Universidad Internacional Latinoamericana de Ciencia y Tecnología
ULACIT

Implementación de herramientas de administración, penetración y monitoreo en el ámbito de la seguridad de las redes de datos y sistemas telemáticos en el sector público.

Realizado por:
Denis Antonio Gaitán Suárez
San José Costa Rica.

Resumen

La seguridad de las tecnologías de información es una de las áreas de la informática con mayor impacto en las organizaciones, así mismo posee una amplia gama de herramientas las cuales en conjunto con los procedimientos y protocolos, buscan garantizar la integridad, accesibilidad y seguridad de que los datos son verídicos y confiables. Esta investigación busca conocer y medir la realidad actual de los departamentos de tecnologías en cuanto a seguridad, así como el impacto y beneficios de las funcionalidades más innovadoras que consideran los departamentos T.I., útiles en sus operaciones. Los resultados obtenidos indican sin lugar a dudas la tendencia actual y el giro que deben realizar los responsables de resguardar la seguridad de la información. La investigación encuentra además el alto interés que existe por parte de los profesionales para innovar en la temática de seguridad y la necesidad de conocimiento más profundos acerca del mismo.

Palabras Claves: Seguridad, herramientas, redes, sistemas.

Abstract

Safety of information technology is one of the areas of computing with greater impact on organizations, also has a wide range of tools which together with the procedures and protocols, seek to ensure the integrity, accessibility and security that data are accurate and reliable. This research seeks to understand and measure the current reality of the IT departments for security as well as the impact and benefits of the most innovative features that IT departments consider useful in their operations. The results indicate undoubtedly the current trend and the turn must make those responsible for safeguarding the security of the information. The research also found that there is high interest on the part of professionals to innovate in the subject of security and the need for deeper knowledge about it.

Keywords: Security, Hardware, networks, systems.

Problema/Pregunta

El uso de las tecnologías en el sector público, conlleva a un riesgo de exposición y pérdida de la información en los procesos vitales internos y externos de las organizaciones públicas, generados por las amenazas y vulnerabilidades inherentes a las tecnologías. Esto representa un conjunto de retos importante que enfrentan los especialistas e ingenieros de redes de sistemas telemáticos, los cuales conlleva a innovar en la temática de seguridad de redes de datos y sus servicios, ante ello, surge la interrogante: ¿Implementan los administradores de TI, herramientas de administración, penetración y monitoreo, en el ámbito de la seguridad informática, como mecanismos de innovación y transformación de las mejores prácticas de procesos de seguridad en los sistemas y redes telemáticos?

Justificación

En el ámbito de la seguridad de las redes de datos y sistemas telemáticos, la innovación es uno de los principales pilares que permiten garantizar la confiabilidad de la información y protección de la misma, ante los constantes cambios y nuevas amenazas en materia de seguridad de T.I. Por ende, se debe establecer y medir el alcance e impacto, que tienen la utilización de herramientas de seguridad informática como medio para la innovación en el mejoramiento de la seguridad del área de T.I. en el sector público.

El principal fundamento es identificar las innovaciones en materia de seguridad propuestas y utilizadas por los administradores de T.I de las entidades públicas, antes los diferentes y diversos riesgos presentes en las tecnologías. Dichas herramientas se enfocan en aquellas que permitan implementar procesos de administración, test de penetración y monitoreo de la seguridad, los cuales son

de una alta utilidad para los especialistas, técnicos e ingenieros en materia de T.I. para la protección de la información y sistemas que lo soportan.

Antecedentes

En concreto la innovación, según Terry Jones, un líder visionario y pragmático (OnInnovation 2012), se define como *"nuestras ideas puestas a trabajar de forma exitosa"*. En resumen, en su obra maestra se puede distinguir que el desarrollo de la innovación, se fundamenta en la creación de una cultura tanto en el ámbito personal como profesional, la conformación de equipo de trabajos competitivos, líderes, con las habilidades necesarias y por último, la selección y desarrollo de aquellas ideas viables.

Es importante mencionar, que el uso de las tecnologías de hoy, es un reflejo "per se" del desarrollo y aplicación de ideas innovadores. Las personas sin darse cuenta son agentes de cambios importantes en la evolución de las tecnologías, lo cual genera ciclos de mejoramiento de cualquier actividad o producto relacionado con los intereses de las personas o empresas, sean públicas o privadas. El clásico ejemplo, conocido para un ingeniero de tecnologías de información, es la actualización de un sistema, sea por nuevas y mejores funcionalidades requeridas; o bien cambios de procesos y estándares o reingeniería de procesos propuestos en la organización.

En la actualidad, el sector público integra un conjunto entidades las cuales proveen servicios a los diferentes sectores del país, cada uno apoyado por una diversidad de plataformas de infraestructura de T.I. englobados en redes y telecomunicaciones y sus correspondientes sistemas y aplicaciones. Se puede concluir del PND 2011-2014, que la importancia de la tecnología en el sector

público es vital, para generar el dinamismo requerido a nivel nacional ("Capítulo VII, Competitividad e Innovación", Mideplan, 2010).

Precediendo al aumento del uso de las tecnologías, también se presentan los riegos y amenazas a la integridad de las plataformas de redes de datos y sistemas telemáticos; por ejemplo a nivel mundial, según el reporte de Seguridad Anual de Symantec, en el año 2012 se intensificaron en un 42% los ataques de virus, se desarrollaron 1700 nuevos virus en promedio, 3.4 millones de computadoras se infectaron y forman parte ahora de BotNets, 248,000 sitios o portales bloqueados, se estimó una media de 30 Billones de correos spams transmitidos y 1 de cada 291 correos tenían virus.(Symantec 2013).

A nivel nacional, se han presentado situaciones que comprometen la seguridad de los datos, ocasionando un daño cualitativo en la imagen en las entidades públicas. (La Nación, 2011, Asamblea Legislativa soluciona 'hackeo') y peor aún, un daño de la imagen como país, (El País, Página de la Presidencia de Costa Rica sufre ataque de "hackers")

Como contraparte a las amenazas que afectan la seguridad de las redes de datos y los sistemas telemáticos, es importante destacar las acciones para contrarrestarlos en forma coordinada, minimizar y ojalá eliminar sus efectos y causas. Cabe mencionar la definición de estándares y buenas prácticas en búsqueda de la protección de la información definidos por los deptos. de T.I. de las entidades públicas, así como la implantación de Equipos de Respuesta a Incidentes de Seguridad Cibernético a nivel de proveedores de servicios tanto de empresas públicas (CSIRT-ICE) como de coordinación pública (La Nación, Costa Rica tendrá Centro de Atención a Incidentes de Seguridad Informática).

El aspecto más importante, es la capacidad de los departamentos de TI en innovar ante las situaciones de riesgo en seguridad que se presenten en las organizaciones. Innovar en el ámbito de la seguridad por medio de la utilización de herramientas de seguridad y monitoreo en los procesos inherentes es la piedra angular ante el futuro desafío de las tecnologías.

Objetivo General

Análisis de la implementación de herramientas de administración, penetración y monitoreo de seguridad llevados a cabo por los administradores de redes de datos y sistemas telemáticos en las instituciones públicas.

Objetivos Específicos

- Identificar la realidad actual de los deptos. T.I. en instituciones en la operación de sus redes de datos.
- Definir y establecer las mayores amenazas que enfrentan los administradores de redes de datos.
- Definir las funcionalidades más innovadoras que integran las herramientas de seguridad, monitoreo y administración de redes de datos.
- Evaluar el impacto y beneficio de las herramientas de seguridad y monitoreo de redes de datos en los departamentos de T.I.

Marco Metodológico.

Se define como marco de trabajo la utilización de una metodología cuantitativa, en donde, de acuerdo al problema planteado y los objetivos específicos referidos a la investigación "***Implementación de herramientas de administración, penetración y monitoreo en el ámbito de la seguridad de las redes de datos y sistemas telemáticos en el sector público***", se conceptualizará en una investigación de campo de alcance descriptivo.

El alcance descriptivo, busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos objetos o cualquier otro fenómeno que se someta a una análisis (Hernández, Fernández, Baptista, 2010).

Instrumentos de recolección de datos

La recopilación de información requerida para el proceso metodológico, se fundamenta en el uso de encuestas en línea a través de la herramienta en internet de encuestas llamada surveymonkey (https://es.surveymonkey.com).

Encuesta

Es un estudio observacional, en el cual el encuestador no modifica el entorno ni controla el proceso que está en observación (Wikipedia, 2014). En la investigación, se aplicará una encuesta de tipo semiestructurado, la cual sirve de soporte metodológico válido para la obtención de información. Está compuesta por:

- Preguntas abiertas (no estructuradas): En este tipo de preguntas abiertas es la fuente de información quien responde con sus propias palabras a la pregunta formulada. Son esenciales para conocer el marco de referencia del auditado y para redactar después las alternativas a ofrecer en las preguntas cerradas.

- Preguntas cerradas (estructuradas): Se trata de un tipo que solo contiene la pregunta y no establece previamente ninguna clase de respuesta. Se utilizan con respuestas de opción única o selección múltiple.

Herramientas de recolección.

El resultado obtenido de dicha herramienta permite obtener y sustentar la información a partir de las siguientes técnicas:

Técnicas	Fuentes de información
Recolección de datos.	Invitación por medio de correo electrónico dirigido a las direcciones de correo de los miembros de la muestra poblacional definida.
Contextualización y alineamiento	Cuantificación de las respuestas y variables definidas, identificación de los resultados a preguntas abiertas.
Análisis de resultados.	Levantamiento de gráficos, análisis cuantitativo y descripción de los datos de mayor relevancia relacionados con la investigación.

Mediante la combinación de la aplicación de herramientas y técnicas descritas, se establece un conjunto de resultados, los cuales serán analizados de acuerdo a los objetivos definidos, para finalmente realizar la definición de las conclusiones y recomendaciones necesarias en el informe final.

Población y muestra

El termino de **población**, Arias (1999) lo define como “un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación”

Por otra parte, para el proceso cuantitativo la **muestra** es un subgrupo de la población de interés sobre el cual se recolectarán datos (Hernández, Fernández, Baptista, 2010). Para ello, el trabajo se realiza, sobre una muestra de 50 personas, que sean miembros de una población caracterizadas por los siguientes aspectos:

- Trabajadores del sector público compuesto por: Ministerios, Municipalidades, Instituciones autónomas y semiautónomas, así como empresas públicas.
- Titulo mínimo de bachiller en ingeniería informática, sistemas, o redes de datos.
- Actividades principales de trabajo o especializaciones sean enfocadas a la administración de las tecnologías de información, redes de datos, administración de sistemas o aplicaciones institucionales, administración de seguridad o bien administración de centros de datos.

Análisis de resultados

La encuesta fue remitida a 300 personas, de las cuales 51 completaron la encuesta. Se identifica que los encuestados se encuentran principalmente trabajando o se especializaron en desarrollo de sistemas, un 29.41%; gestión de base de datos, 43.14%; gestión de redes de datos, 45.10%; soporte técnico, 47.06%. De los resultados obtenidos, se puede interpretar que muchos de los encuestados se encuentran involucrados de forma simultánea en varias ramas de las tecnologías de información.

La gran mayoría de los encuestados, un 88%, afirmaron que en sus organizaciones se han presentado eventos o riesgos a la seguridad en materia de T.I. de los datos administrados por el área de T.I.; en contraste, con el 10% de encuestados que señalaron ningún evento presentado de este tipo. Es importante destacar, que se observa a nivel general, que muchas organizaciones han sufrido riesgos de cualquier índole que compromete la seguridad de los datos.

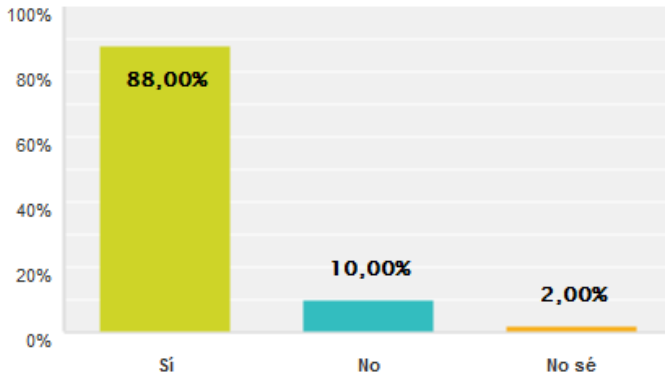

Figura 1. Evento(s) o riesgo(s) presentados en la seguridad de los sistemas.

Como consecuencia de dichas vulnerabilidades, los encuestados indican que el 33.33% de esos eventos produjo pérdidas económicas; 27.45%, daño o causa de corrupciones en los datos; un 29.41% de los encuestados afirma que daño la imagen de la institución, entidad o empresa en la que laboran. Así mismo, el 35.29% de los encuestados en el actual estudio, indica que se tuvieron consecuencias de sistemas o páginas web caídos, es importante observar que el grado de afectación de un sistema no deja de ser significativo porque no necesariamente un sistema deja de funcionar por un evento de seguridad, debido a que muchas veces se encuentran funcionando bajo esquemas de clúster o en alta redundancia.

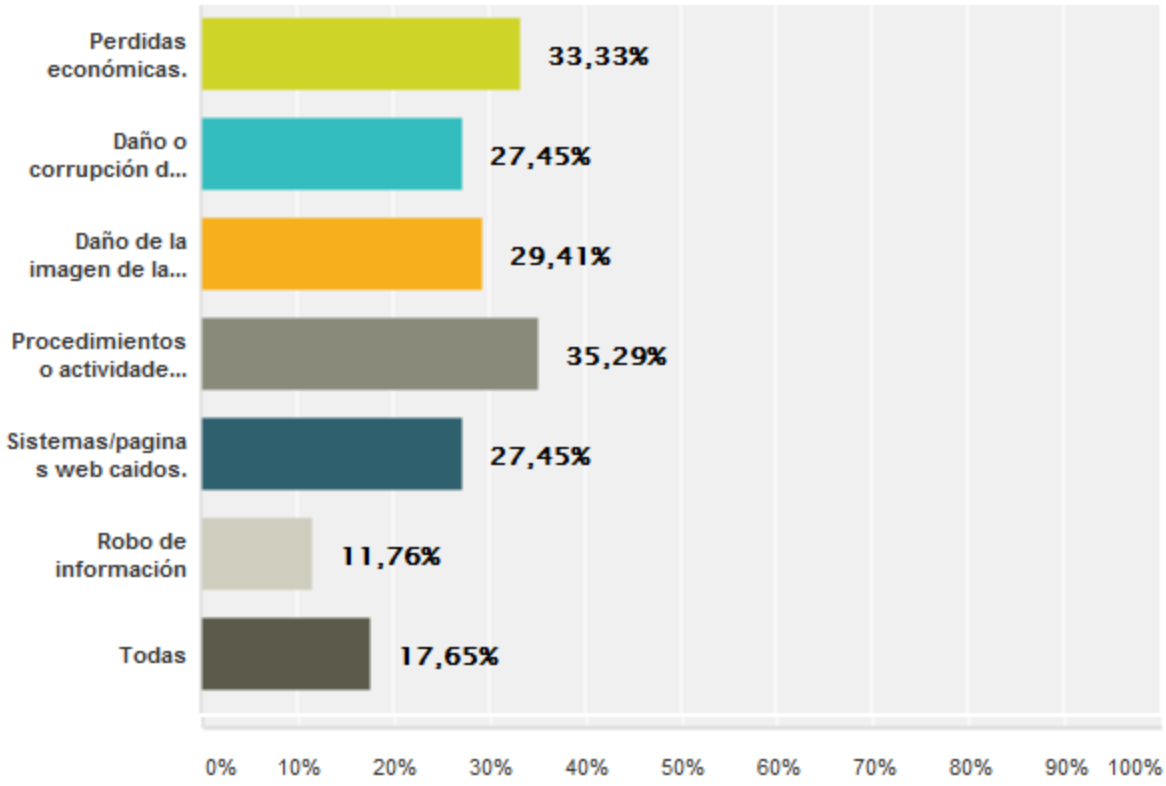

Figura 2. Consecuencias de los eventos y riesgos de seguridad

En cuanto al grado de incidencia u ocurrencia, de las principales amenazas conocidas de virus, troyanos, spams, Hoax, ataques DDos, entre otros; para un intervalo de periodo de los últimos dos meses a la fecha, se encuentran respuestas que cuantifican como bajo el tipo de amenaza ante la cual se enfrentan. En su mayoría, los encuestados indicaron que ninguna amenaza se ha presentado en los últimos dos meses; ubicándose entre un 25.64%, para spam; hasta un máximo de 47.50%, para Hoax, sin embargo, se presentaron 27.08% incidentes de ataques con virus que representan menos de 2 incidentes en dos meses; por otro lado y aún más importante mencionar que entre un 10.42% hasta un máximo de 22.22% indicaron que se han presentado más de 20 incidentes en un lapso de dos meses relacionados a las amenazas descritas anteriormente.

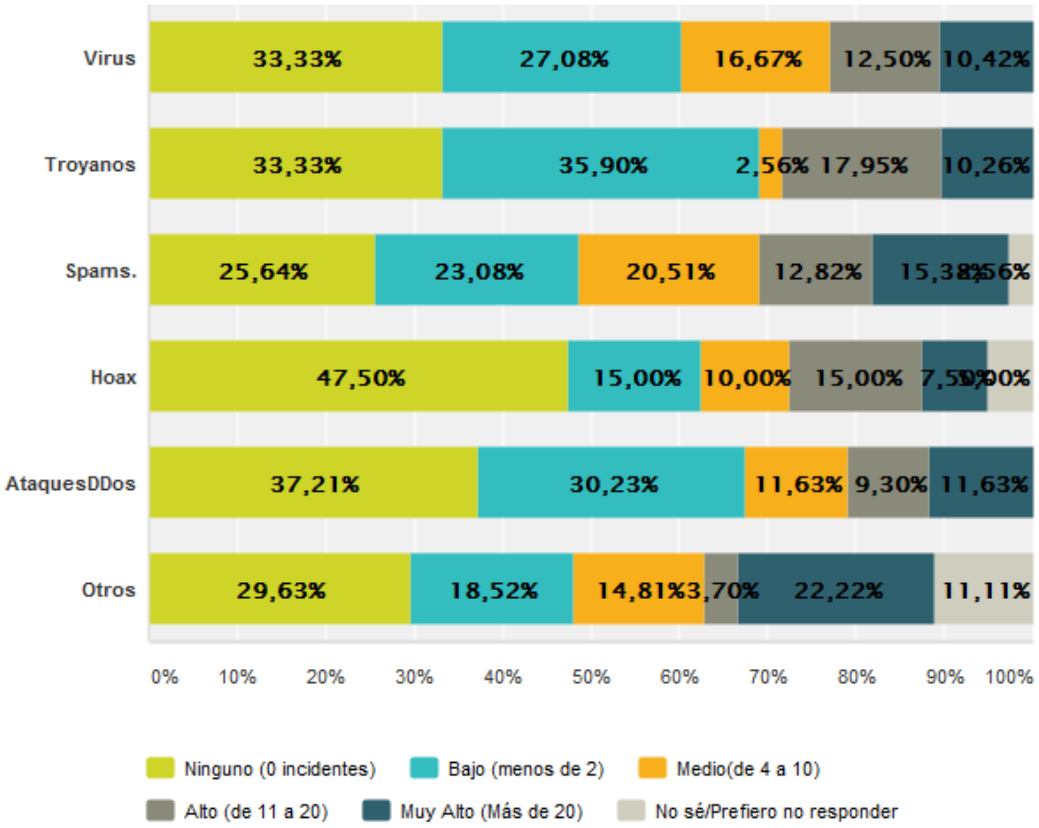

Figura 3. Nivel de incidencia u ocurrencia dentro de los últimos dos meses, en los cuales se hayan presentado riesgos en la seguridad de la infraestructura de TI

Ante la consulta, de si existen los protocolos y procedimientos de atención en el departamento de T.I para atender los incidentes en el ámbito de la seguridad informática, cerca del 86% respondió que sí, caso contrario, a un 11.76% quienes indicaron que no existen.

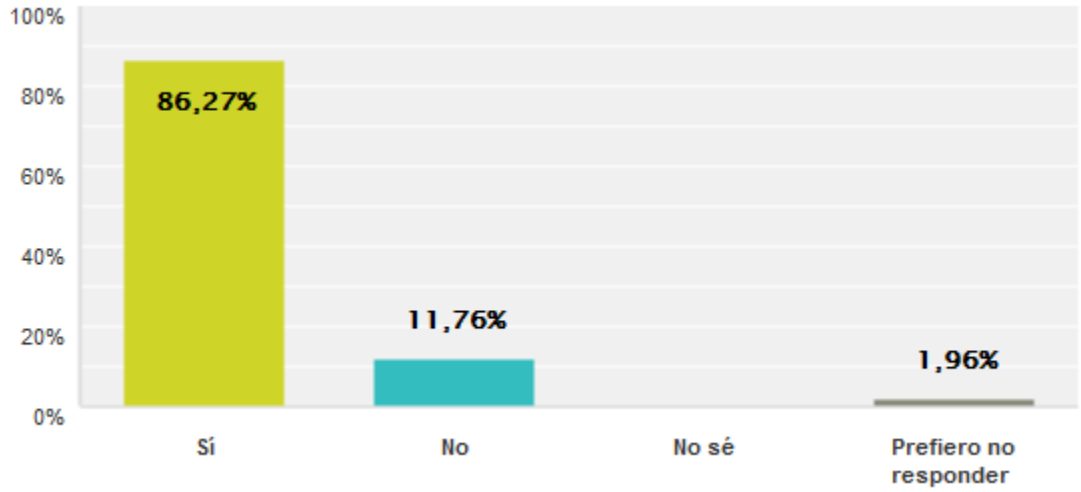

Figura 4. Porcentaje de encuestados que trabajan bajo protocolos y procedimientos de atención en el departamento de T.I. para la atención de incidentes en el ámbito de la seguridad informática

Con respecto, al tema de innovación en el departamento de T.I., a través de la investigación, adquisición, capacitación o implementación de herramientas y procesos, dirigidos a mejorar la seguridad de los sistemas y redes de datos, un 66.67% de los encuestados indicaron que sí y un 17.65% señalaron que no se innova. Es importante mencionar, que estos resultados demuestran la importancia que poseen la innovación para la mayoría de las organizaciones como un medio para mejorar en la seguridad de T.I.

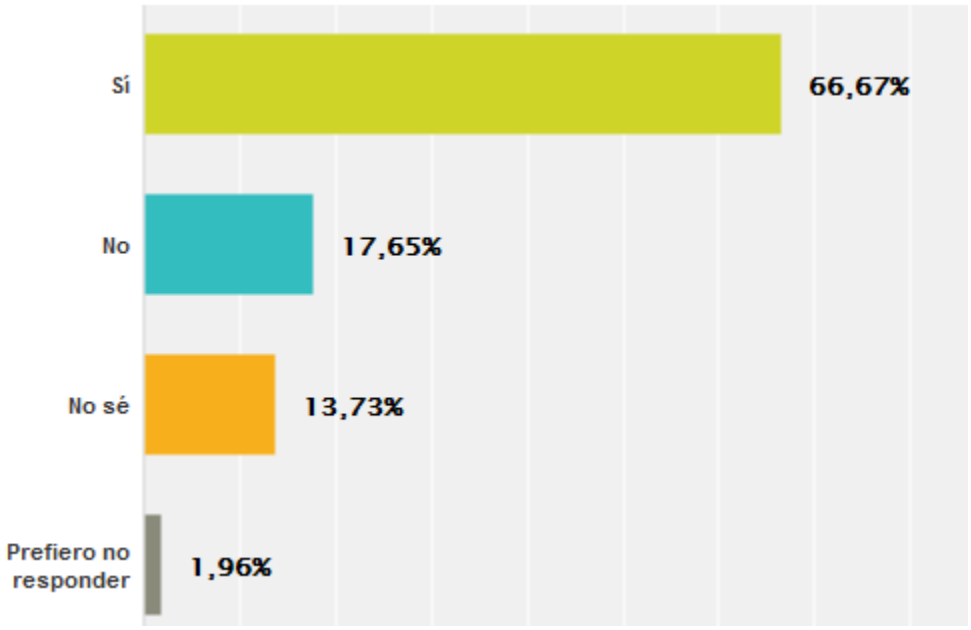

Figura 5. Porcentaje de Deptos. de T.I, que innovan para mejorar la seguridad de los sistemas y redes de datos

Referente a la utilización de las herramientas informáticas, como una vía de innovación para conocer y medir el grado de seguridad y vulnerabilidad de la infraestructura de T.I. es de destacar que se definieron conjuntos de herramientas de acuerdo las funcionalidades principales más importantes, clasificándose como:

- Análisis y detección de vulnerabilidades de páginas web como Exploits Scripting.
- Herramientas de testeo de framework para sitios web open source (por ejemplo WordPress, Joomgla, Moodle, etc.).
- Herramienta de Testeo o monitoreo de Bases de datos.
- Herramientas de monitoreo y detección de vulnerabilidades en sistemas operativos.
- Herramientas de reconocimiento, pruebas de intrusión y vectores de ataque a puertos y protocolos de redes de datos.

En los resultados obtenidos, es interesante encontrar entre el 30% y 40% de los encuestados, indica que no sabe o prefiero no responder a la consulta realizada, se podría interpretar (de parte del encuestador) que posiblemente este porcentaje significativo indique poco conocimiento en cuanto al software informático clave que sea de utilidad ante los eventos y riesgos de seguridad de T.I

Por otra parte, es importante destacar que otro resultado interesante, fue el 57% y hasta un 67% de los encuestados indicó la utilización de otro tipo de herramientas utilizadas, específicamente se indican las siguientes herramientas:

1. wireshark, nmap,Nessus
2. STAF - TOAD - EMBARCADERO - SNORT - ISS
3. Comerciales, appliances y otros.
4. Microsoft Baseline.

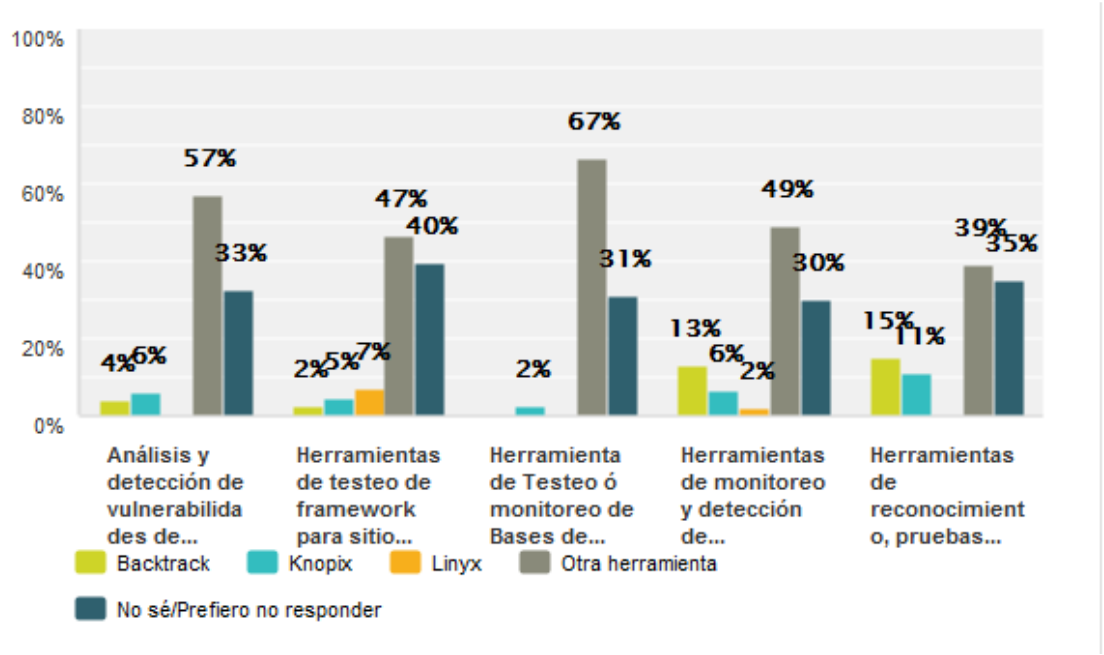

Figura 6. Herramientas utilizadas en el ámbito de seguridad, clasificadas por funciones principales.

Es indiscutible observar, que los resultados demuestran una amplia gama de herramientas utilizadas para verificar, analizar, monitorear y testear la seguridad de las redes y sistemas de datos, más allá de las definidas inicialmente en la encuesta.

Al tratar de establecer el grado de percepción de los encuestados, en cuanto al uso o posibilidad de utilizar, herramientas y procesos para mejorar la integridad, accesibilidad y disponibilidad de los datos y sistemas, entre el 32% y 60 % de los encuestados indicó que era altamente innovador; entre un 21% y un máximo de 35% indicó que era muy innovador.

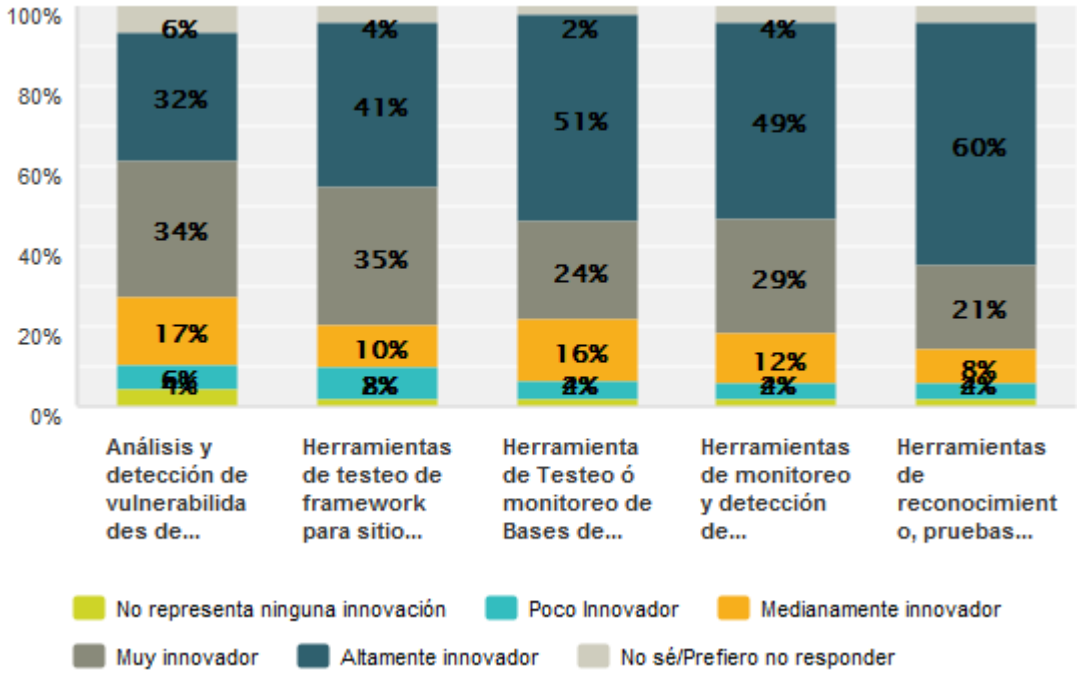

Figura 7. Percepción de los encuestados para innovar por medio de herramientas de seguridad de T.I.

Por último en los resultados obtenidos para conocer cuáles son los beneficios que los encuestados, podrían obtener en cuanto a la utilización de herramientas de seguridad, administración, monitoreo o penetration test, se encuentra que el 72,55% de las respuesta define la Disminución de Ataques/Vulnerabilidades; un 70.59%, mejoramiento de procesos y protocolos internos; 68.63%, mejoramiento de Arquitecturas de sistemas y de redes de datos; 66.67%, reforzamiento en la seguridad de los sistemas; un 1,96% de los encuestados indicó que ningún beneficio se podría obtener.

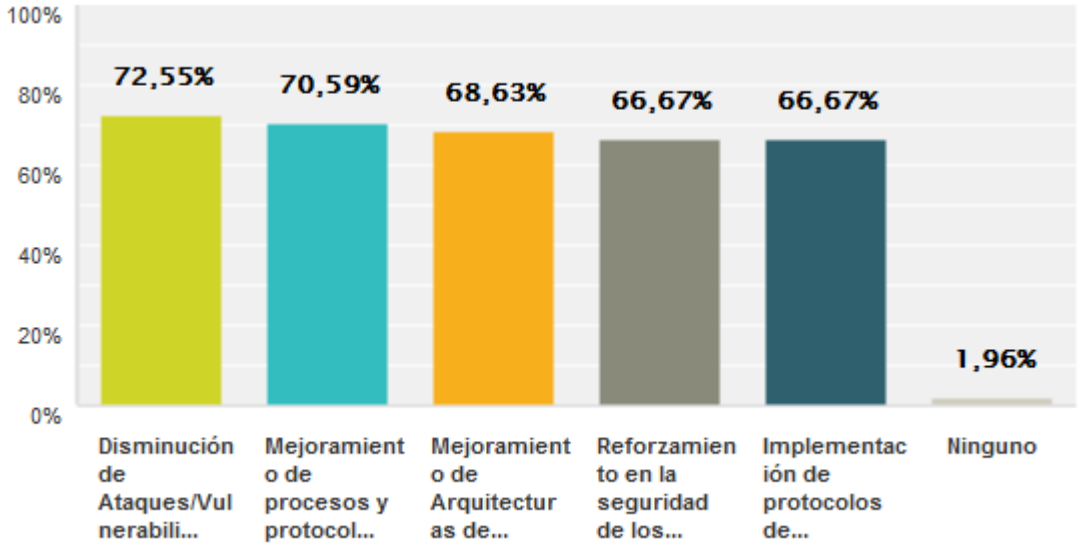

Figura 8. Beneficio obtenido por medio de la innovación con herramientas de seguridad de T.I.

Conclusiones

De acuerdo a los datos obtenidos se observa la tendencia de las organizaciones de innovar por medio de la utilización de nuevas herramientas en materia de seguridad de TI, así mismo a nivel de los profesionales de T.I. existe una alta concientización de la importancia de innovar en seguridad. Sin embargo, hay dos aspectos concluyentes por mencionar:

1. La gran mayoría de los encuestados define como altamente innovador o muy innovador la utilización de herramientas destacadas en materia de seguridad, sin embargo, se encuentra que la mitad de los encuestados (hasta un 40% relativo a la utilización de herramientas de testeo de frameworks de sitios web) no conoce o utiliza una herramienta que le permita mejorar los procesos o actividades internas en su departamento.

2. Por otra parte, la mitad de los encuestados utiliza una herramienta diferente a la expuesta en el estudio, pero íntimamente relacionadas en cuanto a funcionalidades tales como:
   - wireshark, nmap, Nessus.
   - STAF - TOAD - EMBARCADERO - SNORT – ISS.
   - Comerciales, appliances y otros.
   - Microsoft Baseline.

Resalta el hecho de que las organizaciones aún continúan afrontando riesgos y eventos relacionados a materia de T.I. tal y como presenta la tendencia a nivel global de los informes de Symantec, sin embargo, se puede establecer que los incidentes han disminuido en los últimos 2 meses, caso contrario a un 10%

aproximadamente de las organizaciones que tienen más de 20 incidentes en ese periodo.

Los beneficios en cuanto al uso de herramientas de seguridad, son tangibles de acuerdo 73% de los encuestados y es el punto de partida para la transformación de las instituciones u organizaciones que requieran definir estándares de seguridad de T.I.

Por último, se encuentra que la mitad de los encuestados han implementado total o parcialmente herramientas de administración, penetración y monitoreo, en el ámbito de la seguridad informática, como un mecanismo de innovación y transformación de las mejores prácticas de procesos de seguridad en los sistemas y redes telemáticos.

Recomendaciones

- Definir mecanismos de medición periódicos de la efectividad de la innovación en las organizaciones que ya utilizan herramientas de seguridad.

- Instar a los profesionales de las diferentes áreas de las tecnologías de información, así como a los entes educativos a nivel superior, para ampliar el conocimiento de nuevas herramientas de seguridad de T.I. así como los aportes en innovación que brindan dichos medios.

- Definir un estudio, para medir el grado de conocimiento individual y departamental en las organizaciones para evaluar los niveles de seguridad de la información.

Anexos

Encuesta

- Link:
  http://www.surveymonkey.com/s.aspx?PREVIEW_MODE=DO_NOT_USE_THIS_LINK_FOR_COLLECTION&sm=0tG1elqnu8p9UItVx24YES4BjoOkA%2biu8Km0llKuKV0%3d

---

Estimado señor(a)

La presente encuesta es de carácter anónimo y consiste en medir el grado de implementación y/o uso de herramientas de administración, penetración y monitoreo de seguridad llevados a cabo por los administradores de redes de datos y sistemas telemáticos en el ámbito de la seguridad de las instituciones públicas y empresas semiautónomas.

Esta encuesta se completa en un tiempo de 7 minutos aproximadamente, muchas gracias de antemano por su colaboración.

Por favor indique lo siguiente:

Seleccione su área de trabajo o especialización en el departamento informático:

- Desarrollo de sistemas / Páginas –web.
- Gestión de Bases de datos.
- Gestión de redes telemáticas.
- Gestión de Procesos o normativas (ITIL / COBIT).
- Soporte Técnico.
- Datacenter (Servidores y Software).
- Administración o gerencia.

Seleccione, el nivel de incidencia u ocurrencia dentro de los últimos dos meses, en los cuales se hayan presentado riesgos en la seguridad de la infraestructura de TI en su lugar de trabajo.

	Ninguno (0 incidentes)	Bajo (menos de 2)	Medio (Entre 4 - 10)	Alto Entre (11-20)	Muy Alto Más de 20
Virus					
Troyanos					
Spams.					
Hoax					
Ataques DDos					

Otros					

Si se han presentado incidentes en el ámbito de la seguridad en los sistemas administrados por su departamento de T.I., ¿cuáles han sido las consecuencias?

- Pérdidas económicas.
- Daño o corrupción de datos (Archivos/ Bases de datos).
- Daño de la imagen de la institución/entidad/Empresa.
- Procedimientos o actividades internas/externas de trabajo afectados.
- Sistemas/páginas web caídos.
- Robo de información.
- Todas.
- Ninguno.
- Otros. (Especifique)_____

A nivel particular de sistemas y redes de datos, seleccione el nivel de incidencia u ocurrencia dentro de los últimos dos meses, ¿cuáles han sido las subsistemas y servicios más afectados? (Por favor marque con X).

	Ninguno (0 incidentes)	Bajo (menos de 2)	Medio (Entre 4 - 10)	Alto Entre (11-20)	Muy Alto Más de 20
Servicios Internet.					
Servicio de correo electrónico.					
Sistemas particulares de servicios a departamentos.					
Almacenes de bases de datos					
Servicios de protocolos de red como DHCP, LDAP, AD, NTP¨, CDP, o Protocolos de enrutamiento.					
Equipos de telecomunicaciones					
Servidores					
Equipos de usuarios finales.					

¿Existen los protocolos y procedimientos de atención en el departamento de T.I. para la atención de incidentes en el ámbito de la seguridad informática?

- Sí
- No
- No sé.

¿Innova en el departamento de T.I., a través de la investigación, adquisición, capacitación o implementación de herramientas y procesos, dirigidos a mejorar la seguridad de los sistemas y redes de datos?

- Sí
- No
- No sé.

¿Utiliza su departamento, alguna de las siguientes herramientas informáticas, como una vía de innovación, para conocer y medir el grado de seguridad y vulnerabilidad de la infraestructura de T.I.?

	Back Track	Knopixx	Linyx	Otros (Por favor Especifique) _____	Ninguno	No sé
Análisis y detección de vulnerabilidades de páginas web como Exploitsó Scripting						
Herramientas de testeo de framework para sitios						

web open source (por ejemplo, WordPress, Joomgla, Moodle, etc.)						
Herramienta de Testeo o monitoreo de Bases de datos						
Herramientas de monitoreo y detección						
Herramientas de reconocimiento, pruebas de intrusión y vectores de ataque a puertos y protocolos de redes de datos.						

¿Cuál es su percepción, en cuanto al uso, o posibilidad de utilizar, nuevas herramientas y procesos para mejorar la integridad, accesibilidad y seguridad de T.I. en su departamento?

	No sé	Poco Innovador	Medianamente innovador	Muy innovador
Análisis y detección de vulnerabilidades de páginas web como Exploits o Scripting				
Herramientas de testeo de framework para sitios web open source (por ejemplo:WordPress, Joomgla, Moodle, etc.)				
Herramienta de Testeo o monitoreo de Bases de datos.				
Herramientas de reconocimiento, pruebas de intrusión y vectores de ataque a puertos y protocolos de redes de datos.				

¿Cuáles considera usted, que sean los beneficios, en cuanto a la utilización de herramientas de seguridad, administración, monitoreo o penetration test?

- Disminución de Ataques/Vulnerabilidades.
- Mejoramiento de procesos y protocolos internos.
- Mejoramiento de Arquitecturas de sistemas y de redes de datos.
- Reforzamiento en la seguridad de los sistemas.
- Implementación de protocolos de seguridad como encriptación, cifrado.
- Ninguno.
- Otros.

Muchas gracias por su colaboración, si usted desea conocer el informe de resultados obtenidos de la aplicación de esta encuesta, por favor indíquelo enviando un correo a dennis.gaitan@meic.go.cr

Resultado de Encuesta.

Seleccione su área de trabajo o especialización en el Departamento de informática:

Opciones de respuesta	Respuestas	
Desarrollo de Sistemas / Paginas Web	29,41%	15
Gestión de Bases de datos	43,14%	22
Gestión de Redes telemáticas	45,10%	23
Gestión de Procesos ó normativas (ITIL/COBIT)	37,25%	19
Soporte Técnico	47,06%	24
Data Center (Servidores y software)	29,41%	15
Administración o Gerencia	17,65%	9
Total de encuestados: 51		
Comentarios (0)		

¿Se han presentado en su organización, evento(s) o riesgo(s) a la seguridad de los sistemas, procesos o datos administrados en el área de TI?

Opciones de respuesta	Respuestas	
Sí	88,00%	44
No	10,00%	5
No sé	2,00%	1
Prefiero no responder	0,00%	0
Total		50

Si se han presentado incidentes en el ámbito de la seguridad en los sistemas administrados por su departamento de T.I. ¿Cuáles han sido las consecuencias?

Opciones de respuesta	Respuestas	
Perdidas económicas.	33,33%	17
Daño o corrupción de datos (Archivos/ Bases de datos).	27,45%	14
Daño de la imagen de la institución/entidad/Empresa	29,41%	15
Procedimientos o actividades internas/externas de trabajo afectados.	35,29%	18
Sistemas/paginas web caidos.	27,45%	14
Robo de información	11,76%	6
Todas	17,65%	9
Ninguno	19,61%	10
Total de encuestados: 51		

Comentarios (0)

Seleccione, el nivel de incidencia u ocurrencia dentro de los últimos dos meses, en los cuales se hayan presentado riesgos en la seguridad de la infraestructura de TI en su lugar de trabajo.

	Ninguno (0 incidentes)	Bajo (menos de 2)	Medio(de 4 a 10)	Alto (de 11 a 20)	Muy Alto (Más de 20)	No sé/Prefiero no responder	Total
Virus	33,33% 16	27,08% 13	16,67% 8	12,50% 6	10,42% 5	0,00% 0	48
Troyanos	33,33% 13	35,90% 14	2,56% 1	17,95% 7	10,26% 4	0,00% 0	39
Spams.	25,64% 10	23,08% 9	20,51% 8	12,82% 5	15,38% 6	2,56% 1	39
Hoax	47,50% 19	15,00% 6	10,00% 4	15,00% 6	7,50% 3	5,00% 2	40
AtaquesDDos	37,21% 16	30,23% 13	11,63% 5	9,30% 4	11,63% 5	0,00% 0	43
Otros	29,63% 8	18,52% 5	14,81% 4	3,70% 1	22,22% 6	11,11% 3	27

Comentarios (1)

A nivel particular de sistemas y redes de datos. Seleccione, el nivel de incidencia u ocurrencia dentro de los últimos dos meses en los cuáles han sido afectadas las áreas o servicios de T.I.

	Ninguno (0 incidentes)	Bajo (menos de 2)	Medio(de 4 a 10)	Alto (de 11 a 20)	Muy Alto (Más de 20)	No sé/Prefiero no responder	Total
Servicios Internet.	20,93% 9	25,58% 11	16,28% 7	20,93% 9	9,30% 4	6,98% 3	43
Servicio de correo electrónico.	25,58% 11	27,91% 12	13,95% 6	20,93% 9	6,98% 3	4,65% 2	43
Sistemas particulares de servicios a departamentos.	27,03% 10	21,62% 8	18,92% 7	16,22% 6	13,51% 5	2,70% 1	37
Almacenes de bases de datos	35,90% 14	20,51% 8	12,82% 5	15,38% 6	12,82% 5	2,56% 1	39
Servicios de protocolos de red como DHCP, LDAP, AD, NTP, CDP, ó Protocolos de enrutamiento.	36,11% 13	16,67% 6	11,11% 4	25,00% 9	5,56% 2	5,56% 2	36
Equipos de telecomunicaciones	31,71% 13	21,95% 9	14,63% 6	19,51% 8	9,76% 4	2,44% 1	41
Servidores	44,44% 16	11,11% 4	13,89% 5	11,11% 4	19,44% 7	0,00% 0	36
Equipos de usuarios final.	17,39% 8	17,39% 8	19,57% 9	10,87% 5	32,61% 15	2,17% 1	46
Otros.	21,05% 4	0,00% 0	15,79% 3	15,79% 3	36,84% 7	10,53% 2	19

Comentarios (0)

¿Existen los protocolos y procedimientos de atención en el departamento de T.I. para la atención de incidentes en el ámbito de la seguridad informática?

Opciones de respuesta	Respuestas	
Sí	86,27%	44
No	11,76%	6
No sé	0,00%	0
Prefiero no responder	1,96%	1
Total		51

¿Innova en el departamento de T.I., a través de la investigación, adquisición, capacitación o implementación de herramientas y procesos, dirigidos a mejorar la seguridad de los sistemas y redes de datos?

Opciones de respuesta	Respuestas	
Sí	66,67%	34
No	17,65%	9
No sé	13,73%	7
Prefiero no responder	1,96%	1
Total		51

¿Utiliza su departamento, alguna de las siguientes herramientas informáticas, como una vía de innovación, para conocer y medir el grado de seguridad y vulnerabilidad de la infraestructura de T.I.?

	Backtrack	Knopix	Linyx	Otra herramienta	No sé/Prefiero no responder	Total
Análisis y detección de vulnerabilidades de paginas web como Exploits ó Scripting.	4,08% 2	6,12% 3	0,00% 0	57,14% 28	32,65% 16	49
Herramientas de testeo de framework para sitios web open source (por ejemplo WordPress, Joomgla, Moodle, etc.).	2,33% 1	4,65% 2	6,98% 3	46,51% 20	39,53% 17	43
Herramienta de Testeo ó monitoreo de Bases de datos.	0,00% 0	2,38% 1	0,00% 0	66,67% 28	30,95% 13	42
Herramientas de monitoreo y detección de vulnerabilidades en sistemas operativos.	12,77% 6	6,38% 3	2,13% 1	48,94% 23	29,79% 14	47
Herramientas de reconocimiento, pruebas de intrusión y vectores de ataque a puertos y protocolos de redes de datos.	15,22% 7	10,87% 5	0,00% 0	39,13% 18	34,78% 16	46

Comentarios (6)

¿Cuál es su percepción, en cuanto al uso o posibilidad de utilizar, herramientas y procesos para mejorar la integridad, accesibilidad y disponibilidad de los datos y sistemas en su departamento?

	No representa ninguna innovación	Poco Innovador	Medianamente innovador	Muy innovador	Altamente innovador	No sé/Prefiero no responder	Total
Análisis y detección de vulnerabilidades de paginas web como Exploits ó Scripting.	4% 2	6% 3	17% 8	34% 16	32% 15	6% 3	47
Herramientas de testeo de framework para sitios web open source (por ejemplo WordPress, Joomgla, Moodle, etc.).	2% 1	8% 4	10% 5	35% 17	41% 20	4% 2	49
Herramienta de Testeo ó monitoreo de Bases de datos.	2% 1	4% 2	16% 7	24% 11	51% 23	2% 1	45
Herramientas de monitoreo y detección de vulnerabilidades en sistemas operativos.	2% 1	4% 2	12% 6	29% 14	49% 24	4% 2	49
Herramientas de reconocimiento, pruebas de intrusión y vectores de ataque a puertos y protocolos de redes de datos.	2% 1	4% 2	8% 4	21% 10	60% 29	4% 2	48

¿Cuáles considera usted, que sean los beneficios, en cuanto a la utilización de herramientas de seguridad, administración, monitoreo o penetration test?

Opciones de respuesta	Respuestas	
Disminución de Ataques/Vulnerabilidades	72,55%	37
Mejoramiento de procesos y protocolos internos.	70,59%	36
Mejoramiento de Arquitecturas de sistemas y de redes de datos.	68,63%	35
Reforzamiento en la seguridad de los sistemas	66,67%	34
Implementación de protocolos de seguridad como encriptación, cifrado.	66,67%	34
Ninguno	1,96%	1
Total de encuestados: 51		

Comentarios (0)

Presentación

- Ver documento: “Presentación Final - Seminario de Graduacion.ppt”

Video

- http://youtu.be/Ni40d6VUgE0

Bibliografía

- Jones Terry, (September 17, 2012) .ON Innovation. UnitedStates: Essential Ideas, Inc

- Soumitra Dutta and Bruno Lanvin, (2013). The Global Innovation Index 2013. Geneva, Switzerland: Cornell University, INSEAD, and WIPO 2013.

- La Nación, (2011) http://www.nacion.com/tecnologia/Asamblea-Legislativa-soluciona-hackeo-sitio_0_1184681572.html, Asamblea Legislativa soluciona 'hackeo' en su sitio Obtenido el 17/02/2014, Costa Rica.

- El País, 2012-03-19, http://www.elpais.cr/frontend/noticia_detalle/1/64223, Página de la Presidencia de Costa Rica sufre ataque de "hackers". Obtenido el 18/02/2014.

- La Nación, 2012, http://www.nacion.com/archivo/Centro-Atencion-Incidentes-Seguridad-Informatica_0_1255074552.htmlCosta Rica tendrá Centro de Atención a Incidentes de Seguridad Informática, Obtenido el 18/02/2012

- Fidias G. Arias, (Caracas 1999), El Proyecto de Investigación – Guía para su elaboración 3ra ed, Caracas: Editorial Episteme CA / OrialEdiciones.

- Neil J. Salkind, (1998), Métodos de Investigación 3ª Ed. México: Prentice Hall Hispanoamérica.

- Roberto Hernández, Carlos Fernández, Pilar Baptista. (2010), Metodología de la Investigación 5ta Edición, México DF: McGraw-Hill / Interamericana Editores.