$\mathcal{DIFU}_{100}ci@$
Revista de Difusión Científica, Ingeniería y Tecnologías
Vol. 15, No. 3, Septiembre - Diciembre 2021
ISSN:2007-3585
Artículo arbitrado
Publicado: 31 de diciembre de 2021

Analysis of Information Security Culture. A case of study: Leon, Guanajuato, Mexico

Análisis de Cultura de Seguridad Informática. Caso de Estudio: León, Guanajuato, México

Luis C. Villaverde-Hidalgo[1], **José L. Cabrera-Guzmán**[1], **Jorge R. Parra-Michel**[2], **Sandra A. Olivares-Bautista**[3], **Alberto Ochoa-Brust**[4], **Walter Mata**[4], **Leobardo A. Ceja-Bravo**[5], and **Rafael Martínez-Peláez**[*1]

[1] *Universidad De La Salle Bajío (UDLSB), Facultad de Tecnologías de Información,*
Av. Universidad 602, Col. Lomas del Campestre, León, Gto., México, 37150.
{lvh57920, jcg57968}@udelasalle.edu.mx, rmartinezp@delasalle.edu.mx
[2] *Universidad De La Salle Bajío (UDLSB), Facultad de Ingenierías,*
Av. Universidad 602, Col. Lomas del Campestre, León, Gto., México, 37150.
jrparra@delasalle.edu.mx
[3] *Instituto Tecnológico José Mario Molina Pasquel y Henríquez, Unidad Académica Lagos de Moreno,*
Libramiento Tecnológico 5000, Col. Portugalejo de los Romanes, Lagos de Moreno, Jal., México, 47480.
sandra.olivares@lagos.tecmn.edu.mx
[4] *Universidad de Colima (UCOL), Facultad de Ingeniería Mecánica y Eléctrica,*
Carretera Colima-Coquimatlán Km9, Coquimatrlán, Colima, México, 28400.
{aochoa, wmata}@ucol.mx
[5] *Universidad De La Salle Bajío (UDLSB), Facultad de Diseño,*
Av. Universidad 602, Col. Lomas del Campestre, León, Gto., México, 37150.
laceja@delasalle.edu.mx

Abstract

In the last years, the number of cyberattacks has increased, and the creation of malware every day represents new challenges. Against this situation, IT (Information Technology) professionals and senior management continue to invest large sums of money in purchasing hardware and software as the main tools to reduce security breaches; however, awareness campaigns and training on computer security among employees at all levels. Consequently, and with the results of the present study, it is evident that the main safety risk, the human factor, is not addressed. Our results corroborate previous studies, and the results show the lack of a culture of information security in organizations. Moreover, many companies do not have a computer security department.

Keywords— Cyber-attacks, culture, human factor, reputation, information security.

Resumen

En los últimos años, el número de ciberataques se ha incrementado, y la creación de malware cada día representa nuevos desafíos. Ante este panorama, los profesionales de TI (Tecnologías de Información) y la alta dirección continúan invirtiendo fuertes sumas de dinero en la adquisición de hardware y software como principales herramientas para reducir brechas de seguridad; sin embargo, se deja de lado las campañas de concientización y capacitación sobre seg. informática entre los colaboradores de todos los niveles. En consecuencia, y con los resultados del presente estudio, se evidencia que no se atiende el principal riesgo a la seguridad, el factor humano. Los resultados corroboran estudios previos y evidencian la falta de una cultura de seguridad informática en las orgs. Además, se detectó que varias empresas no cuentan con un depto. de seguridad informática.

Palabras clave— Ciberataques, cultura, factor humano, reputación, seguridad informática.

[*]Autor de correspondencia

I. Introducción

Los usuarios de tecnología frecuentemente no se comportan de forma segura cuando utilizan sus dispositivos tecnológicos, comparten información a través de redes sociales o hacen uso de sistemas informáticos. Esta falta de atención en la seguridad informática plantea serios problemas de seguridad tanto para la persona como para la empresa, colocando al usuario final como el eslabón más débil en la cadena de seguridad [1].

Varios informes sobre seguridad informática evidencian que gran parte de las brechas de seguridad e incidentes en materia de seguridad informática han sido causadas por incumplimiento de las políticas de seguridad [2], siendo el principal responsable el usuario final.

En [3, 4] presentan argumentos sobre la importancia de crear y fomentar una cultura de seguridad informática con la intención de cambiar actitudes, inculcar buenas prácticas, y modificar comportamientos riesgosos. A través de una cultura de seguridad informática se pueden reducir más riesgos de seguridad que invirtiendo e instalando equipos o programas de cómputo.

De acuerdo con [5], la seguridad informática se relaciona con el comportamiento de las personas en un contexto laboral para proteger la información a través del cumplimiento de las políticas de seguridad informática y una comprensión de cómo implementar los requerimientos de seguridad de una manera cautelosa y atenta, y la correcta implementación de iniciativas de educación, formación y sensibilización entre todos los miembros de la organización en materia de seguridad informática.

El objetivo general de la investigación fue: conocer la relevancia que tiene el tema de cultura de seguridad informática en organizaciones leonesas a través de un análisis cuantitativo e interpretación de los datos obtenidos para identificar áreas de oportunidad. El presente trabajo corrobora los resultados presentados en trabajos previos, permitiendo identificar la necesidad urgente de impulsar una cultura de seguridad informática entre los profesionales de TI y organizaciones en general.

La estructura del artículo es la siguiente: en la sección II, se presentan antecedentes del tema de investigación, entre los que se encuentran el error humano y principales medidas de seguridad contra incidentes. La sección III presenta la metodología utilizada para desarrollar el proyecto. En la sección IV, se describen los hallazgos más relevantes de la investigación. En la sección V se presenta una discusión sobre los resultados encontrados y su relación con trabajos previos. Finalmente, las conclusiones son presentadas en la sección VI.

II. Antecedentes

El desarrollo tecnológico – Internet, dispositivos móviles, satélites, minería de datos, negocios inteligentes, redes sociales, aplicaciones móviles, etc. – es clave para el crecimiento y desarrollo de las empresas, y en consecuencia, de la economía local y nacional [6]. Por lo tanto, en los últimos años, cada vez más organizaciones han aumentado la inversión en este rubro [7] con el objetivo de obtener ventajas competitivas, desarrollar nuevas estrategias de negocios, suministrar información sobre sus productos y servicios, establecer un canal de comunicación más personal e interactivo con sus clientes y usuarios para aumentar sus ingresos y crecimiento [7, 8].

En un mundo tan activo y globalizado, la tecnología se ha vuelto una necesidad para las empresas debido a que deben ser más eficientes, innovadoras y resolver problemáticas complejas en poco tiempo puesto que, se ha convertido en un promotor de cambios sociales, económicos y culturales [6, 8]. Por lo tanto, la tecnología mejora los procesos de las empresas y estos a su vez producen innovación, lo que hace que las empresas que no se suman a estas tecnologías se vayan quedando atrás [9].

En consecuencia, la tecnología ayuda a tener procesos más eficientes, aumentado la productividad, erradicando las barreras de comunicación entre cliente y empresa, y generando herramientas que ayudan a la toma de decisiones [6, 7, 9]. Sin embargo, en un mundo cada vez más conectado por redes públicas o privadas, y mayor dependencia de dispositivos electrónicos, usuarios mal intencionados utilizan su conocimiento para llevar a cabo acciones que afectan la seguridad y privacidad de los datos almacenados o transmitidos por empresas y personas físicas [10, 11, 12].

Los ciberdelincuentes buscan aprovechar el error humano. De acuerdo con [13], varios incidentes de seguridad informática que fueron analizados, se detectó que las limitaciones humanas fueron la causa principal. Los ciberataques fueron catalogados en software malicioso (Malware), phishing, filtración de datos, y ataques dirigidos donde algún usuario realizó una acción que desencadeno el ataque. Entre las acciones que suelen realizar los usuarios se encuentra dar click en un enlace, abrir un correo electrónico que estaba en la bandeja de spam, descargar y abrir un archivo, e insertar memorias USB en los equipos. Ante este escenario, se han realizado estudios sobre la importancia de crear una consciencia colectiva sobre temas de seguridad informática en las organizaciones públicas y privadas a través de campañas de concientización y capacitación, con la expectativa de crear una cultura de seguridad informática en toda la organización [14, 15].

La cultura es un conjunto de saberes, conocimientos

y pautas de conducta de un grupo social. Crear, fomentar y enseñar acerca de Seguridad Informática se debe convertir en una obligación para las organizaciones [16]; el desconocimiento es la principal fuente de accidentes, riesgos y amenazas. Una sola persona puede comprometer la información, recursos y reputación de toda la organización con un solo click.

II.1. El usuario final es el eslabón más débil

En la actualidad, y debido a la dependencia cada vez mayor de la información y de los sistemas de información en diferentes procesos de la organización, la alta dirección se encuentra ocupada por reducir amenazas de seguridad informática que puedan afectar sus intereses estratégicos. La consecuencia de ser víctimas de un ataque puede significar un fuerte impacto en la economía debido a los costos ocultos para corregir la brecha de seguridad [17]. Entre las consecuencias de un ataque, se encuentran la pérdida de propiedad intelectual, depreciación de la marca, y pérdida de contacto con el cliente, que van a requerir una alta inversión para recuperar la confianza del mercado; además, de los gastos necesarios para subsanar o recuperar la operatividad de la organización.

Ante este panorama es claro que vivimos en una era de virus, hackers, phishing, ciberespionaje, y fraudes por empleados, lo cual nos lleva a la importancia de generar una cultura de seguridad informática. Como se muestra en la Fig. 1, las amenazas de la seguridad de un sistema, son provenientes del mismo personal ya sea por ingeniería social, phishing, actividades maliciosas por empleados, falta de cultura de seguridad informática o carencia de información en este rubro; por lo cual, rara vez es tomado en cuenta este aspecto porque se supone que dentro de las empresas existe un ámbito de confianza que muchas veces es inexistente [18]. Generalmente como podemos observar, estos son accidentes por desconocimiento o inexistencia de políticas de seguridad; que inclusive pueden ser de tipo intencional.

II.2. Principales medidas de seguridad implementadas

En la Fig. 2, se presenta el resultado del reporte ESET Security 2016 de América Latina. Se puede apreciar claramente que, la principal medida de seguridad utilizada fue la adquisición e instalación de un programa antivirus, seguido de un firewall, y en tercer lugar los respaldos de información [19].

También se reafirma que el personal del departamento de TI invierte más en software y hardware para reducir o prevenir ataques [20]. En este punto, se espera que, con la adquisición de herramientas tecnológicas, los ataques se reduzcan; sin embargo, no se considera la

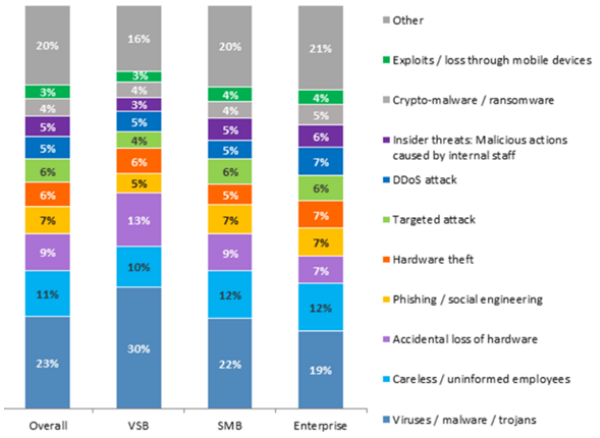

Figura 1: *Vectores de ataques más serios*
Fuente: https://www.kaspersky.com/blog/the-human-factor-in-it-security

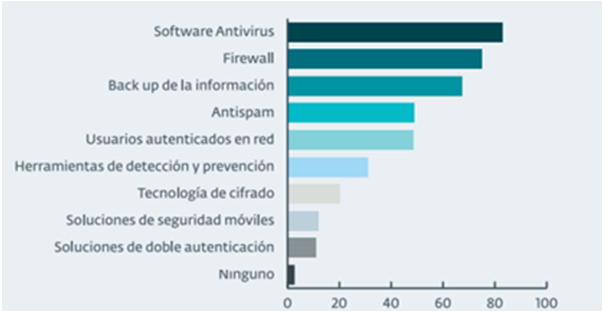

Figura 2: *Controles de seguridad más implementados en Latinoamérica*
Fuente: ESET Security Report Latinoamérica 2016

vulnerabilidad de los usuarios finales quienes, como se ha mencionado previamente, son una amenaza directa o indirecta para la seguridad informática de toda empresa.

Es interesante observar que, la solución de doble autenticación es la penúltima opción implementada en las empresas; esto debido a que un sistema de autenticación robusto puede ayudar a reducir intrusiones. En particular, una medida de doble autenticación requiere que el sistema solicite dos de los tres paradigmas de seguridad (algo que sabes, algo que tienes, y algo que eres).

II.3. Impacto a la reputación de la organización

En las empresas u organizaciones es fundamental que generen una reputación positiva hacia sus clientes o usuarios que utilizan sus servicios o productos, el objetivo es crear confianza por sus resultados para que así los clientes puedan afianzarse, lo que por ende genera la captación de nuevos clientes. La reputación de una empresa depende de la aceptación de los usuarios [21].

"Empresas del sector bancario, telecomunicaciones y

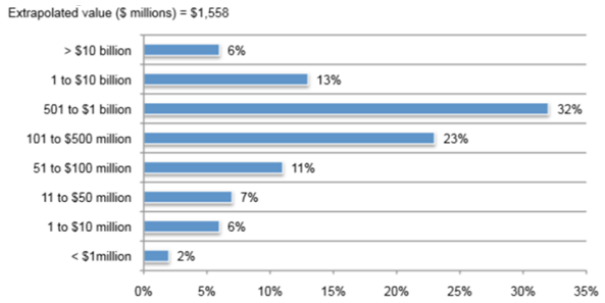

Figura 3: *Punto de equilibro entre costos, seguridad y riesgo Fuente: Reputation Impact of a Data Breach, Ponemon Institute*

retail o minoristas fueron atacadas en México por el ransomware que afectó el 12 de mayo del 2017 a más de 75 mil equipos de cómputo en todo el mundo, dijo Juan Pablo Castro, director de Innovación Tecnológica de Trend Micro".

En un ambiente donde los riesgos avanzan a gran velocidad como lo es Internet no existen soluciones de seguridad definitivas, por lo que todas las empresas, sin importar giro, tamaño o ubicación son susceptibles de recibir ataques informáticos ya sea por obtener un beneficio económico o por ego.

Una consecuencia muy grave a ser víctima de un ciberataque es el daño a la reputación. De acuerdo con el Ponemon Institute [22], recuperar la reputación de la marca después de un ciberataque podría costar hasta 1 billón de dólares aproximadamente (ver Fig. 3).

II.4. Error humano

En la actualidad, la seguridad informática y la protección de los datos en las organizaciones se han convertido en un componente clave. El proceso de mejorar y optimizar procesos empresariales, el desarrollo de redes privadas, el crecimiento de servicios online a través de Internet son algunos factores que explican la creciente preocupación por mejorar la seguridad en los sistemas de información [23].

La implementación de adecuadas medidas de seguridad informática exige contemplar aspectos técnicos (Firewalls, antivirus, Sandboxie), organizativos (Planes de emergencia, análisis y gestión de riesgos) y legales (Cumplimiento de las leyes de protección de datos personales, privacidad de datos y políticas de seguridad). A pesar de ello, en muchas ocasiones se presta muy poca atención a la importancia del factor humano en la seguridad informática.

Cisco (Líder mundial en tecnología de información) en su informe *Fuga de datos a nivel mundial: Riesgos y errores comunes de empleados* [24] menciona que, a pesar de políticas, procedimientos, herramientas de seguridad actualmente en uso, los empleados de todo el mundo exhiben conductas arriesgadas que ponen en peligro los datos personales y empresariales, tales como:

- Acceso no autorizado: el 39 % de los profesionales de TI afirmó que ha otorgado acceso no autorizado a empleados a zonas de la red o a instalaciones de la empresa.
- Uso de aplicaciones no autorizadas: el 70 % de los profesionales de TI cree que el uso de programas no autorizados fue responsable de hasta la mitad de los incidentes de pérdida de información en sus empresas.
- Uso indebido de computadoras de la empresa: el 44 % de los empleados comparte dispositivos de trabajo con otras personas sin supervisión.
- Uso indebido de contraseñas: el 18 % de los empleados comparten contraseñas con sus compañeros de la oficina.
- Transferencia de archivos: el 46 % de los empleados admitió haber transferido archivos del trabajo entre equipos del trabajo y personales, trabajando desde el hogar.

Es importante mostrar cuantos y como empleados exhiben conductas que afectan la seguridad informática, pero lo realmente importante es comprender cual la razón de dichas conductas. Para ellos, las empresas deben entender qué piensan sus empleados sobre la seguridad y porque ignoran y vulneran los procedimientos empresariales.

Por otro lado, Kaspersky menciona que, en muchos casos sucede de forma involuntaria a causa de falta de conocimiento sobre seguridad informática, por no saber sobre amenazas y por distracción [25]:

- 46 % de los incidentes del año 2016 involucraron empleados que han comprometido la seguridad informática de su compañía de forma involuntaria o inconsciente.
- 53 % de las empresas afectadas por software malicioso fue a causa de un empleado distraído.
- 36 % de empleados fueron víctima de alguna técnica de ingeniería social.
- 28 % de los casos de phishing tuvieron éxito.
- 40 % de los casos, los empleados afectados ocultaron el incidente, comprometiendo más la seguridad informática y el daño ocasionado.

Muchos administradores y gerentes se encuentran preocupados por la posibilidad que los empleados puedan compartir secretos industriales, información confidencial, lista de clientes, entre otra información a través del uso de dispositivos móviles o memorias USB.

Prevenir fugas, ataques, amenazas y cualquier posible fallo es un desafío que le incumbe a todas las empresas.

Mientras más personas comprendan dicho desafío, desde profesionales de TI, empleados de todos los niveles, podrán proteger mejor la información. El objetivo es que cada persona, esté convencida que crear una cultura en esta área es fundamental, comprender políticas y procedimientos para lograr entornos seguros y poner en práctica las medidas necesarias cada día.

Crear una cultura de seguridad informática es clave. Comenzar entrenando, concientizando, fomentando, capacitando sobre seguridad informática ayudaría a reducir riesgos, a comprender mejor la seguridad y minimizar errores no intencionados.

La implementación de sistemas de seguridad debería considerar el factor humano como uno de sus elementos más importantes, contemplando aspectos como una adecuada formación y sensibilización de los empleados en este tema, la aprobación de reglamentos sobre el uso de los sistemas con acceso a Internet. Debemos destacar de forma especial la necesidad de inversión y compromiso de altos mandos, la consciencia de garantizar una adecuada utilización de sistemas y servicios tanto para usuarios como para empleados de organizaciones que interactúan con servicios informáticos.

II.5. Punto de equilibrio entre costos y seguridad

El aumento de los ataques informáticos y la complejidad que han adquirido en los últimos años deben llevar a las empresas a considerar el cómo y cuánto se está invirtiendo en seguridad informática, la pauta es que tan valiosa es la información que almacenan y encontrar un punto ideal en la inversión en seguridad informática según los datos almacenados en una organización. Establecer un valor en los datos es un desafío puesto que es algo intangible, pues la información en muchas ocasiones no se valora por las empresas, cosas que claro no ocurre con los equipos, aplicaciones, hardware o documentación. Además, las medidas de seguridad no influyen de manera directa a la productividad o rapidez de un sistema, por lo que las empresas prefieren invertir en agilizar estos procedimientos que proporcionan una ventaja en tiempo [26].

Es importante minimizar el costo de la protección manteniéndolo por debajo de los recursos protegidos. Si proteger es más caro de lo que vale la información entonces sería contraproducente. Por otro lado, los costos en los que puede incurrir una organización por no adoptar las medidas de seguridad considerando que la información es valiosa, por minimizar la inversión en este rubro, puede ocasionar costos mayores, derivados de un error humano o por afectación de un tercero. Para obtener un punto de equilibrio se deben evaluar los riesgos, y los costos en los que la organización está dispuesta a incurrir, además de decidir un nivel de seguridad en el cual la empresa desea adoptar.

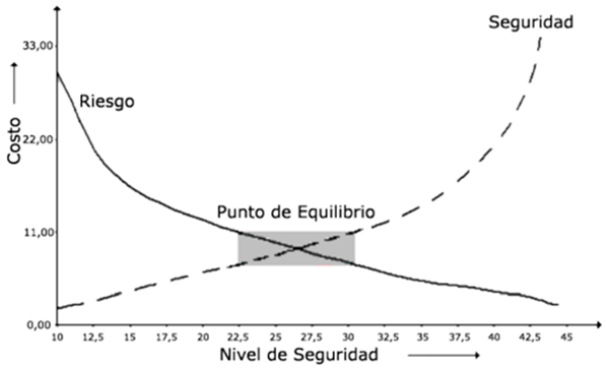

Figura 4: *Punto de equilibrio entre costos, seguridad y riesgo Fuente: El arte de presupuestar: como justificar los fondos de seguridad informática*

Los riesgos disminuyen al aumentar la seguridad, aunque por otro lado, los costos van en aumento. La importancia de la Fig. 4 es demostrar que la inversión en seguridad no debe tender al infinito, sino más bien, se debe considerar un punto de equilibrio entre la inversión y el valor de la información.

III. Metodología

El tipo de estudio fue exploratorio y se utilizaron técnicas de revisión documental y encuesta. A partir de la formulación del objetivo general, se plantearon las siguientes preguntas:

¿Por qué las empresas siguen siendo tan vulnerables a pesar de invertir grandes cantidades de dinero en sistemas de seguridad informática?

¿Se cuenta con un puesto o área de seguridad informática en las empresas leonesas?

¿Cuál es la principal causa de ataques a la seguridad informática en las empresas leonesas?

¿Cuál es la principal herramienta/estrategia utilizada para reducir amenazas?

Para la creación del instrumento de medida, se procedió a revisar la literatura incluyendo benchmarks y reportes ejecutivos publicados por empresas líderes en el mercado. Una vez revisada la literatura, se creó un instrumento para recolectar datos relacionados a inversión en medidas preventivas de seguridad informática, relevancia de las campañas de concientización y capacitación en temas de seguridad informática, principales amenazas a la seguridad informática, y privacidad de datos personales.

El instrumento de medida consta de 5 partes. El primer bloque se encuentra compuesto por 4 preguntas iniciales sobre datos sociodemográficos y laborales. El segundo bloque se encuentra compuesto por 6 preguntas sobre el conocimiento y comprensión de la Ley Federal de Protec-

ción de Datos Personales en Posesión de los Particulares y/o la Ley Federal de Protección de Datos Personales en Posesión de los Sujetos Obligados. El tercer bloque consta de 8 preguntas sobre las medidas preventivas en materia de seguridad informática. El cuarto bloque se encuentra conformado por 3 preguntas relacionadas a las campañas de concientización y capacitación en temas de seguridad informática. En el último bloque se plantean 3 preguntas sobre las principales amenazas a la seguridad informática. El instrumento de medida incluye preguntas del tipo dicotómica, selección múltiple, y orden de clasificación.

El instrumento de medición se distribuyó entre profesionales de TI. Se utilizó el sitio web www.onlineencuesta.com para distribuir el instrumento de medición entre 80 profesionales de TI que trabajan en diferentes empresas de la ciudad de León, Guanajuato. Es importante mencionar que, la distribución del enlace y la carta de presentación fueron enviadas por medio de correo electrónico. De los 80 correos electrónicos enviados, se alcanzó una tasa de respuesta del 28.75 % o 23 respuestas válidas.

IV. Resultados

Entre los resultados relevantes, se encuentra la respuesta a la pregunta 22 - ¿Cuántas personas integran el departamento de seguridad informática?, evidenciando que varias empresas carecen de un departamento de seguridad informática. En las empresas que cuentan con dicho departamento, se aprecia que son pocas personas las encargadas de las medidas de seguridad informática de la organización, entre tres y dos personas. Se evidencia que no se da prioridad al tema de seguridad informática, al menos en las empresas donde se aplicaron las encuestas (ver Fig. 5).

Las respuestas de la pregunta 12 – Seleccione las herramientas de seguridad informática más utilizada en su empresa, la mayoría de los encuestados respondieron que el antivirus y un firewall son las herramientas más empleadas, corroborando trabajos previos (ver Fig. 6).

En la Fig. 7, se evidencia que varios ataques informáticos son consecuencia de acciones de personas, de manera consciente o inconsciente. En algunos casos, el malware es consecuencia de presionar un enlace o acceder a sitios Web no legítimos; por lo tanto, ese ataque puede ser consecuencia del error humano.

En la Fig. 8, se presenta el resultado de las respuestas a la pregunta 6 - ¿Cuánto sería el tiempo que le tomaría a su empresa recuperar su reputación después de un ataque o incidente informático?; siendo evidente que no se tiene claro el concepto e impacto a la reputación. Como se puede apreciar en la Fig. 8, 9 participantes mencionaron que se puede recuperar la reputación del negocio en un mes. Este resultado contradice las evidencias que se

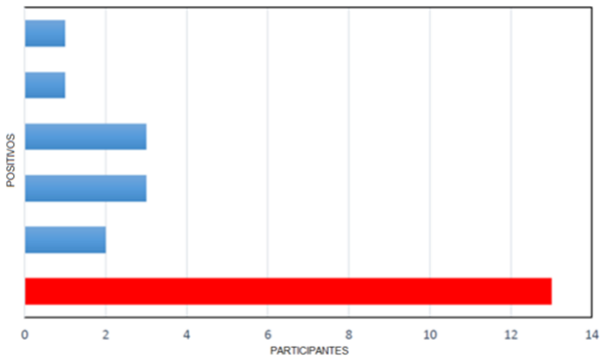

Figura 5: *Evidencia de falta del departamento de seguridad informática*
Fuente: Elaboración propia

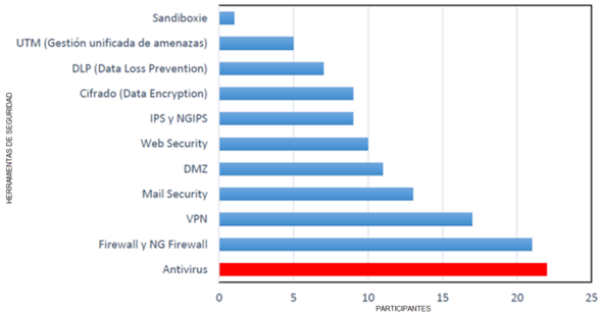

Figura 6: *Evidencia de herramientas más utilizadas para proteger la seguridad informática*
Fuente: Elaboración propia

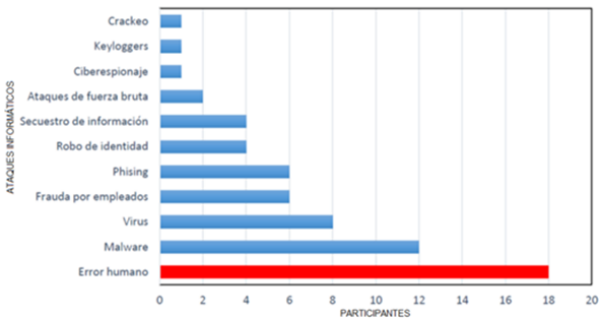

Figura 7: *El error humano como principal causa de ataques*
Fuente: Elaboración propia

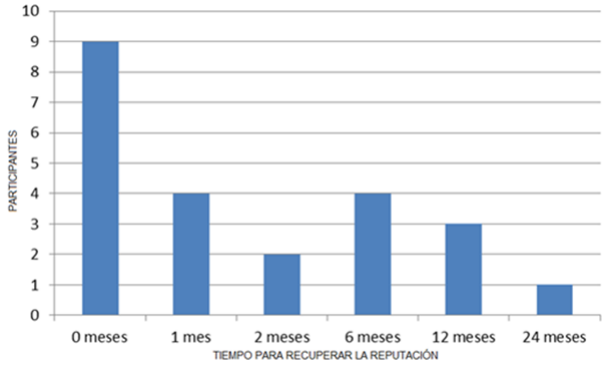

Figura 8: *Evidencia de falta de comprensión del concepto de reputación y su valor asociado*
Fuente: Elaboración propia

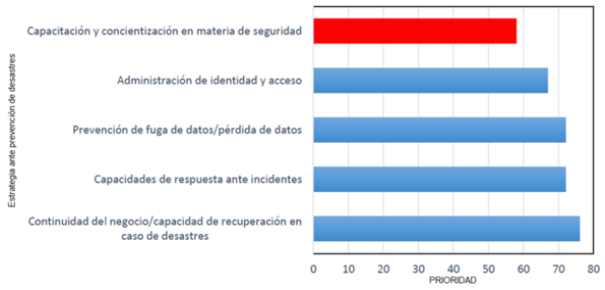

Figura 9: *Prioridad en temas de prevención*
Fuente: Elaboración propia

encuentran en [27, 28] donde se hace evidente el alto costo que se requiere invertir para revertir tal impacto, y por ende, se requiere tiempo.

En la Fig. 9, se presenta el resultado de las respuestas a la pregunta 6 – De las siguientes propuestas de seguridad informática indique la prioridad de cada una en su empresa. La respuesta es clara y contundente, los encuestados no vislumbran como importante, ni mucho menos como prioridad, las campañas de concientización y capacitación de las compañeras(os) en temas de seguridad informática. Siendo este punto, el más revelador del estudio porque se corrobora que las empresas siguen sin invertir en el eslabón más débil en la cadena de seguridad informática, el ser humano, los empleados.

También es importante mencionar que, una campaña de concientización y capacitación debe estar respaldada por la alta dirección y soportada por un departamento de seguridad informática.

Al encontrar que varias empresas carecen de dicho departamento, es evidente la falta de una estrategia de concientización entre los empleados de la empresa, y la alta dirección no tiene como comprender o entender sus ventajas.

V. Discusión

En base las respuestas de la relacionadas con la adquisición de hardware o software de seguridad informática, se llega a la conjetura que las empresas continúan invirtiendo en hardware especializado de seguridad, como son Firewall e IPS (Sistema de Prevención de Intrusos o Intrusion Prevention System en sus siglas en inglés); y software de seguridad, como son Antivirus y seguridad Web. Cabe mencionar que, de los encuestados, el 56.53 % hace mención sobre una constante inversión en el área de seguridad informática; por lo tanto, el 43.47 % hacen inversiones de manera esporádica o de una sola vez. En este sentido, el 78.26 % de los encuestados indican que en su empresa existe una política de seguridad donde se contempla el control de acceso a los recursos. En consecuencia, se puede comprender que a pesar de contar con una política de seguridad, la inversión en medidas de seguridad no se cumple en todas las empresas. Esto se puede deber a varios factores, entre los que se encuentran la economía de la empresa, el número de empleados, o sí cuentan con un departamento de seguridad informática.

También es importante mencionar que, los directivos no ven viable o no comprenden las ventajas en invertir en capacitación en temas de seguridad informática a los empleados. De acuerdo a los resultados obtenidos, la capacitación y concientización en materia de seguridad informática no es contemplado como una necesidad.

Lo anterior reafirma la falta de una cultura de seguridad informática en la organización y a la falta de importancia por parte de la alta gerencia que no contempla la inversión en capacitación como la mejor herramienta de seguridad.

En consecuencia, se puede intuir que la gran vulnerabilidad que se presenta entre las empresas leonesas es el error humano con un 78.26 % de probabilidad que sea la causa de un error de seguridad. Se evidencia que, la capacitación en materia de seguridad a todo empleado de la organización, incluyendo al personal de mantenimiento y limpieza, y personal de outsourcing es una necesidad urgente. También se debe tener claro el tiempo laboral y de descanso de cada empleado.

En cuanto al tema de cultura de seguridad informática, se llega a la conjetura que para los directivos de las empresas participantes, la capacitación y concientización en seguridad informática no es una actividad primordial. Los cursos de seguridad informática lo realizan profesionales del área, descuidando a todos los demás usuarios.

Como lo presenta el informe de Kaspersky Lab, las empresas invierten en capacitación una vez que han sido víctimas de un ataque. Entre las respuestas de los participantes, cuando se les preguntó sobre la capacitación en seguridad informática (pregunta 18), una sobresale porque fue muy clara, “No le dan la importancia debida”.

Además, se evidencia una carencia en la comprensión de un impacto oca

El tema se vuelve más interesante cuando se ven las respuestas de la pregunta 6, donde la capacitación y concientización en materia de seguridad tiene la prioridad más baja en las empresas como medida de seguridad informática.

Por último, el presente trabajo evidencia la falta de interés por contar con un departamento de seguridad informática, ocasionando que los departamentos de TI tengan la responsabilidad de tomar las decisiones sobre la inversión en materia de seguridad. En consecuencia, el esfuerzo y economía se continúan dirigiendo en adquirir software y hardware para mitigar riesgos y vulnerabilidades.

VI. Conclusiones y Trabajo Futuro

Los resultados presentados corroboran trabajos previos realizados por empresas de seguridad informática líderes en el mercado, identificando claramente la necesidad de invertir en campañas de concientización y capacitación para todos los empleados; sin importar el nivel dentro de la organización, e incluyendo a personal externo para reducir el error humano en una brecha de seguridad. También se encontró que, los conceptos de reputación y datos personales sensibles no se encuentran bien comprendidos entre el personal de TI, dificultando su correcta protección ante amenazas.

En estos momentos, se encuentra en validación una ecuación para cuantificar el accionar de una persona ante una amenaza de seguridad informática. Los factores que se utilizan se encuentran asociados a la confiabilidad del comportamiento en el contexto de seguridad informática. Además, se encuentra en desarrollo un marco de referencia para establecer un plan de acción para crear una cultura de seguridad informática en las organizaciones leonesas.

Referencias

[1] Schneier Bruce. *Secrets and Lies–Digital Security in a Networked World*. 2000.

[2] Moneer Alshaikh. «Developing cybersecurity culture to influence employee behavior: A practice perspective». En: *Computers & Security* 98 (2020), pág. 102003.

[3] Nick Wilding. «Cyber resilience: How important is your reputation? How effective are your people?» En: *Business Information Review* 33.2 (2016), págs. 94-99.

[4] Aggeliki Tsohou y col. «Managing the introduction of information security awareness programmes in organisations». En: *European Journal of Information Systems* 24.1 (2015), págs. 38-58.

[5] Adele Da Veiga y col. «Defining organisational information security culture—Perspectives from academia and industry». En: *Computers & Security* 92 (2020), pág. 101713.

[6] Vladimir Alfonso Rodríguez y Edelmis Chapis Cabrera. «Importancia de las tecnologías de la información y las comunicaciones, el internet y las redes sociales en el mejoramiento y desarrollo de las empresas». En: *contribuciones a la Economía* marzo (2019).

[7] Acklesh Prasad. «Information technology and business value in developing economies: A study of intangible benefits of information technology investments in Fiji». En: *The Electronic Journal of Information Systems in Developing Countries* 34.1 (2008), págs. 1-11.

[8] Galo E Cano Pita. «Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones». En: *Dominio de las Ciencias* 4.1 (2018), págs. 499-510.

[9] Ines Mergel, Noella Edelmann y Nathalie Haug. «Defining digital transformation: Results from expert interviews». En: *Government information quarterly* 36.4 (2019), pág. 101385.

[10] OD AMERICANOS. *TENDENCIAS EN LA SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE Y RESPUESTAS DE LOS GOBIERNOS*.

[11] UNAM CERT. *Estadísticas de incidentes detectados en RedUNAM Trimestral 2016 y 2017*. 2017. URL: https://www.seguridad.unam.mx/estadisticas.

[12] Arif Koyun y Ehssan Al Janabi. «Social engineering attacks». En: *Journal of Multidisciplinary Engineering Science and Technology (JMEST)* 4.6 (2017), págs. 7533-7538.

[13] AJ Widdowson y PB Goodliff. «CHEAT, an approach to incorporating human factors in cyber security assessments». En: *10th IET System Safety and Cyber-Security Conference 2015*. IET. 2015, págs. 1-5.

[14] Keman Huang y Keri Pearlson. «For what technology can't fix: Building a model of organizational cybersecurity culture». En: *Proceedings of the 52nd Hawaii International Conference on System Sciences*. 2019.

[15] Luis Joyanes Aguilar. «Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0)». En: *Cuadernos de estrategia* 185 (2017), págs. 19-64.

[16] Tim Kayworth y Dwayne Whitten. «Effective information security requires a balance of social and technology factors». En: *MIS Quarterly executive* 9.3 (2010), págs. 2012-52.

[17] Chris Noble y Gary Dwayne Whitten. *Business impacts of cyber attacks – Forensic Foresight: July 2016*. 2016. URL: https://www2.deloitte.com/au/en/pages/media-releases/articles/business-impacts-cyber-attacks.html.

[18] Kaspersky. *The human factor in IT security: How employees are making businesses vulnerable from within, 2017*. 2017. URL: https://www.kaspersky.com/blog/the-human-factor-in-it-security/.

[19] ESET. *ESET Security Report – Latinamérica 2016*. 2016. URL: https://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf.

[20] Tyler Moore, Scott Dynes y Frederick R Chang. «Identifying how firms manage cybersecurity investment». En: *Available: Southern Methodist University. Available at: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2015-12-14)* 32 (2015).

[21] Dinah Heidinger y Nadine Gatzert. «Awareness, determinants and value of reputation risk management: Empirical evidence from the banking and insurance industry». En: *Journal of Banking & Finance* 91 (2018), págs. 106-118.

[22] Ponemon Institute. *Reputation impact of a data breach: U.S. study of executive & managers*. Ponemon Institute© Research Report. 2011.

[23] Peter Mayer, Alexandra Kunz y Melanie Volkamer. «Reliable behavioural factors in the information security context». En: *Proceedings of the 12th International Conference on Availability, Reliability and Security*. 2017, págs. 1-10.

[24] CISCO. *Fuga de datos a nivel mundial: riesgos y errores comunes de los empleados*. 2008. URL: https://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.pdf, %202008.

[25] Nikolay Pankov. *El factor humano: ¿Pueden aprender los empleados a no cometer errores?* 2017. URL: https://latam.kaspersky.com/blog/human-factor-weakest-link/10790/.

[26] Paul A STRASSMANN. «El arte de presupuestar: como justificar los fondos para Seguridad Informática». En: *Recuperado el* 7 (2009).

[27] Brian Cashell y col. «The economic impact of cyber-attacks». En: *Congressional research service documents, CRS RL32331 (Washington DC)* 2 (2004).

[28] Shinichi Kamiya y col. «Risk management, firm reputation, and the impact of successful cyberattacks on target firms». En: *Journal of Financial Economics* 139.3 (2021), págs. 719-749.