Artículo de Investigación. Revista Killkana Técnica. Vol. 1, No. 3, pp. 1-8, Septiembre-Diciembre, 2017.
p-ISSN 2528-8024 / e-ISSN 2588-0888. Universidad Católica de Cuenca

La concientización como factor crítico para la gestión de la seguridad de la información

Consciousness as a critical issue for the security management of the information

Cristina Flores Urgilés* y Edison Caiza Andrango
Carrera de Ingeniería de Sistemas, Universidad Católica de Cuenca
Cañar, EC030350, Ecuador
*cmfloresu@ucacue.edu.ec

Resumen

Al enfrentar la tarea de gestionar la seguridad de la información de las organizaciones, se pueden proponer muchos enfoques y criterios que al final convergen en un objetivo primario: "garantizar la información para la estrategia del negocio". Son múltiples los riesgos asociados al uso de tecnologías y sistemas de información, principalmente por los nuevos desafíos organizacionales y la creciente cantidad de amenazas en el entorno. La seguridad de la información orientada al recurso humano es el enfoque menos abordado a la hora de implementar políticas y procedimientos de seguridad; pero el más crítico cuando se pone a prueba. Los fraudes, el robo de información, la pérdida de imagen corporativa y los problemas legales, son algunos de los riesgos a los que se encuentra expuesta una organización si no se concientiza al personal sobre la incidencia de sus responsabilidades para con las políticas de seguridad definidas. Ante este escenario se vuelve preciso definir estrategias de concientización alineadas con la estrategia del negocio. Como resultado de un análisis documental se pueden obtener valiosas conclusiones que pueden ser aplicadas a cualquier organización, cuyos objetivos organizacionales se encuentren alineados con la seguridad de la información.

Palabras clave: Concientización, Estrategia, Fraude, Gerencia, Personal, Marco legal, Robo de Información, Seguridad, Sistemas de Información.

Abstract

When facing the task of information security management of organizations, many approaches and criteria can be proposed in order to eventually converge on a primary objective: "To guarantee information for the business strategy". There are multiple risks associated to the use of technologies and information systems, mainly due to the new organizational challenges and the increasing number of environmental threatens. Human resource-oriented information security is the least addressed approach at the time of implementing security policies and procedures, but it is the most critical issue when put to the test. Fraud, information theft, loss of corporate image and legal problems are some of the risks to which an organization is exposed if the staff members do not become aware of the impact of their responsibilities on the defined security policies. Faced with this scenario, it becomes necessary to define awareness strategies in alignment with the business strategy. As a result of a documentary analysis, valuable conclusions can be drawn that can be applied to any organization whose organizational objectives are aligned with information security.

Key words: Awareness, strategy, fraud, management, personnel, legal framework, information theft, security, information systems.

I. Introducción

La información es considerada como el activo más importante y a la vez vulnerable de toda organización, pues de ello depende su existencia y el posicionamiento que consiga en el medio [1]. Con referencia al incremento sustancial de incidentes de seguridad a nivel mundial que a partir del año 2009 ha llegado a traducirse en un 66 % año tras año [2], las organizaciones orientan todos sus esfuerzos al fortalecimiento de la gestión de la seguridad de la información, considerando a este aspecto como crítico dentro de ella. Son tres los factores que deben armonizar para reducir al mínimo los riesgos de seguridad: la tecnología, los procesos y las personas. Muchas organizaciones, por falta de asesoría, invierten de manera desproporcional en tecnología y procesos, dejando a un lado a las personas; Si bien es cierto, se pueden implementar controles de seguridad sofisticados que vayan de la mano con procedimientos bien definidos, pero también cabe considerar que todo esfuerzo puede resultar inútil si no se concientiza al personal sobre los riesgos existentes sobre una gestión de la información

ineficaz [3].

Aunque obligatorio para algunos, la educación de seguridad, conciencia y capacitación puede respaldar la comprensión general de los problemas se seguridad de una organización, a través de varios enfoques que existen para abordar la concientización de la seguridad, sin embargo, el enfoque organizativo se centra generalmente en lograr aspectos de cumplimiento, como por ejemplo: confidencialidad, integridad y control de reducción de riesgo de disponibilidad. En la mayoría de los casos, se aplicaría un enfoque global sin adaptar a los factores humanos reales involucrados, la interacción humana que es central para el negocio, los procesos y la interacción del sistema, por lo tanto se debe analizar si los aspectos de seguridad se encuentran efectivamente abordados [4].

Este estudio se plantea con el objetivo de determinar la importancia del conocimiento y sensibilización por parte del personal para con la seguridad de la información y analizar los riesgos que conlleva el no prestar la debida importancia a este aspecto tan crítico e importante para la organización.

II. Material y Métodos

Para el desarrollo de esta línea de investigación se utilizó como punto de partida un análisis teórico sobre la gestión de la seguridad de la información y la seguridad asociada al recurso humano. Luego, se llevó a cabo el análisis de varios reportes técnicos sobre incidentes de seguridad a nivel mundial emitidos por empresas especializadas en la temática. Análisis realizado con el objetivo de determinar cuán importante es la participación del personal en estrategias de seguridad institucionales.

A continuación se detalla los aspectos considerados en la metodología utilizada en la presente investigación.

A. *Preguntas de investigación*

Este trabajo busca responder a las siguientes preguntas de investigación:

- ¿Es necesaria la participación del personal en la gestión de seguridad de la información dentro de las organizaciones?
- ¿Cuáles son los riesgos que las organizaciones enfrentan al no contar con políticas de concientización sobre seguridad de la información?.

B. *Diseño*

Se realizó una revisión sistemática de documentos de sociedades científicas dedicadas a la seguridad de la información, concentrándose en los informes anuales de estadísticas sobre el comportamiento de los riesgos tecnológicos a nivel mundial, presentados por empresas especializadas en seguridad.

C. *Estrategia de búsqueda*

En primer lugar se llevó a cabo una búsqueda en Google Scholar de documentos asociados a las siguientes áreas: Seguridad de la Información, Seguridad asociada al recurso humano, Riesgos de TI en las organizaciones, Reportes de Incidentes de Seguridad publicados tanto en Ecuador como a nivel mundial. Estas búsquedas se realizaron tanto en español como en inglés.

D. *Propósito de la Búsqueda*

- Establecer cuáles son los riesgos que se presentan con mayor probabilidad de concurrencia a nivel mundial y del Ecuador, que puedan afectar las actividades de una organización.
- Analizar la relación que existe entre el personal de una organización con cada unos de los aspectos de seguridad de la información.
- Analizar estrategias de concientización al personal, propuestas por varios autores como resultados de sus investigaciones.

E. *Fuente de información y Motores de Búsqueda*

- Tesis de Maestría, Artículos científicos, Informes técnicos, Libros.
- Google Scholar, Bases de datos científicas UCACUE.

F. *Criterios de búsqueda*

‘Gestión de la seguridad de la información’, ‘Riesgos de TI’, ‘Estrategias de concientización’, ‘Informe riesgos tecnológicos’.

G. *Criterios de Inclusión*

Documentos que contienen información sobre la seguridad de la información asociada al recurso humano de las empresas y reportes estadísticos de incidencias de seguridad.

H. *Criterios de Exclusión*

Se excluyen los documentos que al referirse a la seguridad de la información abarcan otro tipo de información que no se relaciona al tema central del análisis, además de excluir aquellos reportes técnicos con datos obsoletos de fechas mayores a cinco años.

I. *Evaluación del contenido de los criterios*

Exactitud, objetividad, cobertura, relevancia de acuerdo a las preguntas de investigación.

J. Análisis de los datos

La información analizada contribuyó con las siguientes variables: En lo que respecta sobre documentos seguridad de la información y su relación con el personal se pudieron extraer aspectos como Fundamentación teórica, conclusiones y resultado de casos de estudio. Los reportes técnicos de incidentes aportaron con datos estadísticos de los ataques reportados dentro del país y a nivel mundial, el análisis de los resultados y las conclusiones. En base a la información extraída se conformó un documento que proporciona una visión general de la temática, abordando cada aspecto desde el punto de vista del recurso humano de las organizaciones.

III. Resultados y Discusión

A. Gestión de la Seguridad de la Información

Actualmente existe una estrecha relación entre la gestión organizacional y las tecnologías de la información, en vista que las empresas diariamente producen una gran cantidad de datos, que deben ser procesados por aplicaciones informáticas para la generación de información. En este sentido, es responsabilidad del departamento de TI, identificar mecanismos que permitan resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. Dentro de los aspectos que son tomados en cuenta por una organización en términos de seguridad, se puede contemplar la implementación de políticas de seguridad, misma que tiene como objetivo "proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes" [5].

En realidad casi todas las organizaciones que han implementado políticas de seguridad no las cumplen de manera consciente.

> Los gerentes y los empleados dentro de una organización a menudo tienden a considerar la seguridad de la información como una prioridad secundaria si se la compara con su propia eficiencia o asuntos de efectividad, porque estos tienen un impacto directo y material sobre el resultado de su trabajo [6].

La responsabilidad, confianza, comunicación y cooperación son las cuatro piedras angulares de una atractiva cultura de gestión de la seguridad, usar un enfoque que motive y empodere a los empleados a desempeñar un papel activo en la seguridad es importante para lograr comportamientos positivos [4].

Ante esta situación se necesita un compromiso serio por parte de la gerencia para capacitar al personal y que las políticas de seguridad se encuentren por encima de la eficiencia. Otro factor importante a tomar en cuenta es la identificación de información sensible y crítica que debe ser analizada de manera profesional y objetiva mediante un enfoque de riesgos. Si el encargado de TI alinea los objetivos de TI con los del negocio y es capaz de concientizar a la alta gerencia de los riesgos de seguridad, entonces invertirán recursos para mitigarlos y contribuir a una organización que cuida su activo más importante, su información [7].

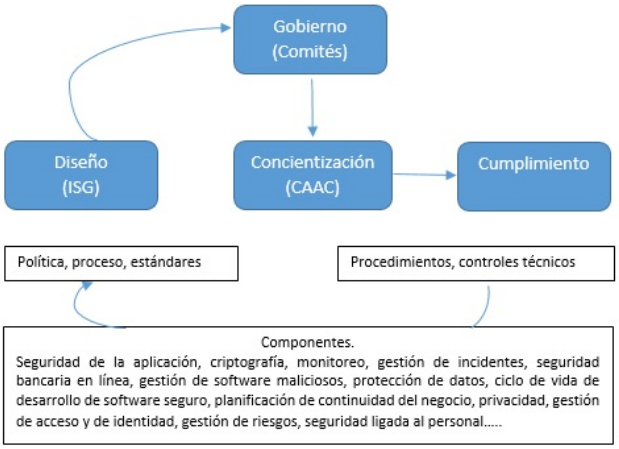

FIG. 1. Gestión de Seguridad de la Información- Gobierno TI. Fuente https://www.isaca.org

B. Seguridad asociada al recurso humano

La seguridad de la información asociada al recurso humano comprende las políticas y procedimientos a cumplir, desde la selección del personal, hasta la finalización de contrato [8]. Tomando como referencia la norma ISO 27002, código de práctica para la seguridad de la información que está compuesto por 14 dominios, 35 objetivos de control Y 114 controles, se debe implantar ciertos controles asociados al dominio 7. Seguridad Ligada a los Recursos Humanos [9].

Este dominio representa la necesidad de educar e informar al personal desde el momento de su ingreso y de manera permanente, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad [11].

1. Controles

- Antes de la contratación.
  - Investigación de antecedentes.
  - Términos y condiciones de contratación.
- Durante la contratación.
  - Responsabilidades de gestión.
  - Concientización, educación y capacitación en segur. de la informac.
  - Proceso disciplinario.
- Cese o cambio de puesto de trabajo.
  - Cese o cambio de puesto de trabajo [12].

La aplicación correcta de estos controles aportaran a la reducción de los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

C. Antes de la contratación

En la etapa de reclutamiento se deben verificar los antecedentes de todos los candidatos en conformidad con los requerimientos del negocio, leyes, regulaciones, ética. Las buenas prácticas de gestión de TI recomiendan poner especial atención al "porcentaje de empleados de TI a los que se han verificado sus antecedentes" [10] con la finalidad de filtrar a potenciales perpetradores.

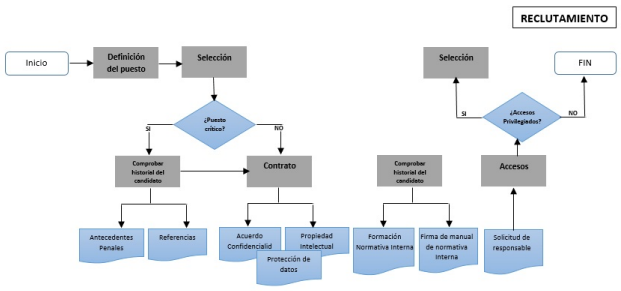

FIG. 2. Reclutamiento Personal. Fuente [8]

Una vez aceptado por la organización, y antes de entregarle accesos a la información, el empleado debe firmar un contrato de confidencialidad y no revelación. Mientras dure el empleo o el tiempo que el negocio considere necesario para no brindar ventaja competitiva a la competencia, la gerencia debe preocuparse que el empleado cumpla con las políticas de seguridad y las responsabilidades que conlleva.

Finalmente, para terminar el contrato laboral se deben retirar los permisos de acceso lógico a la información y advertir de las responsabilidades legales continúas.

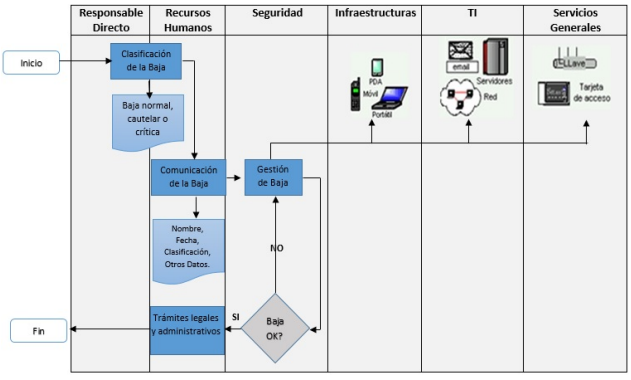

FIG. 3. Salida de Empleados. Fuente [8].

D. Riesgos de la falta de concientización

Mantener la seguridad de la información y proteger los activos de datos sigue siendo una preocupación principal para las organizaciones, muchas violaciones de datos continúan siendo accidentales, intencionales o maliciosos. Factores humanos, que conducen a pérdidas financieras o de reputación [4].

Conductas erradas en relación con las seguridad de la información por parte del personal, conducen a la materialización de amenazas que aprovechan el estado vulnerable de la organización [28].

Algunos de los riesgos que pueden ocasionar un mayor impacto son:

1. El Fraude

Una de las manifestaciones lesivas más intensamente desarrolladas en la Red es precisamente aquella consistente en la producción fraudulenta de perjuicios patrimoniales a terceros. Esto es lo que básicamente podría englobarse bajo el concepto de Fraude[14]. El fraude es cualquier acto ilegal caracterizado por el engaño, el ocultamiento o la violación de la confianza [15]. Los fraudes son perpetrados por organizaciones e individuos para: obtener dinero, evitar pagos o asegurarse una ventaja personal en el negocio.

Resumimos a continuación cuales son algunas de las principales fórmulas de fraude utilizadas en el medio internet:

- Sustracción de las claves de acceso sin el conocimiento de la víctima (spyware)
- Obtención fraudulenta de las claves: Es la propia víctima la que, sin saberlo, hace llegar al defraudador los datos necesarios para realizar las transacciones
- Dialers (conexiones telefónicas fraudulentas)
- Fraudes en operaciones de comercio electrónico
- Envío de mails fraudulentos

El robo de información, al igual que casi todos los tipos de fraude, habitualmente son delitos perpetrados internamente. El fraude vinculado con la información es común y está evolucionando. De acuerdo a los informes globales de fraude realizados por Kroll en el 2013 y 2015, un promedio del 20 % de empresas encuestadas fueron afectadas con robo de información. De los afectados, el 57 % tiene previsto invertir en la capacitación de sus empleados para reducir la exposición a incidentes de seguridad [16] [2], así como la mitad de los encuestados manifiestan que se siente altamente vulnerables a riesgos de fraude.

Estudios realizados por la consultora PWC sobre Gestión de Seguridad de Información de Sistemas (GSIS) develan que los perpetradores pueden ser empleados, proveedores y hackers. Un alto porcentaje de los encuestados atribuye los incidentes de seguridad a los accesos a la información privilegiada por los empleados actuales (31 %) o ex empleados (27 %). "Es importante destacar que las amenazas internas no provienen necesariamente de un "Hacker" o de un "usuario malintencionado", sino que podría ser el perfil de un buen empleado que hace el trabajo justo de manera insegura" [17]. Un empleado inconsciente puede ser fácilmente involucrado en un fraude e imputado ante la justicia.

El robo de identidad es una práctica empleada para realizar actividades fraudulentas. La autenticación en sitios restringidos con credenciales robadas es un problema evidente. Si el empleado no es consciente del riesgo que supo-

TABLA I
PORCENTAJE DE COMPAÑÍAS AFECTADAS POR DISTINTOS TIPOS DE FRAUDE. FUENTE INFORME GLOBAL SOBRE FRAUDE 2013/2014 HTTPS://WWW.KROLL.COM/EN-US

Tipo de Fraude	2012	2013	2015
Robo de activos físicos	28%	24%	22%
Robo de información	22%	21%	15%
Conflicto de intereses de la gerencia	20%	14%	12%
Fraude de vendedores, proveedores o adquisiciones	19%	12%	17%
Fraude financiero interno	16%	12%	9%
Infracción regulatoria o de cumplimiento	16%	11%	12%
Corrupción y soborno	14%	11%	11%
Robo de PI	11%	8%	4%
Colusión de mercado	8%	3%	
Malversación de fondos de la compañía	8%	-	7%
Lavado de dinero	3%	1%	4%

ne revelar sus contraseñas, entonces no le pondrá cuidado a su custodia aun cuando existan políticas referentes a ello. En Ecuador, de acuerdo con reportes de la ECUCERT – SUPERTEL [18], de enero del 2014 a septiembre del 2014, se han reportado 9 casos de suplantación de identidad a sujetos políticos como Mauro Andino e instituciones como la Policía del Distrito Metropolitano de Quito. La modalidad de ataque es principalmente a través de las redes sociales, sin embargo estas cifras evidentemente están alejadas de la realidad, esto se debe a que las personas no realizan las acusaciones formales por desconocimiento o porque no se ven afectadas directamente.

E. Robo de información

El riesgo que supone el robo de la información sensible de una organización es crítico, e incluso puede resultar catastrófico, para la estrategia en el cumplimiento de sus objetivos. Los hackers internos y externos pueden adueñarse de la información y usarla con fines dolosos. El empleado que no es consciente de la seguridad de la información, puede ser blanco fácil de los hackers y entregar la información sin resistencia alguna.

Un ataque informático es metódico y al menos comprende cinco fases: reconocimiento, exploración, obtener acceso, mantener acceso y borrar huellas [19]. En la primera fase el atacante obtiene información de acceso a los sistemas con ayuda de la víctima (persona u organización) utilizando varias técnicas entre ellas la Ingeniería Social. "Una de las últimas categorías de los exploits es el engaño o la mentira. La mayoría de los ataques no se pueden consolidar, si no existe de por medio mecanismos de engaño que se encuentren implicado" [20]. Por lo tanto, resulta clave impedir esa primera fase capacitando al personal.

El Phishing es una de las prácticas más comunes de ataques a través de Ingeniería Social. Según reportes de Viruslist, Brasil encabeza la lista de países más atacados en el año 2015. Las políticas de restricción de contenido para navegar en Internet pueden resultar efectivas, pero si un mensaje malicioso para efectuar Phishing se filtra por un sitio de confianza, entonces se puede poner en riesgo la información de la organización.

TABLA II
TOP 10 DE PAÍSES SEGÚN LA CANTIDAD DE USUARIOS ATACADOS. FUENTE HTTP://WWW.VIRUSLIST.COM

Orden	País	% de usuarios atacados
1	Brasil	21.5%
2	China	16.7%
3	China	14.6 %
4	Reino Unido	13.8%
5	Japón	13.1%
6	India	12.9%
7	Australia	12.4 %
8	Bangladesh	12.4%
9	Canadá	12.2%
10	Ecuador	12.0%

El Phishing también genera incertidumbre en el Ecuador, ya que el mismo estudio realizado por kaspersky lo encasilla en el puesto número doce de los países que han reportado mayor número de ataques. Así también según informe de la ECUCERT – SUPERTEL se registran, de enero del 2014 a septiembre del 2014, un total de 89 casos. La modalidad de ataque es infectar servidores para robar datos y de esa manera suplantar identidad de bancos, cooperativas e instituciones gubernamentales [18].

Conforme a los mismos reportes, se han registrado 3633 casos de desfiguraciones web , con el fin de que los visitantes pierdan la confianza en un sitio web y por ende en la organización. En este punto, todas las organizaciones sean públicas o privadas, de manera primordial las instituciones financieras, deben cuidar su imagen institucional para fomentar la confianza de sus clientes y sobre todo de la comunidad.

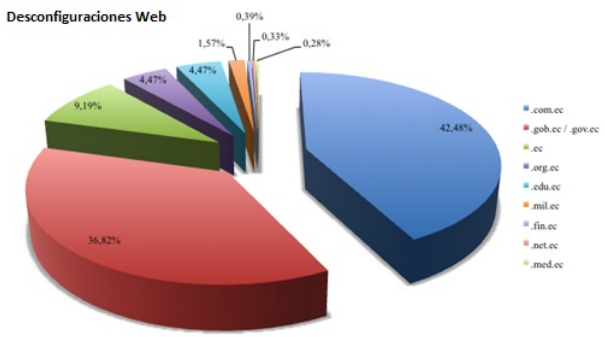

FIG. 4. Ataques de Desfiguración Web a los distintos dominios. Fuente http://www.ecucert.gob.ec/

F. Problemas legales

Junto con los riesgos de fraude y robo de información, se pueden sumar los problemas legales. De acuerdo con la legislación de cada país, se pueden experimentar todo tipo de sanciones por el uso inadecuado de las tecnologías de información. Para la implantación de cualquier tipo de política organizacional, se vuelve mandatorio revisar la jerarquía de leyes a las que debe regirse.

Es responsabilidad de los gerentes entregar la estrategia para capacitar al personal sobre los riesgos que supone el manejo de información privada. Si el recurso humano de la organización no es consciente de las implicaciones legales, entonces puede incurrir en actos ilegales sin mayor reparo ni cuestionamiento. La divulgación de información de terceros puede ser sancionada de manera severa. Cabe recordar que el desconocimiento no exime de culpa .

En Ecuador la Constitución de 2008, garantiza el acceso universal a las tecnologías de información y comunicación (Art.16. Nº 2) y la protección de datos personales (Art.66. Nº 19) [21]. En este sentido se mantienen leyes y decretos que establecen apartados acordes con la importancia de la tecnología, tales como:

- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Ley de Propiedad Intelectual.
- Ley Especial de Telecomunicaciones.
- Ley de Control Constitucional (Reglamento Habeas Data) [22].

G. Estrategia de concientización

Cuando se habla de estrategias de concientización, se expone un conjunto de técnicas tales como selección de controles, entrenamiento de seguridad, educación y desarrollo. Cualquier estrategia debe proporcionar los elementos de juicio para que el personal esté consciente de sus responsabilidades como parte de sus labores.

La concientización debe estar alineada con las políticas institucionales y las necesidades específicas de la organización, independientemente de la guía que utilice como herramienta de trabajo. Tal como lo manifiesta J. Vasquez en su trabajo de investigación [23]. Pero deberíamos considerar que para materializar controles se requiere una adecuación de la organización que se debe realizar dependiendo en gran medida del presupuesto que se tenga asignado para ello. Una vez que se han implementado los controles, entonces se puede seguir un estándar [4].

De igual manera Gundu y Flowerday (2013) señalan que las campañas de seguridad puede requerir un presupuesto adicional en términos de costos directos e indirectos, costos incluidos en la producción y mantenimiento del programa, aunque sugiere que el uso del e-learning puede reducir los costos de distribución, además de trabajar conjuntamente con otros departamentos con el fin de obtener mayor presupuesto y consigo programas de calidad y con mejores resultados [24].

Pero como lograr que el personal tome verdadera conciencia de los aspectos de seguridad, tomamos como referencia el Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información del Ministerio de TIC de Colombia, que propone un programa efectivo de concientización, en el cual se expone las reglas de comportamiento para los usuarios de las áreas que emplean las TI. Los procedimientos y políticas de seguridad deben proceder y se ponen como base para cualquier sanción por incumplimiento. Las distintas responsabilidades solo se justifican solo si el personal está informado, entrenado y consciente [25].

El punto clave para conseguir un entorno seguro es lograr que los empleados entiendan primero la responsabilidad personal del uso de las tecnologías de información y luego puedan aportar a la cultura organizacional. “Esta concientización debe ir más allá de las políticas de alto nivel e incluye ejemplos pragmáticos, como las actividades permitidas y prohibidas al momento de utilizar redes sociales, laptops, tabletas o teléfonos inteligentes. Una lista concreta de “lo que debe y no debe hacerse” es la forma más eficaz de comunicar las políticas y habilitar su uso responsable” [26].

A fin de evitar fraudes y robo de información, un buen programa debe incluir recomendaciones sobre la custodia de credenciales de acceso a espacios físicos y aplicaciones. El robo de contraseñas, cracking e incluso adivinar contraseñas son amenazas de los entornos organizacionales. La mejor forma de protegerse de estas amenazas es desplegar sistemas de autenticación múltiple, pero sobretodo capacitar al personal sobre los hábitos de crear contraseñas seguras y renovarlas periódicamente. Elaborar políticas de seguridad de la información y capacitar a los empleados sobre el riesgo, es una acción muy utilizada para hacer frente a esta problemática [27].

La concientización es realmente un mundo muy amplio pero debe centrarse en las posibilidades de una organización. La tarea de concientización no solo debe esforzarse en capacitar al usuario en los nuevos temas sino que también debe trabajar en erradicar las malas costumbres adquiridas durante mucho tiempo con respecto a la seguridad de la información. Hay que crear conciencia para formar hábitos y cultura. La seguridad es responsabilidad de todos [29].

IV. Conclusiones

En la actualidad las organizaciones enfrentan nuevos retos al emplear las tecnologías y los sistemas de información, debido a los riesgos del entorno y la falta de consciencia de sus empleados en temas de seguridad de la información. Los reportes estadísticos de consultoras especializadas ofrecen un claro panorama de los riesgos a los que se expone una organización por la falta de políticas de seguridad que incluyan la concientización de las responsabilidades del empleado en temas referentes al trabajo con

la información corporativa.

Pero el problema nace directamente desde la alta gerencia de las organizaciones, debido a que desde este punto se le da un valor secundario a los aspectos de seguridad , la cultura informática en los directivos en muchos casos es pobre y por esta razón las responsabilidades directamente se las entrega a TI, con un mínimo presupuesto y sin el apoyo necesario.

Un programa de concientización para ser efectivo debe encontrarse alineado con la estrategia del negocio e incluir a todos y cada uno de quienes la conforman. Las campañas de concientización que incluyen temas de actualidad, tienen resultados aceptables, pero para conseguir mejorar los niveles de seguridad, hace falta primero eliminar los malos hábitos existentes y que se han heredado de una gestión deficiente.

Referencias

[1] Morocho. D, Diseño de un Sistema de Seguridad de la Información para EcuCERT," Master's thesis, Escuela Politécnica Nacional, 2014.

[2] PWC, "Managing cyber risks in an interconnected world Key findings from The Global State of pInformation Security® Survey 2015," tech. rep., PWC, 2015.

[3] Castillo. R & Di Mare. A & Díaz. V & Díez. H, Concientización en Seguridad de la Información," Master's thesis, Universidad de los Andes – Bogotá, Colombia.L, 2004.

[4] Duncan . K *, Shamal . F, Persona-centred information security awareness.," Article,computers & security, 2016.

[5] ISO27002, 5 1 política de seguridad de la información." https://iso27002.wiki.zoho.com/5-1-Pol%C3%ADtica-de-seguridad-de-la-informaci%C3%B3n.html. [Online; accessed 02-05-2016].

[6] ISACA, *Manual de Preparación del Examen CISA 2009. La Seguridad de los Recursos Humanos y Terceros*. https://www.isaca.org/cisabooks, 2009.

[7] Najla . A * and Lazar . R, IT Governance in a Public Organization in a Developing Country: A Case Study of a Governmental Organization.," Article,Procedia Com, 2015.

[8] Matamoros. B, Rodriguez. R, Arteaga . J, SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL AREA DE RECURSOS HUMANO.,"Master's thesis,Escuela Superior Politécnica del Litoral, 2011.

[9] G. Hardy, M. & J Heschl, *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.*. ISACA, 2008. http://www.isaca.org.

[10] ISACA, *Cobit 4.1*, ch. P07. Administrar los Recursos Humanos de TI. Procedimientos de Investigación del Personal. PO7.6., pp. 55–56. ISACA, 2007.

[11] ISO 27002 en Español, 7. Seguridad Ligada a los Recursos Humanos." http://www.iso27000.es/iso27002_7.html, 2012. [Online; accessed 02-05-2016].

[12] GES CONSULTOR, Çontroles ISO 27002:2013". http://www.iso27000.es/download/ControlesISO27002-2013.pdf, 2013.

[13] E. Piattini, M. & Del Peso, *Auditoria Informática un Enfoque.*, ch. Metodología de Evaluación de Sistemas., p. 3(2). 50. RA-MA S.A, 2000.

[14] Fernandez . J,Respuesta Penal Frente a Fraude Cometidos en Internet: Estafa, Estafa Informática y los Nudos de la Red.," Article,Revista de Derecho Penal y Criminología, 2007.

[15] T. I. of Internal Auditors, *Normas Internaciones para el Ejercicio Profesional de la Auditoria Interna*, 2012.

[16] H. T., "Informe global sobre fraude 2013/2014," tech. rep., KROLL, 2014.

[17] PWC, "Key findings from the global state of information security survey," tech. rep., PWC, 2014.

[18] E. SUPERTEL, "Informe de incidentes informáticos. reportes de incidentes 2014," tech. rep., ECUCERT - SUPERTEL, 2014.

[19] M. J., "Ataques informáticos - debilidades de seguridad comúnmente explotadas," tech. rep., Evil Fingers, 2009.

[20] J. Arango, *El Atacante Informático*, ch. Conociendo al Enemigo, p. 38. itforensic, 2010.

[21] A. C. Ecuador, *Constitución de la República del Ecuador 2008*. Quito: CONAMU, diciembre 2008.

[22] L. Ureta, "Retos a superar en la administraciÓn de justicia ante los delitos informÁticos en el ecuador," Master's thesis, ESPOL, 2009.

[23] J. Vázquez, ESTRATÉGIAS DE DIFUSIÓN Y CONCIENTIZACIÓN EN SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. ch. Concientización y Entrenamiento de Seguridad de la Información, Basado en las Mejores Prácticas., pp. 53–54.,"Master's thesis, Instituto Politécnico Nacional, 2009. http://tesis.ipn.mx/jspui/bitstream/123456789/8656/1/98.pdf

[24] T. Gundu , S. Flowerday . Ignorance to awareness: towards an information security awareness process. SAIEE Afr Res J 2013;104(2):69–79.

[25] Ministerio TIC, *Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información.*. Colombia, 2016.

[26] E. . Young, "Seguridad de la información en un mundo sin fronteras," tech. rep., Mancera, S.C, 2011.

[27] M. D. H. J. . G. S. Doroteo, B., "Modelo de concientizaciÓn en la fuga de informaciÓn.," Master's thesis, INSTITUTO POLITÉCNICO NACIONAL, 2010.

[28] Abril. A, Pulido . J; Bohada. JA, Análisis de Riesgos en Seguridad de la Información.," Article, Revista JDC, 2014.

[29] Rahman . A , Lubis. M ,Lubis . A, Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures.," Article,Procedia Computer Science, 2015.

***Recibido**: 15 de agosto de 2017*

***Aceptado**: 12 de diciembre de 2017*

Cristina Flores Urgiles: *Ingeniera de Sistemas , Magister en Evaluación y Auditoria de Sistemas Tecnológicos, Catedrática de la Universidad Católica de Cuenca*

Edison Caiza Andrango: *Ingeniero en Sistemas e Informática, Magister en Evaluación y Auditoria de Sistemas Tecnológicos, Analista Banco Central del Ecuador.*