Seguridad Informática en las Organizaciones Paso Lento pero Seguro

Reyes Alvarez, Marcos Fernando.
mreyes@unisangil.edu.co
Unisangil

Resumen— Desde hace muchos años las empresas se empezaron a sistematizar, reemplazando las máquinas de escribir por computadoras, las cuales requerían en su momento un gran espacio para su ubicación, y contaban con gran cantidad de cables y conexiones, pantallas con resolución de 800x600 que eran la última moda en los años 90, con su gran parecido a los televisores de la época, con memorias ram de 24 megas y discos duros de 4 Gigabytes así como empezaron a reemplazar las tradicionales máquinas de escribir, y fueron empezando a capacitar al personal de las empresas en el uso de Microsoft Word, Excel, Access, Power Point, entre otros, siendo la suite de Officce la herramienta tecnológica más innovadora para el trabajo en las oficinas. Ya un tiempo después, se fueron fortaleciendo las intranets, y con la aparición de la internet, el mundo y el trabajo se empezó a globalizar. Más adelante fueron apareciendo nuevas herramientas y fuentes de información; y con ellos los delincuentes informáticos, los cuales empezaron a cambiar el paradigma de los departamentos de sistemas, los cuales por muchos años tenían como prioridad exclusiva el servicio, pero en la actualidad la Seguridad Informática ha tomado una importancia vital en las organizaciones, y se ha ido insertando paulatinamente entre las prioridades corporativas, aunque muchas direcciones de empresas aún no comprendan la importancia de crear este rol dentro de las mismas.

Índice de Términos— Análisis de Riegos, Departamento de Sistemas, Incidentes de Seguridad, Organizaciones,

I. INTRODUCCIÓN

Los delitos informáticos han sido unas de las palabras que hace unos años no pasaban por la mente de nadie, y mucho menos que tuvieran la trascendencia que llegarían a tener en la actualidad. Incluso aun en muchas organizaciones cuando se les pregunta por la "seguridad de la información de su empresa", responden diciendo: "que ya tienen un ingeniero de sistemas, que hace todas esas cosas", pero la realidad es otra, ya que muchas veces confunden la seguridad de la información con la administración de los dispositivos y la disponibilidad de los servicios informáticos que se realiza para garantizar el normal funcionamiento de la compañía, pero en cuanto a las prácticas de seguridad en realidad dejan mucho que pensar.

Por eso es importante realizar presentaciones gerenciales de lo que es la seguridad de la información en las organizaciones y poderla presentar a los altos mandos de las empresas, mostrándoles el panorama desde el punto de vista que les impacta de una forma más fuerte, desde lo económico, de tal forma que puedan comprender que no es suficiente con tener a un profesional en sistemas que administre la infraestructura tecnológica para garantizar que la empresa está segura.

La siguiente fase después del reconocimiento de las falencias, es la toma de decisiones, por lo tanto muchas empresas que antes no creían en la seguridad de la información, solo cuando han sido fuertemente impactadas por un evento que afecta la organización y su patrimonio, es cuando deciden tomar la decisión de implementar medidas de seguridad de la información, ya sea por asesorías de un tercero o mediante la creación del cargo del especialista en este campo dentro de la entidad.

Un aspecto muy importante por analizar, es la forma de presentar las ideas, pues la mayoría de las ocasiones el profesional en sistemas está programado mentalmente para sostener conversaciones con un vocabulario técnico, pero está claro que los tiempos han cambiado y el profesional debe ser un individuo integral que

pueda ser sometido a los diferentes retos, entre ellos poder sustentar los aspectos que conoce técnicamente de un modo formal, con lenguaje gerencial, a punto de llegar a ser convincente para cualquier persona y no solo para quien maneja su mismo universo profesional.

En el transcurso del tiempo la tecnología ha pasado por diversas etapas evolutivas, de esta forma, el ser humano ha buscado facilitar las actividades y procesos de la vida diaria, y ha encontrado ayudas innovadoras. En algún momento de la evolución se crearon distintos artefactos, tales como despertadores, relojes, celulares, viper, radios, televisores, grabadoras, y así diferentes elementos que con el paso del tiempo fueron haciendo parte del diario vivir. Luego de la aparición de los primeros dispositivos tecnológicos, aparecieron las computadoras como un elemento comercial, pasando de ser elementos inicialmente de lujo para unos pocos, a convertirse en herramientas que en la actualidad se pueden adquirir fácilmente, como por ejemplo tablets, portátiles, celulares inteligentes, entre otros. Dejando de ser un placer más, para convertirse en elementos indispensables en la vida cotidiana, para despertarse, para comunicarse, para divertirse, trabajar, etc [1]. De la misma forma la tecnología aplicada a las organizaciones ha cambiado, y ha han pasado de usar los elementos informáticos más básicos, a usar y requerir sistemas informáticos mucho más completos y mecanismos de control de la seguridad muy variados para aplicarlos en la protección de su activo más preciado, la información.

II. XVI Encuesta Nacional de la Seguridad Informática

A. Dependencia de la Seguridad

Así como se indica en la introducción de este documento, se ha venido dando un incremento en la aceptación de los roles de la seguridad de la información en las organizaciones en los últimos años, donde se tienen datos estadísticos muy significativos, los cuales abren el espacio a nuevos roles dentro de las empresas para los profesionales de la seguridad. *[2]*

Entre los años 2014 y 2016 los sectores que más han incrementado los procesos de seguridad de la información y han vinculado a profesionales en estas áreas son: Servicios financieros y banca, Consultoría Especializada, Gobierno / Sector Público, Educación, Otros, Telecomunicaciones, Salud. *[2]*

En el 2015 no se tenían especificados los cargos de seguridad de la información en un 17% de las organizaciones, y para el 2016 este porcentaje ha bajado a 13%, lo cual indica que las empresas han venido formalizando los cargos de seguridad y abriendo espacios a estos roles dentro de las mismas. *[2]*

B. Roles

Algunos de los roles que se vienen definiendo últimamente en las organizaciones en cuanto a seguridad de la información son:

(42%) Analista de seguridad de la información. *[2]* Es un perfil que abarca el análisis de la seguridad de la información en general dentro de la compañía, no solamente lo relacionado a la tecnología, sino la información física, como documentos, contratos, bodegas de archivos, papel reciclable, etc.

(37%) Analista de seguridad informática (Redes, Información, Aplicaciones). *[2]* Contempla la buena administración de la información que se encuentra alojada en medios informáticos.

(17%) Primer Respondiente / gestionador de incidentes de seguridad. *[2]* Este rol está más enfocado hacia la ocurrencia de incidentes, donde este perfil es el encargado de ser quien se hace cargo de la evidencia y de protegerla para garantizar su integridad, de forma que no se rompa la cadena de custodia.

(27%) Oficial de Seguridad informática (ISO). *[3]* tiene la función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la organización.

(17%) Experto Forense Digital / Investigador Forense Digital. *[2]* Este rol es de aquel que toma las evidencias informáticas recaudadas en un caso judicial, y se encarga de realizar el análisis forense de la evidencia digital, de forma que presente su informe para ser usado como herramienta de los abogados defensores o la fiscalía en los casos judiciales. *[4]*

(17%) Especialista en ciberseguridad y ciber defensa. La cibeseguridad y ciberdefensa es un concepto que ha aparecido en razón a los hechos que se han presentado en los últimos años con los ciberataques en cadena de las comunidades de hackers como lulzsec y anomymous contra las organizaciones y gobiernos, teniendo en algunos casos intereses políticos, económicos, sociales entre otros. *[5]*

(48%) Oficial de la seguridad de la información Ciso. La versión 5 de COBIT, estable que este director es el responsable de la seguridad de la información en todos aspectos y hace parte de la gestión. Diseñar los controles de seguridad para que sean gestionados por los dueños de los procesos del área de TI. Las evaluaciones que ejecute este director pertenecen al auto control ya que las evaluaciones hacen parte del gobierno. *[6]*

(19%) Oficial de riesgos corporativos (CRO). Este rol ya involucra lo que es la gestión de riesgos de la empresa, lo cual empieza a tomar mucha importancia ya que las aseguradoras están incluyendo la información como un factor a asegurar más, y estos analistas de riesgos deben garantizarle a la empresa que si ocurre algún incidente, ellos hayan tomado las medidas necesarias para prevenir los incidentes, y las aseguradoras deban cumplir con sus compromisos de responder por los bienes asegurados, que para este caso es la información. *[7]*

(9%) Otros

(26%) Auditor de seguridad de la información. *[8]*

(22%) Ingeniero especialista en pruebas de seguridad informática. Este rol ha sido uno de los primeros que se vislumbró dentro de la seguridad de la información, ya que apareció como producto de las incursiones que realizaron los piratas informáticos y malware en búsqueda de vulnerar a las organizaciones, las cuales ha recurrido a este rol para comprobar que tan comprometidos pueden estar frente a un ataque informático. *[9]*

(15%) Arquitecto de seguridad. Este rol tiene una visión más generalizada de la seguridad de la información en las organizaciones, saliendo un poco de lo técnico e inclinándose más hacia la gestión estratégica y la planeación de la seguridad corporativa. *[2]*

(12%) Oficial de cumplimiento corporativo (CCO).

(21%) Consultor de seguridad de la información.

Entre 2014 y 2015 las responsabilidades del área de seguridad de la información frente a la compañía oscilaban en un promedio de 40%, y para el 2016, estas responsabilidades alcanzan un aproximado del 50%, lo cual es una muestra de que las juntas directivas de las empresas están dándole una mayor importancia a las opiniones de los encargados de la seguridad, en pro de la toma de decisiones trascendentales para la misma, y que pueden afectar factores como el económico, humano, ambiental, imagen corporativa, entre otros. *[2]*

C. Asignación / Proyección Presupuesto

Este factor también es muy importante e interesante para tener en cuenta, debido a que años atrás, las directivas de las organizaciones

proyectaban para el departamento de sistemas un servidor, lo más económico posible, los equipos de cómputo y la red, de ahí en adelante para muchas compañías cualquier inversión adicional en tecnología era un gasto innecesario, o simplemente un "juguete más" que solicitaban los encargados de sistemas. Pero desde el momento en que empezaron a aparecer las amenazas informáticas, y las empresas empezaron a ser víctimas de ataques, y a su vez sus activos se han visto comprometidos, han ido entendiendo que la seguridad informática no es un gasto, sino una inversión. *[2]*

Entre los años 2014 y 2015, la mayoría de las empresas tenían un presupuesto seguridad entre 20.000 y 110.00 dólares, y en el periodo entre 2015 y 2016, bajo el porcentaje de empresas con presupuesto mencionado en el rango anterior y aumento de un 7% a un 12% aproximadamente la cantidad de empresas con presupuesto de más de 130.000 dólares en seguridad de la información. Y aún queda cerca de un 45% de las empresas de las cuales no se conoce esa información, por lo tanto son mercados potencialmente destinados para explotar. *[2]*

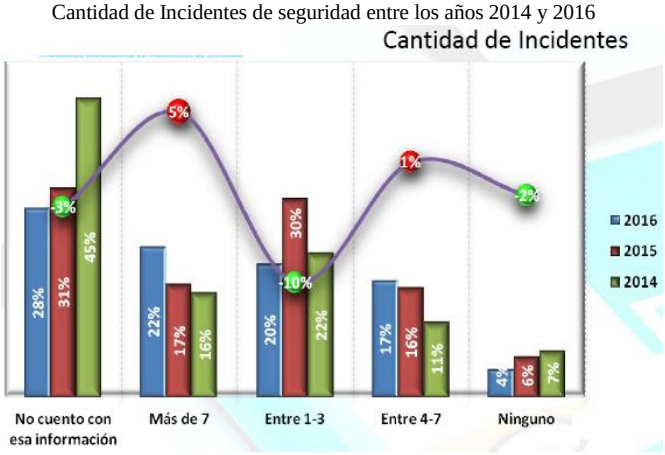
D. Cantidad de incidentes

Los incidentes de seguridad son aquellos eventos que en un principio las organizaciones ignoraban, pero hoy en día aunque la mayoría de las veces lo manejen de forma confidencial, no deja de ser algo supremamente preocupante para quienes dirigen las empresas. *[2]*

Por lo tanto el análisis, prevención y gestión de incidentes es un factor determinante en las organizaciones actuales, ya que de esto depende que se garantice la autenticidad, la confidencialidad y la integridad de su información, y que se vea lo menor comprometida posible frente a los diferentes sucesos que ocurren dentro de la empresa. *[2]*

En el 2014 el 7% de las empresas mencionó no tener ningún incidente de seguridad, en el 2015 en 6%, y en el 2016 el 4% de las empresas, cifra que indica que ha bajado considerablemente el número de empresas que no son víctimas de incidentes de seguridad. *[2]*

FIGURA I
Cantidad de Incidentes de seguridad entre los años 2014 y 2016



XVI Encuesta Nacional de Seguridad/Ciberseguridad

Entre 1 y 3 incidentes de seguridad en las organizaciones se presentaron en el 2014 en el 22% de las empresas, en el 2015 en el 30% y en el 2016 en el 20%, demostrando que en el 2015 hubo una subida exponencial de los incidentes de seguridad, aunque en 2016 apenas va en la mitad y si continua el incremento podría igualarlo, ya que lo corrido de la mitad de año 2016 ya está a solo una diferencia de 2% de empresas que sufrieron esta cantidad de incidentes en 2014. *[2]*

Entre 4 y 7 incidentes reportaron tener en el 2014 el 11% de las empresas, en el 2015 el 15%, y en el 2016 el 17% de las organizaciones, lo cual muestra un aumento en 2 años del 6% de las empresas que tuvieron en un año este margen de incidentes, lo cual ya empieza a ser un valor alto dependiendo de la gravedad de los incidentes, y además, si se considerase que fuera una ocurrencia mensual, se podría decir que en promedio es un incidente cada poco menos de dos meses. *[2]*

Más de 7 incidentes de seguridad ocurrieron en el 2014 en el 16% de las empresas, en el 2015 en el 17%, y en la primera mitad de año del 2016 en el 22%. *[2]*

Y no se tiene información precisa de la ocurrencia de incidentes de seguridad en el 2014 en un 45%, en

TABLA I
INCIDENTES MÁS REPRESENTATIVOS ENTRE 2015 Y 2016

Incidente	2016	2015	Dif
Instalación de software no autorizado.	38%	51%	
Virus / Caballos de Troya.	35%	37%	
* Phishing	35%	29%	6%
Accesos no autorizados al web	20%	23%	
* Negación de Servicio (DOS/DDOS)	20%	14%	6%
* Manipulación de aplicaciones de software	17%	13%	4%
+ Ramsomware	17%	NA	17%
* Acciones de ingeniería social	12%	10%	2%
* Fraude electrónico	12%	8%	4%
* Pérdida de la integridad de la información	12%	9%	3%
Robo de elementos de hardware (notebooks…)	12%	18%	
* Robo de datos	11%	9%	2%
Ataque de aplicaciones Web (Sql Inyection, XSS, Directory…)	11%	14%	
Pérdida / fuga de información crítica	10%	14%	
* Incidentes relacionados con la privacidad de los datos	10%	5%	5%
* Suplantación de identidad	9%	8%	1%
* Ciber ataques (APT o ataques dirigidos, denegación de …)	8%	5%	3%
Monitoreo no autorizado de tráfico	5%	7%	
Ninguno	4%	6%	
Otra	4%	2%	
Pharming	2%	0%	
Espionaje	1%	1%	

* Incidentes que han aumentado de 2015 a 2016
+ Incidentes nuevos

el 2015 en un 31% y en la primera mitad del 2016 en un 28%, lo cual señala que en años anteriores era casi del 50% el desconocimiento de la seguridad en las organizaciones, y por ende ocurrían los incidentes de seguridad sin ser identificados y clasificados, además de desconocerse el impacto que tenían dentro de las mismas, y que ya para el presente año 2016 es menor la cantidad de empresas que no están dando un manejo a la seguridad de la información, o que lo mantienen de forma clasificada por temor a generar pánico entre sus clientes, lo cual es contraproducente pues en esta época es mucho mejor para un cliente saber que una empresa está preparada en cuanto a la seguridad de la información. *[2]*

E. Tipo de incidentes

Así como es importante conocer los diferentes roles de los profesionales en seguridad de la información en la actualidad, y los porcentajes de empresas que han reportado incidentes de seguridad, también es muy importante conocer cuáles son los tipos de incidentes que las han afectado. *[2]*

Entre algunos aspectos a destacar se puede mencionar que algunos tipos de incidentes se han disminuido entre el 2015 y 2016, entre los cuales se pueden mencionar: La instalación de software no autorizado, accesos no autorizados a la web, robo de elementos de hardware, ataque de aplicaciones web, pérdida / fuga de información crítica, entre otras. esta información permite ver que se ha avanzado en algunos aspectos relacionados con los controles, el establecimiento de políticas y el aseguramiento de las organizaciones, sin embargo el hecho de que haya bajado el índice no indica que hayan desaparecido este tipo de incidentes, puesto que accesos no autorizados a sistemas informáticos, robos de información, entre otros tipos de incidentes se siguen presentando así no sea en cantidad de eventos, los que se presentan son bastante graves y afectan a las empresas en un alto porcentaje, de forma que ponen en riesgo el libre desarrollo corporativo y pone a temblar la relación de confianza de la empresa ante sus clientes, dando la sensación de inseguridad. *[2]*

En cuanto a los tipos de incidentes que se incrementaron en el 2016, se encuentran: phishing, negación de servicio, manipulación de aplicaciones de software, ramsomware, acciones de ingeniería social, fraude electrónico, pérdida de integridad de la información, robo de datos, incidentes relacionados con la privacidad de los datos, suplantación de identidad, ciber ataques (Apt o ataques dirigidos …), entre otros. *[2]*

Esta información indica algunos aspectos a analizar, empezando por el phishing, donde se siguen presentando este tipo de sucesos, e incluso como lo muestra la tabla es una de las técnicas delictivas más antiguas usadas para realizar estafas a las personas, pero se percibe que ha evolucionado y se ha mantenido infiltrado haciendo caer permanentemente en el engaño a los cibernautas. *[2]*

La denegación de servicio se volvió muy

popular en especial por parte de anonymous, y otras organizaciones secretas en contra de las grandes marcas a nivel mundial que están en la web, y a medida que fueron realizándose investigaciones especializadas para identificar a ciertos elementos que estaban vinculados a las mismas, y en cierta forma se logró disminuir el gran impacto que estaban logrando en su momento estas organizaciones clandestinas, pero a su vez ocasionó una mutación en el modus operandi, pasando de ser ataques en masa a grandes objetivos, a dividir sus ataques en objetivos más pequeños, y a su vez haciéndolo de una forma más sigilosa y silenciosa, lo cual ocasiona que este tipo de ataques mantengan su vigencia. *[2]*

La manipulación de aplicaciones de software es algo que se seguirá dando mientras personas tengan acceso a computadoras de otros, en especial cuando es con permisos autorizados y que por el desconocimiento, curiosidad u otros, instalan o usan software que no corresponden a la labor y además desconocen el impacto que pueda traer en la red. *[2]*

El Ramsomware hace un tiempo era un factor desconocido para muchos, pero de un tiempo para acá se ha vuelto un problema para muchas personas y organizaciones, las cuales han sido víctimas de estos delincuentes que no contentos con infectar máquinas sin autorización, proceden a cifrar la información de las víctimas y a exigir retribuciones económicas a cambio de liberar su información. *[2]*

El fraude electrónico también es un delito que se ha mantenido en el tiempo y ha evolucionado en sus técnicas, teniendo diferentes variedades, realizándose directamente en los cajeros electrónicos físicos, robando las contraseñas de los usuarios, clonando tarjetas débito y crédito, tratando de hackear y vaciar el cajero, robando credenciales digitales, entre otras técnicas que van apareciendo a medida que avanza la tecnología. *[2]*

Las acciones de ingeniería social, desde un principio fueron uno de los medios más importantes para los intrusos informáticos obtener información de sus víctimas. Así poder planear la mejor forma para ellos lucrarse de eso; y en la actualidad esto se ha multiplicado exponencialmente, pues con el auge de las redes sociales, la gente tiende a hacer publica mucha información, que en algún momento algún ciber atacante puede aprovechar en su contra, dependiendo de los motivos que tenga para realizar su acción. La suplantación de la identidad es otro de los tipos de incidentes que está muy relacionado con la ingeniería social, pues el ciber pirata obtiene toda la información que la misma victima ha colocado en las redes sociales y el internet, para después crear perfiles en diferentes espacios virtuales con la identidad robada, en busca de diferentes fines que atentan contra la buena imagen de la víctima. *[2]*

Ciberataques dirigidos son aquellos que se realizan en especial por parte de comunidades enteras de atacantes que conforman todo un frente de batalla contra su objetivo, y aunque se enfoca más hacia gobiernos, también se presenta contra grandes empresas reconocidas a nivel mundial. *[2]*

III. VIII Encuesta Latinoamericana de la Seguridad de la Información

TABLA II
RESPONSABILIDAD DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

RESPONSABILIDAD DE LA SI

ÚLTIMOS 5 AÑOS	2012	2013	2014	2015	2016
Auditoría interna	2,20%	4,58%	1,85%	1.50%	3.00%
Director de SI/S de I	23,61%	25,83%	26,94%	34.70%	**43.00%**
Director Departamento de Sistemas/Tecnología	36,67%	33,75%	35,42%	13.70%	16.00%
Gerente Ejecutivo	3,61%	2,50%	2,21%	3.40%	3.00%
Gerente de Finanzas	0,28%	0,42%		0.40%	0.00%
Gerente de Operaciones	3,89%	0,83%	3,69%	3.40%	2.00%
Gerente de Riesgos					5.00%
Gerente de Planeación					2.00%
No especificado	14,72%	17,50%	15,87%	14.90%	14.00%
Tercerizado	-	0,83%	1,11%	0.80%	1.00%
Otros cargos	15,00%	13,75%	12,92%	14.90%	14.90%

VIII Encuesta Latinoamericana de Seguridad de la Información

La anterior tabla presenta una tendencia muy interesante a nivel de Latinoamérica, donde se indica cómo ha sido la responsabilidad de la seguridad informática en las organizaciones, mostrando como algunos cargos como auditoria

externa, y director de seguridad informática han crecido de forma muy significativa, duplicándose como este último mencionado que paso de tener en el 2012 a tener una relevancia del 23%, a tener en el 2016 un 43% de responsabilidades en las empresas en el manejo de la seguridad de la información. *[10]*

TABLA III
INCIDENTES DE SEGURIDAD MÁS FRECUENTES

Manipulación de aplicaciones de software	4.0%	43
Instalación de software no autorizado	**12.0%**	122
Accesos no autorizados al web	8.0%	78
Fraude electrónico	3.0%	29
Virus/Caballos de Troya	**13.0%**	129
Robo de datos	3.0%	30
Monitoreo no autorizado del tráfico	2.0%	20
Negación del servicio (DOS/DDOS)	6.0%	56
Pérdida de integridad de la información	3.0%	28
Pérdida/Fuga de información crítica	3.0%	27
Suplantación de identidad	3.0%	26
Acciones de ingeniería social	4.0%	42
Phishing	**11.0%**	107
Pharming	1.0%	7
Espionaje	1.0%	10
Ramsonware	5.0%	50
Ataque de aplicaciones Web (XSS, SQL Injection, Directory Transversal, etc)	5.0%	48
Robo de elementos críticos de hardware (notebooks, discos, etc.)	4.0%	36
Incidentes relacionados con la privacidad de los datos personales (publicación de información personal, solicitudes de eliminación de datos personales, etc.)	3.0%	32
Ciber-Ataques (APT o ataques dirigidos, denegación de servicios masiva)	4.0%	37
Ninguno	1.0%	13
Otra (Por favor especifique)	1.0%	15

VIII Encuesta Latinoamericana de Seguridad de la Información

La tabla III muestra así como en la encuesta Colombiana, que unos de los incidentes que más se repiten son los relacionados con la instalación de software no autorizado, virus o caballos de Troya y el pishing, todos ellos especializados en robar información para defraudaciones económicas contra entidades públicas, bancarias, empresas y personas naturales. *[10]*

Esta es una muestra clara de la importancia de la implantación de la seguridad de la información en todas las organizaciones, no solo a nivel nacional, sino internacionalmente. *[10]*

TABLA IV
PORCENTAJE DE USO DE CONTROLES DE SEGURIDAD EN LAS ORGANIZACIONES

Sistemas de Contraseñas	58.2%	191
Soluciones Anti-Malware	55.5%	182
Firewalls tradicionales (Hardware/Software)	51.8%	170
VPN/IPSec	50.3%	165
Biométricos (huella digital, iris, etc.)	33.2%	109
Cifrado de datos	37.2%	122
Firmas digitales/certificados digitales	33.2%	109
Proxies/Proxies inversos	33.2%	109
Firewalls de nueva generación	32.0%	105
Web Application Firewalls (WAF)	28.4%	93
Sistemas de detección y/o prevención de intrusos IDS/IPS tradicionales	29.3%	96
IDS/IPS de nueva generación	22.3%	73
Smart Cards	16.2%	53
Soluciones de monitoreo de redes sociales	18.9%	62
Firewalls de Bases de Datos (DAF)	15.5%	51
SIEM (Security Information Event Management)	18.9%	62
Servicio de SOC	12.8%	42
Herramientas Anti –DDoD	11.0%	36
Servicios de inteligencia de amenazas	9.5%	31
ADS (Anomaly detection systems)	4.6%	15
Tercerización de la seguridad informática	6.7%	22
Herramientas de validación de cumplimiento con regulaciones internacionales	6.7%	22
Ciber seguros	7.0%	23
Otro (Por favor especifique)	0.9%	3

MECANISMOS PROTECCIÓN (6 en promedio x empr.)

VIII Encuesta Latinoamericana de Seguridad de la Información

La tabla IV presenta los mecanismos de seguridad más usados en las organizaciones, los cuales crean la necesidad de las mismas a tener una dependencia y un grupo encargado de administrar la seguridad de la información, que cada uno de esos mecanismos requiere una gestión y un proceso de control que se debe realizar periódicamente, así como las actividades de constante revisión, monitoreo y modificación. *[10]*

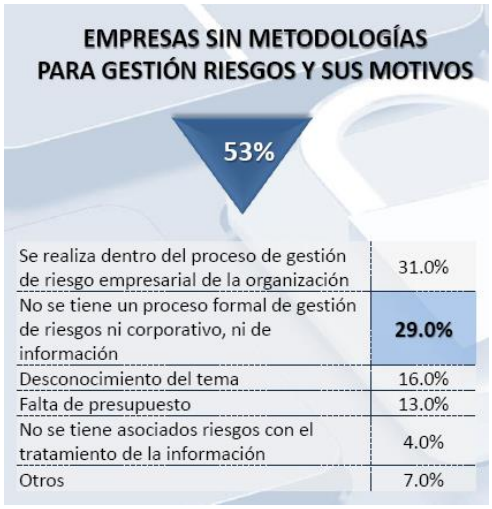
En cuanto a evaluaciones de seguridad en las empresas, se encontró que se realizan en el 41% de las empresas grandes (con más de 1000 empleados), el 29.23% de las empresas medianas (entre 201 y 1000 empleados), y el 29,23% de las empresas Pequeñas (de 1 a 200 empleados). *[10]*

Los estándares más aplicados a nivel latinoamericano son Iso27001 con un 30%, e ITIL con un 15%. *[10]*

A. Gestión de Riesgos

Hace unos años, y actualmente en algunas empresas aún tienen el pensamiento de que si existe un ingeniero de sistemas en la compañía, él se encarga de todo y ya no se necesita escuchar propuestas sobre procesos informáticos. Justamente esto es lo que lleva a muchas compañías a sufrir incidentes de seguridad. Por eso es importante contar con un equipo de gestión de la seguridad de la información, y entre estos procesos se encuentra la gestión de riesgos. *[10]*

TABLA V
MOTIVOS DE LAS ORGANIZACIONES PARA NO ESTAR APLICANDO PROCESOS DE ASEGURAMIENTO DE SU INFORMACIÓN



VIII Encuesta Latinoamericana de Seguridad de la Información

Las empresas tienen algunas razones que en ocasiones exponen para justificar la falta de aplicación de una metodología para la gestión de riesgos, y pues muchas veces con estos motivos evaden por tiempos la aplicación de las mismas y por las misma razón cuando son atacadas el impacto que generan las amenazas es mucho mayor y el golpe económico y moral que recibe la organización en muchas ocasiones puede ser muy grave para la misma, dejándola en casos extremos en riesgos incluso de quiebra. *[10]*

TABLA VI
SECTORES QUE NO ESTÁN DESARROLLANDO PROCESOS DE EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

VIII Encuesta Latinoamericana de Seguridad de la Información

Pareciera increíble, pero a nivel latinoamericano se ha identificado que diferentes sectores muy importantes en el desarrollo económico no realizan, o si lo realizan es en un porcentaje muy reducido de gestión de riesgos de Seguridad Informática. Algunos de estos sectores son: sector de energía e hidrocarburos, manufactura, construcción / ingeniería, entre otros. Y para redondear la cifra, el sector que más gestión de riesgos está realizando es el sector Público / Gobierno, y el porcentaje apenas alcanza el 40%. *[10]*

B. Obstáculos

TABLA VII
OBSTACULOS PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES

OBSTÁCULOS PARA LOGRAR LA SEGURIDAD DE LA INFORMACIÓN	2015	2016
Ausencia o falta de una cultura en seguridad de la información		38.7%
Falta de apoyo directivo	41.6%	32.3%
Poco entendimiento de la seguridad de la información	33.5%	32.0%
Falta de colaboración entre áreas/departamentos	45.7%	30.5%
Falta de formación técnica	24.9%	25.6%
Poca visibilidad del tema a nivel ejecutivo	35.7%	25.3%
Inexistencia de política de seguridad	24.9%	20.4%
Poco entendimiento de los flujos de la información en la organización	22.6%	20.1%
Falta de tiempo	31.2%	19.8%
Complejidad tecnológica	24.0%	19.5%
Escasa formación en gestión segura de la información		19.5%
Habilidades gerenciales de los CISO's	15.8%	13.1%

VIII Encuesta Latinoamericana de Seguridad de la Información

Es importante mencionar cuales son los factores que obstaculizan la aplicación de la seguridad de la información en las organizaciones, y en esa escala se resaltas 3 que tienen un porcentaje relativamente alto, y que además denotan cuales son esos factores que se deben fortalecer para que mayor cantidad de empresas estén al tanto de la aplicación de la seguridad de la información. Los factores más influyentes son: ausencia o falta de una cultura de la seguridad de la información, falta de apoyo directivo, poco entendimiento de la seguridad de la información. *[10]*

Por lo tanto, se evidencia la necesidad de convencer a la gerencia de la importancia de la seguridad de la información, indicar a las organizaciones que deben hacer una gestión de riesgos si no quieren que el impacto de las amenazas sea demasiado alto, y así no tener que lamentarse demasiado tarde. *[10]*

C. Certificaciones

TABLA VIII
CERTIFICACIONES MÁS FRECUENTES EN LOS DEPARTAMENTOS DE SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS

VIII Encuesta Latinoamericana de Seguridad de la Información

Es importante mencionar cuales son las certificaciones en seguridad de la información que más se presentan entre los profesionales al servicio de las empresas a nivel latinoamericano, siendo así que el mayor porcentaje, de un 27% contienen Auditores ISO 27001 en sus compañías, el 17% de las empresas tienen CEH o Certified Ethical Hacker, otro 17 5 tienen CISSP o Certified Information System Security Profesional, el 15% CISM o Certified Information Security Manager, y aún existe un 24% de los profesionales en estas áreas que no tienen ninguna certificación internacional en seguridad informática. *[10]*

D. Área de la Investigación

Este trabajo es un elemento muy importante para el área de investigaciones, ya que nos presenta una descripción clara a nivel de país, de cómo por medio de la evolución tecnológica, se van abriendo nuevos espacios que son fuente potencial de explotación profesional, nuevos campos, nuevas áreas, nuevas experiencias.

Estos nuevos campos que se abren van siendo producto de las experiencias positivas y negativas de las compañías, ya que se ven muchas veces obligadas a buscar alternativas extra en temas de seguridad de la información, porque se dan cuenta que el área de desarrollo tecnológico por sí solo no puede abarcarlo todo.

Las áreas de investigaciones también pueden aportar mucho en esta temática, ya que ellas son las que siempre están buscando y motivando a la adquisición de conocimiento y mejora de los procesos, y justamente es un factor que hace falta en estos entes, la gestión en los procesos de certificaciones, ya que muchas veces buscan tener departamentos de sistemas expertos en todo, pero olvidan que eso debe ir acompañado de procesos de certificación en diferentes aspectos de calidad. Por lo tanto se debe hacer una reflexión desde el interior de las organizaciones en cuanto a la mejora en los procesos de calidad de los mismos y los medios y recursos físicos, humanos y financieros que deben ser aportados para obtener los mejores resultados.

IV. Acceso Abusivo a Aplicaciones Web desarrolladas en .JSP

Como en este documento se busca presentar la necesidad de la inclusión de los procesos y profesionales de seguridad informática en las organizaciones, se van a mencionar algunos detalles técnicos de una situación que se ha venido presentando en algunas aplicaciones web que están desarrolladas en .JSP, en las cuales simplemente descuidaban o ignoraban este aspecto y venían siendo vulnerados frecuentemente.

Continuando con la descripción de esta situación que se viene presentando, se debe mencionar el nombre de Boris von Loesch, quien ha desarrollado un código llamado "Jsp File Browser", el cual consta de una secuencia de comandos que permiten al atacante cuando logra infiltrar su código dentro de la víctima poder tener un control total de la misma, permitiéndole crear, modificar y eliminar directorios, asignarse permisos, entre otros procesos. De esta forma robar o modificar información de sus víctimas para usarla en sus diferentes fines ilícitos. *[11]*

Proceso que realiza el atacante:

1. El intruso realiza su ataque contra la plataforma web, utilizando las backdoors y Cross-site Scripting.

2. Se realiza la conexión con la sesión de un usuario o el mismo intruso sobrepasando las barreras. (este es opcional en caso de tener un usuario con permisos limitados).

3. Captura la información de la sesión de la memoria.
4. Logra vulnerar la plataforma o robar una sesión.

5. El atacante mantiene la sesión y reemplaza la página oficial de Servidor_Victima por su página modificada dentro del mismo Servidor_Victima.

6. El atacante puede moverse dentro de las páginas del Servidor_Victima saltando las barreras, creando páginas, subiendo archivos, modificándolos, y en especial modificando notas.

7. El atacante deja en el servidor sus páginas infectadas y modificadas esparcidas en todos los lugares posibles, así como terminales remotas ocultas en imágenes para seguir teniendo acceso.

FIGURA II
PROCEDIMIENTOS PRINCIPALES DE SCRIPT PARA UN SUPER ADMIN EN JSP

```
//Button names
private static final String SAVE_AS_ZIP = "Download selected files as (z)ip";
private static final String RENAME_FILE = "(R)ename File";
private static final String DELETE_FILES = "(Del)ete selected files";
private static final String CREATE_DIR = "Create (D)ir";
private static final String CREATE_FILE = "(C)reate File";
private static final String MOVE_FILES = "(M)ove Files";
private static final String COPY_FILES = "Cop(y) Files";
private static final String LAUNCH_COMMAND = "(L)aunch external program";
private static final String UPLOAD_FILES = "Upload";
```

Este es un proyecto de un experto en seguridad Alemán, pero como se puede ver en esta sección, un código que fue creado con buenas intenciones está siendo utilizado para cometer delitos informáticos, por lo cual queda en manos de los expertos en seguridad de la información de cada organización el velar por la integridad de sus datos, ya que permanentemente van apareciendo agujeros en los software que afectan las compañías, y de la misma forma es una motivante preocupación para las empresas que han descuidado el aseguramiento de la infraestructura tecnológica de sus organizaciones, el análisis de riesgos, entre otros procesos de seguridad. *[11]*

V. Conclusiones

Muchas empresas tienen aplicaciones que usan permanentemente, y contienen información confidencial que está dentro de la compañía, pero virtualmente desprotegida. Por diferentes motivos no realizan los adecuados controles de seguridad y con eso están dando la oportunidad a los delincuentes informáticos de poder vulnerar sus sistemas de información.

Aún existen empresas que consideran que con un solo ingeniero de sistemas pueden cubrir todas las necesidades informáticas, ya sea por desconocimiento o por querer economizar. Por lo tanto hace falta más sensibilización en la seguridad de la información, para presentarles los riesgos que está corriendo su organización por evadir este importante aspecto en cuanto a la protección de su información.

El phishing, el malware y la instalación de software no autorizado, establecen el 36% de las amenazas más materializadas a nivel de latinoamerica. *[10]*

Se advierte una tendencia en el uso de autenticación de doble factor (contraseñas, biométricos, tokeens), así como de firewalls de base de datos y la adquisición de ciberseguros. *[10]*

Las empresas en latinoamerica exigen minimo 2 años de experiencia en seguridad informática para contratar a su personal en esta área. Adicionalmente privilegian que los seleccionados tengan certificaciones como la ISO 27001, CISSP o CEH. Adicionalmente tienen un promedio de 5 personas dedicadas de tiempo completo a la seguridad informática. *[10]*

Tres temas claves deben tener en cuenta los ejecutivos en la seguridad de la información: APT (ataques tele dirigidos), ciberseguridad y seguridad y control en la nube. *[2]*

REFERENCIAS

[1] Grupo Control. “Evolución de la seguridad informática” [Online].Available:https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica

[2] Almanza, Junco, A. XVI Encuesta Nacional de Seguridad/Ciberseguridad. 2016. Asociación colombiana de Ingenieros de sistemas ACIS.

[3] M Farias, E. (2016). Perfil del Oficial de Seguridad Informática. [online] Cudi. Available at: http://www.cudi.edu.mx/rfc/drafts/draft4.pdf [Accessed 9 Jul. 2016].

[4] López Delgado, M. (2016). Análisis Forense Digital. Organización de los Estados Americanos [online] Available at: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf [Accessed 9 Jul. 2016].

[5] ENTER.CO. (2016). Así Construye Colombia Su Política De Ciberseguridad Y Ciberdefensa. [online] Available at: http://www.enter.co/chips-bits/seguridad/ciberdefensa-colombia-politica/ [Accessed 9 Jul. 2016].

[6] Gestiondeti.com. (2016). *Funciones de CEO, CIO y el responsable de seguridad informática - gestiondeti*. [online] Available at: http://www.gestiondeti.com/definicion-de-terminos-de-tecnologia/funciones-de-ceo-cio-y-el-oficial-de-seguridad-informatica [Accessed 9 Jul. 2016].

[7] Banco Santander, (2016). *Informe de Gestión del Riesgo*. [online] Reporte anual Banco Santander. Available at: http://www.santanderannualreport.com/2015/sites/default/files/informe-riesgos-2014.pdf [Accessed 9 Jul. 2016].

[8] CISA, F. and →, V. (2013). *Auditoría de seguridad de la información… ¿Por dónde empezar? | Magazcitum*. [online] Magazcitum.com.mx. Available at: http://www.magazcitum.com.mx/?p=2185#.V4GILPl9600 [Accessed 10 Jul. 2016].

[9] OpenWebinars.net. (2015). *¿Qué es el Pentesting?*. [online] Available at: https://openwebinars.net/que-es-el-pentesting/ [Accessed 10 Jul. 2016].

[10] CANO, J. VIII ENCUESTA LATINOAMERICANA DE SEGURIDAD DE LA INFORMÁCIÓN.

[11] VON LOESCH, B. (2016). VONLOESCH.DE |. [ONLINE] VONLOESCH.DE. AVAILABLE AT: HTTP://WWW.VONLOESCH.DE/INDEX.HTML [ACCESSED 7 JUL. 2016].

Autor

Marcos Fernando Reyes Alvarez, Ingeniero de Sistemas Egresado de Unisangil, con Especialización en Seguridad Informática en la Universidad Pontificia Bolivariana, y Certificación como Auditor ISO 27001. Actualmente vinculado a Unisangil como docente cátedra y coordinador del semillero de seguridad informática Sigsu, el cual pertenece al grupo de investigación Hydra. Perito informático vinculado a la rama judicial como auxiliar de la justicia desde el año 2010, y trabajando como ingeniero contratista en diversos proyectos de desarrollo de software y prestación de servicios de ingeniería en diferentes empresas. Contacto: markfdo@hotmail.com