GUÍA ESTRATÉGICA PARA AUMENTAR LA EFECTIVIDAD DE LAS CAMPAÑAS DE SENSIBILIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Oscar Iván Saavedra Noriega

Universidad Pontificia Bolivariana
Bucaramanga, Colombia

Resumen

Este artículo se realiza con el fin de presentar una guía estratégica, que aumente en una organización, la efectividad de las campañas de sensibilización en seguridad de la información. La cultura de la seguridad informática a nivel estratégico, es en estos tiempos determinante para mantener la confidencialidad, integridad y disponibilidad de la información; parte del problema se está generando por la falta de compromiso que tienen los usuarios para con su organización, cuando de proteger la información se trata. Se realizó un diagnóstico, resultado de la aplicación de un instrumento de análisis en una Empresa del sector de la salud en Santander, en la cual se implementó una campaña de sensibilización de seguridad de la información, así mismo se relacionaron conceptos como cambio organizacional, innovación tecnológica, resistencia al cambio, ingeniería social entre otros, de los cuales se analizó el modo de pensar, creer y actuar al interior de una organización relacionado con la seguridad de la información, cumpliendo con lo establecido en la norma ISO/IEC 27001 de 2005.

Palabras claves

Seguridad Informática, Cultura Organizacional, Sensibilización, innovación, Ingeniería Social.

Abstract

This article was done in order to present a strategic guide for organizations that want to increase the effectiveness of awareness information security campaigns. The culture of computer security strategic level, these days is decisive to maintain the confidentiality, integrity and availability of the information. Part of the problem is being generated by the lack of engagement the users have with your organization when is a data protection issue. A diagnosis, resulting from the application of an analytical tool in a health sector company in Santander, which was implemented an information security awareness campaign and related concepts such as same organizational change, innovation technology, resistance to change, social engineering among others, which examined how to think, believe and act inside the organization related to information security, complying with the provisions of ISO / IEC 27001 2005.

Keywords:
Information Security, organizational culture, sensibilization, innovation, social engineering.

1. Introducción

La seguridad de la información, como disciplina que defiende los activos de una organización, ha venido presentando una alta demanda, debido a los grandes alcances informáticos, es constante recibir reportes de las diferentes vulnerabilidades en sistemas de información, que de alguna manera son aprovechadas, esto consecuencia de fallas procedimentales o tecnológicas, o lo que en estos tiempos es más común fallas humanas. [1].

En el ámbito organizacional, la información se ha convertido en un insumo de la mayoría de las tareas que se realizan al interior de ellas. Cada día las organizaciones adquieren sistemas de información y herramientas para facilitar el procesamiento de los datos con el fin de generar informes y estadísticas las cuales se utilizan como guía para el desempeño y/o cumplimiento de los objetivos estratégicos trazados por cada organización.

Las organizaciones en la búsqueda de la protección de la información, se encuentran en procesos de implementación y adopción de lineamientos y/o directrices de seguridad de la información. Dichos lineamientos son plasmados en un documento de Política de Seguridad de la Información. Para dar cumplimiento a la política se requiere de un proceso de culturización y/o sensibilización de seguridad de la información de los integrantes de la organización, dicho proceso se ve reflejado en las campañas de sensibilización que emprenden las organizaciones. [2][4][5].

La efectividad de las campañas de sensibilización en seguridad de la información, ocasionalmente dependen de la forma como la organización puede llegar a abordar la ejecución de las mismas, así mismo en la actitud y compromiso que tengan los funcionarios con su organización. [2].

Según el National Security Institute, el 75% de la inseguridad de la información son fallas de seguridad al interior de la organización, como por ejemplo el descuidado empleado que escribe su contraseña a la vista de todos, o el que se lleva información sensible para su hogar o

simplemente el empleado que permite que los visitantes merodeen por su área de trabajo sin acompañamiento alguno [2].

Es importante contar con un nivel de concienciación de seguridad de la información, que establezca medidas preventivas y que se estandaricen en la organización, es decir, que el personal se responsabilice y tenga el conocimiento y la actitud para dar cumplimiento a los lineamientos y campañas que la organización despliega alrededor del tema de seguridad de la información [3].

La información no solo se encuentra en los medios digitales o físicos; no siempre los riesgos se van a mitigar con soluciones técnicas, también debe haber un nivel de conocimiento y conciencia sobre el manejo de la información, es importante para la organización la adopción de formas y actitudes que vayan en beneficio de la seguridad de la información.

Basado en ésta problemática, esta propuesta busca determinar el porqué de la poca efectividad de las campañas de sensibilización de seguridad de la información, así mismo, plantear estrategias que permitan que los esfuerzos que la organización realiza para proteger la información sean satisfactorios.

2. Sensibilización en Seguridad de la Información.

Las campañas de sensibilización son un instrumento conformado por diversas actividades, que buscan que el usuario al interior de una organización, se encamine por las buenas prácticas en seguridad de la información, respaldando así a la organización en la responsable tarea de proteger los activos de información [5], [6].

En una campaña de sensibilización nada puede quedar en el aire todo deber ser debidamente planificado y elaborado según sus objetivos finales, de los cuales los resultados deben ser los esperados por la organización, es necesario establecer indicadores que reflejen los diferentes estados de aplicabilidad de las actividades que componen la campaña.

Importante que el usuario primero sea educado y posteriormente capacitado.
Las alternativas que se recomiendan utilizar para que el plan de sensibilización sea factible son:

- Folletos
- Carteles
- Material BTL [1]
- Material POP [2]
- Uso de tecnología
- Presentaciones de Capacitación.

Es importante y necesario que cambie la mentalidad que existe en el factor humano de que no hay nada importante por proteger en su computador [15].

[1] Material BTL: desarrollo e implementación de actividades de publicidad dirigidas a un grupo específico empleándose medios de comunicación alternos, innovadores y muy creativos.

[2] Material POP: material promocional colocado en sitios estratégicos para captar la atención del usuario e impulsarlo a participar, incluye los letreros, anuncios, etc.

3. Cultura Organizacional en Seguridad de la Información.

La cultura organizacional es en esta era de la información uno de los más importantes elementos que caracterizan una organización[3], se da en el quehacer diario en las rutinas y acciones que se ejecutan al interior y que afectan el bienestar de la organización. A nivel empresarial puede llegar a comprometer el circulo en el que se mueve (clientes, empleados, proveedores y competencia).

Básicamente la cultura deja al descubierto la intención estratégica de una organización, es decir; como la organización desea cumplir con los objetivos o las metas que se ha propuesto, estableciendo su comportamiento como un elemento clave a la hora de competir con su entorno. [7][11].

Es frecuenté encontrar a nivel organizacional diversos tipos de culturas y comportamientos, existen metodologías y modelos[4] encargados de estudiar ese comportamiento y una vez identificado responder a la pregunta ¿Qué se puede mejorar? Por éstas estructuras es que la cultura se transforma, se vuelve reflexiva y adopta ideologías de aceptación. Siendo la información entonces tan importante para la sociedad, entra a jugar el término cultura organizacional como un factor determinante a la hora de fortalecer el eslabón más débil (usuario).

Cultura organizacional se describe como el conjunto de modos de vida, costumbres, valores y creencias que generan al interior de una organización una identidad, la cual fortalece o debilita los objetivos planteados para el futuro éxito de las metas trazadas de la organización. Lo anterior nos permite inferir que mientras más cercanos estén los comportamientos de los individuos a dichos valores y principios, más integrada y congruente será la organización y sus resultados. En el sentido contrario, mientras más alejados estén los comportamientos de los individuos a dichos valores y principios, más desintegrada será la organización y sus resultados. Entonces, si se quiere gestionar la cultura de la seguridad de la información, se debe planear y ejecutar las medidas necesarias para que todos y cada uno de los usuarios que componen la organización se transformen en los aliados estratégicos a la hora de cumplir con los objetivos trazados por la organización para el futuro.

La seguridad de la información se ve afectada por los comportamientos de los usuarios dentro y para con la organización, en el compromiso de los empleados para con su organización, en la actitud de los empleados frente al cambio, en cómo se enfrentan los problemas y como se plantean las soluciones y entre muchos otros en el saber que tan importante somos para la organización en la que trabajamos y cuál es el grado de pertenencia que tenemos para con la misma [8].

[3] Se hace especial referencia al artículo LA CULTURA EN LAS ORGANIZACIONES, Un fenómeno central en el saber administrativo escrito por Paola Podestá, publicado en el 2009.

[4] Modelo de Shein (1987), En este popular modelo de cultura organizacional, la cultura se manifiesta en tres niveles: los artefactos se encuentran en la superficie, descansando sobre los valores y los supuestos en la base.

De la buena gestión del grupo de TI encargado de promover la seguridad de la información, depende que nuestra cultura no se vuelva una cultura anómica, definida como de desinterés, falta de involucramiento, apática, indiferente viviendo en la incertidumbre, en la confusión, en la perdida de entusiasmo debido a la ausencia de recompensas para la premiación de éxitos, si no en una cultura integrativa, basada en la combinación de la orientación de los usuarios y los lineamientos estratégicos, en su visión, compromiso, trabajo en equipo, adaptación al cambio, llena de motivaciones, comunicación fluida y una alta preocupación por proteger y apoyar los objetivos de la organización para la cual trabaja. [30]

4. Innovación Tecnológica.

Las motivaciones a medida que avanza el mundo son diferentes, claramente hay un interés por la innovación tecnológica; pero se deja a un lado la protección y las buenas prácticas que se deben implementar a medida de que existan cambios en la organización.

Aquí entra otro concepto adicional como lo es la administración o manejo del cambio, que interviene directamente con los factores ya mencionados.

Para establecer un modelo exitoso de manejo del cambio se deben seguir una serie de pasos como lo son las expectativas, estrategias de comunicación, definición de roles, mecanismos de transferencia de conocimiento y lo más importante la adopción por parte de todos en la organización de las buenas prácticas en seguridad de la información.

Cada uno de los conceptos mencionados (Manejo del cambio, buenas prácticas de seguridad de la información, desarrollo de estrategias de enfrentamiento, sicología de la seguridad de la información, modelos organizacionales) serán los que de alguna forma faciliten el diseño de la estrategia para el aseguramiento de la información. [22].

5. Análisis de resultados de la encuesta aplicada a la fundación oftalmológica de Santander.

El instrumento de recolección de datos fue aplicado con el objetivo de diagnosticar la falta de compromiso y adopción por parte de la organización al implementar una campaña de sensibilización de seguridad de la información. Ver anexo 1. (*Encuesta-Foscal*, aplicada a la fundación Oftalmológica de Santander Foscal)

Población = 1000 Personas

Muestra de Población Encuestada = 159 Personas

Nivel de confianza de 93%

Se entregaron 210 encuestas con 15 preguntas; fueron contestados 159 encuestas correctamente, el resto no fueron contestados. Ver Anexo 2. *Resultados-Análisis-Encuesta-FOSCAL*

A continuación se presentan las conclusiones más importantes, resultado del análisis de las respuestas a las 15 preguntas de la encuesta.

Las conclusiones fueron las siguientes:

- Solo el 80% del personal encuestado presencio o estaba informado de la campaña de sensibilización en seguridad de la información realizada al interior de la organización. Lo Importante no es que la mayoría se entere de la campaña si no todos los que conforman la organización, desde el presidente de la organización hasta las empleadas de servicio y vigilantes.

- Solo el 87% de la muestra encuestada sabe a que se refiere el termino seguridad de la información el resto lo desconoce siendo una cifra producto de la conclusión anterior.

- El 34% de la muestra desconoce o no identifica lo que es un activo y las responsabilidades que tiene en su labor sobre el mismo. Que importante es que el 100% tenga claro el concepto de activos de información e identifique los mismos en su labor diaria.

- Solo el 79% de la muestra piensa que su labor de protección ante la inseguridad de la información es importante para la empresa. Aquí debe ser claro que el 100% de la población debe sentirse importante y parte fundamental de la empresa, así mismo que entienda que un descuido puede llevar a afectar la continuidad de las actividades fundamentales de la organización.

- El 63% de la población encuestada no hizo parte de la identificación de activos o información valiosa que tiene la organización. Este porcentaje es muy alto lo ideal sería que la identificación se realizara con cada una de las personas que hace parte de la organización, realmente son ellos los que pueden sacar a la luz todo lo que saben y que se debe proteger.

- El 15% de la muestra desconoce las sanciones que existen en caso tal de que ponga en riesgo los activos de la organización, ósea, es para ellos transparente si pierden, divulgan o incumplen con las políticas de la seguridad de la información, esto es el resultado de que el 18% desconozcan las políticas de seguridad de la información. Siguiendo por este mismo tema se evidencia así mismo que el 38% señala que nadie les supervisa su labor de protección en seguridad de la información, un valor muy alto si se quiere concienciar a todo el personal que labora en la organización.

- Importante que en las campañas de sensibilización en seguridad de la información se tengan en cuenta a todos los usuarios, incluyendo terceros, practicantes, altos ejecutivos es decir el 100% del personal que labora en la organización.

6. Ingeniería Social

La ingeniería social es uno de los métodos más usados para obtener de parte de la organización información significativa o sensible. Actualmente las organizaciones están realizando inversiones en seguridad de la información para la parte de tecnología, dejando a un lado el factor humano, que hace parte de los 3 pilares a resguardar dentro de la seguridad de la información, las personas se considera como el objetivo principal de la ingeniería social para la fuga de información. Un ataque de ingeniería social puede estar dirigido a una organización objetivo, a un determinado empleado, a un grupo de empleados o a un usuario y puede ser efectuado por un colega, compañero o simplemente un anónimo.

Los medios utilizados para este tipo de ataques de ingeniería social pueden presentarse por medio de un correo, una encuesta o por la recolección de información por medio de un dialogo. No es necesario tener el conocimiento técnico para cometer una intrusión atravez de la seguridad de la red, solo es suficiente con que existan usuarios despistados y poco informados con las buenas prácticas de la seguridad de la información.

La firma Imperva, especializada en Seguridad Informática presento un informe en el cual se mencionan las vulnerabilidades en el 2011, entre las que se encuentran la perdida de información en dispositivos móviles y en segundo lugar las redes sociales y robo de información por parte de los mismos empleados [17], [18], [20]. Así mimo Netasq afirma que para el 2012 las principales brechas de seguridad se concentran en dispositivos móviles y nuevamente la fuga de información por medio de las redes sociales, haciendo énfasis en que el factor humano se presenta como el eslabón débil a la hora de proteger la información [19], [13], [14], [21].

7. Estrategia de Sensibilización seguridad de la información.

El modelo estratégico planteado a continuación se compone de un conjunto de acciones que implementados al interior de una organización, contribuye al cumplimiento del principal objetivo de este artículo, el cual es aumentar la efectividad de las campañas de sensibilización en seguridad de la información, así mismo servirá como punto clave de referencia para el cumplimiento de algunos de los puntos de la norma ISO 27001:2005, la cual brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI).

La norma ISO 27001:2005 se compone de una serie de requerimientos que proponen un enfoque basado en procesos, y estos últimos en el modelo PHVA (Planear, Hacer, Verificar y Actuar). La cláusula 5.2.2 de la norma hace referencia a la formación, toma de conciencia y competencia, y describe que la organización debe asegurar que todo el personal apropiado, tiene conciencia de la pertinencia e importancia de sus actividades de seguridad de la información, así mismo a la contribución al logro de los objetivos de SGSI.

Con base a lo anteriormente descrito, a continuación se listan un conjunto de pasos, que proponen una guía a seguir para elevar el nivel de efectividad de las campañas de sensibilización en seguridad de la información, teniendo en cuenta que sería de vital ayuda para las organizaciones que pretenden mantener su entorno corporativo protegido de amenazas que rodean los sistemas de información y por ende sus activos (usuarios finales).

Para todo diseño e implementación de campañas de sensibilización en seguridad de la información, y para obtener mejores resultados al momento de culturizar todos y cada uno de los usuarios que componen la organización, se propone seguir el siguiente procedimiento:

7.1 NORMA ISO/IEC 27001:2005

Se debe adquirir por parte de la organización, el material fundamental, que para el caso de la seguridad de la información es el estándar internacional ISO/IEC 27001:2005 (Tecnología de Información, Técnicas de Seguridad, Sistema de Gestión de Seguridad de la Información y Requisitos), donde se describen cada uno de los pasos a seguir para mantener los 3 pilares que soportan la protección de la información, es decir, mantener la confidencialidad, integridad y disponibilidad de la información.

Es importante destacar que la información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

7.1.1 Sistema de Gestión de Seguridad de la Información – SGSI

Si bien es cierto, la norma ISO 27001 describe en su totalidad el modelo para el establecimiento del SGSI, pero para este procedimiento, es indispensable tener presente, algunos de los puntos que servirán como soporte para la culturización en seguridad de la información en toda organización.

Es necesario que una vez, el SGSI sea diseñado, y alineado con el contexto de la organización sea adoptado por la misma, si desde el principio los objetivos no se encuentran debidamente trazados, al final los resultados no van a ser los contemplados o esperados por la organización.

El SGSI es la parte del sistema de gestión de la organización, que basado en un enfoque de riesgos del negocio, aterriza y presenta los posibles problemas que se pueden presentar si no se realiza la gestión necesaria, por tal motivo es necesario para todo proceso de culturización y/o sensibilización se tengan en cuenta las siguientes actividades:

- Definir, desarrollar políticas, normas y procedimientos de seguridad de la información, que sirvan como soporte o punto de referencia para todos y cada uno de los usuarios de la organización, es decir, se dan a conocer roles y responsabilidades, así como las

autoridades que estarán al pendiente de garantizar que las campañas de sensibilización, reflejen el resultado deseado.

- Es indispensable, y por ningún motivo se puede pasar por alto, que las políticas de seguridad de la información, obtengan la aprobación de la alta gerencia. No tiene sentido que se quiera crear y exigir cultura al interior de una organización, si desde el puesto más alto no se brinda evidencia del compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI.

Dentro del modelo PHVA (Planear), antes del diseño de los planes de sensibilización, la organización debe realizar:

- Identificación, inventario y clasificación de todos los activos que posee la organización, si se desconoce lo verdaderamente valioso para la organización, si no se realiza un inventario de activos de información, no se puede saber qué información es confidencial, y por lo tanto que es lo que debo proteger.
- Identificar las vulnerabilidades y en du defecto las amenazas de cada uno de los activos identificados con anterioridad. Si conocemos las vulnerabilidades y amenazas podemos advertir en las campañas de sensibilización a todos y cada uno de los usuarios, de los posibles riesgos que se pueden generar por el no cumplimiento de las políticas de seguridad de la información.
- Identificar los propietarios de cada uno de los activos identificados con anterioridad; esto con el fin de establecer roles y responsabilidades, es decir, implementada la campaña de sensibilización en seguridad de la información, el usuario estará en capacidad de adoptar los controles que se ajusten al activo que tiene a su custodia.
- Entrevistar a cada uno de los usuarios propietarios de los activos, esto con el fin de identificar hasta qué punto la información que tienen a su disposición, es de vital importancia para la organización. Quien más que el propio usuario para que determine los requisitos que se deben tener para que la información se salvaguarde ante accesos no autorizados, modificación, o perdida de la confidencialidad o destrucción deliberada. Si se hace al usuario parte de la estrategia de las campañas de sensibilización en seguridad de la información, se le estaría dando un lugar al interior del proceso, por tal motivo se le daría a entender que el es importante para la organización, generando un sentido de pertenencia y compromiso con la misma.
- Identificar y hacerle saber a todos y a cada uno de los usuarios, el impacto que representa la perdida de confidencialidad, integridad y disponibilidad, de los activos que tiene a su custodia, es decir, si se le hace entender al usuario, que por su culpa o descuido, la organización puede sufrir un impacto negativo, se le creara la preocupación y por tal motivo el interés de protegerse y proteger los activos identificados de la organización.
- Diseñar los planes de sensibilización en seguridad de la información, es decir, una vez definidas las políticas, roles y responsabilidades, identificados los activos, identificados los propietarios de los activos e identificados los riesgos, se estará en la capacidad de diseñar a la medida de la organización, una campaña que cree la conciencia en los clientes internos y externos, en el papel que desempeña cada uno de ellos, para la consolidación y estructuración de un plan de seguridad acorde a las necesidades actuales de la organización.

Dentro del modelo PHVA (Hacer), posterior al diseño de los planes de sensibilización y con el propósito de continuar con el proceso de culturización en seguridad de la información se recomienda realizar las siguientes actividades:

- Definir el personal que será parte de la publicación y formación y los tiempos de divulgación de la campaña; es decir, asignar el personal que ejecutara las campañas de sensibilización en seguridad de la información y el momento oportuno de su aplicación.
- Implementar los planes o campañas de sensibilización en seguridad de la información; es decir, poner en marcha la etapa de formación y capacitación de los usuarios, asegurando que todo el personal se encuentre en la capacidad y competencia de responder al cualquier evento que coloque en riesgo la integridad, disponibilidad y confidencialidad de la información, y por tal motivo, que ponga en peligro la continuidad del negocio.

Dentro del modelo PHVA (verificar), posterior a la implementación de la campaña de sensibilización en seguridad de la información y con el propósito de continuar con el proceso de culturización en seguridad de la información se recomienda realizar las siguientes actividades:

- Medir constantemente la eficacia de las campañas de sensibilización en seguridad de la información; es decir, por medio de auditorías, pruebas de intrusión o mediciones de desempeño, se valida la efectividad y se le recuerda repetidamente al usuario, que el compromiso de proteger la información sigue en pie, y por lo tanto que debe seguir firme en su postura frente a cualquier riesgo. Es importante hacerle ver al usuario que no se capacita por capacitar, si no que se hace por un propósito común, y que de ello depende su puesto de trabajo o la misma estabilidad de la organización.

Dentro del modelo PHVA (actuar), posterior a la verificación de las pruebas realizadas en la anterior actividad, y con el propósito de continuar con el proceso de culturización en seguridad de la información se recomienda realizar las siguientes actividades:

- Publicar los resultados de las mediciones que se realizaron en el punto anterior; es importante darle a conocer al usuario el reflejo de su desempeño, en el camino por garantizar la protección de la información.
- Se deben establecer procesos disciplinarios, para aquellos usuarios, que no cumplen o que de cierta forma, no tienen sentido de pertenencia con la organización; es decir, hay que hacerles entender que las políticas de seguridad de la información están establecidas y hay que cumplirlas, que no solo están en el papel, que el compromiso es de todos, desafortunadamente el ser humano, hace las cosas bajo presión, por tal motivo es indispensable, poner en práctica este tipo de sanciones, en algún momento las políticas las cumplirá no porque se las exijan, sino porque se le ha convertido a través del tiempo en una costumbre o mejor aún en una habito.
- Se deben establecer incentivos, tanto personales como por áreas de trabajo, que premien el hecho de estar comprometidos con la organización; es decir, si un usuario se siente incentivado, motivado en su labor diaria, reflejara un comportamiento de agradecimiento con su organización y por lo tanto evolucionara de tal manera que sus

costumbres, valores organizacionales estén alineados con los propósitos estratégicos de la organización.

- Por último y no menos importante, se debe Involucrar a todos y a cada uno de los usuarios y en cada uno de los niveles que componen la organización, y de manera activa, con el propósito fundamental de la seguridad de la información, que es la de proteger el ciclo completo de la información.

8. Conclusiones

Las organizaciones entienden la importancia que tiene actualmente los activos de información pero desconocen las buenas prácticas para protegerlos.

Las organizaciones pretenden protegerse de amenazas en seguridad de la información pero invirtiendo solo en una de 2 de los pilares fundamentales como los son la tecnología y los procesos, dejando a un lado quizás el más importante en estos tiempos de fuga de información las personas.

Es fundamental que las organizaciones implementen estrategias de sensibilización en seguridad de la información, que se centren en educar por medio de campañas de concienciación y posteriormente en capacitar al factor humano con respecto a las nuevas tecnologías implementadas en la organización.

El promover la cultura organizacional en seguridad de la información es una tarea continua y de seguimiento total, debido a la innovación tecnológica y a las amenazas que conlleva a utilizarla.

9. Referencias Bibliográficas

[1] Jeimy J. Cano. (2012) Pronósticos de seguridad de la información. [En Linea]. Disponible: http://www.infosecurityvip.com/newsletter/palabras_feb12.html

[2] National Security Institute. (2004). Improving Security from the Inside Out Improving Security from the Inside Out. [En línea]. Disponible: http://nsi.org/SECURITYsense.html

[3] C. F. Borghello. Capacitación y Concientización de Seguridad en Organizaciones. [En línea]. Disponible: http://www.segu-info.com.ar

[4] L. J. Ugas. (2002). Seguridad en organizaciones con tecnologías de información. [En línea]. Disponible: http://www.urbe.edu/publicaciones/telematica/indice/pdf-vol1-1/1-seguridad-en-organizaciones-con-tecnologias-de-informacion.pdf.

[5] FISMA. (2002). Construcción de una Seguridad de la Información, Tecnología de sensibilización y formación. [En línea]. Disponible: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[6] D. Rodriguez. (26/04/07). ¿Realmente Sirven los Programas de Culturización en Seguridad informática? [En línea]. Disponible http://www.portaldeseguridad.com/gdc_notapub.php?cod_nota=372.

[7] P. Podestá. (2009). Culture In Organizations A central phenomena in administrative knowledge. [En Línea]. Disponible: http://www.esan.edu.pe/publicaciones/cuadernos-de-difusion/26/Podesta.pdf.

[8] I. Rodríguez Guerra. (2004). Cultura Organizacional. [En linea]. Disponible: http://www.uned.ac.cr/paa/pdf/Materiales-autoev/10.pdf.

[9] S. Jaimes Beltrán, Á. Osorio Domínguez. (2009). La cultura Organizacional Y La Gestión Del Conocimiento. [En línea]. Disponible: http://www.javeriana.edu.co/biblos/tesis/economia/tesis218.pdf.

[10] G. Meléndez. Cultura organizacional. [En línea]. Disponible: http://cicia.uprrp.edu/Papers/Cultura%20Organizacional.pdf.

[11] Diccionario de la Real Academia Española. [2009] Cultura. [En línea]. Disponible: http://www.rae.es/rae.html.

[12] ACIMED. (2009). Clima Y Cultura Organizacional [En línea]. Disponible: http://scielo.sld.cu

[13]. J. Hernández. (2003). Estudio socio psicológico del clima organizacional. [En linea]. Disponible: http://www.uo.edu.cu/ojs/index.php/stgo/article/viewFile/14503333/765.

[14].P. Szabunia. (2010). El cerebro y la cultura organizacional: ¿Similitudes casuales?. [En linea]. Disponible: http://biblioteca2.icesi.edu.co/cgi-olib?session=66860510&infile=details.glu&loid=219547&rs=2514806&hitno=16.

[15]. F. Ferrá Homar. (2003). La Formación, Concienciación Y Sensibilización En Seguridad. [En linea]. Disponible: http://www.revistasic.com/revista56/pdf_56/SIC_56_quepreocupa.PDF.

[16].Área de Investigación y planeación. (2008). Modelo de seguridad de la información para la Estrategia de gobierno en línea. [En Linea]. Disponible: http://programa.gobiernoenlinea.gov.co/apc-aa-iles/5854534aee4eee4102f0bd5ca294791f/GEL_IP_CapacitacionSensibilizacion_ModeloSeguridad.pdf

[17] Watch Guard Technologies (2008). Las 10 principales amenazas a la seguridad de los datos de las PyMEs. [En Linea]. Disponible: http://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp_es.pdf.

[18] Inforgalte (2010). Las diez principales amenazas a la seguridad informática en 2011. [En Línea]. Disponible: http://www.inforgalte.com/blog/las-diez-principales-amenazas-a-la-seguridad-informatica-en-2011.php

[19] Fabien Thomas, Chief Technology Officer, NETASQ (2012). Las 5 principales amenazas para la seguridad en 2012. [En Línea]. Disponible: http://seguridad-informacion.blogspot.com/2012/01/las-5-principales-amenazas-para-la.html.

[20] Symantec Corp. (2012). El informe anual de Symantec sobre amenazas a la seguridad en Internet indica un incremento del 81% en los ataques maliciosos. [En Línea]. Disponible: http://www.symantec.com/es/es/about/news/release/article.jsp?prid=20120507_01

[21] Carlos Tori. Hacking Etico – Ingenieria Social Paper. Rosario: Segunda Edición, 2008, Capitulo III, pp. 87-106.

[22] A. Van de Ven, D. Polley, R. Garud , S. Venkataraman, Desarrollo de una cultura organizacional para innovar. Mexico: Oxford University Press, 2001, pp. 23 – 70.

10. Bibliografía

[1] Abravanel, Allane, Firsirotu, Hobbs, Poupart. Cultura organizacional aspectos teóricos prácticos y metodológicos. Editorial legis, 1988, pp. 15 – 80.

[2] C.F. Borghello (2007, Oct). Informe anual de seguridad del FBI/CSI [En línea]. Disponible: http://www.segu-info.com.ar. Fecha de consulta Noviembre 12 de 2009.

[3] J. Cano. (2004). Hacia un concepto extendido de la mente segura. Pensamiento sistémico en seguridad informática. Artículo de investigación (En revisión). Universidad de los Andes.

[4] J. Cano. (17-Jun-2008). Métricas en Seguridad Informática. [En linea]. Disponible: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/07-MetricasSeguridadInformaticaUnaRevisionAcademica.pdf.

[5] D. Páramo Morales. (Jun-2001). Hacia La Construcción De Un Modelo De Cultura Organizacional Orientada Al Mercado. [En linea]. Disponible: http://editorial.unab.edu.co/revistas/rcmarketing/pdfs/r22_art5_c.pdf.

[6] C. A. Biscione - Technical Account Manager North of Latin America Sun Microsystems. (1999). Ingeniería Social Para No Creyentes. Disponible: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf.

[7] O. Ruiz. (22-Jun-2007). La fuga de información - la amenaza y sus contramedidas. [En línea]. Disponible: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/VIIJNSI_ORuiz.pdf. Fecha de consulta Agosto de 2010.