1302/1061

Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

TRABAJO FINAL

Título

Los desafíos de la concientización en las organizaciones actuales

Autor:
Stella Maris Vilca

Tutor:
Raúl Saroka

Año de presentación: 2017

Año Cohorte: 2009

Declaración Jurada de origen de los contenidos

Por medio del presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis o Trabajo Final de Maestría vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Stella Maris Vilca

DNI 23.611.082

1. Resumen

El incremento del uso de medios y herramientas informáticas proporciona beneficios y ventajas a las organizaciones. Sin embargo, también implica el surgimiento de nuevos riesgos. Para mitigar estos riesgos las organizaciones implementan diferentes medidas, una de ellas es promover en sus integrantes, el conocimiento y el sentido de la responsabilidad en seguridad de la información. Para cumplir con este objetivo, las organizaciones realizan actividades de concientización que responden a las necesidades y particularidades de las mismas.

La concientización debe propender a que las personas entiendan sus responsabilidades en materia de seguridad de la información, conozcan sus obligaciones ante la organización y utilicen y protejan apropiadamente los recursos informáticos confiados a ellos.

En consecuencia, los profesionales de seguridad de la información deben analizar los aspectos fundamentales de la concientización y conocer los desafíos que deben afrontar las organizaciones actuales para implementar las acciones efectivas que mitiguen los riesgos asociados al factor humano y lograr que las organizaciones tengan una cultura de la seguridad.

Finalmente, se acota que la metodología utilizada en el presente trabajo es del tipo descriptiva. Se realizó la recolección, sistematización de la información relativa al tema y se evaluaron determinadas variables o particularidades para caracterizar la realidad estudiada.

1.1. Palabras claves

Concientización – factor humano – riesgos

Indice

Cuerpo Introductorio 1
Capítulo I 3
1.1 Definición de concientización 3
1.2 Fundamentos de la concientización 3
1.3 Responsables de la concientización 9
1.4 Proceso de concientización 10
Capítulo II 16
2.1 La evolución de la gestión de los ciber-riesgos y la seguridad de la información - encuesta 2016 sobre tendencias de los ciber-riesgos y la seguridad de la información en Latinoamérica realizado por Deloitte 16
2.2 Reporte de seguridad para Latinoamérica realizado por ESET 19
2.3 Tendencias del año 2016, encuesta nacional de seguridad informática llevado a cabo por ACIS 22
2.4 Encuesta de seguridad cibernética en las principales empresas australianas realizada por el CERT y el ACSC de Australia 25
2.5 Estado de la seguridad cibernética para el año 2016, realizado por ISACA y la conferencia RSA 27
2.6 Reporte de concientización en seguridad de la información efectuado por Sans 30
2.7 Resumen de los resultados de las encuestas 40
Capítulo III 48
3.1 Propuesta de Concientización 49
Conclusión 56
Anexo A: Roles involucrados en la concientización 61
Anexo B: Proceso de concientización 65
Anexo C: Detalle de las actividades de Concientización 76
Anexo D: Material de soporte de las actividades de Concientización 79
Bibliografía 122

Cuerpo Introductorio

El presente trabajo pretende dar respuestas a las siguientes preguntas: ¿qué es la concientización?, ¿por qué una organización debe concientizar a su personal?, ¿quiénes son los responsables de concientizar?, ¿cómo se realiza la concientización? y ¿cuáles son los desafíos que debe abordar la concientización en las organizaciones actuales?

Asimismo, se definió como objetivo general analizar los aspectos fundamentales de la concientización en seguridad de la información y los principales desafíos que debe abordar la concientización en las organizaciones actuales. Por otro lado, se establecieron como objetivos particulares:

- Definir el concepto de concientización.
- Identificar los responsables de la concientización.
- Describir los pasos para realizar la concientización.
- Analizar los principales desafíos de la concientización.
- Elaborar una propuesta de concientización para una empresa mediana, pequeña o micro de Argentina.

Para cumplir con los objetivos mencionados se definió la siguiente estructura en el presente documento:

Capítulo I: corresponde al marco teórico conceptual, incluye las definiciones de los conceptos relevantes. Al respecto, por cada tema evaluado se consultaron diversas fuentes de información y se presentó una conclusión del análisis de las mismas.

Capítulo II: presenta los resultados de las encuestas efectuadas por entidades reconocidas en Latinoamérica, Estados Unidos de América, Australia y Europa entre otros lugares. En particular, se focalizó el análisis de los resultados de las encuestas en identificar el estado actual de la concientización. Adicionalmente, se incluyó un resumen de los resultados obtenidos.

Capítulo III: describe una propuesta para llevar a cabo un proyecto de concientización en una empresa mediana, pequeña o micro de Argentina.

Finalmente, se considera que el presente trabajo aporta una revisión apropiada de los conceptos fundamentales de la concientización en seguridad de la información, un análisis que permite conocer los desafíos que debe afrontar la concientización para disminuir la brecha existente entre su nivel de madurez actual y el estado esperado según las buenas prácticas y una propuesta de concientización que puede ser utilizada como ejemplo para empresas medianas, pequeñas o micros de Argentina.

Capítulo I

1.1 Definición de concientización

Para el presente trabajo concientizar significa hacer que alguien sea consciente de algo [1]. Alguien será consciente de algo cuando tenga idea del alcance y las consecuencias que tienen sus actos.

En materia de seguridad de la información, la concientización debe lograr que los integrantes de la organización tomen conciencia de la importancia de la seguridad de la información e incorporen en su comportamiento habitual las buenas prácticas para garantizar la protección de la integridad, la confidencialidad y la disponibilidad de la información.

La concientización en seguridad de la información, al menos, debe:

- comunicar las políticas y procedimientos relativos a la seguridad.
- explicar las reglas de comportamiento para el uso de los sistemas y la información.
- informar las sanciones por no cumplimiento.
- identificar las distintas audiencias a las que se deben dirigir los mensajes de concientización.
- ser medible y verificable.
- responder a las necesidades de concientización detectadas.
- contemplar que el aprendizaje es continuo y los usuarios pueden requerir entrenamiento adicional para desarrollar habilidades específicas. [2]
- revisar y actualizar regularmente el contenido de los mensajes a difundir.
- Incluir en el contenido de los mensajes a difundir el 'qué', 'cómo' y 'porque' con el fin de que las personas entiendan el impacto, tanto positivo como negativo, que puede tener su comportamiento en la organización. [3]

1.2 Fundamentos de la concientización

La seguridad de la información es una cuestión humana y tecnológica. El "factor humano" y no exclusivamente la tecnología, es la clave para

proveer un nivel adecuado y apropiado de seguridad. La concientización es primordial para garantizar que las personas entiendan sus responsabilidades en materia de seguridad, las políticas de la organización y como usar apropiadamente y proteger los recursos informáticos confiados a ellos. [2]

Las empresas que dependen de la tecnología, pero descuidan el factor humano y particularmente los niveles de concientización, pasan por alto un factor crucial en la protección de la información, debido a que los controles técnicos no ofrecen una solución completa y absoluta en materia de seguridad. [12]

Por ejemplo, las recomendaciones de seguridad para los ataques con código malicioso del tipo ransomware consisten en realizar un adecuado entrenamiento de los usuarios, gestionar apropiadamente la actualización del sistema operativo y el antivirus, realizar copias de seguridad regularmente y restringir la asignación de los permisos de control total y escritura sobre los archivos a proteger. [4] En este tipo de ataque las medidas técnicas no son suficientes y es esencial que los usuarios se encuentren adecuadamente concientizados. Ransomware es un tipo de código malicioso que se puede instalar de forma encubierta en una computadora sin el conocimiento del usuario. Dicho programa permanece sin interactuar con el usuario hasta que recibe una orden del atacante para cifrar los archivos o bloquear por completo el equipo. Finalmente, el equipo vuelve a la normalidad cuando el atacante recibe el beneficio financiero solicitado. Este tipo de ataque ocasionó importantes perjuicios en varias organizaciones durante los últimos años a nivel mundial. Según publicaciones de internet algunas víctimas de este tipo de ataque fueron:

- Universidad de Calgary, quien pagó a los atacantes 20.000 dólares canadienses para recuperar su información [5]
- Kansas Heart Hospital [6]
- Departamento de Policía de Melrose en Massachusetts, Estados Unidos [7]
- Centro Médico Presbiteriano de Hollywood, quien pagó a los atacantes 17.000 dólares para recuperar su información [8]

Por otro lado, la concientización es mencionada en importantes documentos sobre buenas prácticas en seguridad de la información, tanto

nacionales como internacionales, incluyendo normativas de cumplimiento obligatorio. A continuación, se describen los principales comentarios sobre la concientización en algunos documentos de buenas prácticas:

Documento	Comentarios
ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls	En el apartado que trata sobre la seguridad de los recursos humanos, menciona, entre otros puntos que: - los empleados y proveedores deben ser conscientes y cumplir con sus responsabilidades en materia de seguridad de la información. - todos los empleados de la organización y los proveedores deben recibir educación y entrenamiento en las políticas y procedimientos de seguridad de la información que sean requeridos para realizar su trabajo, como así también las actualizaciones regulares en la materia. [3]
COBIT 5.0.para la Seguridad de la Información de ISACA	Presenta un enfoque integral y orientado al negocio para la gestión de la seguridad de la información y tiene un capítulo específico sobre cultura, ética y comportamiento y otro titulado personas, habilidades y competencias. Entre otros puntos, sostiene que: - debe existir una cultura de la seguridad de la información. Al respecto, Isaca describe la cultura de la seguridad de la información de la siguiente forma: "Todas las empresas tienen una cultura en seguridad de la información. En la mayoría de los casos, carece de intencionalidad y es inconsistente a las medidas que existen;

	en otros, es robusta y guía las actividades diarias de los empleados y otras personas que entran en contacto con la empresa". - para implementar con eficiencia una función de seguridad de la información en una empresa, los individuos que ejercen esta función deben contar con un conocimiento y experiencia apropiado. Las habilidades y competencias tienen un ciclo de vida. Se debe conocer la línea base de habilidades actual y luego se debe planificar según el objetivo que se desea alcanzar. Las habilidades y aptitudes relacionadas con la seguridad de la información son: gobierno de la seguridad de la información, formulación estratégica de la seguridad de la información, gestión del riesgo de la información, desarrollo de la arquitectura de la seguridad de la información, operaciones de la seguridad de la información y evaluación, pruebas y cumplimiento de la información. [9]
Política de Seguridad de la Información Modelo	En la cláusula de recursos humanos, establece: - educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, 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. De la misma forma, es necesario definir las sanciones que se

	aplicarán en caso de incumplimiento -Establecer compromisos de confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información. -Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia. - responsabilidades para el área de Recursos Humanos (incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política) y el área Jurídica (participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención)

	- todos los empleados del Organismo y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el organismo, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del Organismo. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general.[10]
Comunicación "A" 5374 del Banco Central de la República Argentina. Normas sobre "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras". Modificación	Define requisitos mínimos para la concientización y entrenamiento, tales como: - los contenidos deben formularse y mantenerse actualizados en base a un análisis de las vulnerabilidades y los resultados de la gestión de incidentes. - definir temas específicos a incluir en el contenido de la concientización y entrenamiento. Por ejemplo: recomendaciones específicas sobre el uso seguro de los dispositivos propios del usuario y los dispositivos provistos por la entidad/operador. - definir la segmentación de la audiencia, en al menos en personal interno, personal responsable por la gestión del canal electrónico, proveedores y clientes. - efectuar con una periodicidad mínima anual un análisis de las actividades de

	concientización con respecto a la evolución de los incidentes [11]

En resumen, se observa que las buenas prácticas comparten los siguientes lineamientos:

- la concientización alcanza a usuarios internos y a otras personas que no pertenecen a la organización, pero interactúan con la misma.
- la organización debe realizar tareas de concientización.

1.3 Responsables de la concientización

Todos los integrantes de la organización tienen un rol y responsabilidad en el éxito de la concientización, inclusive las personas externas a la organización, por ejemplo, visitantes y proveedores.

Se destaca que para lograr la efectividad de la concientización se requiere contar con el apoyo y compromiso de la máxima autoridad de la organización. Por otro lado, las áreas de recursos humanos y de seguridad de la información tienen una participación relevante en el proceso de la concientización. Adicionalmente, se considera valiosa la colaboración de áreas especialistas en temas como marketing, comunicación, relaciones públicas, legales y auditoría, entre otras.

En particular, los responsables que participan en la concientización pueden variar según el tamaño, ubicación y requerimientos de cumplimiento de cada organización. A modo de ejemplo, se enuncian en el anexo A distintas variantes de responsables de la concientización propuestos por la publicación especial n° 800-50 "Building An Information Technology Security Awareness and Training Program" del National Institute of Standards and Technology [2], el documento "How to Build an Enterprise Security Awareness Program" de Gartner [12] y el libro "Managing an Information Security and Privacy Awareness and Training Program" de Rebecca Herald [13].

Con respecto a los documentos analizados en el anexo A se observa que presentan una amplia separación de funciones acorde con organizaciones de estructuras orgánicas grandes. Además, únicamente en el

texto de Rebecca Herald se hace referencia a la cantidad de tiempo que deben dedicarles los responsables a las tareas de concientización. Se considera que este dato es útil porque la mayoría de las organizaciones no cuenta con personal de dedicación exclusiva para las tareas de concientización.

En resumen, se considera que los principales responsables de la concientización deben incluir al menos al:

- máximo responsable de la organización, encargado de brindar su compromiso con la seguridad de la información y definir la estrategia y los objetivos de la concientización.
- responsable primario de llevar a cabo las tareas de la concientización, encargado de evaluar los resultados, efectuar métricas y reportar los resultados a la máxima autoridad de la organización.
- usuarios, incluye a los empleados, proveedores, visitantes y colaboradores externos de la organización.

1.4 Proceso de concientización

La concientización es un proceso que debe incluir al menos las siguientes fases:

- Identificar el contexto de la organización.
- Evaluar las necesidades de concientización específicas.
- Diseñar el plan de concientización.
- Implementar el plan de concientización.
- Evaluar los resultados obtenidos.

Con el fin de profundizar dichas fases, en el anexo B se detallan distintos enfoques sobre el proceso de la concientización. Las fuentes de información consideradas son la publicación especial n° 800-50 "Building An Information Technology Security Awareness and Training Program" del National Institute of Standards and Technology [2], el documento "How to Build an Enterprise Security Awareness Program" de Gartner [12] y el libro "Managing an Information Security and Privacy Awareness and Training Program" de Rebecca Herald [13].

Del análisis de los documentos consultados se observa que todos incluyen las mismas fases del proceso: diseño, desarrollo, implementación y post- implementación. En particular, a diferencia de los otros documentos, el material de Gartner brinda algunos puntos interesantes sobre la concientización, a saber: menciona la importancia de la participación de los "stakeholders" en el proceso de concientización, recomienda enunciar los objetivos de concientización con una perspectiva desde el negocio y enuncia que el personal de seguridad informática podría no ser el mas apto para actuar como capacitadores de la concientización. En relación al documento del National Institute of Standards and Technology se considera un aporte valioso la descripción de los factores claves de éxitos para el proceso de concientización. Según el Nist los factores claves de éxitos son:

- Disponer del financiamiento suficiente para implementar la estrategia acordada.
- Contar con la estructura apropiada de la organización para que los responsables claves puedan llevar a cabo su estrategia.
- Disponer del soporte pertinente para la difusión y distribución del material.
- Garantizar que la comunicación de mensajes de concientización, en primera instancia, debe realizarla el máximo nivel ejecutivo.
- Incluir el uso de métricas.
- Lograr que alta dirección no recurra a su jerarquía para evitar los controles de seguridad.
- Obtener un alto nivel de asistencia de los usuarios a las actividades de seguridad de carácter obligatorio.
- Brindar reconocimiento a los usuarios que colaboran con la seguridad. Por ejemplo: la implementación de concursos con premios.
- Conseguir que los roles claves involucrados demuestren su motivación al proyecto de concientización. [2]

En cuanto al libro de Rebecca Herald se destaca como un aporte valioso el enunciado de los posibles errores que pueden cometerse en la concientización, a saber:

- No tener en cuenta la cultura de la organización.
- No considerar o investigar los requerimientos legales y regulatorios que aplican a la organización.

- No contar con el apoyo y la colaboración de la máxima autoridad de la organización.
- No estimar o contar con el presupuesto adecuado.
- No emplear el material adecuado para la organización.
- Sobrecargar de información las piezas del material de la concientización. Muchos estudios indican que las personas pueden recordar como máximo solo cinco ítems nuevos por vez.
- No incluir en el material de la concientización elementos que sean útiles y aplicables al trabajo del destinatario del mensaje.
- No recurrir a instructores idóneos.
- No utilizar métodos que la audiencia pueda relacionar, entender y aprender.
- No contemplar la motivación del personal para conocer y aprender aspectos de seguridad.
- No realizar una planificación adecuada de los eventos de la concientización.
- No evaluar la efectividad del programa.
- Utilizar un lenguaje inapropiado o políticamente incorrecto.
- Difundir la totalidad del contenido del programa en un periodo corto de tiempo. [13]

Finalmente, se destaca que la concientización puede convertirse en una herramienta poderosa para desarrollar una cultura en seguridad de la información. Una concientización efectiva requiere de una planificación cuidadosa, la participación de los "stakeholders", métricas definidas apropiadamente y la implementación de mecanismos que garanticen la continuidad de los comportamientos aprendidos. De acuerdo al documento "Best Practices in Information Security Awareness Training" de Gartner [14], se identificaron cuatro factores claves para el desarrollo e implementación de la concientización:

1- Expectativas de la administración

Las máximas autoridades y los "stakeholders" deben acordar los objetivos y propósitos de la concientización. La concientización debe tener como objetivos:

- El cambio cultural a largo plazo: haciendo foco sobre el conocimiento de los empleados en la política de seguridad y los procedimientos correspondientes.
- El cambio del comportamiento en el corto plazo, focalizándose en las acciones actuales de los empleados para cumplir con las políticas y procedimientos establecidos.

El diseño de la concientización debería cumplir con ambos objetivos.

Asimismo, los "stakeholders" deben entender que resultados pueden esperar de la concientización a largo y corto plazo.

2- Diseñar la concientización para lograr un impacto sostenido

Para que el diseño de la concientización sea efectivo se debe:

- utilizar estilos de aprendizaje probados exitosamente y reconocer los distintos tipos de audiencia.
- emplear técnicas de marketing para motivar la participación y adopción de los comportamientos recomendados.
- entender la diversidad de factores que caracterizan a la organización, tales como: diferencias regionales y/o de cultura.
- recurrir a entrenadores o capacitadores profesionales.
- organizar los contenidos según los roles de los empleados y los objetivos de la organización.
- distribuir el material de la concientización a través de mecanismos probados como efectivos.
- realizar charlas de inducción a los nuevos empleados.

3- Reconocer la relevancia de los aspectos de comunicación y marketing para la concientización

Para cambiar el modo de pensar de los empleados pueden resultar útiles las técnicas de comunicación y marketing, las que pueden aportar nuevos paradigmas, por ejemplo: creación de blogs o extender el contenido de la concientización a consejos de seguridad que la familia del empleado puede aplicar en su hogar. Por otro lado, la concientización debe reflejar la cultura e identidad de la empresa, por ejemplo, a través del uso de la marca de identidad de la empresa, mensajes que reflejen una visión unificada y consistente y demuestren que la iniciativa de seguridad es respetuosa de la cultura de la organización.

4- Medir los resultados

Previamente a elaborar el material de concientización y definir los métodos de entrega del mismo, se deben establecer las métricas que medirán el impacto de la concientización. Estas métricas deben estar alineadas al objetivo de la concientización y deben reflejar expectativas realistas del cambio en el comportamiento en el trabajo. Por ejemplo, si el objetivo es concientizar sobre los casos de phishing, se podría analizar:

- Cantidad de casos de phishing reportados por el personal de la organización.
- Cantidad de casos de phishing que no son detectados por los productos antiphishing.
- Cantidad de casos de phishing que si son detectados por los productos antiphishing.
- Cantidad de casos de usuarios que fueron víctimas de casos de phishing.

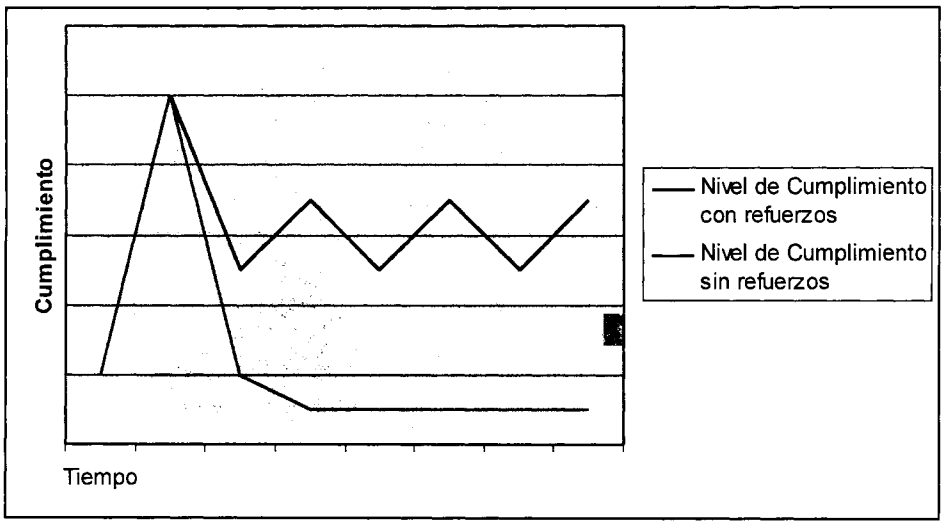
Estas métricas proveen información crítica que puede ser usada para el desarrollo del contenido de la concientización. Las métricas deben ser reportadas a los "stakeholders". Además, se debe agregar la evolución de las métricas e indicar los métodos preferidos de comunicación de los empleados debido a que estos factores pueden guiar las decisiones de inversión en la concientización.

Se debe evitar definir métricas que no pueden ser identificadas como un resultado directo de las actividades de la concientización.

Se recomienda:

- Seleccionar un conjunto de doce métricas como máximo.
- Evaluar las métricas antes y después de la actividad de concientización.
- Agrupar las métricas según la fuente de información utilizada para colectar los datos.

Adicionalmente se recomienda realizar refuerzos periódicos de los mensajes de concientización impartidos. Al respecto, se observa que al impartir por primera vez un conocimiento se inicia un cambio en el comportamiento de la persona y para que este cambio perdure en el tiempo se requiere reiterar dichos temas. A continuación, se presenta un gráfico que refleja la situación descripta previamente [14]:


Cumplimiento
Tiempo
Nivel de Cumplimiento con refuerzos
Nivel de Cumplimiento sin refuerzos

Capítulo II

Con el fin de analizar los desafíos que debe afrontar la concientización en el contexto actual se estudiaron los datos y resultados de los siguientes documentos:

- La evolución de la gestión de los ciber-riesgos y la seguridad de la información - encuesta 2016 sobre tendencias de los ciber-riesgos y la seguridad de la información en Latinoamérica, efectuado por Deloitte [15]
- Reporte de seguridad para Latinoamérica realizado por ESET. [16]
- Tendencias del año 2016, encuesta nacional de seguridad informática llevado a cabo por ACIS (Asociación colombiana de ingenieros en sistemas). [17]
- Encuesta de ciberseguridad en las principales empresas australianas realizada por el CERT y el ACSC de Australia [18]
- Estado de la seguridad cibernética para el año 2016, realizado por ISACA y la conferencia RSA [19]
- Reporte de la concientización en seguridad de la información efectuado por el instituto SANS [20]

Para cada documento se analizó los datos relativos a la concientización y adicionalmente se incluyó la información considerada relevante en el presente trabajo. La mayoría de los estudios abarcan la temática de la seguridad de la información o seguridad cibernética en general y no tratan específicamente la concientización. Únicamente el reporte realizado por el instituto SANS presenta un análisis exclusivo para la concientización en seguridad de la información.

A continuación, se describe un breve resumen de cada documento y finalmente, se presenta un cuadro comparativo de los distintos documentos.

2.1 La evolución de la gestión de los ciber-riesgos y la seguridad de la información - encuesta 2016 sobre tendencias de los ciber-riesgos y la seguridad de la información en Latinoamérica realizado por Deloitte

Deloitte realizó durante los meses de enero y mayo de 2016 un estudio sobre las tendencias en la gestión de ciber-riesgos y la seguridad de la información en Latinoamérica que contó con la participación de 13 países (Argentina, México, Chile, Nicaragua, Colombia, Panamá, Costa Rica, Perú, Ecuador, Republica Dominicana, El Salvador, Uruguay y Guatemala). En total participaron 89 organizaciones de las siguientes industrias: banca (43%), consumo masivo y manufactura (24 %), otros servicios financieros (10 %), tecnología, medios y telecomunicaciones (9%), energía y recursos naturales (8%), sector público (6 %) y ciencias de la vida y cuidado de la salud (1 %). Por otro lado, el perfil de los encuestados corresponde a CISO (40 %), personal de seguridad informática (17 %), sistemas (17 %), otros (12 %), riesgo y cumplimiento (8 %), auditoria (5 %) y planificación y desarrollo (1 %).

Según las respuestas de los encuestados se observó:

- El 84 % de las organizaciones cuentan con un responsable de seguridad (CISO).
- El CISO reporta al ejecutivo de TI en el 34 % de los casos y en el 65 % de las organizaciones encuestadas a áreas fuera de TI.
- Entre las funciones que debe realizar un CISO el 78 % de los participantes respondió la concientización.
- El 47 % de las organizaciones tienen de 1 a 5 integrantes en el área de seguridad.
- Los principales obstáculos identificados son la falta de presupuesto y recursos (51 %), falta de visibilidad e influencia dentro de la organización (37 %), falta de apoyo ejecutivo o del negocio (27 %), falta de recursos humanos competentes (26 %), el aumento en la complejidad de las amenazas (24 %), dificultad para encontrar recursos humanos con las capacidades requeridas (20 %), falta de una estrategia y hoja de ruta de implementación (17 %), falta de claridad sobre el mandato, las funciones y responsabilidades (16 %), el impacto de las nuevas tecnologías (16 %), no se detectaron obstáculos (4 %) y otros (12 %). La falta de presupuesto y recursos puede responder a diversas razones, como la madurez de la gestión, la necesidad de profundizar la concientización a los niveles ejecutivos sobre los riesgos o

incluso que el nivel de riesgo existente no fue adecuadamente evaluado y/o comunicado dentro de la organización.

En cuanto a las tecnologías mas utilizadas, se observa que el 80 % de las organizaciones tienen implementadas: antivirus (98 %), firewalls (96 %), soluciones de filtro de spam (88 %), software anti spyware (80 %), sistemas de prevención (72 %), filtro de contenido (67 %), administración de vulnerabilidades (58 %), control de acceso a la red (55 %), soluciones anti phishing (53 %) y autenticación de correo electrónico (52%).

Con respecto a las medidas implementadas por las organizaciones para cumplir con los requisitos de protección de privacidad y datos personales, el 51% respondió que aplica la sensibilización y capacitación sobre políticas y recomendaciones de privacidad de datos.

En resumen, se observaron las siguientes tendencias:

- Cuatro de cada diez organizaciones sufrieron una brecha de seguridad en los últimos 24 meses y menos del 20 % cuenta con un SOC (Security Operation Center)
- El principal obstáculo es la falta de presupuesto y/o recursos suficientes.
- Menos del 10 % de las organizaciones cuentan con un tablero con indicadores que permita evaluar la gestión de riesgos cibernéticos y de seguridad de la información.
- La capacitación y concientización es la iniciativa que mayor cantidad de organizaciones ejecutarán durante el año 2016.
- La función de gestión de los ciber-riesgos y seguridad de la información está evolucionando hacia un nuevo paradigma que incluye tres componentes centrales y estratégicos: asegurar, monitorear y responder.

En conclusión, se observa:

- Si bien existe conciencia sobre la importancia de la seguridad de la información, los CISOs en Latinoamérica aún luchan por convencer a la organización para que inviertan en seguridad.
- Los CISOs tienen bastante claridad y acuerdo en el alcance de sus responsabilidades y procesos. En ese alcance generalmente no se incluye la seguridad física ni la continuidad de negocio.
- En un contexto de nuevas y más sofisticadas ciber-amenazas, las auditorías de seguridad siguen identificando debilidades básicas de

seguridad en segregación de funciones y administración de usuarios. Estos aspectos continúan siendo un área a mejorar por los CISOs.

- El desarrollo de capacidades para monitorear y responder a las ciber-amenazas representa una necesidad urgente, las organizaciones aún se encuentran en un estado temprano de madurez en prácticas de monitoreo y SOC. [15]

2.2 Reporte de seguridad para Latinoamérica realizado por ESET

El estudio realizado por Eset durante el año 2015 incluyó 3044 respuestas de encuestas distribuidas en distintos eventos de seguridad realizados en 13 países (Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Paraguay, Perú y Venezuela). Los encuestados pertenecen a organizaciones de distintos tamaños y rubros, y poseen diferentes responsabilidades vinculadas con la seguridad.

Las preocupaciones de seguridad identificadas fueron: vulnerabilidades de software (58 %), malware (54 %) y acceso indebido a la información (46 %).

Los principales incidentes de seguridad detectados fueron la infección por malware (40%), casos de phishing (16%) y el fraude interno/externo (13%). En particular los países mas afectados por códigos maliciosos fueron, Nicaragua con el 58.3%, Guatemala con el 55.8% y Ecuador con 51.9%.

Los controles tecnológicos con mayor porcentaje de implementación fueron software antivirus (77%), firewalls (71%) y respaldos de la información (63%).

En relación a las prácticas para la gestión de la seguridad de la información, el primer lugar lo ocupó el desarrollo y publicación de políticas de seguridad (68%), como una medida para generar un entorno que dicte los lineamientos generales para proteger la información y otros activos. En el segundo y tercer lugar se ubican las auditorías internas/externas (36%) y la clasificación de la información (30%). Se destaca que las grandes

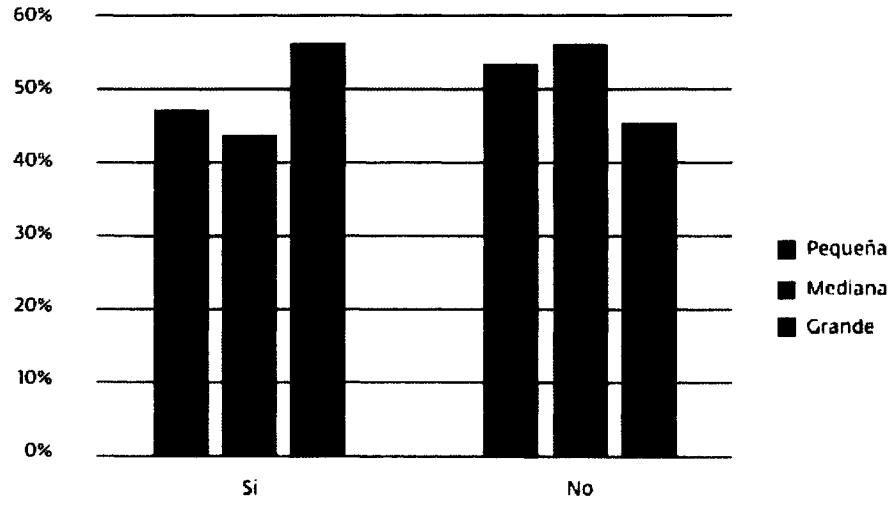
organizaciones son las que más controles han aplicado y el 20 % de las empresas pequeñas no aplica este tipo de prácticas.

Con respecto a las actividades de educación y concientización en materia de seguridad de la información, se observó que las organizaciones realizan estas actividades con la siguiente frecuencia:

2014	2015	
41%	16%	Periódicamente
38%	35%	Ocasionalmente
12%	19%	No las llevo cabo
9%	30%	Planeo hacerlo al corto plazo

Al respecto, se observó una reducción de estas actividades respecto al año 2014. Sin embargo, alrededor del 35% de las organizaciones, sin importar el tamaño de la misma llevan a cabo iniciativas de educación y concientización de manera ocasional y un porcentaje similar no las aplica, aunque planea hacerlo en el corto plazo.

Si bien es ideal que las actividades educativas sean constantes, es importante destacar que un gran porcentaje de las empresas lo hace al menos ocasionalmente y entiende que es necesario para mitigar el impacto de las amenazas informáticas. Aunque los porcentajes son parecidos en torno a los diferentes tamaños de empresas se destaca que el 55% de las empresas grandes lleva a cabo actividades de concientización, como se muestra en el siguiente gráfico:



Porcentajes de las empresas que realizan actividades de concientización para sus empleados (por tamaño de empresa).

Por otro lado, se observa que el porcentaje de las empresas pequeñas y medianas que no llevan a cabo actividades de concientización supera a las que sí las realizan.

En cuanto a quien depende el sector de seguridad de la información se observaron los siguientes datos:

Dependencia	Porcentaje
Gerencia de TI	51 %
Gerencia de Seguridad	13 %
Gerencia General	13 %
Otros	10 %
No hay área conformada	9 %
Gerencia de Operaciones	4 %

Se observa que más del 50% de los encuestados afirmaron que el área de Seguridad de la Información de sus empresas depende de la gerencia de TI. Aunque las mejores prácticas indican que el área de seguridad debe ser independiente para brindar objetividad e imparcialidad, claramente es una condición limitada a los recursos con los que cuenta cada organización.

En conclusión, se observa como principal causa de incidentes los programas maliciosos. Por otro lado, el phishing sigue creciendo y se ubicó

en el segundo lugar como el causante de incidentes, a pesar de que se trata de una amenaza fácilmente detectable, continúa siendo efectivo.

Los principales controles tecnológicos siguen siendo los productos antimalware, firewalls y soluciones de backup. No obstante, es importante aclarar que se los debe acompañar con prácticas de gestión y campañas de educación, es decir, enfocándose en la tecnología, procesos y colaboradores.

Asimismo, casi la mitad de las organizaciones encuestadas realiza iniciativas de educación y concientización en temas de Seguridad de la Información para su personal.

En general, es posible ver una lenta, pero sostenida mejora en el nivel de madurez de la Seguridad de la Información corporativa en la región, lo que certifica que muchos de los esfuerzos para promoverla son eficientes. No obstante, todavía existe un importante espacio para mejoras y aprendizaje en la búsqueda de la mitigación de los riesgos de seguridad de la actualidad. [16]

2.3 Tendencias del año 2016, encuesta nacional de seguridad informática llevado a cabo por ACIS

La encuesta nacional de seguridad informática realizada por ACIS (Asociación Colombiana de Ingenieros de Sistemas) contó con la participación de 121 encuestados. Los sectores que tuvieron mayor participación fueron los servicios financieros y banca (24 %), consultoría especializada (14 %), gobierno (13 %) y educación (12 %). En cuanto al tamaño de las organizaciones se observó que la mayor participación fue de empresas de 1001 a 5000 empleados (33%); le siguen las empresas de 201 a 500 empleados (16 %) y luego las compañías mayores a 5000 empleados (15 %). Por otro lado, los participantes se desempeñan en áreas de tecnologías de información (38 %), áreas de seguridad de la información (38 %), áreas de control (16 %) y cargos de niveles ejecutivos (8 %).

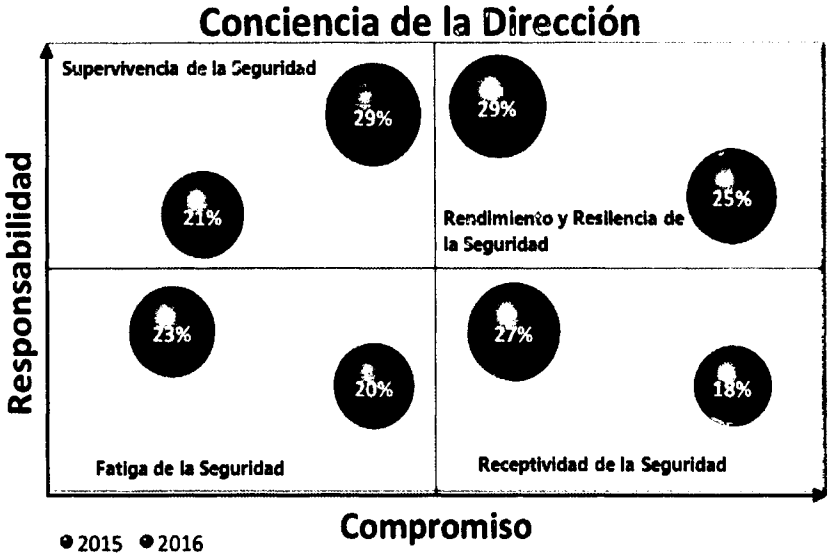
El 29 % respondió que el responsable de la seguridad de la información es el director de seguridad, el 15 % el jefe de seguridad y el 21 % el área de tecnología.

En cuanto a las habilidades del personal de seguridad, el 19 % de los participantes respondieron que cuenta con certificaciones en la materia, el 49 % tiene la certificación de Auditor Líder/Interno ISO 27001 y el 26 % la certificación CEH (Certified Ethical Hacker). Asimismo, las expectativas de disponer a futuro de personal con estas certificaciones son Auditor Líder/Interno ISO 27001 (57 %), CEH (Certified Ethical Hacker) (46 %) y ISACA CSX (Cyber Security Nexus (1 %).

En cuanto a las causas de los obstáculos para la seguridad de la información y su desempeño, el 39% de los encuestados sostiene que corresponde a la ausencia o falta de cultura en seguridad de la información y el 12 % respondió que se debe a la escasa formación en gestión segura de la información.

En cuanto a los incidentes de seguridad mas del 33 % responde a la instalación de software no autorizado, phishing y caballos de troya. En particular los ataques de ransomware representa el 17 % del total de las amenazas.

Además, la encuesta indagó sobre la conciencia de los directivos y su nivel de involucramiento y responsabilidad a la hora de participar en las tomas de decisiones con relación a la seguridad. Los resultados fueron los siguientes



Cada cuadrante tiene el siguiente significado:

Rendimiento y resilencia de la seguridad: el compromiso y la responsabilidad de la alta dirección son altas.

Supervivencia de la seguridad: el compromiso es bajo y la responsabilidad alta. La alta dirección atiende y entiende las recomendaciones de protección de la información, y, si bien no se involucra, sí tiene claro que es necesario entender los riesgos en materia de seguridad de la información.

Fatiga de la seguridad: bajo compromiso y baja responsabilidad de la alta dirección con relación a la seguridad de la información y los riesgos involucrados.

Receptividad de la seguridad: baja responsabilidad y alto compromiso por parte de las altas direcciones de las organizaciones. La alta dirección delega las responsabilidades a otros, pero sí esperan ser informados de lo que sucede en materia de la seguridad y cómo se avanza en este tema.

La conciencia de la seguridad es otro de los ítems que se incrementó en el año 2016 para Colombia, se observa que el 29% de los encuestados manifestó que sus niveles directivos entienden y atienden recomendaciones en materia de seguridad con respecto al 25 % reportado en el año 2015.

En conclusión, la seguridad de la información exige un enfoque multidimensional para ver desde todas las aristas, no sólo las técnicas a la protección de la información como un instrumento que le permita a la organización avanzar de una manera más consistente en los nuevos

entornos digitales, sino tener en cuenta su permanente transformación. De esa forma, los riesgos y las amenazas que van mostrando las nuevas realidades, llevan a las organizaciones a proteger su recurso más valioso, la información

En conclusión, se observó:

- se sigue afianzando la transformación de paradigmas de la seguridad de la información en las organizaciones y su relación con los directivos de las mismas. Se incrementó el interés y el apoyo de la dirección en temas de seguridad.
- existen aproximaciones para entender la seguridad como un orientador del negocio. No obstante, algunos todavía ven en la seguridad de la información sólo herramientas y tecnologías de apoyo.
- el entorno es cada vez más volátil, incierto, complejo y ambiguo. Requiere de mayor observación, atención y capacidad de entender de manera profunda las interrelaciones corporativas y lo selectivo que puede llegar a ser un adversario digital.
- en Colombia existen normativas para los sectores financieros y la ley de protección de datos personales. Por otro lado, las regulaciones internacionales inclinan la balanza hacia la seguridad de la información y enfrentan a un panorama todavía denso, en materia de ataques informáticos.
- ISO 27000, ITIL y Cobit se consolidan como marcos para construir arquitecturas de seguridad de la información. Por otro lado, los participantes reflejan la necesidad de utilizar algún marco de referencia, que les permita construir modelos adaptados a las necesidades de las empresas. [17]

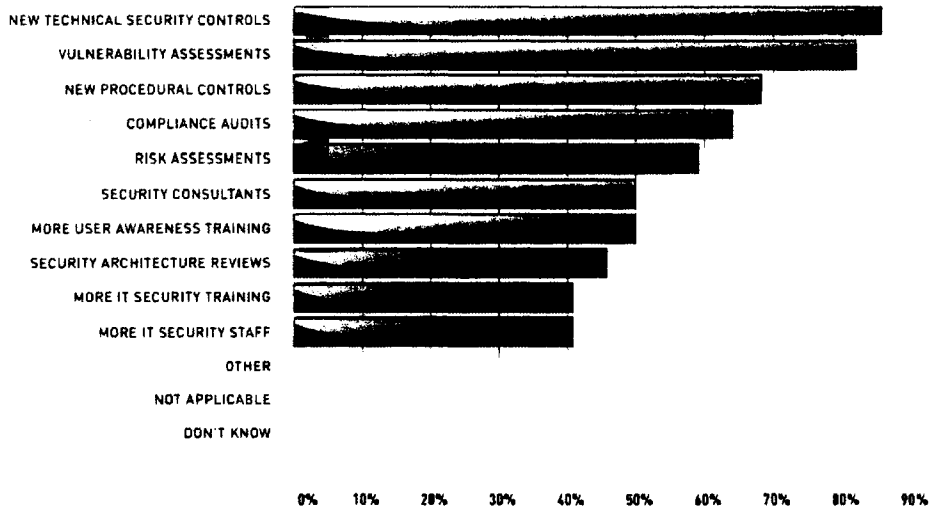
2.4 Encuesta de seguridad cibernética en las principales empresas australianas realizada por el CERT y el ACSC de Australia

La encuesta sobre seguridad cibernética realizada durante el año 2015 por el CERT de Australia y el Centro de Seguridad Cibernética de Australia identificó los conocimientos que tienen las organizaciones sobre las amenazas cibernéticas y como están posicionadas las mismas para asegurar sus redes. La encuesta fue completada por 149 organizaciones de

12 sectores distintos de la industria. Las industrias que registraron mayor participación fueron defensa (18%), energía (17%) y banca y finanzas (11 %). Además, el 67 % de las organizaciones tienen mas de 199 empleados, el % 23 entre 20 y 199 empleados y el 17% menos de 20 empleados.

En particular, el ataque de ransomware fue la amenaza que tuvo mayor incremento respecto al año 2013 constituyendo el 72 % de los incidentes reportados mientras que el resto de las amenazas permanecieron estables. El aumento de este tipo de amenazas podría estar asociado a que la inversión en concientización se trasladó a implementar controles más técnicos en pos de un esfuerzo para evitar que el usuario tenga que tomar la decisión.

El 56% de los participantes respondieron que incrementaron su gasto en seguridad. Al respecto, más del 80 % invirtió en nuevos controles técnicos y el 50 % en mayor concientización para los usuarios finales. El detalle de los gastos es el siguiente:



Por otro lado, los participantes identificaron a la concientización (87 %), el apoyo del liderazgo de alto nivel (79 %) y los controles técnicos (75 %) como mecanismos de respuestas a las amenazas cibernéticas.

En cuanto a las habilidades y entrenamiento del personal de seguridad el 87% de los participantes respondió que su personal tiene 5 años de experiencia y aproximadamente el 70 % tiene calificaciones terciarias. Asimismo, el 69 % contestó que su personal tiene certificaciones

o ha participado de cursos a medida y el 7 % respondió que el personal no tiene entrenamiento formal.

Se identificó que los sectores de las organizaciones que necesitan incrementar sus conocimientos en seguridad son los siguientes:

Sector	**Porcentaje**
Personal en general	89 %
Administración	83 %
Personal de IT	76 %
CEO	66 %
Junta Directiva	62 %

En conclusión, se observó:

- El 3 % respondió no tener un área de seguridad. Esto es una mejora significativa con respecto al 16 % reportado en el año 2013.
- El 77 % respondió tener planes para responder incidentes de seguridad.
- El 56 % respondió que incrementaron su presupuesto en los últimos 12 meses.
- El 82 % de las organizaciones usan estándares de seguridad externos. Los marcos de referencia son ISO/IEC 27001 (85%), PCI DSS (46%) e ISO/IEC 31000 (24 %).
- El 100 % reportó usar software antivirus y todos menos uno informó usar firewalls de red.
- El 50 % respondió haber experimentado al menos un incidente el año pasado y el 8 % no estar seguro si tuvieron un incidente.
- El 43 % respondió que no reporta incidentes a entidades externas porque no percibe los beneficios de reportarlos. [18]

2.5 Estado de la seguridad cibernética para el año 2016, realizado por ISACA y la conferencia RSA

En la encuesta sobre el estado de la seguridad cibernética efectuada por ISACA y la conferencia RSA entre noviembre y diciembre del año 2015 participaron 461 responsables cuya responsabilidad primaria es la seguridad

cibernética. El 55 % de los participantes manifestaron que su actividad principal es la seguridad de la información y el 81 % de los participantes pertenecen a ISACA. Además, el 21 % de los participantes desarrollan tareas de consultoría o servicios de tecnología y el 22 % pertenece al sector financiero. El 69 % de los participantes pertenecen a organizaciones con mas de 1000 empleados. En cuanto al lugar de residencia de los encuestados, se observó que el 46 % es de américa del norte, 24 % de Europa, 15% de Asia, 5% de áfrica, 5% de Latinoamérica y el 5% de Oceanía.

En particular, se observó que los ataques que tuvieron mayor éxito en el 2015 fueron el phishing (60 %), la ingeniería social (41 %), el código malicioso (52 %) y los intentos de hacking (36 %). Esto indica una clara necesidad de incrementar la concientización en casos de phishing e ingeniería social en los empleados. Al respecto, el 87 % de los encuestados respondió contar con un programa de concientización y el 53 % de los mismos cree que el programa es efectivo. Este último porcentaje representa una caída significativa desde 2014, cuando el 71 % creía que su programa de concientización era eficaz.

En cuanto al interés que tiene la alta dirección en la seguridad de la información se obtuvieron los siguientes datos:

Respuesta	**Porcentaje**
Muy interesado	36 %
Interesado	46 %
No tiene interés	8 %
No tiene interés del todo	7 %
No sabe	1 %
N/A	3 %

Según las respuestas, se observa que el 82 % de la alta dirección está interesada o muy interesada en la seguridad de la información. Asimismo, el 63 % de los casos encuestados reporta al CIO y solo el 14 % al CEO. En general se observa que el grupo de seguridad de la información sigue dependiendo de tecnología y la alta dirección apoya sus tareas.

Por otro lado, el 61 % de los encuestados consideró que su presupuesto se incrementaría en el 2016 y sería destinado a contratar trabajadores capacitados, entrenamiento, programas de concientización y planificación de respuestas.

Por otro lado, el apoyo de la alta dirección en mitigar los riesgos de la seguridad de la información se demuestra de las siguientes formas:

Respuesta	**Porcentaje**
Imponiendo la política de seguridad	66 %
Proporcionando la financiación adecuada	63 %
Haciendo obligatoria la concientización	58 %
Cumpliendo ellos mismos las buenas de prácticas de seguridad	43 %
No sabe	6 %
N/A	7 %

Las carencias de las habilidades de los profesionales de seguridad detectadas fueron: habilidad para entender el negocio (75 %), comunicación (61 %) y habilidad técnica (61 %). En particular, las habilidades técnicas se refieren a la capacidad de identificar, contener y mitigar incidentes de seguridad complejos que pueden incidir en los costos de la empresa.

En conclusión, se observó que las amenazas a la seguridad cibernética siguen afectando a las empresas, el 74 % de los encuestados esperaba ser víctima de un ataque cibernético en el año 2016. Además, el 60 % de los encuestados experimentó un ataque de phishing en 2015 y en el 30 % de los casos este tipo de ataque se produjo diariamente. Los resultados indican que la ciberdelincuencia es una amenaza creíble. El phishing, ingeniería social y los intentos de hacking son los tres principales tipos de ataques que tuvieron éxito en el año 2015. Esto indica una clara necesidad de incrementar la concientización de los empleados en casos de phishing e ingeniería social. Si bien las tendencias emergentes continúan evolucionando, los profesionales de seguridad tendrán que ser capaces de proteger de las amenazas que podrían afectar a las empresas y debido a que las personas no van a desaparecer, deberán continuar desarrollando programas de concientización para ayudar a inspirar a una cultura de la

seguridad. Un dato inquietante es que el 24 % de los responsables de seguridad encuestados respondieron que no pudieron identificar de una lista de amenazas cual había actuado en su organización. Este hecho podría indicar algunos problemas tales como la necesidad de mejorar el control, la capacidad de interpretar mejor los logs y otros datos, o, potencialmente, una necesidad para mejorar las habilidades de los empleados. Sin embargo, se observa que existe un claro entendimiento de que los incidentes de seguridad cibernética pueden dar lugar a un impacto significativo en el negocio. Las empresas se están convirtiendo en organizaciones mejor preparadas y están empezando a mirar a la seguridad cibernética como un caso de negocio. Al respecto, el 75 % informó que su estrategia de seguridad cibernética está alineada a los objetivos de la empresa. [19]

2.6 Reporte de concientización en seguridad de la información efectuado por Sans

La encuesta elaborada por el instituto SANS fue llevada a cabo en noviembre de 2015 con un total de 369 participantes. Contó con la participación de distintos tipos de industrias, el 70 % de los participantes residen en Estados Unidos de América y el 30 % en otros lugares geográficos. Asimismo, dicha encuesta es la segunda que se efectúa. Las industrias que mayor participación tuvieron fueron los servicios de educación (20 %), servicios financieros y de seguros (17%) e información (14 %). La distribución geográfica de las respuestas se detalla en el siguiente gráfico.

La encuesta brinda información sobre como mejorar las actividades de concientización y compara el estado de la concientización entre las organizaciones.

En particular, los retos de la concientización detectados se agruparon en las siguientes siete categorías:

Número	**Categoría del problema**	**Cantidad de respuestas**	**Porcentaje**
1	Carencia de recursos	50	19 %
2	Aceptación de la concientización	48	19 %
3	Falta de apoyo de la alta dirección	47	18 %
4	Falta de apoyo del usuario final	27	10 %
5	Carencia de tiempo disponible para las tareas de concientización	24	9 %
6	Dificultades en la elaboración del contenido de la concientización	23	9 %
7	Personal insuficiente para las tareas de concientización	22	9 %

Con el fin de simplificar el análisis, las categorías fueron divididas en dos grupos generales:

- carencia de recursos, falta de apoyo de la administración y escasez de tiempo (los porcentajes suman un 46 % y se refieren a las categorías 1, 3 y 5 del cuadro precedente).
- fallas en generar el impacto necesario (los porcentajes suman un 47 % y se refieren a las categorías 2, 4, 6 y 7 del cuadro precedente).

En cuanto al presupuesto asignado a la concientización se obtuvieron los siguientes datos:

Presupuesto (dólares americanos ($))	Cantidad de respuestas	Porcentaje (%)
Mas de 100000	23	6,67
50000-100000	26	7,54
25000-50000	40	11,59
5000-25000	62	17,97
Menos a 5000	105	30,43
Desconoce	89	25,80

Al respecto, se observa que el 56 % de los participantes tiene un presupuesto de $ 5.000 o menos o desconoce el monto del presupuesto de concientización y el 25 % de los encuestados tiene un presupuesto mayor de $ 25.000. En particular, se observó que los presupuestos superiores a $ 25.000 se emplean en organizaciones de diferentes tamaños.

En relación al tiempo que dedica el personal a realizar tareas de concientización, se observan los siguientes datos:

Tiempo dedicado a tareas de concientización en relación a la totalidad de las horas laborales	**Cantidad de respuestas**	**Porcentaje**
90 - 100 %	50	14,53
50 - 90 %	35	10,17
25 - 50 %	37	10,76
15 - 25 %	80	23,26
0 - 15 %	142	41,28

Del análisis de dichos datos, se observa que solo el 15 % del personal se dedica exclusivamente a tareas de concientización. Asimismo, en la mayoría de las organizaciones, independientemente de su tamaño, el personal solo tiene una dedicación parcial a las tareas de concientización.

Con respecto al apoyo que brinda la alta dirección a la concientización, se obtuvieron los siguientes datos:

La concientización tiene el apoyo de la alta dirección necesario?	**Cantidad de respuestas**	**Porcentaje**
No	9	2,61
Menos del necesario	115	33,33
Suficiente	211	61,16
Mas que el necesario	10	2,90

En este caso se observa la relevancia y necesidad de contar con el apoyo de la alta dirección en el proceso de la concientización.

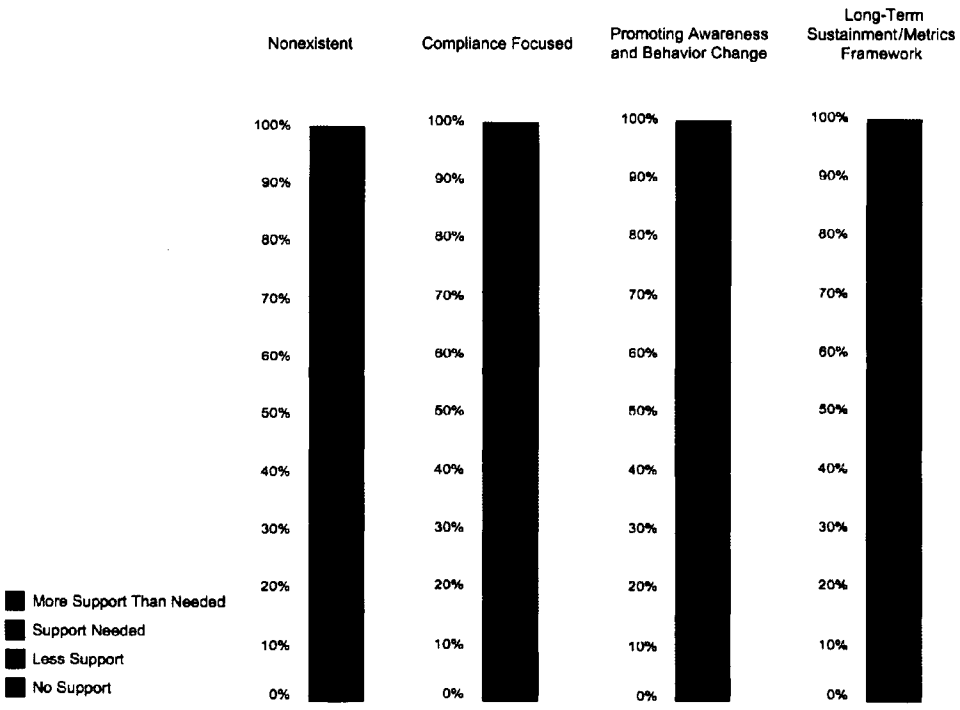
Adicionalmente se demostró que cuanto mayor es el apoyo de la alta dirección a la concientización mayor madurez tiene el programa de concientización.

La madurez se mide utilizando un modelo que tiene cinco estados. En particular cada estado se construye en base al estado previo. Los posibles estados de madurez de la concientización son:

Estado	**Descripción**
No existe	No se realizan actividades de concientización. Los empleados desconocen que sus acciones tienen un impacto directo en la seguridad de la organización, no conocen o no entienden las políticas de la organización y pueden ser víctimas fáciles de ataques.
Focalizada en el cumplimiento	La concientización se realiza para satisfacer los requisitos de cumplimiento o de la auditoria. Los empleados no tienen conocimientos certeros de la política de la organización y de su rol en la protección de la información de la organización.

Promoción de la concientización y el cambio de comportamiento	La concientización identifica los tópicos de entrenamiento que tienen un mayor impacto en la organización. El contenido se comunica en una manera atractiva y positiva que fomenta el cambio del comportamiento del empleado en el trabajo, en su hogar y durante sus vacaciones. Los empleados entienden y siguen las políticas de la organización y reconocen, previenen y reportan incidentes de seguridad.
Sostenible a largo plazo y con un cambio cultural	La concientización cuenta con los procesos, recursos y el apoyo de la alta dirección sostenible en el tiempo. Se realiza al menos una revisión y actualización anual del programa de concientización. La concientización es parte de la cultura de la organización.
Métricas	La concientización tiene un conjunto de métricas para medir su progreso e impacto. La concientización es continuamente mejorada y es capaz de demostrar el retorno de la inversión.

La relación entre la madurez del proceso de concientización y el apoyo de la alta dirección se refleja en el siguiente gráfico



Al respecto, se observa que cuando no existen actividades de concientización se observa que el no apoyo de la alta dirección tiene mayor porcentaje. Según los datos analizados, si no hay actividades de concientización el 10 % de los participantes no cuenta con el apoyo de la alta dirección. Por otro lado, para los dos estados de mayor madurez en la concientización los porcentajes correspondiente al no apoyo de la alta dirección es nulo.

Con respecto a los distintos niveles de madurez de concientización, se obtuvieron los siguientes resultados en las organizaciones encuestadas:

Estado	**Porcentaje**
No existe	8,2 %
Focalizada en el cumplimiento	25,4 %
Promoción de la concientización y al cambio de comportamiento	51,1 %
Sostenible a largo plazo y con un cambio cultural	13;2 %
Métricas	2,2%

Al respecto, se observa que el 33 % de las organizaciones no realizan tareas de concientización o ejecutan actividades de concientización por cumplimiento. El 51 % de los encuestados efectúa una concientización que promociona la concientización y el cambio de comportamiento y únicamente el 2% de los participantes tiene un nivel de madurez con cambios de comportamiento, cultura de seguridad y cuentan con métricas para probarlo.

En relación a las métricas utilizadas para medir la concientización se observó que muy pocas de ellas representan el problema del factor humano y el impacto que tiene la concientización en resolver este tipo de problemas. De los resultados analizados, la métrica mas utilizada fue la evaluación de casos de phishing. El phishing es uno de los riesgos relacionados al factor humano, sin embargo, se requiere avanzar en la definición de métricas que midan otros riesgos relacionados al factor humano y el valor de la concientización en la organización. De acuerdo a las respuestas a la encuesta, se observó que las métricas mas empleadas para medir la concientización son:

Métrica	**Cantidad de respuestas**
Evaluación de phishing	162
Violaciones de seguridad	125
Dispositivos infectados	121
Sin métricas	98
Incidentes con exposición de datos	93
Pérdida de dispositivos	81
Otras	62
Costos ahorrados	20

Continuando con el estudio en una segunda ciudad, se observó que el grupo encargado de la concientización contaba con los recursos necesarios, pero no conseguía lograr el impacto pertinente en los usuarios. Para medir el impacto de la concientización se consideraron las siguientes categorías:

- Grado de adopción: los usuarios no modifican su comportamiento.

- Apoyo de los usuarios finales: los usuarios no participan de las actividades de concientización, no les interesan y son reacios a participar.
- Disponibilidad de tiempo: los usuarios no encuentran tiempo para participar de las actividades de la concientización, para ellos la concientización tiene una baja prioridad.
- Contenido: dificultades para crear el contenido de concientización apropiado.

Además, se identificó que el 79 % del personal que lidera la concientización tiene un perfil técnico. En particular, se observó que dicho personal previamente a realizar tareas de concientización llevó a cabo actividades del siguiente tipo:

Funciones previas a la concientización	**Cantidad de respuestas/ Porcentajes**
Recursos Humanos	2 (0,5 %)
Marketing /Diseño Gráfico	12 (3,3 %)
Comunicaciones/ Relaciones Públicas	15 (4,1 %)
Entrenamiento	20 (5,4 %)
Otro	28 (7,6 %)
Seguridad Física/ Seguridad de la Información	124 (33,6 %)
Tecnología de la Información	168 (45,5 %)

En la concientización es muy importante la comunicación debido a que se requiere explicar a los participantes porque la misma es importante para ellos y que es lo que deben hacer.

En general el personal de seguridad asume que la seguridad es algo simple porque es parte de su vida cotidiana y asume que es simple para el resto del personal de la organización. Si se diseña la concientización asumiendo estas suposiciones la comunicación puede no reflejar lo que necesitan las personas. Por ejemplo, el personal de seguridad suele indicar a las personas que creen y usen claves complejas. Cuando las personas fallan con esta indicación, el personal de seguridad piensa que los mismos no tienen motivación, sin embargo, la mayoría de las personas piensan que las claves complejas son confusas y difíciles. En este caso, sería

recomendable que en lugar de recordarles a las personas la importancia de las claves, se focalice en difundir el uso de frases para la conformación de las claves, fomentar el uso de herramientas de gestión de claves o recomendar el empleo de la autenticación con doble factor.

Adicionalmente, ante la consulta: ¿cuál es el sector que mas obstaculiza la concientización? se obtuvieron los siguientes resultados:

Sector que mas obstaculiza	**Cantidad de respuestas/ Porcentajes**
Legales/Auditoria	17 (5.1%)
Seguridad de la Información	20 (6.0%)
Otros	21 (6.3%)
Recursos Humanos	36 (10.7%)
Finanzas	40 (11.9%)
Administración (general)	41 (12.2%)
No hay sectores que obstaculicen	43 (12.8%)
Operaciones	51 (15.2%)
Comunicaciones	66 (19.7%)

Como resultado de la consulta se observó que el 20% de los participantes considera que el sector de Comunicaciones es el que mas obstáculos presenta a la concientización.

Con respecto al sector al que se reporta los resultados de la concientización, se observa que en la mayoría de los casos se comunica los resultados a sectores técnicos. Los datos resultantes son los siguientes:

Sector al que se reportan los resultados de la concientización	**Cantidad de respuestas/ Porcentajes**
Otros	11 (3.0%)
Riesgo	5 (1.4%)
Legales/Auditoria/Cumplimiento	12 (3.3%)
Comunicaciones	5 (1.4%)
Entrenamiento	2 (0.5%)
Recursos Humanos	2 (0.5%)
Administración (general)	121 (32.9%)

COO	14 (3.8%)
CISO	111 (30.2%)
CIO /CTO	85 (23.1%)

En resumen, se observa que personas con un alto perfil técnico reportan los resultados de la concientización a un sector técnico con mayor jerarquía que debe difundir su trabajo a la organización y el sector de Comunicaciones de la organización es el principal obstaculizador de la concientización.

La comunicación es una de las principales habilidades que requiere la concientización. La comunicación se refiere a la capacidad de involucrar a los empleados con un mensaje significativo, identificar y entregar el contenido apropiado a las personas correctas, aprovechando múltiples métodos de comunicación. Para cumplir con estas tareas, en algunas organizaciones empieza a aparecer el rol de Security Communications Officer. Otras alternativas son: incorporar al grupo encargado de la concientización a un integrante del sector de Comunicaciones, entrenar al personal en las habilidades sociales pertinentes o contratar a personal especializado. Además, se recomienda incorporar al sector de Comunicaciones desde un primer momento en la fase del diseño de la concientización.

Se recomienda iniciar la concientización explicando a las personas porque les debe importar la misma. En lugar de racionalizar la necesidad de seguridad con estadísticas y números, se debe involucrar a las personas a un nivel emocional. Para ello se recomienda realizar charlas y asumir compromisos donde los empleados se convierten en una parte activa de la concientización.

Finalmente, SANS concluye que a pesar que la concientización se encuentra en un estado inicial empiezan a surgir señales de madurez. Los puntos clave son:

- El apoyo es esencial: los grupos que realizan la concientización no tienen el apoyo de la alta dirección suficiente. El 50 % de los entrevistados tiene un presupuesto de $ 5000 o menor o desconoce su presupuesto. Menos del 15 % del personal tiene una dedicación full time a la concientización y el 64 %

solo destina una cuarta parte de su tiempo en tareas de concientización. Finalmente, el 35 % afirma no contar con el apoyo necesario. Según lo demostrado, existe una fuerte interrelación entre el apoyo de la alta dirección y el nivel de madurez de la concientización. Se requiere mejorar la educación a los líderes para que comprendan que la seguridad no puede ser resuelta solamente por la tecnología y debe tener en cuenta el factor humano.

- Carencia de habilidades sociales (soft skills). El 80 % del personal que realiza la concientización tiene un perfil técnico con habilidades tales como configurar firewall, analizar logs y no entiende los conceptos y las técnicas de cambio de comportamiento o cultura organizacional. Asimismo, se identificó que la comunicación es la habilidad clave en la concientización y en general los equipos encargados de la concientización carecen de dicha habilidad. Las soluciones posibles son: incorporar a alguien del sector de Comunicaciones, entrenar al equipo de concientización en las habilidades que requieran o contratar a un especialista en esta temática. [20]

2.7 Resumen de los resultados de las encuestas

Con el fin de presentar un resumen de los distintos documentos analizados en el presente trabajo se efectúo un cuadro con las siguientes columnas:

Encuesta : Nombre del documento que referencia a la encuesta efectuada

Encuestador : Entidad que llevo a cabo la encuesta.

Origen de los participantes : Origen geográfico de los participantes de la encuesta.

Cantidad de participantes : Cantidad total de los participantes que respondieron la encuesta.

Industria con mayor participación : Rubro o industria que tuvo mayor participación en la encuesta.

Concientización : Resultados de la encuesta sobre la temática de la concientización.

Conclusión general de la encuesta : Conclusión general de la encuesta.

Encuesta	Encuestador	Origen de los participantes	Cantidad de participantes	Industria con mayor participación	Concientización	Conclusión general de la encuesta
La evolución de la gestión de los ciber-riesgos y la seguridad de la información - encuesta 2016 sobre tendencias de los ciber-riesgos y la seguridad de la información en Latinoamérica	Deloitte	13 países de Latinoamérica	89 organizaciones	Banca (43%)	El 78 % respondió que la concientización es una funcion del CISO. El 51 % de las organizaciones para cumplir con los requisitos de protección de privacidad y datos personales, aplica la sensibilización y capacitación sobre políticas y recomendaciones de privacidad de datos. Por otro lado, la capacitación y concientización es la iniciativa que mayor cantidad de organizaciones ejecutarán durante 2016.	El principal obstáculo es la falta de presupuesto y/o recursos suficientes. Existe conciencia sobre la importancia de la seguridad de la información, sin embargo, los CISOs en Latinoamérica aún luchan por convencer a la organización para que inviertan en seguridad El desarrollo de capacidades para monitorear y responder a las ciber-amenazas aún se encuentran en un estado temprano de madurez. Las auditorías de seguridad siguen identificando debilidades de seguridad en la segregación de funciones y administración de usuarios, estos aspectos continúan siendo un área a mejorar por los CISOs.

Reporte de seguridad para Latinoamérica	Eset	13 países de Latinoamérica	3044 participantes	S/D	El 55% de las empresas grandes llevan a cabo actividades de concientización. Más del 50 % de las empresas pequeñas y medianas no realizan actividades de concientización, mientras que mas del 40 % si lo efectúan. La concientización se realiza con una frecuencia periódica en el 16 % de los casos, ocasionalmente en el 35 % de los casos, mientras que el 19 % no las lleva a cabo y el 30 % planea hacerlo a corto plazo. Por otro lado, en comparación con el año 2014, se observó una reducción de las actividades de concientización.	Se observa como principal causa de incidentes los programas maliciosos y en segundo lugar los casos de phishing. Los principales controles tecnológicos siguen siendo los productos antimalware, firewalls y soluciones de backup. No obstante, es importante aclarar que se los debe acompañar con prácticas de gestión y campañas de educación, es decir, enfocándose en la tecnología, procesos y colaboradores. Casi la mitad de las organizaciones realizan iniciativas de educación y concientización en seguridad de la información. Se observan mejoras en el nivel de madurez de la Seguridad de la Información en la región. No obstante, todavía existe un importante espacio para mejoras y aprendizaje en la búsqueda de la mitigación de los riesgos de seguridad de la actualidad

Tendencias del año 2016, encuesta nacional de seguridad informática	Acis	Colombia	121 participantes	Servicios financieros y Banca (24 %)	Los resultados del análisis del nivel de concientización en la alta dirección demuestran que el 29 % de la alta dirección atiende y entiende las recomendaciones de protección de la información, y, si bien no se involucra, sí tiene claro que es necesario entender los riesgos en materia de seguridad de la información, el 20 % de la alta dirección tiene un bajo compromiso y baja responsabilidad, 25 % de la alta dirección tiene un compromiso y responsabilidad altos y el 18 % de la alta dirección delega las responsabilidades a otros, pero sí espera ser informada de lo que sucede en materia de la seguridad y cómo se avanza en este tema. La conciencia de la seguridad es otro de los ítems que se incrementó en el año 2016 para Colombia, se observa que el 29% de los encuestados manifestó que sus niveles directivos entienden y atienden recomendaciones en materia de seguridad con respecto al 25 % reportado en el año 2015.	Se observa que se continúa afianzando el paradigma de la seguridad de la información en las organizaciones. Existen aproximaciones para entender la seguridad como un orientador del negocio. No obstante, algunos todavía ven en la seguridad de la información sólo herramientas y tecnologías de apoyo. Existen normativas para los sectores financieros y la ley de protección de datos personales. ISO 27000, ITIL y Cobit se consolidan como marcos para construir arquitecturas de seguridad de la información. Por otro lado, los participantes reflejan la necesidad de utilizar algún marco de referencia, que les permita construir modelos adaptados a las necesidades de las empresas.

Encuesta de seguridad cibernética en las principales empresas australianas	Cert y ACSC de Australia	Australia	149 participantes	Defensa (18%), energía (17%) y banca y finanzas (11 %)	El 87 % de los participantes identifica a la concientización como un mecanismo para contrasrestar las amenazas cibernéticas. El 56% de los participantes respondieron que incrementaron su gasto en seguridad y de ellos el 50 % invirtió en la concientización para los usuarios finales. Los sectores de las organizaciones que necesitan incrementar sus conocimientos en seguridad son personal en general (89 %), administración (83 %),personal de IT (76 %), CEO (66 %) y Junta Directiva (62 %)	Se incrementaron las organizaciones con áreas de seguridad (97%) y los presupuestos a invertir en seguridad. El presupuesto de seguridad se gastó en su mayoria en controles técnicos (80%). Se usan los marcos de referencia extranjeros ISO/IEC 27001, PCI DSS e ISO/IEC 31000. El ataque de ransomware fue la amenaza que tuvo mayor incremento respecto al año 2013 constituyendo el 72 % de los incidentes reportados mientras que el resto de las amenazas permanecieron estables. El aumento de este tipo de amenazas podría estar asociado a que la inversión en concientización se trasladó a implementar controles más técnicos en pos de un esfuerzo para evitar que el usuario tenga que tomar la decisión. El 43 % respondió que no reporta incidentes porque no percibe los beneficios de reportarlos.

Estado de la seguridad cibernética para el año 2016	Isaca y RSA conference	América del norte (46 %), europa (24 %) , asia (15%), áfrica (5%), latinoamérica (5%) y oceanía (5%)	461 participantes	servicios financieros y Banca (22 %) y servicios de tecnología (21 %)	El 87 % de los encuestados respondió contar con un programa de concientización y el 53 % de los mismos cree que el programa es efectivo. Este último porcentaje representa una caída significativa desde 2014, cuando el 71 % creía que su programa de concientización era efectivo. El 61 % de los encuestados tenía previsto incrementar su presupuesto en el 2016 y lo destinaría a contratar trabajadores capacitados, entrenamiento, programas de concientización y planificación de respuestas. El 58 % de la alta dirección sostuvo que hacer obligatoria la concientización es una forma de mitigar los riesgos asociados a la seguridad de la información. Se requiere continuar desarrollando programas de concientización para ayudar a inspirar a una cultura de la seguridad debido a que la mayor cantidad de ataques del 2015 fueron casos de phishing e ingeniería social.	Las empresas se están convirtiendo en organizaciones mejor preparadas y están empezando a mirar a la seguridad cibernética como un caso de negocio. Al respecto, el 75 % informó que su estrategia de seguridad está alineada a los objetivos de la empresa. Además, se observó un alto apoyo de la alta dirección a la seguridad, el 82 % se encuentra interesado y/o muy interesado. En cuanto a las carencias en las habilidades de los profesionales de seguridad el 75 % reportó a la habilidad para entender el negocio, el 61% la compentencia de comunicación y el 61 % la habilidad técnica. En particular, las habilidades técnicas se refieren a la capacidad de identificar, contener y mitigar incidentes de seguridad complejos que pueden incidir en los costos de la empresa. Por otro lado, las amenazas a la seguridad

						cibernética siguen afectando a las empresas, el 74 % de los encuestados esperaba ser víctima de un ataque cibernético en el año 2016. Además, el 60 % de los encuestados experimentó un ataque de phishing en 2015 y en el 30 % de los casos este tipo de ataque se produjo diariamente. Esto indica una clara necesidad de incrementar la concientización de los empleados en casos de phishing e ingeniería social.

Reporte de concientización en seguridad de la información	SANS	Estados Unidos de América (70%) y otros lugares (30%)	369 participantes	educación (20%), servicios financieros (17%)	El 50 % de los entrevistados tiene un presupuesto de $ 5000 o menor o desconoce su presupuesto. Menos del 15 % del personal tiene una dedicación full time a la concientización y el 64 % solo destina una cuarta parte de su tiempo en tareas de concientización. El 35 % afirma no contar con el apoyo necesario. Además, existe una fuerte interrelación entre el apoyo de la alta dirección y el nivel de madurez de la concientización. El 10 % que no realiza actividades de concientización no tiene apoyo de la alta dirección. Los que realizan concientización que propende al cambio de comportamiento y el cambio cultural cuentan con un apoyo de la alta dirección superior al 60 %. Se observa que el 33 % de las organizaciones no realizan tareas de concientización o ejecutan actividades de concientización por cumplimiento. El 51 % de los encuestados efectúa una concientización que promociona la concientización y efectúa cambios de comportamiento y únicamente el 2% de los participantes tiene un nivel de madurez con cambios de comportamiento, cultura de seguridad y cuentan con métricas para probarlo.	La concientización se encuentra en un estado inicial y empiezan a surgir señales de madurez. Los grupos que realizan la concientización no tienen el apoyo de la alta dirección suficiente. Se requiere mejorar la educación a los líderes para que comprendan que la seguridad no puede ser resuelta solamente por la tecnología y debe tener en cuenta el factor humano. El personal que realiza la concientización carece habilidades sociales (soft skills). Las soluciones posibles son: incorporar a alguien del sector de Comunicaciones, entrenar al equipo de concientización en las habilidades que requieran o contratar a un especialista en esta temática.

Capítulo III

En el presente capítulo se describe una propuesta para llevar a cabo un proyecto de concientización en una empresa mediana, pequeña o micro de Argentina (pyme). Se define a una pyme como una empresa prototipo evaluando su dimensión e importancia en el marco de una estructura productiva nacional. En Argentina el plantel de una pyme no debe superar a los cuarenta trabajadores y debe tener una facturación anual inferior a la cantidad que para cada actividad se reglamente. [21]

La presente propuesta corresponde a las etapas de desarrollo e implementación del proceso de concientización y es el resultado de efectuar previamente las siguientes acciones:

- Relevar las características de la organización (misión, objetivos, principales referentes, tipo de cultura).
- Relevar los antecedentes relativos a la concientización en la organización (actividades realizadas, recomendaciones de la Auditoria, cumplimiento de regulaciones nacionales e internacionales, incidentes de seguridad detectados).
- Identificar las necesidades de concientización a mediano y largo plazo.

Para la elaboración de la propuesta se tuvieron en cuenta las siguientes pautas:

- definir objetivos a corto y largo plazo entendiendo que la concientización es un proceso y no acciones aisladas.
- diseñar actividades de corta duración con pocos tópicos que posteriormente sean fáciles de reforzar. [22]
- incorporar el concepto 'learn and lunch' en el desarrollo de algunas actividades de concientización. [23]
- garantizar la participación del máximo responsable de la pyme en los eventos claves de la concientización.
- emplear diversos mecanismos para la difusión del material de la concientización, incluyendo el uso de las redes sociales como nueva herramienta de difusión.
- reiterar oportunamente las recomendaciones de seguridad para reforzar los conocimientos utilizando diferentes medios de comunicación.

- difundir recomendaciones de seguridad que el usuario pueda aplicar fuera del ámbito laboral, por ejemplo: recomendaciones de seguridad para padres.
- realizar actividades que incrementen el nivel de participación de los usuarios, por ejemplo, competencias con premios.
- resaltar el "como" mas que el "que" en el contenido del material de concientización. Por ejemplo, demostrar como llevar a cabo las buenas prácticas de seguridad recomendadas a través de videos.
- definir métricas que midan el desarrollo de la concientización y el impacto de la misma. [24]

Finalmente, con el fin de acotar el alcance del presente trabajo, el cronograma de actividades se desarrolló únicamente para las actividades dirigidas a todo el personal de la pyme en el primer año del proceso de concientización.

3.1 Propuesta de Concientización

Objetivo

A corto plazo

Lograr que el personal de la pyme tome conciencia y conozca los riesgos y amenazas que afectan la seguridad de la información y cuenten con el conocimiento suficiente para implementar las medidas de protección pertinentes.

A largo plazo

Realizar acciones que permitan continuar afianzando la concientización en pos de implementar una cultura de seguridad en la pyme y generar métricas que evalúen su eficacia. Se pretende crear una cultura en la cual los empleados utilicen la tecnología con la misma conciencia y responsabilidad que la mayoría de las personas manejan sus automóviles. La mayoría de los conductores están relajados al manejar y a su vez alertas a las señales de peligro. Cualquiera que use la tecnología podría estar relajado pero alerta ante posibles riesgos y dispuesto a tomar una acción ante los mismos. [25]

Alcance

El alcance de la propuesta incluye:

- definir los roles con sus respectivas responsabilidades.
- identificar las distintas audiencias.
- elaborar un cronograma con las actividades de concientización detallando el objetivo, fecha estimada, material a emplear, mecanismo de difusión a aplicar y medio de evaluación en caso de corresponder.
- establecer métricas para evaluar la eficacia de la concientización.

Roles y responsabilidades

Se identificaron los siguientes roles y responsabilidades:

- máximo responsable de la organización: tiene a su cargo brindar su compromiso con la seguridad de la información y definir la estrategia y los objetivos de la concientización.
- responsable primario de llevar a cabo las tareas de la concientización, encargado de evaluar los resultados, efectuar métricas y reportar los resultados a la máxima autoridad de la organización. Para el presente trabajo este rol lo ejerce el consultor externo contratado para realizar la concientización en la pyme.
- usuarios: incluye a la totalidad de los empleados, los proveedores, los visitantes y los colaboradores externos de la organización.

Audiencias identificadas

La pyme cuenta con los siguientes sectores:

Sector	Características
Alta dirección	Personal que tiene a cargo tareas directivas
Comercial	Personal que realiza tareas de ventas, logística y distribución.
Recursos Humanos	Personal que realiza tareas de gestión del personal, capacitación y relaciones laborales.

Financiera	Personal que realiza tareas de contabilidad, tesorería y control de la gestión financiera.
Informática	Personal que realiza tareas de mantenimiento de sistemas, arreglos de computadoras, tratamiento y respuesta a incidentes de seguridad, entre otras.
Producción	Personal del sector de producción

A los fines de la concientización, se establecen las siguientes audiencias de acuerdo a los temas de seguridad a tratar:

Directivos

Usuarios de información confidencial

Técnicos informáticos

Todo el personal de la pyme

Cronograma de actividades

En el anexo C y D se brinda un detalle de las actividades y el material de la concientización relacionado con el siguiente cronograma.

Actividad	**Objetivo**	**Fecha estimada**
A1. Promoción del programa de concientización	Despertar el interés de los integrantes de la pyme en el programa de concientización	Marzo, luego del período vacacional
A2. Presentación del programa de concientización	Iniciar formalmente las actividades de concientización	Abril
A3. Charla sobre los principales riesgos de la seguridad de la información y buenas prácticas de protección	Concientizar en los principales riesgos de seguridad de la información y dar a conocer las buenas prácticas de protección	Mayo
A4. Saludo de cumpleaños al empleado de la pyme	Afianzar el vínculo con los empleados	Durante la totalidad de

	de la pyme	duración de la concientización
A5- Difusión de información y recomendaciones de seguridad de la información a través de Twitter y Facebook	Emplear las redes sociales para difundir la concientización	Junio a marzo
A6. Empleo de afiches mensuales con recomendaciones de seguridad de la información	Reforzar los conocimientos impartidos en las charlas de concientización	Junio a marzo
A7. Videos de buenas prácticas de seguridad de la información	Reforzar los conocimientos impartidos en las charlas de concientización	Junio a marzo
A8. Consejos para padres sobre seguridad	Entregar a los empleados un DVD con videos para que compartan con sus hijos temas sobre seguridad y un folleto con tips para guiar a los padres [25]	Julio
A9.Concurso del día de seguridad	Realizar un concurso a través de la red social donde los participantes envían una foto en la que expresan que es la seguridad para ellos [25]	Noviembre
A10. Boletín mensual de seguridad	Enviar por correo electrónico un boletín con información sobre seguridad	Junio a marzo

Métricas

Se definen las siguientes métricas relacionadas con las actividades definidas previamente.

Métrica	Medida	Frecuencia	Detalle

Concientización en phishing	Cantidad de usuarios víctimas de phishing	Mensual	Se simulan casos de phishing y se contabiliza la cantidad de víctimas. La cantidad debería disminuir en el transcurso del tiempo
Reporte de caso de phishing	Cantidad de usuarios que detectaron y reportaron casos de phishing	Mensual	Se contabiliza la cantidad de usuarios que detectan y reportan casos de phishing. La cantidad debería incrementarse en el transcurso del tiempo
Computadoras infectadas	Cantidad de computadoras infectadas	Mensual	Se contabiliza la cantidad de computadoras infectadas por adjuntos infectados, links maliciosos, código malicioso, etc. Al ser entrenados los usuarios debería disminuir la cantidad de computadoras infectadas.
Datos confidenciales	Cantidad de usuarios que divulgan información confidencial de las pymes en las redes sociales	Mensual	Se realizan búsquedas exhaustivas de información confidencial de la pyme publicada en las redes sociales: facebook, twitter, linkedin, etc.
Dispositivos sin actualizaciones	Cantidad de dispositivos provistos por la pyme	Mensual	Se contabilizará la cantidad de dispositivos provistos por la pyme (computadoras, celulares,

	(computadoras, celulares, tablet) que no tienen su software actualizado		tablet) que no tienen su software actualizado. Al ser entrenados los usuarios debería disminuir la cantidad de casos de este tipo
Claves fuertes	Cantidad de usuarios que utilizan claves fuertes	Mensual	Con la debida autorización se realizará un ataque de fuerza bruta o crackeo de hashes de claves para contabilizar la cantidad de usuarios que emplean claves fuertes.
Pérdida de información confidencial	Cantidad de usuarios que perdieron información confidencial por no disponer de copias de respaldo	Mensual	Se contabiliza la cantidad de usuarios que reportan que perdieron información confidencial por no disponer de copias de respaldo. Al ser entrenados los usuarios debería disminuir la cantidad de casos de este tipo

[24]

Revisión del plan de concientización

Anualmente, en este caso en el mes de marzo, se evaluará el grado de avance y eficacia del plan de concientización, según el análisis de las métricas obtenidas y los resultados obtenidos de las evaluaciones de las actividades efectuadas.

Se elaborará un informe con los resultados y conclusiones obtenidas y, en caso de corresponder se propondrán los posibles cursos de acción para efectuar los ajustes pertinentes.

Conclusión

Como resultado del presente trabajo se concluye que fue factible definir el concepto de concientización, analizar las principales causas por las que una organización debe concientizar a su personal, identificar a los responsables de la concientización, los pasos a seguir para llevarla a cabo y elaborar una propuesta de concientización para una empresa mediana, pequeña o micro de Argentina . Además, fue posible analizar los desafíos de la concientización en Latinoamérica y otros países del mundo de acuerdo a los resultados de diferentes encuestas realizadas sobre la temática de la seguridad de la información.

A continuación, se detallan las principales conclusiones obtenidas:

- La seguridad de la información debe contemplar tanto los aspectos técnicos como la cuestión humana. El "factor humano" y no exclusivamente la tecnología, es la clave para proveer un nivel adecuado y apropiado de seguridad, debido a que los controles técnicos no ofrecen una solución completa y absoluta en materia de seguridad. Según las encuestas de seguridad, la mayoría de las organizaciones reportan ser víctimas de phishing y ataques de rasomware lo que da cuenta de la necesidad de incrementar los niveles de concientización en el personal de las organizaciones. Las buenas prácticas en seguridad de la información incluyen a la concientización como una parte relevante en la gestión de la misma.
- La concientización en seguridad de la información debe lograr que los integrantes de la organización tomen conciencia de la importancia de la seguridad de la información e incorporen en su comportamiento habitual las buenas prácticas para garantizar la protección de la integridad, la confidencialidad y la disponibilidad de la información. Las personas deben ser conscientes del alcance y las consecuencias que tienen sus actos en materia de seguridad de la información.

- La concientización es un proceso que incluye identificar el contexto de la organización, evaluar las necesidades de concientización específicas, diseñar el plan de concientización, implementar el plan de concientización y evaluar los resultados obtenidos.
- Los principales responsables de la concientización deben incluir al menos al máximo responsable de la organización, encargado de brindar su compromiso con la seguridad de la información y definir la estrategia y los objetivos de la concientización, el responsable primario de llevar a cabo las tareas de la concientización, encargado de evaluar los resultados, efectuar métricas y reportar los resultados a la máxima autoridad de la organización y los usuarios en general (empleados, proveedores, visitantes y colaboradores externos de la organización).
- Según los datos relevados en distintas encuestas, se observaron distintos niveles de madurez entre Latinoamérica, Australia, Estados Unidos de América y Europa. Al respecto, se considera que el nivel de madurez de la concientización es igual o menor al nivel de madurez de la gestión de la seguridad de la información de la organización. En general, se observa que en Latinoamérica el apoyo de la alta dirección se encuentra entre el 50 % y el 60% y en Australia, Estados Unidos de América y Europa el apoyo de la alta dirección es superior al 80 %. Por otro lado, en Latinoamérica se reconoce a la concientización como parte de la seguridad de la información y en Australia, Estados Unidos de América y Europa se considera a la concientización como una medida para mitigar los riesgos de la seguridad de la información y se destina un presupuesto para la concientización. Se acota que, para la presente conclusión, en lo atinente a Estados Unidos de América y Europa, se tuvo en cuenta los resultados de la encuesta efectuada por Isaca y RSA Conference.
- En Latinoamérica la concientización se encuentra en una madurez temprana. En la mayoría de los casos, se observa interés e iniciativas para desarrollar la concientización y actividades de concientización asociadas al cumplimiento de la divulgación de políticas, normativas y leyes de protección de datos, entre otras. No se observan datos de organizaciones que hayan implementado cambios de comportamiento o una cultura de seguridad. Ante lo expuesto, se interpreta como el principal desafío para las organizaciones

de Latinoamérica mejorar sus estrategias de gestión de la seguridad de la información con el fin de incorporar la concientización como un mecanismo relevante para mitigar los riesgos de seguridad e incrementar el apoyo de la alta dirección.

- Por otro lado, en Australia la concientización reviste un nivel de madurez mayor que Latinoamérica. En particular, se reconoce a la concientización como una medida contra las amenazas a la seguridad cibernética, en la mitad de los casos analizados el incremento del presupuesto del año 2016 se destinó para la concientización y el personal que menos necesita ser concientizados son los niveles jerárquicos de la organización. Asimismo, se observó que se invirtió mayor presupuesto en controles del tipo técnico que en concientización. Ante lo expuesto y según los datos aportados por la encuesta, se considera que el desafío de las organizaciones de Australia es continuar afianzando la concientización en pos de implementar una cultura de seguridad y generar métricas que evalúen su eficacia.
- En cuanto a la encuesta efectuada por Isaca y Rsa conference, con un 70 % de respuestas de Estados Unidos de América y Europa, se observó que el 87 % de los encuestados disponen de un programa de concientización y el 53 % de los mismos cree que el programa es efectivo. Se acota que este último porcentaje representa una caída significativa desde 2014, cuando el 71 % creía que su programa de concientización era eficaz. Además, el incremento del presupuesto del año 2016 sería destinado a la concientización y la mayoría de la alta dirección considera que hacer obligatoria la concientización es una forma de mitigar los riesgos asociados a la seguridad de la información. Ante lo expuesto y según los datos aportados por la encuesta se considera que el desafío de las organizaciones es continuar desarrollando programas de concientización para ayudar a inspirar a una cultura de la seguridad en la organización y generar métricas que evalúen su eficacia.
- El estudio efectuado por el instituto Sans contó con una participación mayoritaria de organizaciones de Estados Unidos de América (70%). Al respecto, se observó que la concientización se encuentra en un estado inicial y empiezan a surgir señales de madurez. El 51 % de los encuestados efectúa una concientización que promociona la concientización y efectúa

cambios de comportamiento y únicamente el 2% de los participantes tiene un nivel de madurez con cambios de comportamiento, cultura de seguridad y cuentan con métricas para probarlo. Además, se identificó que el nivel de madurez de la concientización está relacionado directamente con el grado de apoyo de la alta dirección y que el personal que realiza la concientización carece de habilidades sociales (soft skills). Ante lo expuesto y según los datos aportados por la encuesta se considera que el desafío de las organizaciones participantes del estudio es mejorar la educación a los líderes para que comprendan que la seguridad no puede ser resuelta solamente por la tecnología y debe tener en cuenta el factor humano y conformar los grupos que realizan la concientización con personal que cuente con las habilidades sociales pertinentes.

- En particular, se considera un aporte muy valioso el reporte efectuado por el instituto Sans porque trata con mayor detalle la concientización que las otras encuestas incluidas en el presente trabajo.
- Se destaca que el análisis de los resultados de las distintas encuestas permite conocer el estado de la concientización principalmente en Latinoamérica, Australia, Estados Unidos de América y Europa y los desafíos que deben enfrentar las organizaciones para lograr que la concientización implementé una cultura de seguridad y métricas efectivas. Por otro lado, en futuras investigaciones un tema interesante a tratar sería analizar la evolución de la concientización desde los resultados obtenidos en el presente trabajo y profundizar e identificar las habilidades sociales que requieren los ejecutores de la concientización.
- En relación a la propuesta de concientización para una pyme, expuesta en el capítulo III, se destaca que para su elaboración se tuvieron en cuenta las principales recomendaciones enunciadas en el capítulo I y la propia experiencia profesional en la materia. Al respecto, se destaca que la propuesta en cuestión contempló los siguientes aspectos:

  - incluir la participación del máximo responsable de la pyme en los eventos claves de la concientización.

  - definir objetivos a corto y largo plazo entendiendo que la concientización es un proceso y no acciones aisladas.

- diseñar actividades atractivas para el personal, de corta duración y que generen la participación de los usuarios.
- emplear diferentes medios de comunicación, incluyendo las redes sociales.
- reiterar oportunamente un mismo mensaje a través de distintos medios de comunicación.
- destacar el "como" mas que el "que" en los mensajes de concientización.
- difundir recomendaciones de seguridad que el usuario pueda aplicar fuera del ámbito laboral.
- definir métricas acotadas y medibles.

- En particular, se considera que la elaboración de una propuesta de concientización es una tarea que requiere no solamente de los conocimientos técnicos sobre seguridad de la información sino de conocimientos sobre comunicación para garantizar que los mensajes a difundir son los apropiados y serán interpretados correctamente por los destinatarios. Al respecto, se coincide con lo observado en el estudio realizado por el Instituto Sans en cuanto que los grupos que realizan la concientización deben incluir personal con las habilidades sociales pertinentes.
- Finalmente, se concluye que llevar a cabo la concientización en una organización es un gran desafío para los profesionales de seguridad y que para elaborar un proyecto de concientización efectivo, los especialistas en seguridad deben contemplar en su propuesta aspectos relacionados a las ciencias sociales, tales como psicología social, comunicación, marketing, diseño y técnicas de aprendizaje, entre otras.

Anexo A: Roles involucrados en la concientización

Según la publicación especial n° 800-50 "Building An Information Technology Security Awareness and Training Program" del National Institute of Standards and Technology [2], los roles involucrados en la concientización son los siguientes:

Jefe de agencia

Debe garantizar que se le asigne alta prioridad a la concientización del personal.

Responsabilidades:

- Designar al Chief Information Officer_CIO.
- Asignar responsabilidades relativas a la seguridad.
- Garantizar que el programa tenga presupuesto, recursos y sea efectivo.
- Garantizar que la agencia tenga el suficiente personal capacitado en seguridad de la información para proteger los recursos de la organización.

Chief Information Officer (CIO)

Debe gestionar el entrenamiento y supervisar al personal con responsabilidades de seguridad significativas.

Principales responsabilidades:

- Establecer una estrategia global para la concientización.
- Garantizar que los principales involucrados entienden la estrategia y sean debidamente informados de los grados de avance de la concientización.
- Garantizar que todos los usuarios son entrenados y capacitados en sus responsabilidades de seguridad.

Information Technology Security Program Manager

Debe gestionar a nivel táctico las actividades relacionadas a la concientización.

Principales responsabilidades:

- Garantizar que el material de la concientización es apropiado y oportuno para la audiencia destinataria.
- Garantizar que todos los usuarios tienen disponible un mecanismo de retroalimentación sobre el material y presentaciones de la concientización.
- Garantizar que el material es revisado y actualizado periódicamente.

Administradores

Deben cumplir con los requerimientos específicos de concientización para los usuarios bajo su cargo.

Principales responsabilidades:

- Trabajar con el CIO y el Information Technology Security Program Manager para conocer sus responsabilidades compartidas.
- Desarrollar planes individuales para el personal con altas responsabilidades de seguridad.
- Garantizar que todos los usuarios reciben el entrenamiento pertinente antes de acceder a los sistemas de información.
- Trabajar para disminuir los errores y las omisiones de usuarios por falta de entrenamiento.

Usuarios

Son la mayor audiencia en la organización. Los usuarios pueden incluir empleados, proveedores, visitantes y colaboradores externos, entre otros.

Responsabilidades:

- Entender y cumplir con las políticas y procedimientos de seguridad.
- Estar apropiadamente entrenados y capacitados en las reglas de seguridad relativas a los sistemas y aplicaciones a las que acceden.
- Comunicar a la dirección sus necesidades de entrenamiento y capacitación.
- Ser conscientes de las acciones válidas que aportan a la seguridad, por ejemplo: el uso seguro de su contraseña. [2]

Según el documento "How to Build an Enterprise Security Awareness Program" de Gartner [12], los responsables de la concientización son:

- Comité de supervisión, integrado por varios "stakeholders".
- Administrador de la concientización.
- Chief security officers (CSOs).
- Chief information security officers (CISOs).
- Todos aquellos que realizan actividades relativas a la tecnología: los empleados, contratistas independientes, proveedores, socios y clientes, entre otros.
- Áreas de marketing y relaciones públicas. [12]

Según el libro "Managing an Information Security and Privacy Awareness and Training Program" de Rebecca Herald [13], los roles involucrados en la concientización son:

Administradores de la unidad de negocio

Responsabilidades:

- Diseñar la estrategia a desarrollar en la unidad de negocio
- Definir y documentar el modelo desarrollado para la unidad de negocio.

Consejeros de seguridad y privacidad

Este rol requiere de un buen entendimiento de las políticas, procedimientos y prácticas de seguridad en la organización; actualización permanente de las novedades o noticias sobre seguridad; habilidades de comunicación escrita y verbal efectiva; experiencia y conocimiento de los servicios y productos de la unidad del negocio; disponibilidad de dedicar un 10%-15% del tiempo para su responsabilidad de consejero y participar en las actividades de concientización requeridas.

Responsabilidades:

- Colaborar en la comunicación entre el área de seguridad y privacidad y los empleados, como así también con la implementación de la concientización.
- Actuar como el primer contacto para las preguntas y recomendaciones de seguridad y privacidad.
- Garantizar actividades de concientización para el personal.

Administrador regional de seguridad y privacidad

Responsabilidades:

- Desarrollar módulos principales y funcionales.
- Comunicar asuntos de seguridad y privacidad para su región.
- Actuar como expertos sobre asuntos legales, regulatorios y específicos de la región.

Administrador del personal

Responsabilidades:

- Apoyar visiblemente las actividades de concientización.
- Garantizar la participación del personal en las actividades de concientización.

Ejecutivos defensores de la seguridad y la privacidad

Este rol podría ser cubierto por un ejecutivo administrador de una unidad de negocio; deberá brindar una dedicación aproximada del 3%-5% del total de

su tiempo de trabajo; tener un buen conocimiento de los aspectos de seguridad; capacidad para apoyar visiblemente las políticas y procedimientos de seguridad y participar en las actividades de concientización requeridas.

Responsabilidades:

- Proveer el soporte local para su unidad de negocio.
- Promover y apoyar la implementación de la estrategia.
- Mantener la red de los defensores de la seguridad y privacidad. [13]

Anexo B: Proceso de concientización

Según la publicación especial número 800-50 "Building An Information Technology Security Awareness and Training Program" del National Institute of Standards and Technology [2], las fases del ciclo de vida de la concientización son:

1. Diseño
2. Desarrollo
3. Implementación
4. Post-implementación

A continuación, se detallan cada una de las fases:

Fase 1: Diseño

La concientización debe dar soporte a las necesidades del negocio y ser relevante para la cultura y la arquitectura de la tecnología de la información de la organización.

En esta etapa se deberá:

- Identificar las características relevantes de la organización, por ejemplo: estructura orgánica.
- Definir las necesidades de concientización, involucrando al personal clave para esta tarea, a saber: ejecutivos, personal de seguridad, dueños de datos, administradores de sistemas, personal de soporte de IT, encargados de operaciones y usuarios de los sistemas. Para definir las necesidades previamente se pueden realizar:
  - Entrevistas a los grupos claves identificados. Por ejemplo, ejecutivos, dueños de los sistemas, dueños de las aplicaciones principales y responsables de funciones de IT.
  - Encuestas o sondeos organizacionales.
  - Revisar y evaluar el material disponible en materia de concientización. Por ejemplo: material reciente utilizado en la concientización, actividades de concientización y listado de asistentes a dichas actividades.
  - Analizar las métricas de concientización existentes. Por ejemplo: porcentaje de empleados que completaron el curso de concientización o usuarios con responsabilidades de seguridad que recibieron una capacitación específica.

- Identificar a los dueños de datos y representantes de seguridad designados a las aplicaciones principales.
- Identificar los usuarios que tienen accesos a los sistemas y a las bases de datos.
- Revisar las recomendaciones de los programas de control interno, disposiciones de cumplimiento obligatorio, recomendaciones de las auditorias y los programas relativos a la seguridad de la información.
- Analizar los eventos de seguridad (logs) para detectar necesidades de entrenamiento o capacitación. Por ejemplo, pueden identificarse ataques de denegación de servicios, defacement de sitios web o ataques de virus.
- Revisar cambios técnicos en la infraestructura informática.
- Estudiar las principales tendencias en concientización en materia de la seguridad de la información, a nivel académico, en publicaciones del gobierno y/o en sitios de internet reconocidos.

Para definir las necesidades de concientización se debe responder a las siguientes preguntas:

- ¿Qué concientización se necesita?
- ¿Qué acciones se empezaron a realizar para satisfacer las necesidades de concientización identificadas?
- ¿Cuáles son las diferencias entre las necesidades identificadas y lo que se empezó a hacer? ¿cuánto más se necesita hacer?
- ¿Cuáles son las necesidades más críticas?

Fase 2: Desarrollo

El desarrollo del plan de concientización debe incluir los siguientes puntos:

- Objetivo general.
- Alcance.
- Roles y responsabilidades.
- Distintas audiencias identificadas.
- Cursos obligatorios u opcionales. Definición de los objetivos de aprendizaje de cada curso y elaboración del material para cada audiencia incluyendo los tópicos de cada curso.
- Métodos a aplicar.

- Documentación, retroalimentación y evidencia del aprendizaje de las actividades del plan de concientización.
- Evaluación y actualización del material utilizado para la concientización.
- Frecuencia de la difusión del material.

Luego de establecer la estrategia y el plan, es necesario identificar las prioridades de las actividades. Los factores claves a tener en cuenta son:

- La disponibilidad de los recursos involucrados.
- Los roles de las distintas audiencias y el impacto que tendrá su concientización en la organización.
- El estado actual del cumplimiento de la concientización en la organización.
- Las dependencias que trabajan en proyectos críticos para la organización.

En cuanto al presupuesto del plan se sugiere agrupar los costos por usuario y rol o mostrar el porcentaje del costo de la concientización en el presupuesto global o en el presupuesto de tecnología de la información.

En relación al material a desarrollar se debe tener en cuenta que el mismo debe dar respuesta a las necesidades de concientización identificadas. A modo de ejemplo se enuncian algunos posibles tópicos a incluir en el material de la concientización:

- Uso de claves de accesos, creación, frecuencia de cambio y protección de las mismas.
- Medidas de protección ante virus, troyanos y código malicioso. Uso del antivirus.
- Políticas de seguridad, implicancias de su no cumplimiento.
- Empleo seguro del correo electrónico.
- Uso de la navegación por internet, accesos prohibidos y permitidos, monitoreo de la actividad de los usuarios.
- Copias de resguardo de información.
- Ingeniería social.
- Respuesta a incidentes, a quién contactar y que hacer ante un posible incidente de seguridad.
- Medidas de seguridad en el trabajo remoto.
- Seguridad de uso para dispositivos móviles.
- Empleo de criptografía.

- Seguridad de las computadoras portátiles en viajes, seguridad física y de la información.
- Sistemas y software de la propiedad de la organización, casos permitidos y no permitidos.
- Actualizaciones de software.
- Control de accesos lógico, asignación del menor privilegio y separación de funciones.
- Responsabilidad del individuo en la organización.
- Control de visitantes y accesos a los espacios físicos restringidos.
- Escritorios y pantallas limpios.
- Protección de la información confidencial, incluye: eliminación, destrucción, copias de resguardo y accesos, entre otras acciones.

Para la elaboración del material de la concientización se puede emplear la información provista por:

- Correos electrónicos de instituciones académicas u organizaciones de seguridad que asesoran sobre esta temática.
- Organizaciones profesionales y de proveedores.
- Sitios de internet con noticias de seguridad.
- Publicaciones específicas de seguridad.
- Conferencias, seminarios y cursos.

Para las actividades de concientización que pretendan producir habilidades relevantes, necesarias y competencias se requiere que el material sea desarrollado en tres niveles: inicial, intermedio y avanzado. En particular, puede emplearse una metodología que identifica distintos roles que tienen algún grado de responsabilidad en seguridad como se detalla en la publicación especial del NIST número 800-16 "Information Technology Security Training Requirements: a Role- and Performance-Based Model"

Fase 3: Implementación

El plan de concientización debe ser explicado a la totalidad de los integrantes de la organización para lograr el apoyo en su implementación y provisión de los recursos necesarios. La explicación debe incluir las expectativas, resultados y beneficios que aportará la concientización a la organización. Es esencial que todos los involucrados entiendan sus roles y

responsabilidades. Además, deben informarse el cronograma de las actividades.

Además, para la implementación deben seleccionarse las técnicas a emplear para difundir el material de concientización. La selección dependerá de los recursos requeridos y la complejidad del mensaje. Algunas técnicas son:

- Difusión de los mensajes de concientización a través de los elementos empleados en las tareas laborales, por ejemplo: mensajes impresos en lapiceras, anotadores, relojes, señaladores y mouse pad, entre otros.
- Publicación de posters con listas de acciones permitidas y prohibidas.
- Implementación del protector de pantallas y mensajes de alertas.
- Distribución de newsletters.
- Comunicación de alertas de seguridad distribuidas a través del correo electrónico de la organización.
- Difusión de videos.
- Empleo de teleconferencia.
- Dictado de cursos presenciales con instructor.
- Organización del día de la seguridad o eventos similares.
- Uso de mascotas de la concientización.
- Realizar crucigramas con palabras relacionas a la seguridad de la información.
- Implementar actividades con premios.

La mayoría de estas técnicas no requieren grandes recursos. Asimismo, se recomienda repetir un mismo mensaje de concientización a través de varias técnicas.

Si en el marco de la concientización se requiere realizar actividades de entrenamiento para desarrollar una habilidad se pueden emplear videos interactivos o e-learning.

Fase 4: Post implementación

Para que el plan de concientización no se vuelva obsoleto se deben contemplar los avances de la tecnología, modificaciones en las misiones y prioridades de la organización y cambios en la tecnología implementada en la organización.

Luego de la implementación del plan, debe verificarse su cumplimiento y efectividad. Se sugiere utilizar una herramienta sistematizada para recolectar la

información clave para que pueda ser consultada por todos los involucrados. Con estos datos se podrán identificar los "gaps", los problemas, tomar acciones correctivas y realizar su seguimiento.

Se debe contar con un mecanismo formal de evaluación y retroalimentación que permita llevar a cabo la mejora continua de la concientización. Para ello se pueden emplear: cuestionarios de evaluación, foros de grupos, entrevistas personalizadas, análisis independiente o una evaluación externa.

Finalmente, se consideran como factores de éxito de la concientización:

- El financiamiento suficiente para implementar la estrategia acordada.
- La estructura apropiada de la organización para que los responsables claves puedan llevar a cabo su estrategia.
- El soporte pertinente para la difusión y distribución del material.
- La comunicación de mensajes de concientización, en primera instancia, debe realizarla el máximo nivel ejecutivo.
- El uso de métricas.
- La alta dirección no debe recurrir a su jerarquía para evitar los controles de seguridad.
- El alto nivel de asistencia de los usuarios a las actividades de seguridad de carácter obligatorio.
- El reconocimiento a los usuarios que colaboran con la seguridad. Por ejemplo: la implementación de concursos con premios.
- La muestra de motivación por parte de los roles claves involucrados con la concientización. [2]

Por otro lado, en el documento "How to Build an Enterprise Security Awareness Program" de Gartner el proceso de concientización incluye los siguientes siete pasos [12]:

Paso 1: Definir el alcance preliminar

La definición preliminar del alcance de la concientización permitirá un marco de trabajo para discutir con los "stakeholders", quienes podrán modificarlo en función de sus prioridades. El alcance deberá describir las distintas audiencias y el cronograma de las actividades. La audiencia incluye a todos aquellos que realizan tareas relacionadas con la tecnología: los empleados, contratistas independientes, proveedores, socios y clientes.

La concientización cubre un plazo mínimo de dos a tres años, con revisiones en las fechas de rendición del presupuesto y al finalizar el ciclo de la misma.

Paso 2: Captar a los "stakeholders"

Si la concientización no cuenta con el apoyo de los "stakeholders" puede transformarse en una pérdida de tiempo y recursos. Cuando los ejecutivos no cumplen con las políticas y procedimientos de seguridad, su comportamiento será emulado por los otros empleados.

Se recomienda realizar entrevistas con los ejecutivos, en las cuales el entrevistado no debe percibir que se lo presiona para aprobar o apoyar el proyecto, sino que debe interpretar las ventajas que tiene para él la concientización.

Paso 3: Construir un caso de negocio

La concientización debe definir con precisión los objetivos y los beneficios esperados. Para la definición de los objetivos se recomienda emplear expresiones de negocio, por ejemplo, el objetivo de disminuir los pedidos de cambios de contraseñas a la mesa de ayuda puede expresarse como mejorar la productividad del personal a través de disminuir la solicitud de cambios de contraseñas de usuarios.

Se recomienda formar un comité de supervisión, integrado por varios "stakeholders", para dirigir las acciones del administrador de la concientización. Además, se deben definir los mecanismos por los cuales el administrador de la concientización reportará al CIO, CISO y al comité de supervisión. Al respecto se deben detallar los formatos, los contenidos y las frecuencias de las presentaciones de los informes de avance.

También se deben identificar los recursos requeridos para llevar a cabo la concientización. Los recursos serán determinados por el alcance definido para la concientización y podría incluir los fondos destinados al administrador de la concientización, desarrollo de planes del proyecto, costos de actividades específicas de concientización y análisis de métricas de la concientización.

El caso de negocio debe definir como serán medidos los éxitos de la concientización. Cada plan del proyecto de la concientización incluirá métricas sobre el aprendizaje y cambios de comportamientos específicos del personal. Las métricas de todo el programa estarán basadas sobre cambios de cultura y

eficiencia de la organización. Medir cambios de la cultura es una actividad compleja y sutil. Algunas posibles medidas para identificar cambios en actitudes y tendencias culturales son:

- Números de empleados que han participado en las actividades de concientización comparadas con la cantidad total de empleados.
- Incidentes de seguridad reportados por los empleados que completaron las actividades de concientización.
- Inquietudes de seguridad reportadas por empleados que completaron las actividades de concientización.
- Número de solicitudes del personal sobre materiales y actividades de concientización.

Se recomienda tomar estas métricas en forma previa al inicio de las actividades de la concientización. Esta evaluación previa establecerá el punto de partida para evaluar el progreso de la concientización posteriormente.

Paso 4: Planificar una concientización factible con objetivos claros y medibles

Luego de identificar las distintas audiencias, se deberá entrevistar a los administradores y ejecutivos de la organización para determinar que necesitan de la concientización y que pueden contribuir a la misma. Por ejemplo, las áreas de marketing y relaciones públicas pueden ser sectores útiles para evaluar la propuesta de comunicación de la concientización

En particular los profesionales de seguridad deberían reconocer que su experiencia en seguridad y tecnología no necesariamente los hace entrenadores o comunicadores efectivos. Si la organización realiza tareas de entrenamiento y cuenta con el personal idóneo para este tipo de tarea, la concientización puede utilizar este recurso para que ellos desarrollen las actividades de concientización con el contenido aportado por el personal de seguridad. En forma análoga se puede recurrir a los sectores de marketing, relaciones públicas o comunicaciones para elaborar videos, posters u otros elementos de difusión. Si no se cuentan con los recursos internos idóneos se recomienda contratar estos servicios con los proveedores apropiados.

Antes y durante el diseño de la concientización se deben evaluar las necesidades de la audiencia para cada actividad para determinar los estilos de aprendizaje que precisan los participantes y los mecanismos apropiados para entregar el contenido de la concientización. Dicha evaluación permitirá definir:

- Cambios alcanzables y realistas en el comportamiento del personal.
- Materiales requeridos.
- Tiempos obligatorios requeridos al personal para participar en las actividades de concientización.
- Costos del desarrollo de los materiales, incluyendo costos del desarrollo en guías de entrenamiento para entrenadores y participantes.
- Costos de los consultores externos.

Paso 5: Implementar la concientización

Los materiales de la concientización deben garantizar:

- El uso de logos de la empresa, colores, slogans y otros identificadores que alinean la concientización con la marca de identidad de la organización.
- Cubrir todas las audiencias.
- Cumplir con los objetivos estratégicos y tácticos del programa.

Luego de diseñar cada actividad, se recomienda verificar la misma con una prueba piloto para identificar fallas y realizar las modificaciones necesarias. Es recomendable que las primeras presentaciones estén dirigidas a la alta dirección porque ellos serán esenciales para lograr el apoyo a la concientización. Una vez que ellos son entrenados, serán capaces de reconocer y corregir el comportamiento del personal a su cargo.

Para implementar cada fase de la concientización se debe garantizar que su ejecución esta fundamentada en objetivos razonables y conmensurables.

Paso 6: Medir y optimizar la concientización

Una vez que la concientización está en curso se puede empezar a medir las métricas definidas en el paso 4 y reportar tanto los éxitos como los problemas.

El proceso de medición permitirá mejorar el contenido y los mecanismos de entrega del material de concientización.

Paso 7: Reportar a los "stakeholders" y renovar su compromiso con la concientización

Es importante informar el progreso de la concientización a los "stakeholders" y a los responsables de tomar decisiones. Para los reportes a presentar se recomienda emplear gráficos, información fácil de comprender y que requiera una mínima lectura. Los reportes deben ser distribuidos a los

niveles ejecutivos de la organización, auditoría interna, líderes de unidades de negocios y algunas partes de los reportes pueden ser publicados en la intranet de la organización. Luego de que los "stakeholders" y el comité de supervisión ha sido correctamente informados, es la oportunidad de renovar su compromiso con la concientización. [12]

En cuanto al libro "Managing an Information Security and Privacy Awareness and Training Program" de Rebecca Herald, los pasos críticos en el ciclo de vida de la concientización son [13]:

1. Diseño

Incluye las siguientes acciones:

- Dirigir una evaluación de necesidades.
- Desarrollar la estrategia de la concientización y contar con su aprobación.
- Identificar las tareas claves a implementar para apoyar los objetivos de la concientización.

2. Desarrollo

- Identificar las fuentes de información disponibles para el material de la concientización.
- Identificar las audiencias.
- Definir el alcance.
- Crear los contenidos del material.
- Confeccionar el material de la concientización.

3. Implementación

- Comunicar y distribuir el material de la concientización.

4. Post-implementación

- Mantener actualizado el material de la concientización.
- Monitorear y medir la efectividad de la concientización.
- Emplear métodos de retroalimentación.

Adicionalmente, se recomienda evitar los siguientes errores:

- No tener en cuenta la cultura de la organización.
- No considerar o investigar los requerimientos legales y regulatorios que aplican a la organización.
- No contar con el apoyo y colaboración de la máxima autoridad de la organización.
- No estimar o contar con el presupuesto adecuado para el programa.

- No emplear el material adecuado para la organización.
- Sobrecargar de información las piezas del material de la concientización. Muchos estudios indican que las personas pueden recordar como máximo solo cinco ítems nuevos por vez.
- No incluir en el material de la concientización elementos que sean útiles y aplicables al trabajo del destinatario del mensaje.
- No recurrir a instructores idóneos.
- No utilizar métodos que la audiencia pueda relacionar, entender y aprender.
- No contemplar la motivación del personal para conocer y aprender aspectos de seguridad.
- No realizar una planificación adecuada de los eventos de la concientización.
- No evaluar la efectividad del programa.
- Utilizar un lenguaje inapropiado o políticamente incorrecto.
- Difundir la totalidad del contenido del programa en un periodo corto de tiempo. [13]

Anexo C: Detalle de las actividades de Concientización

Actividad : **A1.** Promoción del programa de concientización **Detalle** : Con quince días de anticipación se promocionará el inicio de una actividad que incluirá a todo el personal y que es muy importante para la organización. Se comunicará al personal de la pyme a través de correos electrónicos y el uso de afiches. **Evaluación** : Se contabilizarán las consultas que se realicen al sector de Recursos Humanos sobre la promoción efectuada.
Actividad : **A2**. Presentación del programa de concientización **Detalle** : Se comunicará el inicio de la concientización y su importancia para la pyme a través de un desayuno de 30 minutos antes del inicio de las actividades laborales. Una semana antes, se enviará un correo electrónico con la invitación al desayuno y se empleará un poster para difusión. Se requiere la presencia del máximo directivo de la pyme y unas breves palabras suyas que avalen el proyecto. **Evaluación** : Se tomará asistencia de los participantes. Se enviará un mail a aquellos que no pudieron asistir al desayuno informando el inicio de la concientización.
Actividad : **A3**. Charla sobre los principales riesgos de seguridad de la información y las buenas prácticas de protección. **Detalle** : Se realizarán cuatro charlas con 10 participantes cada una. Los principales temas a tratar son: Ingeniería social: definición y demostración Phishing: definición y demostración Código malicioso: principales variantes de códigos maliciosos. Teléfonos inteligentes: potenciales riesgos actuales. Redes sociales: potenciales riesgos actuales. Buenas prácticas para protegerse de los riesgos de seguridad, tales como: uso de claves de accesos seguras, actualizaciones y antivirus, copias de seguridad y uso seguro de correo electrónico, internet, teléfonos inteligentes y redes sociales.

Evaluación : Se entregará a los participantes un material impreso con el contenido de la charla. Durante la charla se dividirá a los participantes en dos grupos que competirán en distintos desafíos. Las consignas de los desafíos serán: - Generar claves seguras. - Identificar cómo actuar ante las determinadas situaciones planteadas. Al grupo ganador de cada consiga se le sumarán los puntos estipulados por cada desafío. Al finalizar la charla al grupo con mayor cantidad de puntos se le entregará una caja de bombones.
Actividad : **A4**. Saludo de cumpleaños al empleado de la pyme **Detalle** : Se enviará un correo electrónico con humor para el día del cumpleaños del empleado. **Evaluación** : Se contabilizará la cantidad de respuestas al correo electrónico de salutación.
Actividad : **A5**. Difusión de información y recomendaciones de seguridad de la información a través de Twitter y Facebook. **Detalle** : Se utilizará una cuenta de Twitter y otra de Facebook exclusivamente creadas para difundir recomendaciones de seguridad para uso personal, chistes de seguridad y noticias sobre seguridad de la información. No se publicará información confidencial de la pyme. Se publicará con una frecuencia semanal en Twitter y Facebook. **Evaluación** : Se realizará un seguimiento de la cantidad de seguidores en Twitter y Facebook, la cantidad de "Me gusta" y se analizarán los comentarios de los participantes.
Actividad : **A6.** Empleo de afiches mensuales con recomendaciones de seguridad de la información. **Detalle** : Se reforzará la concientización en los temas de redes sociales, teléfonos inteligentes, copias de seguridad de archivos, actualizaciones, claves, código malicioso y phishing a través de afiches pegados en oficinas y lugares comunes del edificio de la pyme. **Evaluación** : No se realiza
Actividad : **A7.** Videos de buenas prácticas de seguridad de la

información.

Detalle : Se difundirán videos que detallan paso a paso o con ejemplos, como:

- Configurar en forma segura los teléfonos inteligentes
- Configurar la privacidad en redes sociales
- Analizar los correos sospechosos
- Realizar backup y restauración de información crítica

Los videos estarán focalizados en el "cómo" deben implementarse las recomendaciones de seguridad.

Evaluación : No se realiza

Actividad : **A8.** Consejos para padres sobre seguridad

Detalle : Se entregará a cada empleado un DVD con videos y un folleto impreso con recomendaciones de seguridad para padres o tutores de niños. El folleto incluirá consejos para el uso de internet, redes sociales y prevención de victimización a niños.

Se entregará a todo el personal incluyendo al personal que no tiene hijos.

Evaluación : Se analizará la repercusión del material entregado a través de una encuesta.

Actividad : **A9.** Concurso del día de seguridad

Detalle : Se realizará un concurso a través de la red social Facebook en el cual los participantes enviarán una foto en la que expresan que es la seguridad de la información para ellos. La foto con mayor cantidad de votos será la ganadora. El ganador recibirá un pendrive de 32 Gb. La convocatoria se realizará a través de correo electrónico.

Evaluación : Se evaluará la cantidad de participantes

Actividad : **A10.** Boletín mensual de seguridad

Detalle : Se enviará por correo electrónico a todo el personal un boletín con información sobre seguridad. La temática será seleccionada en función de los riesgos que se identifiquen en la pyme.

Evaluación : Se analizarán las consultas que se reciban sobre el contenido del boletín de seguridad.

Anexo D: Material de soporte de las actividades de Concientización

A1. Promoción del programa de concientización

1) Contenidos de los correos electrónicos a enviar:

Asunto: Lanzamiento abril 2017

"A partir de abril de 2017 iniciaremos un trabajo conjunto para aprender y crecer con nuestra empresa.
Todos podrán participar y ser parte del crecimiento de nuestra empresa.
¡Contamos con vos!"

Asunto: Falta poco para empezar
"Te recordamos que en una semana iniciamos un gran proyecto para nuestra empresa.
Ya falta poco, contamos con vos."

2) Poster

dreamstime.com [26]

A2. Presentación del programa de concientización

1) Contenido del correo electrónico a enviar:

Asunto: Invitación desayuno gratis el 3/4

"Buenos días

El 3 de abril a las 8:30 hs te invitamos a participar del desayuno de lanzamiento de nuestro gran proyecto.

¡Te esperamos!"

2) Poster

[27]

3) Contenido de la presentación

La presentación estará a cargo del directivo de la pyme y tendrá una duración de 5 minutos.

Se sugieren las siguientes palabras:

"Bienvenidos

Gracias por participar de este desayuno. A partir de hoy empezaremos a aprender como protegernos de las nuevas amenazas relacionadas con el uso de la tecnología.

Podemos afirmar que el uso de medios y herramientas informáticas proporciona beneficios y ventajas. Sin embargo, también implica el surgimiento de nuevos riesgos. Por ejemplo: a principios de año todos vimos en las noticias

que hackearon la cuenta de twitter de la ministra de Seguridad. Ante este tipo de noticias no podemos negar que estos nuevos riesgos son parte de nuestra vida cotidiana

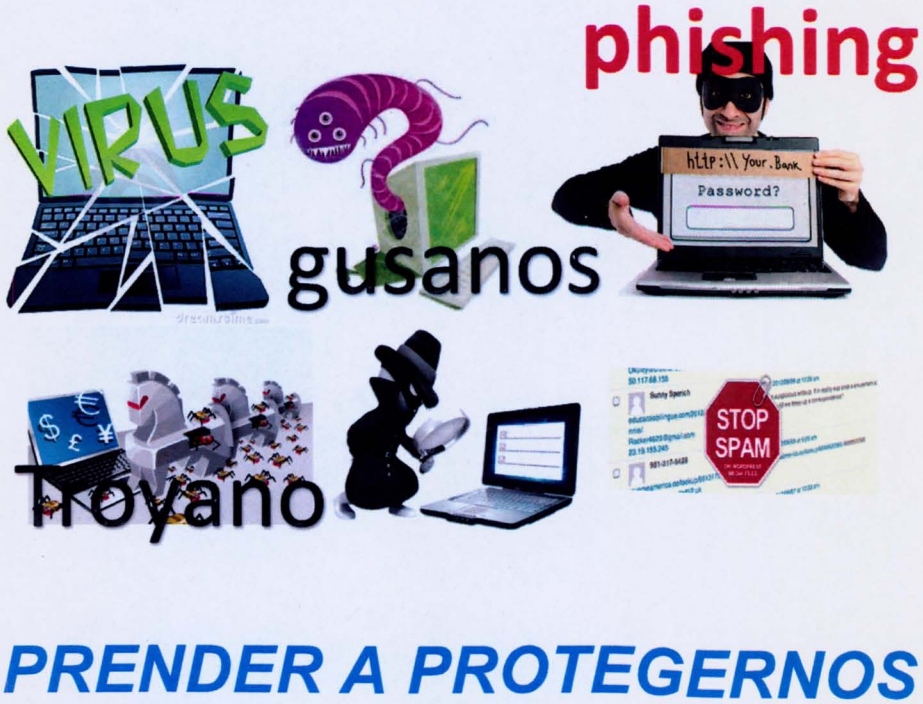
En el contexto actual debemos conocer las amenazas y saber que debemos hacer para protegernos.

Es importante que sepan que lo que vamos a aprender no es solo para aplicarlo en el ámbito laboral sino también en nuestro entorno privado o familiar.

Por último, les informo que a partir de mayo se iniciarán unos cursos dirigidos a todo el personal y a través de distintos medios de comunicación les iremos informando las distintas actividades

Muchas gracias por asistir a este desayuno"

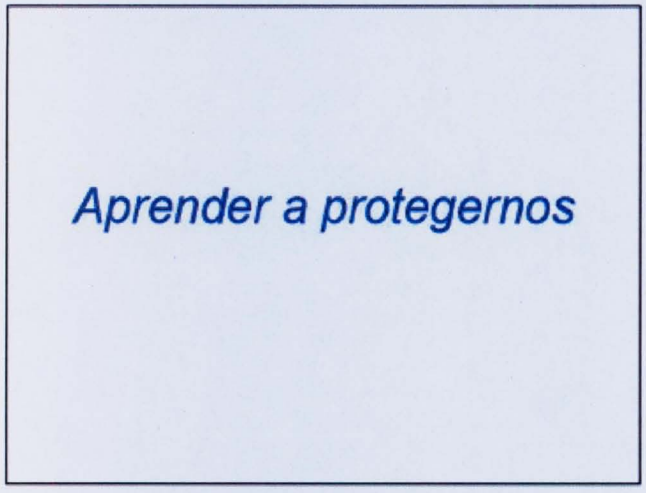
4) Imagen a mostrar en la presentación con proyector

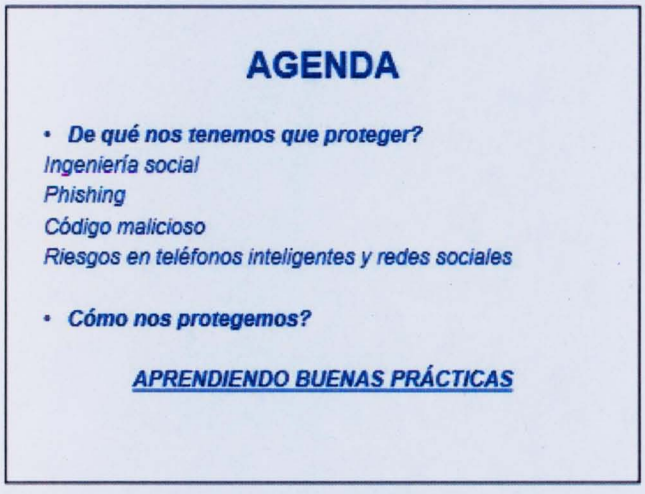


[28]

A3. Charla sobre los principales riesgos de la seguridad de la información y las buenas prácticas de protección.

El contenido de la charla es el siguiente:





INGENIERIA SOCIAL

- *La ingeniería social es un conjunto de trucos, engaños o artimañas que permiten confundir a una persona para que entregue información confidencial*

INGENIERIA SOCIAL

- ***¿Por qué funciona?***

Según Kevin Mitnick, uno de los ingenieros sociales más famosos de los últimos tiempos, la ingeniería social se basa en estos cuatro principios:

- ***Todos queremos ayudar.***
- ***El primer movimiento es siempre de confianza hacia el otro.***
- ***No nos gusta decir "No".***
- ***A todos nos gusta que nos alaben.***

Recuerdan esta película?

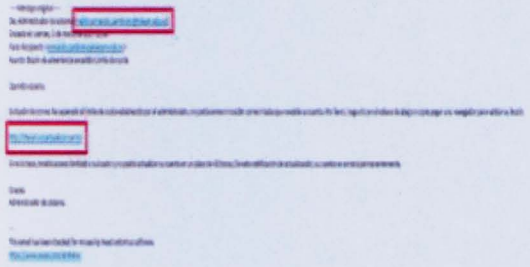
INGENIERIA SOCIAL

- **Actividad: video de la película Nueve Reinas**

PHISHING

- *El Phishing es una combinación de ingeniería social y elementos técnicos para engañar a un usuario y lograr que éste entregue involuntariamente información confidencial a usuarios malintencionados. La forma más común es mediante el envío de mails falsos, escritos como si hubieran sido enviados por una organización auténtica.*

PHISHING



CÓDIGO MALICIOSO

- *VIRUS: son programas que alteran el normal funcionamiento del dispositivo (computadora, telefono inteligente, tablet, notebook, etc). Pueden destruir datos, dañar los sistemas o bloquear las redes.*
- *TROYANOS: Son programas que permiten el acceso a usuarios externos, a través de una red informatica o de Internet, con el fin de recabar información o controlar remotamente a la máquina.*

SPYWARE: Es un programa espía que recopila información personal sin nuestro conocimiento.

CÓDIGO MALICIOSO

- **RANSOMWARE**

Es una técnica para bloquear sus dispositivos y exigir un rescate a cambio de recuperar el acceso.

Puede entrar en su dispositivo:

- *mediante un adjunto de correo electrónico*
- *a través de su navegador si visita una página web infectada*
- *a través de su red informática*

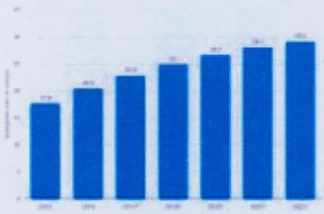
Cómo evitar el ransomware

- *Actualizar todo el software de su equipo siempre*
- *Antivirus*

REALICE COPIAS DE SEGURIDAD CON FRECUENCIA

TELÉFONOS INTELIGENTES

Para el año 2017, Argentina tendrá 22.9 millones de usuarios con teléfonos inteligentes



TELÉFONOS INTELIGENTES

RIESGOS

- *Mayor cantidad de potenciales víctimas*
- *Menor conciencia del usuario sobre la información que manipula el dispositivo*
- *Inconvenientes para actualizar el software del dispositivo*
- *Ataques de código malicioso*
- *Robo/pérdida del dispositivo*

REDES SOCIALES

Las redes sociales son herramientas poderosas y divertidas. Algunas de ellas son: Facebook, Twitter, Instagram, Snapchat, LinkedIn

Posibles riesgos

- *daños a tú carrera profesiona*
- *ataques en tú contra o contra tú empresa*
- *ataques a tú computadora*
- *estafas*

CÓMO NOS PROTEGEMOS?

APRENDIENDO BUENAS PRÁCTICAS

BUENAS PRÁCTICAS

- *Claves seguras*
- *Antivirus y actualizaciones*
- *Uso seguro del correo electrónico*
- *Uso seguro de Internet*
- *Copias de seguridad*
- *Uso seguro de teléfonos inteligentes*
- *Uso seguro de redes sociales*

CLAVES SEGURAS

Conjunto de caracteres asociados a nuestro identificador, que nos permite realizar el acceso a un sistema o aplicación.

Características deseables:

- *Debe ser personal y secreta*
- *No se debe prestar*
- *Puede ser cambiada sólo por el usuario al que pertenece*
- *Debe ser difícil de descubrir*
- *Debe cambiarse periódicamente*

BUENAS PRACTICAS PARA LA ELECCION DE UNA CLAVE

- ***No utilizar palabras comunes (aunque sean extranjeras) ni nombres de fácil deducción(usuario, familiar, mascota, su ciudad, su equipo de fútbol).***
- ***No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, etc.)***
- ***No emplear terminología técnica conocida (nombre de la pyme, etc)***
- ***Elegir una contraseña que combine caracteres alfabéticos (mayúsculas y minúsculas), números y caracteres especiales.***
- ***Utilizar una contraseña larga, cuanto más larga más segura.***
- ***Usar contraseñas distintas para sistemas diferentes. Puede usar una contraseña base y ciertas variaciones lógicas para distintos sistemas.***
- ***Emplear claves fáciles de recordar para no verse obligado a escribirlas.***

BUENAS PRACTICAS PARA LA ELECCION DE UNA CLAVE (EJEMPLO)

Pensar en una oración que pueda recordar:

•Por ejemplo: "Argentina ganará el mundial de fútbol de Rusia y Messi será el máximo goleador"

•Tomar la primera letra de cada palabra: "agemdfdrymsemg"(Longitud de clave=14)

•Para agregar complejidad reemplazar algunas letras por su correspondiente en mayúscula=> "agEmdFdrYmsEmg"(cada tres letras)

•Para incorporar más seguridad agregar a la clave algún caracter especial y/0 algún número, no necesariamente al principio o al final. Por ejemplo: "agEmdFdr18YmsEmg"

CLAVES SEGURAS

- Actividad grupal de claves seguras

ANTIVIRUS Y ACTUALIZACIONES

- *Comprobar periódicamente que esté activo el antivirus de su estación de trabajo, visualizando el ícono que se encuentra en la barra inferior, a la derecha de la pantalla*
- *En caso que el ícono no sea visualizado deberá contactarse con el sector de asistencia al usuario.*
- *Usar la versión de software antivirus corporativo para proteger los recursos brindados por la pyme*
- *En caso de encontrar un virus, DETENER toda operación, desconectar el cable de red de su PC y llamar inmediatamente solicitando soporte al sector de asistencia al usuario*

ANTIVIRUS Y ACTUALIZACIONES

- *La actualización de los sistemas operativos y de las aplicaciones es primordial, debido a que un sistema no actualizado es vulnerable a ataques de virus, ransomware, troyanos, intrusos, entre otros.*
- *Las pc's de las pymes se actualizan automáticamente, en caso de necesitar soporte deberá contactarse con el sector de asistencia al usuario.*

USO SEGURO DEL CORREO ELECTRONICO

- *Verificar los archivos adjuntos a cada mensaje de correo electrónico, independientemente de su origen para evitar el ingreso de virus. Sólo abrir y/ó guardar archivos adjuntos esperados. Tener en cuenta que las extensiones tales como: ".exe", ".bat", ".vbs" podrían ocasionar daños activando algún tipo de código malicioso.*
- *Verificar toda solicitud de información inusual o sospechosa, tanto personal como laboral. Especialmente cuando llegue retransmitida por otro usuario.*
- *No responder mensajes en general sin tener la certeza del remitente y del destino de la información que se proporcione.*
- *No responder a mensajes que le soliciten información de sus cuentas bancarias y/ó datos personales.*
- *Ignorar y eliminar los correos electrónicos recibidos de remitentes desconocidos.*
- *No participar en las cadenas.*

USO SEGURO DE INTERNET

- *Permitir ventanas emergentes sólo desde sitios confiables.*
- *Verificar la procedencia del sitio a visitar y la utilización de conexiones seguras al realizar transacciones en línea.*
- *Acceder a los sitios ingresando la dirección directamente en la barra de direcciones del navegador.*
- *No modificar las opciones de seguridad del navegador. Esto puede hacer que su pc sea más vulnerable a ataques.*
- *No instalar aplicaciones descargadas de sitios que no son de confianza.*

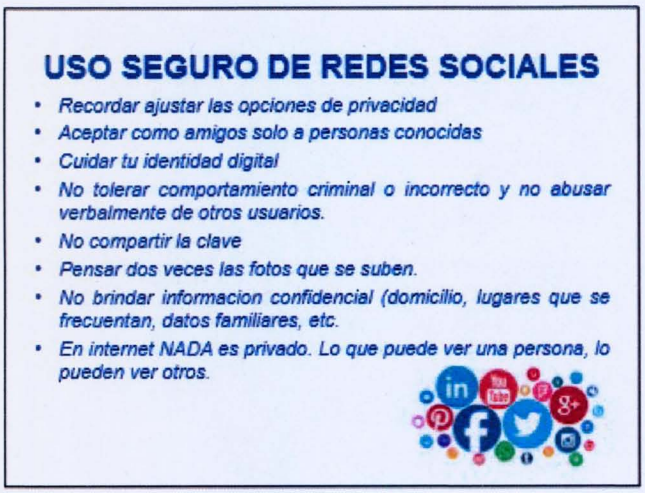
COPIAS DE SEGURIDAD

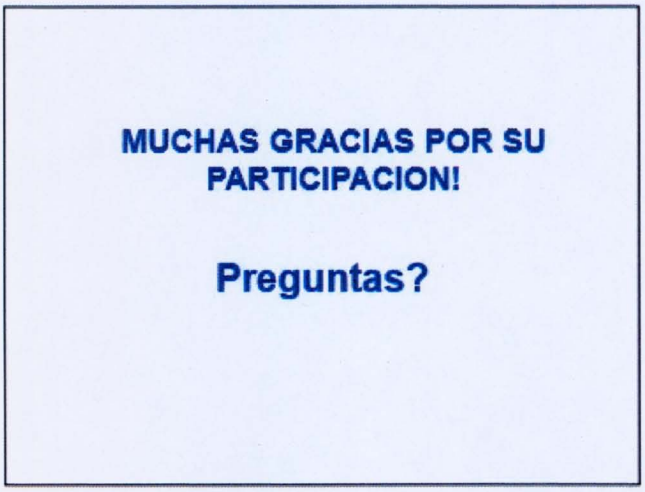
- *La copia de seguridad o backup es la copia total o parcial de información importante del disco duro, DVDs, bases de datos u otro medio de almacenamiento. Se almacenan generalmente en discos duros, CDs, DVDs, pen drives o cintas magnéticas.*

- *Permiten recuperar información en caso de pérdida de la copia original*
- *Realizar periódicamente copias de seguridad de la información importante.*

USO SEGURO DE TELÉFONOS INTELIGENTES

- *Activar el bloqueo*
- *Habilitar el cifrado de datos*
- *Utilizar contraseñas fuertes*
- *Controlar el acceso de las aplicaciones a datos*
- *Emplear la geolocalización responsablemente*





[29] [30] [31] [32] [33]

Nota: el video de la película Nueve Reinas muestra la estafa que realiza el protagonista (Ricardo Darín) a una señora. El protagonista toca el portero eléctrico de un edificio y se hace pasar por el sobrino favorito de la señora que atiende el portero. Le cuenta a la tía que tuvo un problema con el auto y que se había olvidado la billetera. Le pide algo de dinero. La señora dice que no tiene problema y bajará a entregarle el dinero. El protagonista le dice que no puede dejar el auto solo y mandará un amigo para que reciba el dinero. La señora baja y le entrega el dinero y un anillo al cómplice del estafador (Gastón Pauls).

Actividades a desarrollar en la charla de concientización:

1) Claves seguras

Cada integrante del grupo debe pensar en la clave que utilizará para acceder a la red y luego evaluar la misma. Se otorga un tiempo de 5 minutos para que cada usuario escriba su clave en un papel.

Reglas del juego:

Cada usuario inicia el juego con 50 puntos. A ese puntaje, descontará o sumará puntos de acuerdo a las siguientes pautas:

1. La contraseña contiene el nombre de un familiar o mascota (resta 10 puntos)
2. Contiene el número de teléfono, fecha de nacimiento o DNI propio o de un familiar (resta 10 puntos)
3. Contiene una palabra de diccionario inglés o castellano (resta 10 puntos)
4. Contiene caracteres consecutivos alfabéticos, numéricos o de teclado (resta 10 puntos)
5. Tiene sólo letras o tiene sólo números (resta 10 puntos)
6. Tiene una longitud menor que 8 caracteres (resta 10 puntos)
7. Si incluye caracteres especiales suma 12 puntos
8. Si incluye el uso de mayúsculas suma 12 puntos

Cumplido el tiempo de 5 minutos, se calcula la puntuación de acuerdo a las pautas previamente detalladas. Se anotarán los puntos obtenidos en la siguiente tabla

Item	Puntaje
Inicial	50 puntos
1	
2	
3	
4	
5	
6	
7	
8	
Valor final	

Finalmente, se suman los puntos obtenidos entre los integrantes del grupo para determinar el grupo ganador.

2) Detectar cómo actuar ante las situaciones planteadas

Los grupos participantes deben detectar las buenas prácticas que deben implementar en respuesta a las situaciones descriptas. Para ello deben relacionar las situaciones de la columna de la izquierda con las buenas prácticas de la columna de la derecha. Se brindará como máxima 20 minutos para realizar la actividad. Luego se verificará en conjunto las respuestas y se sumará para cada grupo los aciertos. Cada respuesta correcta suma 50 puntos.

1) Recibí un mail que me solicita ingresar a un sitio para el cambio de mi contraseña del home banking	a) Como configure la opción de cifrado en mi celular les resultará muy difícil acceder a mis datos
2) Mi pc tiene un virus!	b) Gentilmente, le respondo a mi compañero de la pyme que las claves son personales e intransferibles (cómo el cepillo de dientes!)
3) No puedo acceder a mí pc, fui víctima de un ransomware!	c) Espero pacientemente que finalicé la actualización de mi pc (y me tomo un cafecito)
4) Recibí un mail de un remitente desconocido con fotos adjuntas	d) No accedo a sitios dudosos. Además, puedo

5) En el chat de Facebook un "amigo" me solicita información sobre los clientes de la pyme

6) Perdí mi celular (con todos los contactos que tenía!!)

7) Todos mis contactos de Facebook pueden ver todas mis fotos (no quisiera que vieran algunas fotos privadas)

8) Un empleado de la pyme me solicita mi clave del sistema de facturación porque no recuerda la suya

9) Mi clave de acceso solo tiene números

contactar a mi Banco para reportar el mail sospechoso

e) Cambio mi clave por una nueva que tenga mayúsculas, minúsculas y números. Compongo la clave a partir de una frase fácil de recordar para mí.

f) No ejecutó archivos adjuntos de un mail de un remitente desconocido

g) Puedo recuperar la información importante de mi pc del backup que hice ayer (menos mal que hice lo que me recomendaron en ese curso aburrido...)

h) Respondo amablemente a mi "amigo" de facebook que no puedo compartir información de la pyme

i) Desconectó mi pc de la red y llamó al sector de

asistencia al usuario

10) Volví al trabajo luego de dos semanas de vacaciones, enciendo mi pc y un mensaje me informa que se iniciará la actualización de la pc

j) Configuro en Facebook distintos grupos con distintos permisos de acceso a los datos de mi perfil

Respuestas:

6 – a

8 – b

10 – c

1 – d

9 – e

4 – f

3 – g

5 – h

2 – i

7 - f

A4. Saludo de cumpleaños al empleado de la pyme

Ejemplos del correo electrónico a enviar con motivo del cumpleaños del empleado de la pyme.

1) Asunto: Muy feliz cumpleaños!

¡Muchas felicidades en el día de tú cumpleaños!
En este día tan especial queremos compartir contigo un poco de humor

Saludos
[34]

2)Asunto: Muy feliz cumpleaños!

¡Muchas felicidades en el día de tú cumpleaños!

En este día tan especial queremos compartir contigo un poco de humor

[35]

A5. Difusión de información y recomendaciones de seguridad de la información a través de Twitter y Facebook.

A continuación, se presentan algunos ejemplos de publicaciones en twitter

1)

"Sumate para lograr una internet mejor. ¿Qué podemos hacer?"

"Mantener un comportamiento correcto a la hora de navegar por internet, se respetuoso con todos los usuarios"

2)

"Cuida tú privacidad en las redes sociales. ¿Cómo lo hacemos?"

"No comuniques nunca tus datos personales (dirección, teléfono, cuenta bancaria, etc). Tampoco los de ningún familiar o usuario"

"Sólo acepta solicitudes de amistad de gente que conoces"

"Protege tu contraseña. No comuniques a nadie tu clave. Si sospechas que han entrado en tú perfil cambia tú clave rápidamente"

"Personaliza la privacidad de tu perfil. Organiza a tus amigos en listas para configurar tú privacidad por grupos de personas"

"Define la privacidad de las fotos que subes. Comparte los álbumes de fotos con los grupos adecuados"

"Configura la privacidad de tu biografía.Decide quienes pueden acceder a tus datos y evita que se hagan publicaciones sin tú consentimiento"
[36]

3)

"Sabías que el 75% de los adolescentes (con edades entre 12 y 17 años) tienen teléfonos celulares?"

"Para aprender como proteger a sus hijos que utilizan celulares acceda a http://es.netsmartz.org/CellPhones" [37]

A continuación, se presentan algunos ejemplos de publicaciones en Facebook

1)

"El 7 de febrero de 2017 fue el día internacional de la internet segura. Si queres saber mas, podes ingresar al siguiente link https://www.saferinternetday.org/"

[38]

2) El 28 de enero fue el día internacional de la protección de datos personales. Te invitamos a conocer más sobre el 28 de enero en este video http://www.jus.gob.ar/datos-personales/comunicados/2017/01/28/dia-internacional-de-la-proteccion-de-datos-personales.aspx

[39]

3) ¿Qué debemos hacer ante un robo de contraseñas de casillas de correo electrónico y redes sociales? Si queres saber mas, te invitamos a ver el siguiente video que brinda una serie de recomendaciones para evitar ser víctima de un delito informático y proteger la identidad digital, y concluye con los datos de contacto de la Unidad Fiscal Especializada en Ciberdelincuencia para denunciar este tipo de delitos http://www.fiscales.gob.ar/genero/se-emitieron-los-primeros-programas-realizados-por-el-ministerio-publico-fiscal-y-canal-encuentro/ [40]

4)

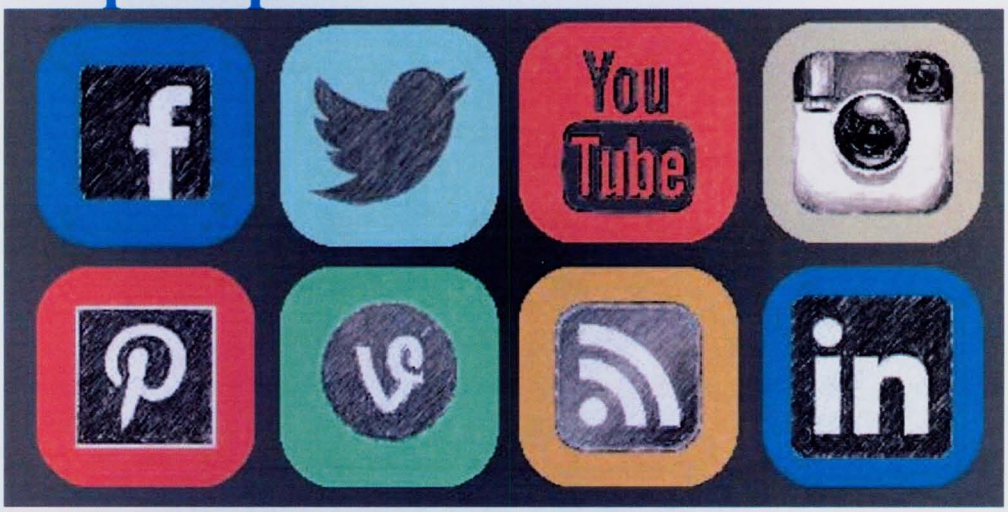
Muchos juegos en línea tienen funciones de comunicación que permiten a los usuarios interactuar de forma anónima. Algunas personas pueden aprovecharse de este anonimato para acercarse a los niños. Por ejemplo, los predadores pueden enviar contenido inapropiado o usar las funciones de comunicación del juego para concertar encuentros en persona. Los hostigadores cibernéticos pueden acosar a los demás jugadores y los estafadores en línea pueden prometer regalos virtuales para intentar obtener la información de la tarjeta de crédito. ¿Queres saber mas?, te recomendamos visitar este sitio http://es.netsmartz.org/Gaming [41]

A6. Empleo de afiches mensuales con recomendaciones de seguridad de la información.

A continuación, se detallan algunos ejemplos de los posters a utilizar para redes sociales, claves de acceso y phishing.

1)

Tú paso por



Es igual que un tatuaje (PERMANENTE!!)

[42]

2)

Cuidado con lo publiques
en las redes sociales!
Piensa como se pueden unir estos datos y hacerte
vulnerable y víctima de un ciberdelito

[42]

3)

Tú clave debería ser única

como VOS!

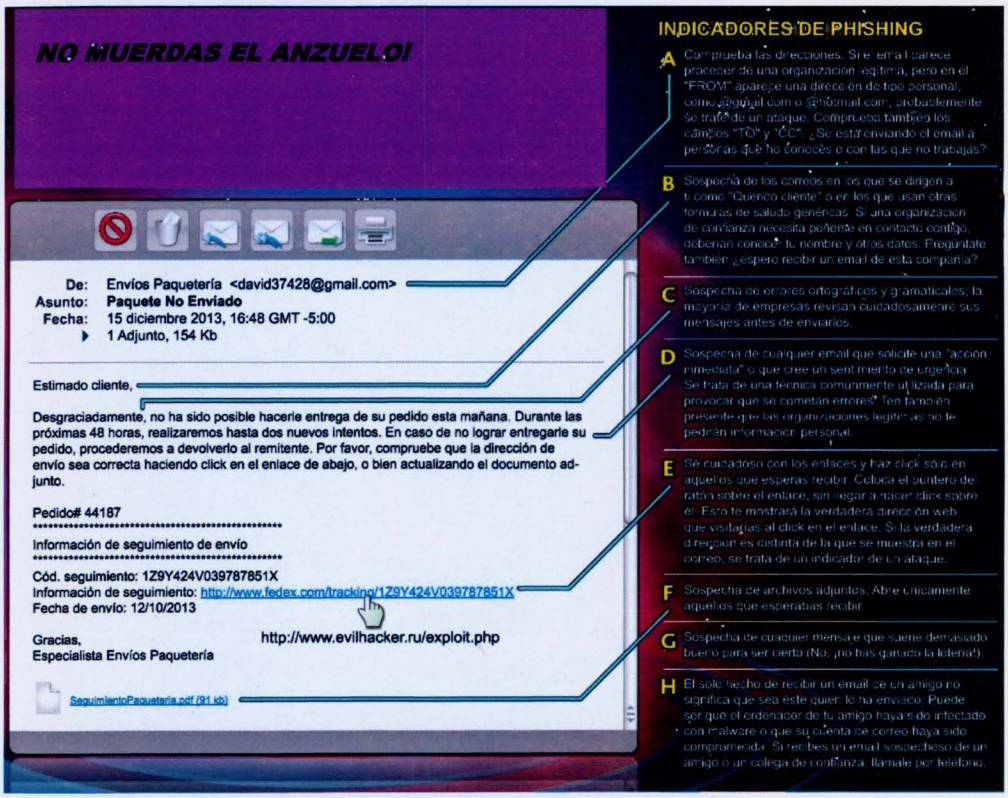
[43]

4)

Las claves son como los chicles
no se comparten
son fuertes cuando son frescas
y si las dejas por allí pueden
volverse un lío pegasoso

[44]

5)


NO MUERDAS EL ANZUELO!
De: Envíos Paquetería <david37428@gmail.com>
Asunto: Paquete No Enviado
Fecha: 15 diciembre 2013, 16:48 GMT -5:00
1 Adjunto, 154 Kb
Estimado cliente,
Desgraciadamente, no ha sido posible hacerle entrega de su pedido esta mañana. Durante las próximas 48 horas, realizaremos hasta dos nuevos intentos. En caso de no lograr entregarle su pedido, procederemos a devolverlo al remitente. Por favor, compruebe que la dirección de envío sea correcta haciendo click en el enlace de abajo, o bien actualizando el documento adjunto.
Pedido# 44187
Información de seguimiento de envío
Cód. seguimiento: 1Z9Y424V039787851X
Información de seguimiento: http://www.fedex.com/tracking/1Z9Y424V039787851X
Fecha de envío: 12/10/2013
Gracias,
Especialista Envíos Paquetería
http://www.evilhacker.ru/exploit.php
SeguimientoPaquete.pdf (91 kb)
INDICADORES DE PHISHING
A Comprueba las direcciones. Si el email parece proceder de una organización legítima, pero en el "FROM" aparece una dirección de tipo personal, como @gmail.com o @hotmail.com, probablemente se trate de un ataque. Comprueba también los campos "TO" y "CC". ¿Se está enviando el email a personas que no conoces o con las que no trabajas?
B Sospecha de los correos en los que se dirigen a ti como "Querido cliente" o en los que usan otras formulas de saludo genéricas. Si una organización de confianza necesita ponerse en contacto contigo, deberían conocer tu nombre y otros datos. Pregúntate también ¿espero recibir un email de esta compañía?
C Sospecha de errores ortográficos y gramaticales. La mayoría de empresas revisan cuidadosamente sus mensajes antes de enviarlos.
D Sospecha de cualquier email que solicite una "acción inmediata" o que cree un sentimiento de urgencia. Se trata de una técnica comunmente utilizada para provocar que se cometan errores. Ten también presente que las organizaciones legítimas no te pedirán información personal.
E Sé cuidadoso con los enlaces y haz click sólo en aquellos que esperas recibir. Coloca el puntero del ratón sobre el enlace, sin llegar a hacer click sobre él. Esto te mostrará la verdadera dirección web que visitarías al click en el enlace. Si la verdadera dirección es distinta de la que se muestra en el correo, se trata de un indicador de un ataque.
F Sospecha de archivos adjuntos. Abre únicamente aquellos que esperabas recibir.
G Sospecha de cualquier mensaje que suene demasiado bueno para ser cierto (No, ¡no has ganado la lotería!).
H El solo hecho de recibir un email de un amigo no significa que sea éste quien lo ha enviado. Puede ser que el ordenador de tu amigo haya sido infectado con malware o que su cuenta de correo haya sido comprometida. Si recibes un email sospechoso de un amigo o un colega de confianza, llámale por teléfono.

[45]

A7. Videos de buenas prácticas de seguridad de la información.

Se generarán los siguientes videos con una modalidad de tutorial o con indicaciones paso a paso.

- Como realizar paso a paso la configuración segura de un teléfono inteligente con Android

- Como realizar paso a paso la configuración segura de un teléfono inteligente IPhone

- Como configurar paso a paso la privacidad de Facebook

- Como configurar paso a paso la privacidad de Twitter

- Como realizar paso a paso copias de seguridad y recuperación de información, según la tecnología implementada en la pyme

- Como analizar si un mail es sospechoso

A8. Consejos para padres sobre seguridad

Videos contenidos en el DVD

"6 niveles de información"

Resumen: Cinco adolescentes descubren cuánta información puede encontrar un investigador de Internet sobre ellos en línea. [46]

"La sorpresa de cumpleaños de Router"

Resumen: Clicky hace una fiesta para su buen amigo Router, el cachorro robot. Pero es difícil planear una fiesta cuando tienes que proteger al Internet de forajidos escurridizos y ayudar a sus amigos Nettie y Webster a lidiar con personas tramposas en la vida real. [47]

"¿Amigo o impostor?"

Resumen: El nuevo amigo virtual de Keyan quiere que se conozcan cara a cara, pero ¿es buena idea? ¡A Tad y Slick les parece que no! [48]

"Juegos"

Resumen: ¿Juegas? ¡Estos adolescentes sí! Escucha lo que tus compañeros tienen para decir sobre juegos en línea.[49]

Folleto

Consejos

Aprenda los aspectos básicos de la seguridad en el Internet

Los niños usan una amplia variedad de servicios en línea, y cada uno de estos servicios encierra sus propias preocupaciones. Sin embargo, existen algunos consejos básicos que puede emplear sin importar la forma cómo su hijo usa el Internet.

- Poner la computadora en un lugar muy transitado de su casa.
- Establecer límites respecto a los sitios en línea que sus hijos pueden visitar y de la duración de dichas visitas.
- Recordar que la tecnología del Internet puede ser móvil, y asegurarse de controlar teléfonos celulares, dispositivos para juegos y computadoras portátiles.
- Navegar en el Internet con su hijo y permitir que le muestre lo que le gusta hacer cuando está en línea.
- Saber con quién se está conectando su hijo en línea y establecer normas sobre sitios de redes sociales, mensajes instantáneos, correos electrónicos, juegos en línea y el uso de cámaras web.
- Dialogue continuamente con su hijo acerca de la seguridad en línea.

Inicio de Conversación

Inicie una conversación con su hijo

- ¿Cuáles son las cosas que más te gusta hacer en línea?
- ¿Qué es la información personal? ¿Por qué deberías mantenerla en privado?
- ¿Qué podrías hacer para estar más seguro en línea?
- ¿Qué harías si alguien en línea te propusiera encontrarse cara a cara contigo?
- Además de mí, ¿con quién sientes que podrías hablar si te encontraras en una situación atemorizadora o incómoda?

[50]

Consejos

Ayude a prevenir la victimización de menores

Mucha gente supone que los niños que corren riesgo de ser víctimas son aquellos descuidados por sus hogares o que provienen de familias disfuncionales. Sin embargo, todos los niños, incluso aquellos provenientes de familias que les brindan apoyo, pueden correr el riesgo de ser victimizados. Aliente a su hijo a que acuda a usted inmediatamente si alguien lo hace sentir incómodo en línea o si intenta encontrarse con él personalmente.

Señales que indican que es posible que un predador en línea esté en contacto con su hijo

- Su hijo comienza a retraerse y aislarse de su familia y amigos.
- Encuentra material inapropiado en la computadora.
- Su hijo recibe correspondencia, dinero o regalos de desconocidos.
- Observa números de teléfonos desconocidos al revisar la factura.

Qué hacer si su hijo es victimizado

- Tenga en claro que la victimización no es culpa de su hijo/a.
- Guarde toda evidencia de victimización, tales como correos electrónicos o conversaciones por medio de mensajes instantáneos.
- Comuníquese con la policía local.

Inicio de Conversación

Inicie una conversación con su hijo

- ¿Con quién hablas usualmente en línea?
- ¿Confías en la gente que conoces en línea? ¿Por qué sí o por qué no?
- ¿Qué podría pasar si conoces personalmente a alguien que sólo conoces en línea?
- ¿Alguna vez has conocido a alguien en línea que te haya ofrecido regalos?
- ¿Con quién hablas cuando tienes un problema? ¿Te sientes cómodo hablando conmigo?

Consejos

Ayude a sus hijos a usar los sitios de redes sociales de forma segura

Los sitios de redes sociales pueden brindar muchos beneficios a los niños, como por ejemplo, permitirles explorar nuevos intereses. Ayude a sus hijos a usarlos de manera más segura repasando los siguientes consejos y temas para iniciar una conversación.

- Verifique la lista de amigos de su hijo para ver quién tiene acceso a su perfil. Asegúrese de que su hijo conozca a todos sus amigos personalmente.
- Enséñele a su hijo a configurar sus perfiles como privados, pero tenga en cuenta que la configuración de privacidad no garantiza una privacidad total.
- Haga que su hijo retire fotografías y contenidos inapropiados, y elimine cualquier tipo de información personal.
- Verifique los perfiles de los amigos de sus hijos para ver si contienen información reveladora o fotografías de sus hijos.
- Denuncie los comportamientos inapropiados o delictivos a la autoridad correspondiente. La mayoría de los sitios cuentan con mecanismos para denunciar comportamientos no delictivos. Los comportamientos delictivos deben denunciarse ante las autoridades

Inicio de Conversación

Inicie una conversación con su hijo

Use estos temas para iniciar una conversación sobre seguridad en el Internet con sus hijos. Cuanto más les hable sobre seguridad en línea, más fácil será. Por lo tanto, ¡no se desanime si no responden inmediatamente!

- ¿Podrías mostrarme tu(s) perfil(es) en línea?
- ¿Usas tu nombre o tu edad real cuando te comunicas con otras personas en línea?
- ¿Qué clase de cosas publicas en tu página?
- ¿Cómo decides a quién agregar como amigo?
- ¿Te sentirías cómodo si yo verificara tu perfil?

[52]

A9. Concurso del día de seguridad

Correo electrónico a enviar al personal para el concurso del día de seguridad a enviar en la primera semana de noviembre.

Asunto: ¡Gánate un pendrive!

¿Qué tenes que hacer?

Postea una foto a nuestro facebook contándonos que es la seguridad para vos.

¿Cuándo puedo postear la foto?

A partir del 6/11/2017

¿Hasta cuándo puedo hacerlo?

Hasta el 30/11/2017

¿Cómo se define al ganador?

El ganador será el que posteo la foto que obtenga mayor cantidad de votos ("Me gusta"). En caso de empate se realizará un sorteo entre aquellos que obtengan mayor cantidad de votos.

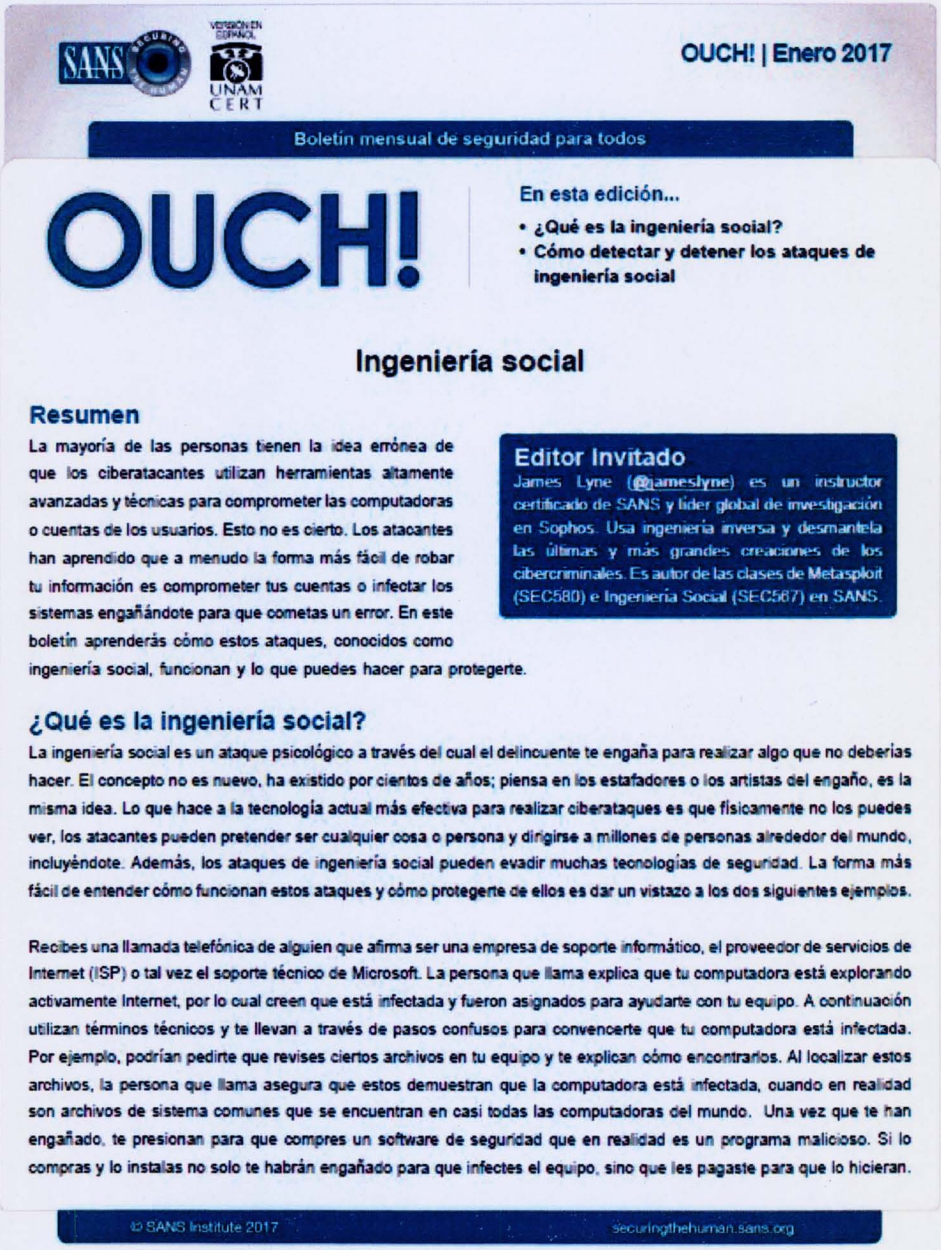
El director de la pyme entregará el premio al ganador el 1/12/2017

Te recordamos que solo pueden participar los empleados de la pyme, ya sea posteando una foto y/o votando por una foto.

A10. Boletín mensual de seguridad

A continuación, se presentan ejemplos de algunos boletines de seguridad a distribuir por correo electrónico sobre ingeniería social y ransomware. Se acota que la principal fuente de información es el material publicado por el instituto SANS.

1)



OUCH! | Enero 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- ¿Qué es la ingeniería social?
- Cómo detectar y detener los ataques de ingeniería social

Ingeniería social

Resumen

La mayoría de las personas tienen la idea errónea de que los ciberatacantes utilizan herramientas altamente avanzadas y técnicas para comprometer las computadoras o cuentas de los usuarios. Esto no es cierto. Los atacantes han aprendido que a menudo la forma más fácil de robar tu información es comprometer tus cuentas o infectar los sistemas engañándote para que cometas un error. En este boletín aprenderás cómo estos ataques, conocidos como ingeniería social, funcionan y lo que puedes hacer para protegerte.

Editor Invitado

James Lyne (@jameslyne) es un instructor certificado de SANS y líder global de investigación en Sophos. Usa ingeniería inversa y desmantela las últimas y más grandes creaciones de los cibercriminales. Es autor de las clases de Metasploit (SEC580) e Ingeniería Social (SEC567) en SANS.

¿Qué es la ingeniería social?

La ingeniería social es un ataque psicológico a través del cual el delincuente te engaña para realizar algo que no deberías hacer. El concepto no es nuevo, ha existido por cientos de años; piensa en los estafadores o los artistas del engaño, es la misma idea. Lo que hace a la tecnología actual más efectiva para realizar ciberataques es que físicamente no los puedes ver, los atacantes pueden pretender ser cualquier cosa o persona y dirigirse a millones de personas alrededor del mundo, incluyéndote. Además, los ataques de ingeniería social pueden evadir muchas tecnologías de seguridad. La forma más fácil de entender cómo funcionan estos ataques y cómo protegerte de ellos es dar un vistazo a los dos siguientes ejemplos.

Recibes una llamada telefónica de alguien que afirma ser una empresa de soporte informático, el proveedor de servicios de Internet (ISP) o tal vez el soporte técnico de Microsoft. La persona que llama explica que tu computadora está explorando activamente Internet, por lo cual creen que está infectada y fueron asignados para ayudarte con tu equipo. A continuación utilizan términos técnicos y te llevan a través de pasos confusos para convencerte que tu computadora está infectada. Por ejemplo, podrían pedirte que revises ciertos archivos en tu equipo y te explican cómo encontrarlos. Al localizar estos archivos, la persona que llama asegura que estos demuestran que la computadora está infectada, cuando en realidad son archivos de sistema comunes que se encuentran en casi todas las computadoras del mundo. Una vez que te han engañado, te presionan para que compres un software de seguridad que en realidad es un programa malicioso. Si lo compras y lo instalas no solo te habrán engañado para que infectes el equipo, sino que les pagaste para que lo hicieran.

© SANS Institute 2017 securingthehuman.sans.org

Ingeniería social

Si les das acceso remoto a tu computadora, van a tomar control de ella y robar tu información o usarla en sus pujas.

El sentido común es tu defensa más poderosa para identificar y detener la mayoría de los ataques de ingeniería social.

Otro ejemplo es el ataque por correo electrónico conocido como la estafa del CEO, que ocurre frecuentemente en el trabajo. Un ciberatacante investiga tu organización en línea e identifica el nombre de tu jefe o compañero de trabajo. El atacante redacta un correo pretendiendo ser la persona que eligió y te lo envía. El correo te pide con urgencia que realices una acción, como realizar una transferencia o enviar información sensible sobre un empleado. Muy a menudo estos correos pretenden que hay una emergencia que requiere que omitas los procedimientos de seguridad estándar, por ejemplo, te pueden pedir que envíes información altamente sensible a una cuenta @gmail.com personal. Lo que hace que los ataques dirigidos como este sean peligrosos es que los atacantes investigan de antemano a su víctima. Además, las tecnologías de seguridad como los antivirus y los firewall no pueden detectar o detener estos ataques porque no hay un malware o vínculo malicioso involucrado.

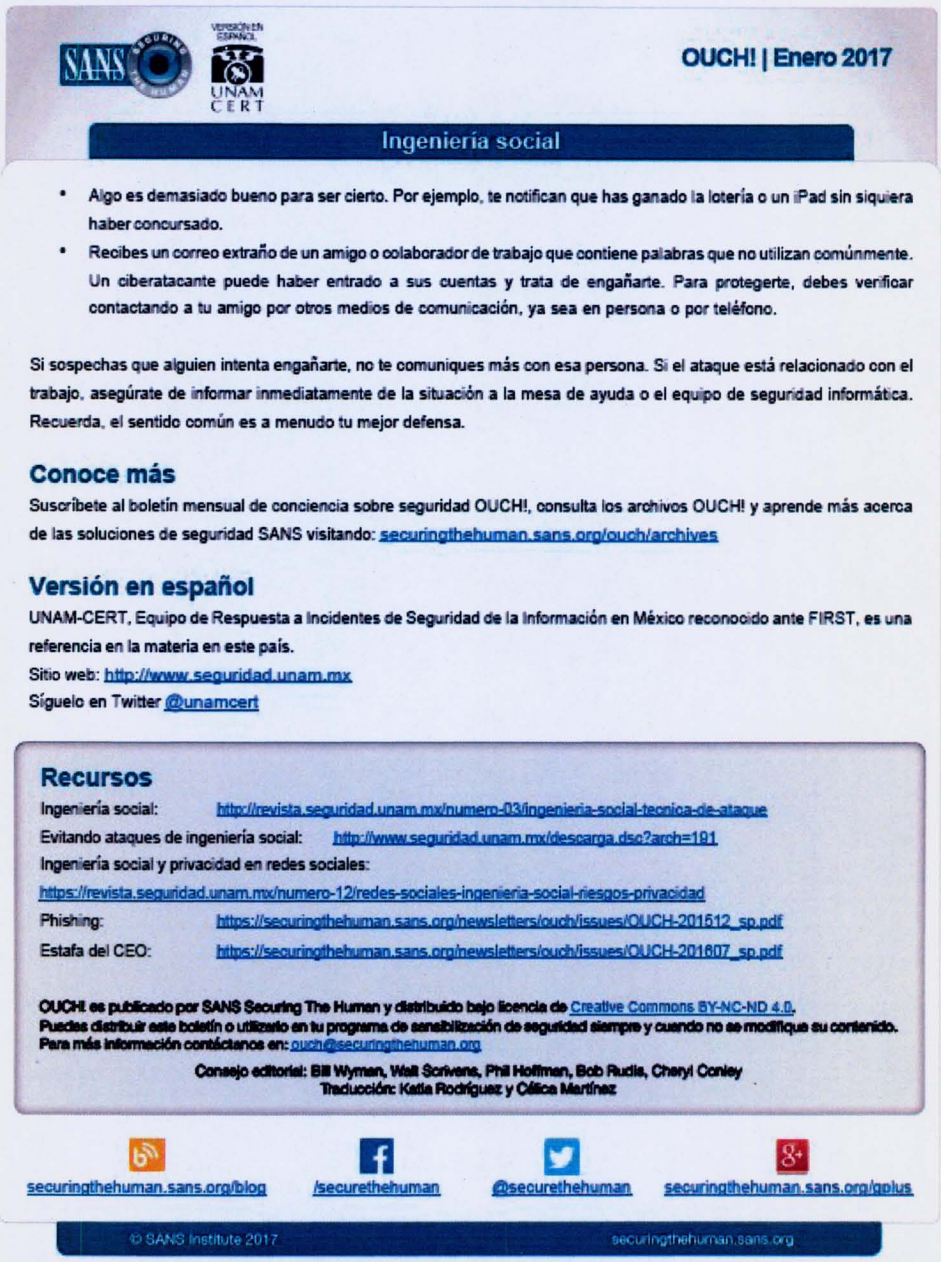
Ten en cuenta que los ataques de ingeniería social no se limitan a llamadas telefónicas o correos electrónicos; estos pueden presentarse en cualquier forma, a través de mensajes de texto a tu teléfono, en tus redes sociales o incluso en persona. La clave es saber qué proteger, tú eres tu mejor defensa.

Cómo detectar y detener ataques de ingeniería social

Afortunadamente detener este tipo de ataques es más sencillo de lo que podrías imaginar, el sentido común es tu mejor defensa. Si ves algo sospechoso o no te sientes bien haciéndolo, puede ser un ataque. Las pistas más comunes son:

- Alguien crea un tremendo sentido de urgencia, tratando de engañarte para que cometas un error.
- Alguien te pregunta por información a la cual no deberían tener acceso o que ya debería saber, como los números de tus cuentas.
- Alguien te solicita tu contraseña, ninguna organización legítima te pediría eso.
- Alguien te presiona para que evadas o ignores los procedimientos de seguridad o procedimientos que se espera sigas en tu trabajo.

© SANS Institute 2017



OUCH! | Enero 2017

Ingeniería social

- Algo es demasiado bueno para ser cierto. Por ejemplo, te notifican que has ganado la lotería o un iPad sin siquiera haber concursado.
- Recibes un correo extraño de un amigo o colaborador de trabajo que contiene palabras que no utilizan comúnmente. Un ciberatacante puede haber entrado a sus cuentas y trata de engañarte. Para protegerte, debes verificar contactando a tu amigo por otros medios de comunicación, ya sea en persona o por teléfono.

Si sospechas que alguien intenta engañarte, no te comuniques más con esa persona. Si el ataque está relacionado con el trabajo, asegúrate de informar inmediatamente de la situación a la mesa de ayuda o el equipo de seguridad informática. Recuerda, el sentido común es a menudo tu mejor defensa.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: securingthehuman.sans.org/ouch/archives

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

Recursos

Ingeniería social: http://revista.seguridad.unam.mx/numero-03/ingenieria-social-tecnica-de-ataque

Evitando ataques de ingeniería social: http://www.seguridad.unam.mx/descarga.dsc?arch=191

Ingeniería social y privacidad en redes sociales:
https://revista.seguridad.unam.mx/numero-12/redes-sociales-ingenieria-social-riesgos-privacidad

Phishing: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201612_sp.pdf

Estafa del CEO: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201607_sp.pdf

OUCH! es publicado por SANS Securing The Human y distribuido bajo licencia de Creative Commons BY-NC-ND 4.0.
Puedes distribuir este boletín o utilizarlo en tu programa de sensibilización de seguridad siempre y cuando no se modifique su contenido.
Para más información contáctanos en: ouch@securingthehuman.org

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: Katia Rodríguez y Célica Martínez

securingthehuman.sans.org/blog /securethehuman @securethehuman securingthehuman.sans.org/gplus

© SANS Institute 2017 securingthehuman.sans.org

2)

OUCH! | Agosto 2016

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- ¿Qué es el ransomware?
- ¿Deberías pagar el rescate?
- Respalda tus archivos
- Otras medias de protección

Ransomware

¿Qué es el ransomware?

El ransomware es un tipo especial de malware que amenaza con destruir los documentos y otros archivos de las víctimas; hoy en día se está propagando activamente a través de Internet. El malware es un software, un programa de computadora, utilizado para realizar acciones maliciosas. Si bien el ransomware es sólo uno de los diferentes tipos de malware, se ha vuelto muy común ya que es rentable para los criminales. Una vez que el ransomware infecta tu equipo, cifra ciertos archivos o incluso todo el disco duro. A continuación, bloquea todo el sistema o no te deja acceder a tus archivos importantes como documentos o fotografías. El malware te informa que la única forma en que puedes descifrar tus archivos y recuperar el sistema es pagar al cibercriminal un rescate (ransom en inglés, de ahí que se llame ransomware), el cual se debe pagar a través de alguna moneda digital como Bitcoin. El ransomware se propaga como otros tipos de malware; el método más común involucra el envío de correos electrónicos maliciosos a las víctimas, los cibercriminales te engañan para que abras un archivo adjunto infectado o hagas clic en un vínculo que te lleva al sitio web del atacante.

Editor Invitado

Lenny Zeltser se encarga de salvaguardar las operaciones de los clientes de TI en NCR Corp y enseña a combatir el malware en el Instituto SANS. Puedes encontrar a Lenny en Twitter como @lennyzeltser y en su blog de seguridad zeltser.com.

¿Deberías pagar el rescate?

Es una pregunta difícil de contestar. El problema es que cada vez más gente paga cuando son infectados, esto motiva a los criminales para que infecten a otros; sin embargo, es posible que no exista otra opción para recuperar tus archivos. No obstante, advertimos que incluso si pagas el rescate no hay garantía que obtengas los archivos de nuevo. Estás tratando con delincuentes que pueden no descifrar los archivos o inclusive si te proporcionan un método para descifrarlos a cambio de un pago, algo puede ir mal durante el proceso o tu computadora puede ser infectada con malware adicional.

Respalda tus archivos

Tal vez la mejor forma de recuperarte de una infección de ransomware y no pagar por un rescate es recuperar tus archivos a través de copias de seguridad. De esta forma, aunque te infectes con ransomware, tendrás una manera de recuperar los

© SANS Institute 2016

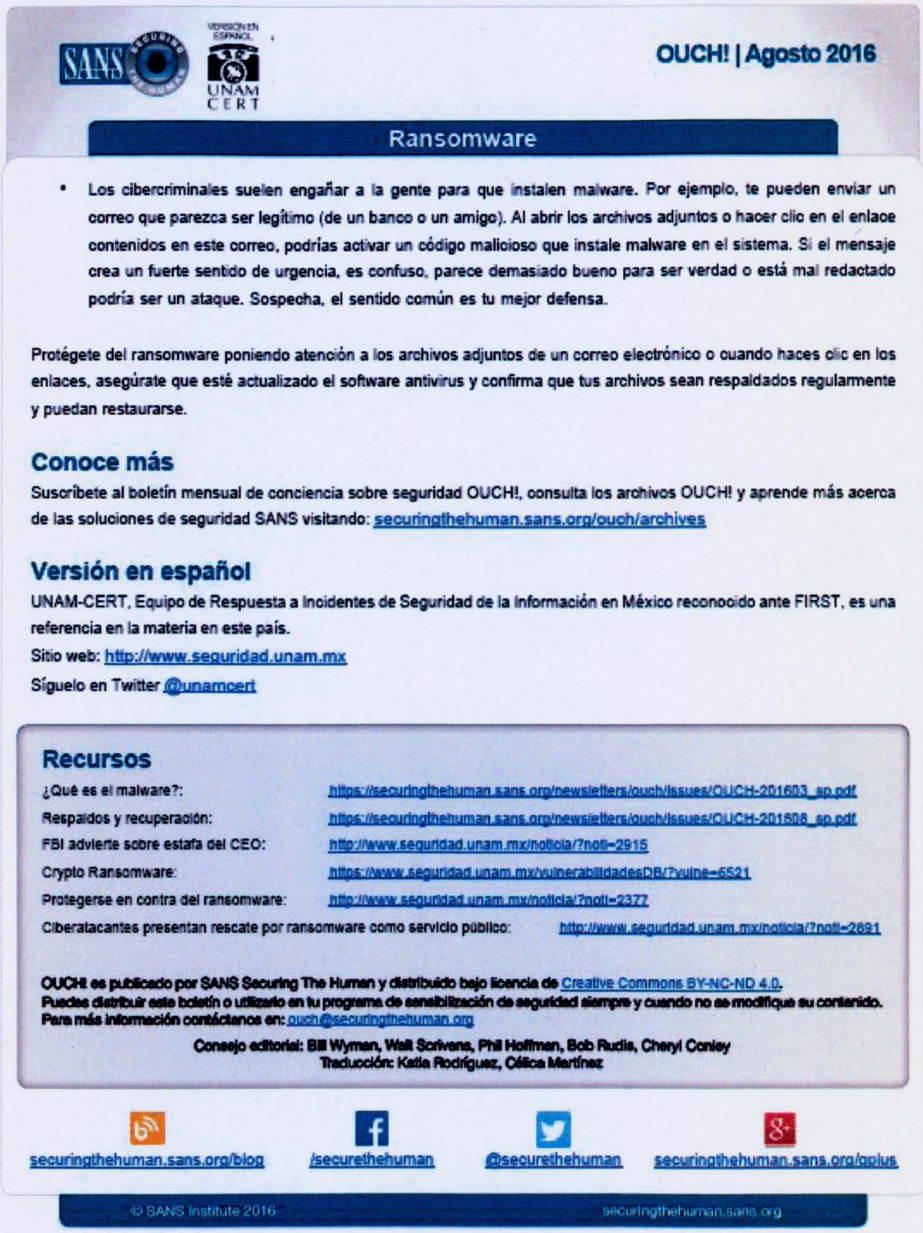
archivos antes de reconstruir o limpiar tu computadora. Ten en cuenta que si accedes a tu copia de seguridad desde el sistema infectado, el ransomware podría borrar o cifrar tus archivos de respaldo. Por lo tanto, es importante que respaldes los archivos en servicios en la nube de buena reputación o los almacenes en discos duros externos que no siempre estén conectados a tu sistema. Un error común es que la gente asume que las copias de seguridad funcionan sin probar si efectivamente se pueden recuperar los archivos; asegúrate de realizar pruebas regulares para verificar que las copias de seguridad funcionen y puedas recuperar los archivos que necesites en caso de que el sistema sea infectado con ransomware. Las copias de respaldo son importantes ya que te pueden ayudar a recuperar tus archivos si accidentalmente los borras o en el caso que tu disco duro falle.

El ransomware es un malware que, una vez que infecta tu computadora, cifra todos los archivos y te niega el acceso a ellos.

Otras medidas de protección

Puedes protegerte del ransomware de la misma forma que lo haces contra otro tipo de malware: no infectarte. Asegúrate de tener un software antivirus actualizado de un proveedor de confianza. Dichas herramientas, algunas veces llamadas software antimalware, están diseñadas para detectar y detener el malware. Sin embargo, un antivirus no puede bloquear o eliminar todos los programas maliciosos. Los ciberdelincuentes están constantemente innovando, desarrollando nuevo y más sofisticado malware que evada la detección. A su vez, los proveedores de antivirus están actualizando sus productos con nuevas capacidades para detectar malware. En muchos sentidos se ha convertido en una carrera armamentista pues ambas partes tratan de burlar al otro. Desafortunadamente los criminales están un paso adelante, por lo que debes asegurar las copias de respaldo de tus archivos e implementar estas medidas:

- Los delincuentes a menudo infectan computadoras o dispositivos explotando las vulnerabilidades en el software. Entre más actual sea tu software, menos vulnerabilidades tendrá el sistema y será más difícil infectarlo. Por lo tanto, asegúrate que los sistemas operativos, aplicaciones y dispositivos tengan habilitados la instalación de actualizaciones de forma automática.
- En las computadoras utiliza una cuenta estándar que tenga privilegios limitados, en lugar de las cuentas con privilegios de "administrador" o "raíz". Esto proporciona una protección adicional al prevenir que se instalen distintos tipos de malware.



OUCH! | Agosto 2016

Ransomware

- Los cibercriminales suelen engañar a la gente para que instalen malware. Por ejemplo, te pueden enviar un correo que parezca ser legítimo (de un banco o un amigo). Al abrir los archivos adjuntos o hacer clic en el enlace contenidos en este correo, podrías activar un código malicioso que instale malware en el sistema. Si el mensaje crea un fuerte sentido de urgencia, es confuso, parece demasiado bueno para ser verdad o está mal redactado podría ser un ataque. Sospecha, el sentido común es tu mejor defensa.

Protégete del ransomware poniendo atención a los archivos adjuntos de un correo electrónico o cuando haces clic en los enlaces, asegúrate que esté actualizado el software antivirus y confirma que tus archivos sean respaldados regularmente y puedan restaurarse.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: securingthehuman.sans.org/ouch/archives

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

Recursos

¿Qué es el malware?:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_sp.pdf
Respaldos y recuperación:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_sp.pdf
FBI advierte sobre estafa del CEO:	http://www.seguridad.unam.mx/noticia/?noti=2915
Crypto Ransomware:	https://www.seguridad.unam.mx/vulnerabilidadesDB/?vulns=6521
Protegerse en contra del ransomware:	http://www.seguridad.unam.mx/noticia/?noti=2377
Ciberatacantes presentan rescate por ransomware como servicio público:	http://www.seguridad.unam.mx/noticia/?noti=2691

OUCH! es publicado por SANS Securing The Human y distribuido bajo licencia de Creative Commons BY-NC-ND 4.0.
Puedes distribuir este boletín o utilizarlo en tu programa de sensibilización de seguridad siempre y cuando no se modifique su contenido.
Para más información contáctanos en: ouch@securingthehuman.org

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: Katia Rodríguez, Célica Martínez

securingthehuman.sans.org/blog /securethehuman @securethehuman securingthehuman.sans.org/gplus

© SANS Institute 2016 securingthehuman.sans.org

[53]

[54]

Bibliografía

[1] Diccionario de la lengua española | Edición del Tricentenario http://dle.rae.es/?id=A8mrPcH (consultada el 13/5/2016)

[2] Building An Information Technology Security Awareness and Training Program
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf (consultada el 6/12/2016)

[3] ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), Information technology — Security techniques — Code of practice for information security controls, ISO copyright, Geneve, 2013

[4] Enterprise Survival Guide for Ransomware Attacks
https://www.sans.org/reading-room/whitepapers/malicious/enterprise-survival-guide-ransomware-attacks-36962
(consultada el 26/6/2016)

[5] University of Calgary paid $20K in ransomware attack
http://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979
(consultada el 22/6/2016)

[6] Kansas Heart Hospital hit with ransomware; attackers demand two ransoms
http://www.networkworld.com/article/3073495/security/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html
(Consultada el 22/6/2016)

[7] Us Police Pay Ransomware Hackers
http://www.fraudhelpdesk.org/us-police-pay-ransomware-hackers/
(Consultada el 22/6/2016)

[8] By The Numbers: Ransomware Rising
http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/by-the-numbers-ransomware-rising
(Consultada el 22/6/2016)

[9] ISACA, Cobit 5 para Seguridad de la Información, ISACA copyright, Estados Unidos de América, 2012

[10] Jefatura de Gabinete de Ministros - Secretaría de Gabinete y Coordinación Administrativa - Subsecretaría de Tecnologías de Gestión - Oficina Nacional de Tecnologías de Información, Disposición 1/2015 "Política de Seguridad de la Información Modelo", Argentina, 2015

[11] Banco Central de la República Argentina, Normas sobre "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras", Argentina, 2012

[12] Perry Carpenter, Kristen Noakes-Fry, Andrew Walls, How to Build an Enterprise Security Awareness Program, Gartner Inc, Estados Unidos de América. 2008

[13] Herald, Rebecca, Managing an Information Security and Privacy Awareness and Training Program, CRC Press Taylor & Francis Group, Estados Unidos de América, 2010

[14] Kristen Noakes-Fry, Perry Carpenter, Andrew Walls, Best Practices in Information Security Awareness Training, Gartner Inc, Estados Unidos de América, 2008

[15] La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información - Encuesta 2016 sobre Tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica
https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%C3%A9rica%20-%20Resultados%20Generales%20vf%20(Per%C3%BA).pdf
(Consultada el 26/10/2016)

[16] Eset Security Report Latinoamérica 2016
http://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf
(Consultada el 25/10/2016)

[17] Tendencias 2016 Encuesta nacional de seguridad informática
http://acis.org.co/revista139/content/tendencias-2016-encuesta-nacional-de-seguridad-inform%C3%A1tica

(Consultada el 21/10/2016)

[18] Cyber security survey: major australian businesses
https://www.cert.gov.au/system/files/614/691/2015-ACSC-Cyber-Security-Survey-Major-Australian-Businesses.pdf
(Consultada el 6/12/2016)

[19] State of Cybersecurity Implications for 2016 - An ISACA and RSA Conference Survey
http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf
(Consultada el 12/10/2016)

[20] Security Awareness Report - Awareness Is Hard: A Tale of Two Challenges
https://securingthehuman.sans.org/media/resources/STH-SecurityAwarenessReport-2016.pdf
(Consultada el 31/10/2016)

[21] Definición Pyme en la Argentina
www.abappra.com/documentos/definicion_PyME_Argentina.doc
(Consultada el 13/12/2016)

[22] Top Human Risks
https://securingthehuman.sans.org/media/resources/presentations/STH-TopSevenHumanRisks.pdf
(Consultada el 10/1/2017)

[23] Qué es Lunch and Learn?
http://www.lafabricadevalor.com/web/lunchandlearn.php
(Consultada el 9/1/2017)

[24] Human metrics
https://files.sans.org/summit/cyberdefense2014/PDFs/Security%20Awareness%20Metrics%20-%20Measuring%20Human%20Behavior%20-%20Lance%20Spitzner,%20SANS.pdf
(Consultada el 25/1/2017)

[25] Joanna G. Huisman, Perry Carpenter, 10 ways to improve security awareness on a tight budget, Gartner Inc, Estados Unidos de América. 2016

[26] Ilustración del Vector: Nuevo inicio del proyecto del negocio

https://es.dreamstime.com/fotografa-de-archivo-nuevo-inicio-del-proyecto-del-negocio-image40422512
(consultada el 16/2/2017)

[27] NO te olvides del desayuno!
http://www.paraserbella.com/2017/01/no-te-olvides-del-desayuno/
(consultada el 16/2/2017)

[28] Seguridad Informática
http://seguridadinformaticagbi21.blogspot.com.ar/2015/09/definicion-de-seguridad-informatica.html
(consultada el 17/2/2017)

[29] Ce.S.P.I-Universidad Nacional de La Plata, Concientización en Seguridad de la Información, Buenos Aires, Argentina, 2008

[30] Ransomware
https://www.avast.com/es-es/c-ransomware
(consultada el 10/3/2017)

[31] Number of smartphone users in Argentina from 2015 to 2021 (in millions)
https://www.statista.com/statistics/285600/number-of-smartphone-users-in-argentina/
(consultada el 10/3/2017)

[32] Cristián Borghello, Usa tú teléfono inteligente con seguridad, Buenos Aires, Argentina, 2015.

[33] Este es un mapa de las redes sociales más utilizadas en el mundo
http://socialgeek.co/redes-sociales/este-es-mapa-redes-sociales-mas-utilizadas-mundo/
(consultada el 14/3/2017)

[34] Taller de cómputo
https://s-media-cache-ak0.pinimg.com/736x/34/51/ef/3451ef71c4c36c940d7b0fa804686185.jpg
(consultada el 9/2/2017)

[35] Seguridad en redes de telecomunicaciones e informática
https://exopus.files.wordpress.com/2008/12/hackers-y-dios.jpg?w=450&h=502
(consultada el 9/2/2017)

[36] 4.1 ¿Cómo proteger tu privacidad en las redes sociales?

http://canaltic.com/internetseguro/manual/41_cmo_proteger_tu_privacidad_en_las_redes_sociales.html
(consultada el 2/3/2017)

[37] Teléfonos celulares
http://es.netsmartz.org/CellPhones
(consultada el 2/3/2017)

[38] Safer internet day
https://www.saferinternetday.org/documents/167278/1512147/SID2017_pdf.pdf/9486b408-1540-4236-bc1b-7387dd167bc6
(consultada el 2/3/2017)

[39] Día internacional de la protección de datos personales.
http://www.jus.gob.ar/datos-personales/comunicados/2017/01/28/dia-internacional-de-la-proteccion-de-datos-personales.aspx
(consultada el 2/3/2017)

[40] Se emitieron los primeros programas realizados por el Ministerio Público Fiscal y Canal Encuentro
http://www.fiscales.gob.ar/genero/se-emitieron-los-primeros-programas-realizados-por-el-ministerio-publico-fiscal-y-canal-encuentro/
(consultada el 2/3/2017)

[41] Juegos
http://es.netsmartz.org/Gaming
(consultada el 2/3/2017)

[42] FISSEA Security Awareness training, education Contest
http://csrc.nist.gov/organizations/fissea/2016-conference/contest_winners/FISSEA_2016_ATE_contest_winners_all.pdf
(consultada el 3/2/2017)

[43] Contest Winners for 2014: Poster Winner
http://csrc.nist.gov/organizations/fissea/2014-conference/contest_winners/fissea_2014_dos_poster_contest_winner_alexis_benjamin.pdf
(consultada el 3/2/2017)

[44] Contest Winners for 2013: Poster Winner
http://csrc.nist.gov/organizations/fissea/2013-conference/contest_winners/fissea_2013_contest_winner_poster.pdf

(consultada el 3/2/2017)
[45] No muerdas el anzuelo!
file:///C:/Users/I10334/AppData/Local/Temp/Temp1_STH-Poster-DontGetHooked-Spanish.zip/STH-Poster-DontGetHooked-Spanish.pdf
(consultada el 20/2/2017)
[46] 6 niveles de información
http://es.netsmartz.org/RealLifeStories/6DegreesOfInformation
(consultada el 13/2/2017)
[47] La sorpresa de cumpleaños de Router
http://es.netsmartz.org/NetSmartzKids/RBS
(consultada el 13/2/2017)
[48] ¿Amigo o impostor?
http://es.netsmartz.org/NSTeens/FriendOrFake
(consultada el 13/2/2017)
[49]Juegos
http://es.netsmartz.org/TeensTalkBack/Gaming
(consultada el 13/2/2017)
[50] Seguridad en la internet básica
http://es.netsmartz.org/InternetSafety
(consultada el 15/2/2017)
[51] Niños como víctimas
http://es.netsmartz.org/ChildrenAsVictims
(consultada el 15/2/2017)
[52] Redes Sociales
http://es.netsmartz.org/SocialMedia
(consultada el 15/2/2017)
[53] Ouch! Ingenieria Social
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201701_sp.pdf
(consultada el 20/2/2017)
[54] Ouch! Ransomware
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_sp.pdf
(consultada el 20/2/2017)