profesional en seguridad informática por planilla mientras que un 30% manifiesta que ya



	Si lo contrataria		No lo contrataría		Ya cuento con uno	
Por planilla	30	60%	5	10%	15	30%
Por outsourcing	25	50%	15	30%	10	20%

Gráfico 2. Fuente Propia

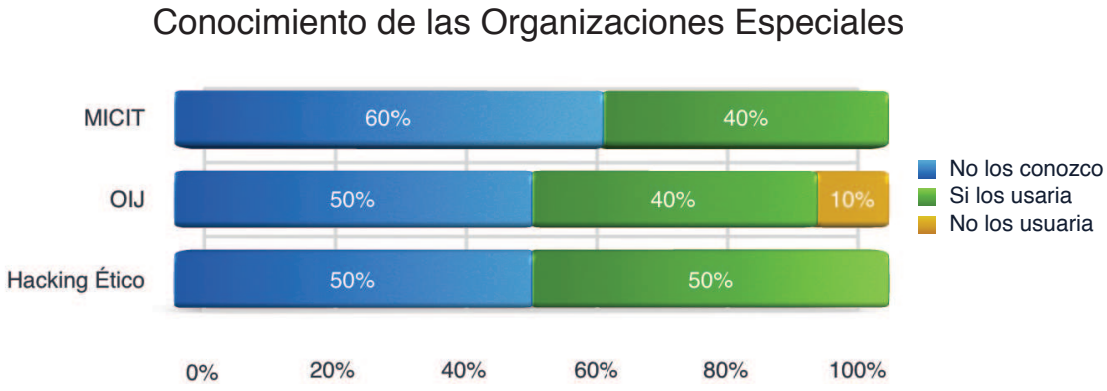
cuenta con esta clase de personal calificado en planilla y un 10% no lo contrataría por planilla. Por otro lado un 50% de la empresas lo contrataría por *outsourcing*, 10% ya cuenta con esta clase de personal contratado por *outsourcing* y un 30% no esta dispuesto a contratar esta clase profesionales.



	Porcentaje	Respuestas
El Usuario	38,5%	25
La Empresa	46,2%	30
El Tecnico	7,7%	5
El Gobierno	7,7%	5

Gráfico 3. Fuente Propia

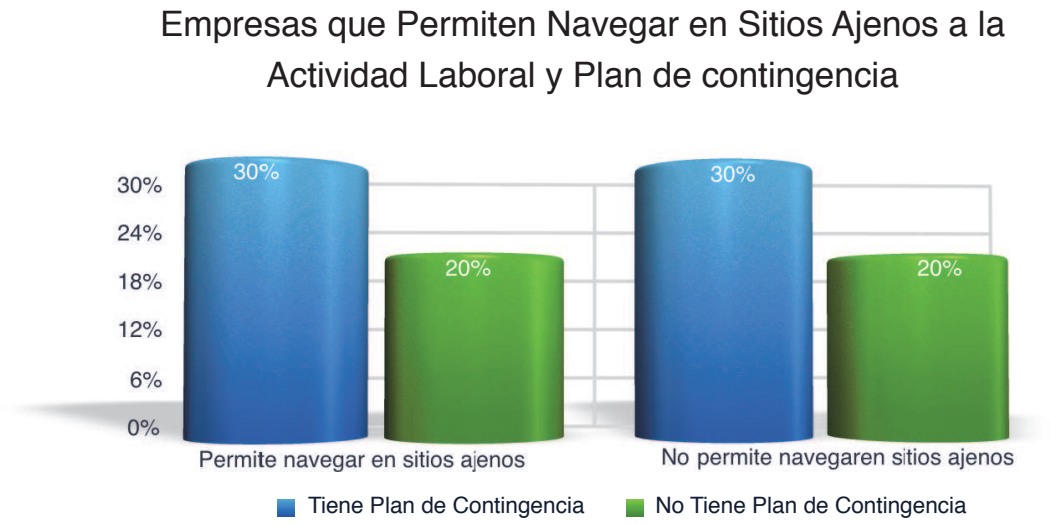
En el gráfico 3 se puede observar como la mayoría de empresas reconocen que en ellas recae la responsabilidad de la seguridad sin embargo un 38.5% manifiesta que la responsabilidad le pertenece también al usuario, un 7.7 % opina que el técnico es responsable de la seguridad y el mismo numero de empresas le achaca esto al gobierno.



	No los conozco		Si los usaria		No los usuaria	
MICIT	30	60%	20	40%	0	0%
OIJ	25	50%	20	40%	5	10%
Hacking Ético	25	50%	25	50%	0	0%

Gráfico 4. Fuente Propia

En el gráfico 4 se mide la percepción de los servicios de dos organismos estatales y los servicios de alguna compañía experta en temas de seguridad, el 60% de las empresas entrevistadas desconoce la existencia de un departamento especializado en seguridad en el MICIT, un 50% desconoce la existencia del mismo en el OIJ y el mismo numero de empresas no se que hay terceros que brindan servicios de *hacking* ético. En el mismo



		Empresas que permiten navegar en sitios ajenos la actividad laboral			
		Si		No	
Plan de contingencia	**Si**	15	30%	15	30%
	No	10	20%	10	20%

Gráfico 5. Fuente Propia

gráfico se aprecia que un 40% usaría los servicios del MICIT, el mismo numero los del OIJ y un 50% usaría servicios de *hacking* ético, sin embargo hay un pequeño 10% que no usuaria los servicios que brinde el OIJ.

En el gráfico 5 se cruzan los resultados de las preguntas que corresponden al plan de contingencia y la posibilidad que tienen los empleados de la empresa de navegar en sitios ajenos a sus actividades laborales, el 50% de las empresas permite que sus empleados navegue en sitios ajenos a sus actividades, sin embargo el 20% de las empresas no posee un plan de contingencia, mientras que un 30% si lo posee, se puede observar el mismo comportamiento dentro de las empresas que no otorgan estas libertades a sus empleados.

	Muy Poco	Poco	Algo	Mucho	Demasiado	Sin Respuesta
Phishing	10%	10%	20%	20%	20%	20%
Scam	20%	0%	30%	30%	0%	20%
Pharming	10%	20%	20%	30%	0%	20%
Troyanos Bancarios	20%	10%	0%	40%	30%	0%
Inteligencia Social	20%	0%	30%	20%	10%	20%
Chat in the middle	20%	10%	0%	40%	10%	20%
Key Loggers	10%	10%	10%	30%	20%	20%
Secuestro	20%	0%	10%	40%	10%	20%
Revelacion de Informacion	10%	0%	10%	40%	40%	0%
Denegacion de Servicio	10%	10%	30%	10%	20%	20%

Tabla1. Fuente Propia

En la tabla1 se puede apreciar como los ataques que mas le preocupan a la mayoría de las empresas son la Revelación de Información y los troyanos bancarios, para otro gran grupo de empresas el secuestro, los *key loggers* y los chats generan cierta preocupación, llama la atención como la inteligencia social casi no genera preocupación y que las empresas desconozcan ataques como la denegación de servicio o el secuestro.

Discusión

Los ataques de denegación de servicio son los que últimamente se mencionan más en los noticieros y demás medios de información, pues han sido muy efectivos para los ciberdelincuentes y sin embargo unas 10 empresas no mostraron un grado de interés en esta clase de ataques, y es que una irrupción de estas puede cause estragos en las compañías que tengan que consumir información desde la web masivamente.

Iniciar analizando este punto se puede observar a un nivel muy superficial la falta de compromiso por parte de algunas empresas en ofrecerle al usuario un ambiente con seguridad para que se realicen las actividades ya sea laborales o personales, y toma mayor importancia cuando se encuentra que 2,534 incidentes de pishing fueron detectados (Oriol, 2012), por cierto que 10 empresas tampoco mostraron algún grado de preocupación para esta modalidad de fraude.

Por otro lado en el 2007 las empresas requerían el doble de personas graduadas en informática y eso lo revelan las cifras de graduados del 2007 donde el mercado laboral pedía el doble de titulados (Cordero, 2007), estos informáticos son jóvenes con ganas de terminar de aprender y futuros eslabones en la guerra cibernética pues bajo sus hombros recae en cierta medida el nivel de seguridad informática de las empresas, y es claro sobre quien recae la responsabilidad pues según los resultados de las encuestas el 46% de las empresas se declaro ser totalmente responsable de brindar seguridad a sus usuarios, otro 38.5% considero que era responsabilidad del usuarios.

En el tema de las responsabilidades muy pocas empresas consideraron al gobierno como una opción solo, un 5%, a pesar de que el año pasado el Ministerio de Ciencia y Tecnología anuncio la creación un ente para implementar medidas de seguridad cibernética (Fonseca, 2011), 60% de las empresas confeso no conocer de este organismo y un 40% se mostró dispuesto a utilizarlo en caso de ser necesario, y no solo existe el Micit, pues el OIJ cuenta con un equipo desde 1996 y para el 2001 ya llevaban 300 casos reportados (Solano 2001), la mitad de las empresas no conocen de este organismo, sin embargo el 40% si lo usuaria y un 10% admitió que no los usuaria los servicios del OIJ, a pesar de este dato para el 2005 la tendencia de casos mostró un ascenso (Chen, 2011).

Es importante conocer el sector comercial cuando nos involucramos con estudios de mercado, muchas de las empresas encuestados pertenecen al sector de servicios, lo que nos indica que están en un contacto muy cercano con el usuario y la mitad de las empresas ya están posicionadas en el país, pues llevan mas de 11 años de creación

Esto es una pista que se podría utilizar para observar la aparición de oportunidades de colocación para los expertos en seguridad, pues a hoy, y según los resultados, 20 empresas que no contratarían personal en seguridad informática, un 10% no lo haría por planilla y un 30% no lo haría por *outsourcing*, hay que analizar que ya 30% de las empresas cuentan con personal de este tipo por planilla y 20% ya lo tiene por *outsourcing*, el 50% de las empresas se mostró dispuesta a contratar profesionales en seguridad en la modalidad de *outsourcing* y 60% lo haría por planilla, es allí donde debemos ver claramente pues esto nos indica una apertura, pequeña, hay que ser realistas y ver el suelo que pisamos.

Es importante hacer mención que dentro de los elementos para brindar seguridad se han creado mecanismos con el propósito de proteger la información, así se pueden mencionar las técnicas de encriptación, certificados digitales, *firewalls*, eso motivo a conocer si las empresas manejaban un plan de contingencia para los ataques informáticos, y se cruzo esta pregunta con una tercera para conocer que empresas permiten que sus empleados naveguen libremente incluso a sitios que no tengan que ver con la actividad laboral, un 20% de las empresas dijo no contar con un plan de contingencia y permiten que sus empleados naveguen libremente a sitios que nada tienen que ver con su trabajo.

En la otra esquina el escenario cambia, a las empresas que no permiten la navegación a sitios exteriores y que no tienen plan de contingencia, acá hablamos de un 20%, cualquiera diría que no hay mucho peligro, el error esta en relajarse por que los estudios demuestran que del 20% al 25% de los ataques son producidos desde desde adentro de la empresa (Prosic , 2011), bien hay que apuntar otra falencia y es que la mayoría de gente piensa que con un *firewalls* y un anti virus ya están protegidos, el 95% de las empresas dice confiar en solo el anti virus, según websense (Ruiz, 2012).

Conclusiones y Recomendaciones

Costa Rica como país apenas esta dando sus primeros pasos en cuanto a tecnologías de información, un ejemplo de ello es que a nivel estatal ni siquiera se ha pensado en asignar un presupuesto para que las oficinas brinden seguridad cibernética a las entidades estatales (Prosic, 2011). En los resultados que se aprecia que un porcentaje considerable de empresas no cuentan con plan de contingencia producto de la ausencia de profesionales en seguridad informática dentro de las empresas..

Aunque seamos un país pequeño, con poca capacidad de tecnología, debemos avanzar en la creación de oportunidades de desarrollo para expertos en seguridad informática y por que Costa Rica sí es un país donde hay posibilidades de desarrollo en este campo es por ello que las universidades deberían comenzar a preparar esta clase de profesionales.

Como lo menciona el Prosic las campañas son importantes para que las personas a cargo de las empresas comprendan sobre los peligros que se generan en las redes gracias a la falta de información es así como los resultados demuestran el desconocimiento debido a que varias personas no contestaron varias opciones de la pregunta sobre las amenazas que mas le preocupan, por tanto el Gobierno o algún ente como el Colegio de Informáticos podría realizar estas campañas de información.

De la misma forma los resultados mostraron el desconocimiento sobre los organismos del OIJ y el MICIT y su funcionamiento. Estas son organizaciones que han sido creadas para manejar los temas de seguridad informática por lo que también se deberían hacer campañas de información para que los ciudadanos sepan como utilizar sus servicios y aun mas importante a quien acudir cuando sea necesario.

En caso de que las empresas no puedan abrir el espacio para que un experto en seguridad labore dentro de su empresa por algún motivo económico o de espacio podrían contratar los servicios de una empresa de *hacking* ético para que tengan un nivel de conocimiento de como esta la seguridad en su empresa pues en el financiero del 2007, Carlos cordero menciona que ellas tienen conocimiento y experiencia. La mitad de las empresas dijo que desconocía de esta clase de servicios.

Los resultados son muy claros y muestran que un 60% de las empresas participantes en este estudio estaban dispuestas a contratar personal de seguridad informática bajo la forma de *outsourcing*, esto demuestra una posibilidad para que los interesados en laborar en seguridad informática puedan colocarse dentro del mercado. Se tendrían que hacer estudios de un alcance mayor para certificar el nivel de apertura que existe actualmente en el mercado.

Bibliografía

Castro, J. (2002, Marzo 18). Costa Rica atrae firmas de seguridad informática. La República, p. 4B.

Cordero , C. (2006, Octubre 20). Empresas comenten graves errores de seguridad informática. En elfinancierocr.com. Recuperado en Junio 1, 2012, de http://www.elfinancierocr.com/ef_archivo/2006/octubre/29/lomasreciente868180.htmlcc

Cordero Pérez , C. (2007, Marzo 26). Costa Rica requiere duplicar graduados informáticos. El Financiero, p. 26.

Cordero, C. (2007, Julio 8). Un examen a la seguridad informática de su empresa . En elfinancierocr.com. Recuperado en Junio 1, 2012, de http://www.elfinancierocr.com/ef_archivo/2007/julio/08/tecnologia1146046.html_

Chenk, S (2008, febrero 8). Alcance de la legislación costarricense en materia de delitos informáticos: Un análisis preliminar. Recuperado en Junio 1, 2012, de Inter Sedes. Vol. VIII

Fonseca, P. (2011, Noviembre 8). Costa Rica carece de protocolo para responder a ataques informáticos. En nacion.com. Recuperado en Junio 1, 2012, de http://www.nacion.com/2011-08-11/Tecnologia/costa-rica-carece-de-protocolo-para-responder-a-ataques-informaticos.aspx

Oriol, M. (2010, Octubre). Solo cuestión de sentido común ?.En Seguritecnia. Recuperado en Junio 1, 2012, de http://www.borrmart.es/articulo_seguritecnia.php?id=2428

Pascual, A. (2012, Enero 20). Anonymous lanza el mayor ataque informático contra EEUU y la industria musical. En elconfidencial.com. Recuperado en Junio 1, 2012, de http://www.elconfidencial.com/tecnologia/2012/01/20/anonymous-lanza-el-mayor-ataque-informatico-contra-eeuu-y-la-industria-musical-1720/

Prosic (2011, Octubre) .Ciberseguridad en Costa Rica. Recuperado en Junio 1, 2012, de Impresión Gráfica del Este S.A

Ruiz Vega, C. (2012, Mayo 30). Casi dos de cada 10 internautas navega desde equipos sin protección contra malware. En elfinancierocr. Recuperado en Junio 1, 2012, de http://www.elfinancierocr.com/ef_archivo/2012/junio/03/tecnologia3193133.html

Vindas, L. (2012, Junio 14). MEIC desconoce cuántas pymes existen y da poca cobertura al sector. El financiero. Recuperado en Agosto 3, 2012, de http://www.elfinancierocr.com/ef_archivo/2012/junio/17/negocios3210314.html

Henderson, J. (2012, Agosto 2). Trend Micro report reveals cyber-attack increase. Techday. Recuperado en Agosto 4, 2012, de http://www.techday.co.nz/itbrief/news/trend-micro-report-reveals-cyber-attack-incre/24307/2/

Anexos

Respuestas Tabuladas

1. Cuenta su empresa con un plan de contingencia en caso de ?

	Si	No	Response Count
Falla del Sistema Electrico	35	15	50
Desastre Natural	20	30	50
Ataque Informático	30	20	50

2. Con respecto al personal de seguridad informática?

	Si lo contrataria	No lo contrataria	Ya cuento con uno	Response Count
Por planilla	30	5	15	50
Por outsourcing	25	15	10	50

3. Considera que las medidas de seguridad en las redes son responsabilidad de?

Answer Options	Response Count	Response Percent
El Usuario	25	38,5%
La Empresa	30	46,2%
El Tecnico	5	7,7%
El Gobierno	5	7,7%

4. Muchas empresas en el mundo contratan servicios de hackeo ético para asegurarse de que sus redes estén correctamente protegidas, así mismo el OIJ y el MICIT cuentan con departamentos especiales para los ataques informáticos, con lo anterior usted?

Answer Options	No los conozco	Si los usaria	No los usuaria	Response Count
MICIT	30	20	0	50
OIJ	25	20	5	50
Hacking Ético	25	25	0	50

5. De los siguientes ataques califique de 1 a 5, siendo 5 el ataque que mas le preocuparía

Answer Options	Muy Poco	Poco	Algo	Mucho	Demasiado	Sin Respuesta	Response Count
Phishing	5	5	10	10	10	10	50
Scam	10	0	15	15	0	10	50
Pharming	5	10	10	15	0	10	50
Troyanos Bancarios	10	5	0	20	15	0	50
Inteligencia Social	10	0	15	10	5	10	50
Chat in the middle	10	5	0	20	5	10	50
Key Loggers	5	5	5	15	10	10	50
Secuestro	10	0	5	20	5	10	50
Revelación de Información	5	0	5	20	20	0	50
Denegación de Servicio	5	5	15	5	10	10	50

6. Tienen sus empleados posibilidad de navegar en sitios ajenos a su actividad laboral?

Answer Options	Response Percent	Response Count
Si	50,0%	25
No	50,0%	25

7. Cuantos años tiene su empresa?

Answer Options	Response Count	Response Percent
menos de 5	5	10,0%
de 6 a 10	20	40,0%
mas de 11	25	50,0%

8. En cual área califica su empresa?

Answer Options	Response Count	Response Percent
Servicios	35	70,0%
Industrial	5	10,0%
Comercial	10	20,0%

El presente cuestionario forma parte de una investigación sobre el mercado laboral, para el cual se ha tomado la siguiente pregunta de Investigacion ¿Que oportunidad de colocación tienen los profesionales en Seguridad Informatica en Costa Rica?. El cuestionario es fácil y rápido de completar, esta destinado a PYMES, se estima que usted deberá disponer de unos 10 minutos o menos para responderlo.

Su participación es voluntaria, no tiene que darnos su nombre, los datos que nos facilite serán publicados y serán trabajados para responder la pregunta planteada. Le solicitamos contestar de forma objetiva debido a que se desea contar con un análisis actual sobre la situacion laboral de las personas que se estan desarrollando en este campo.

Si tiene alguna pregunta sobre la naturaleza, los objetivos de la encuesta o sobre el cuestionario propiamente dicho y si desea una copia de esta Investigación, puede comunicarse con Felix Sandoval Vargas a su correo electrónico: felix.sandoval@hotmail.com.

Muchas gracias por su colaboración.

1. Cuenta su empresa con un plan de contingencia en caso de ?

	Si	No
Falla del Sistema Electrico	○	○
Desastre Natural	○	○
Ataque Informático	○	○

2. Con respecto al personal de seguridad informatica?

	Si lo contrataria	No lo contrataria	Ya cuento con uno
Contrataría uno por planilla	○	○	○
Contrataría uno por outsourcing	○	○	○

3. Considera que las medidas de seguridad en las redes son responsabilidad de?

☐ El Usuario ☐ La Empresa ☐ El Tecnico ☐ El Gobierno

4. Muchas empresas en el mundo contratan servicios de hackeo ético para asegurarse que sus redes esten correctamente protegidas, así mismo el OIJ y el MICIT cuentan con departamentos especiales para los ataques informáticos, con lo anterior usted?

	No los conozco	Si los usaría	No los usuaría
Usaría los servicios del MICIT	○	○	○
Usaría los servicios del OIJ	○	○	○
Usaría los servicios de hacking ético	○	○	○

5. De los siguientes ataques califique de 1 a 5, siendo 5 el ataque que más le preocuparía

	1	2	3	4	5
Phishing	○	○	○	○	○
Scam	○	○	○	○	○
Pharming	○	○	○	○	○
Troyanos Bancarios	○	○	○	○	○
Inteligencia Social	○	○	○	○	○
Chat in the middle	○	○	○	○	○
Key Loggers	○	○	○	○	○
Secuestro	○	○	○	○	○
Revelación de Información	○	○	○	○	○
Denegación de Servicio	○	○	○	○	○

6. Tienen sus empleados posibilidad de navegar en sitios ajenos a su actividad laboral?

- ○ Si
- ○ No

7. Cuántos años tiene su empresa?

- ○ menos de 5
- ○ de 6 a 10
- ○ mas de 11

8. En cual área califica su empresa?

- ○ Servicios
- ○ Industrial
- ○ Comercial

Colocación Laboral de Profesionales en Seguridad Informática

ULACIT
Félix Sandoval Vargas
felix.sandoval@hotmail.com

¿Qué posibilidad de colocación tienen los profesionales de seguridad informática en Costa Rica?

Introducción

El mundo a evolucionado drásticamente desde la aparición de las computadoras, las cuales han traído muchos beneficios, sin embargo con ellas también han nacido peligros para los usuarios de la red, estas amenazas navegan de forma silenciosa entre los bytes de la telaraña de servidores y computadoras poniendo en jaque tanto a empresas como a personas. En el 2002 en Costa Rica "las perdidas por infecciones de virus informáticos pudieron haber llegado a más de $23 millones en el mercado nacional", varias compañías como Bysupport, Computer Associates, Sidif abrieron oficinas en el país gracias a sus posibilidades de desarrollo por la ausencia de presupuesto para la seguridad informática, (Castro J, 2002).

Referencias

Son cada vez más sofisticadas las tecnologías que utilizan los delincuentes por la Red(phishing, scam, pharming, troyanos bancarios, inteligencia social, chat in the middle, keyloggers...). En el quinto Informe de Fraude Online y Cibercirmen de S21sec, la compañía española informaba de que, durante 2009, detectaron y solucionaron un total de 2.534 incidentes de phishing, códigos maliciosos, redirectores y otras actividades calificadas de fraude online, dirigidas a entidades en España. Según la firma, el phishing continua siendo una de las principales preocupaciones de las empresas, ya que supuso el 63 por ciento del total de incidentes en 2009, y se mantiene respecto al año anterior (62 por ciento) (Oriol, 2012).

De acuerdo con los resultados de una encuesta sobre Seguridad y Almacenamiento en las PyMEs realizada por Symantec en 2009, aproximadamente una de cada tres pequeñas y medianas empresas en América Latina ha enfrentado una brecha de seguridad en los últimos doce meses . Esta brecha se debe principalmente a gallas (sic) en el sistema, el robo o pérdida de medios de almacenamiento y de medios portátiles como laptops, smartphones o PDAs, las tres principales preocupaciones en materia de seguridad que enfrentan las PyMEs en la región son los virus (77 por ciento), las fugas de datos (73 por ciento), y el control y la protección de dispositivos portátiles que se conectan a la red de forma remota (72 por ciento). (Prosic, 2011).

Método

Se procede a hacer la búsqueda de la información bibliográfica con el fin de generar temas que sirvan para debatir, con estos se plantean las preguntas y se construye un cuestionario de 8 preguntas el cual se aloja en el sitio web de encuestas survey monkey , el enlace es distribuido vía email a unas 50 personas que laboran y ocupan un puesto de gerencia en pequeñas y medianas empresas (PYMES).

- Margen de error: 6%
- Cantidad de la Muestra: 50
- Confianza: 95%
- Población: 62,909 (CCSS)

Conclusiones y Recomendaciones

En los resultados se aprecia que un porcentaje considerable de empresas no cuentan con plan de contingencia producto de la ausencia de personal de seguridad informática dentro de la empresa.

Los resultados son muy claros y muestran que un 60% de las empresas participantes en este estudio estaban dispuestas a contratar personal de seguridad informática bajo la forma de *outsourcing*, esto demuestra una posibilidad para que los interesados en laborar en seguridad informática puedan colocarse dentro del mercado. Se tendrían que hacer estudios de un alcance mayor para certificar el nivel de apertura que existe actualmente en el mercado.

Resultados

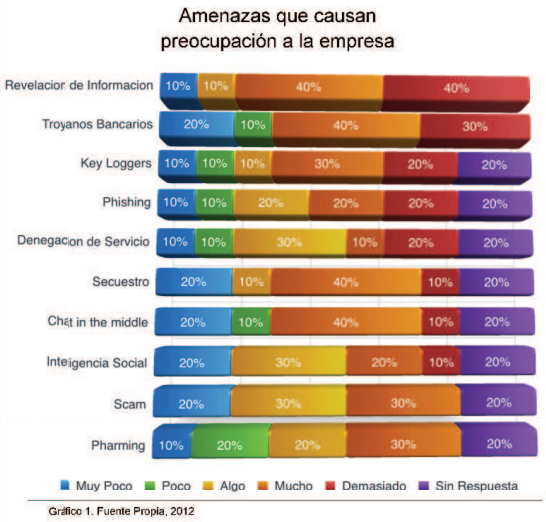


Gráfico 1. Fuente Propia, 2012

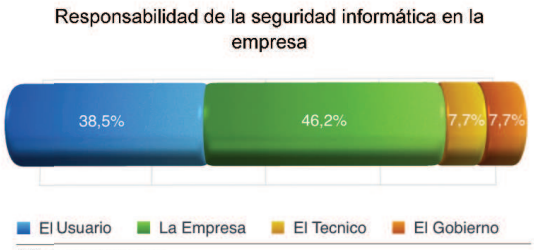


Gráfico 2. Fuente Propia, 2012

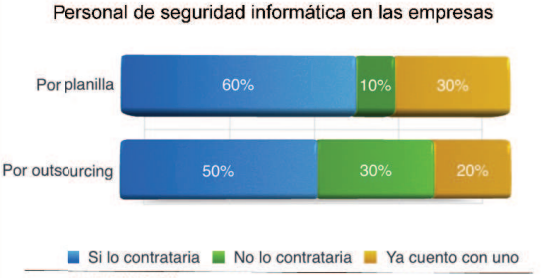


Gráfico 3. Fuente Propia, 2012

Referencias Bibliográficas

- Fonseca, P. (2011, Noviembre 8). Costa Rica carece de protocolo para responder a ataques informáticos. En nacion.com. Recuperado en Junio 1, 2012, de http://www.nacion.com/2011-08-11/Tecnologia/costa-rica-carece-de-protocolo-para-responder-a-ataques-informaticos.aspx
- *Prosic (2011, Octubre) .Ciberseguridad en Costa Rica. Recuperado en Junio 1, 2012, de Impresión Gráfica del Este S.A*
- *Henderson, J. (2012, Agosto 2). Trend Micro report reveals cyber-attack increase.Techday. Recuperado en Agosto 4, 2012, de http://www.techday.co.nz/itbrief/news/trend-micro-report-reveals-cyber-attack-incre/24307/2/*