Metodologías para instruir a los colaboradores en buenos hábitos de seguridad informática Methodologies to instruct employees in good computer security habits

Alonso José Mesen Quesada
Universidad Latina, Costa Rica
amesen14@gmail.com

Recibido 20/ago/2020
Aprobado 20/nov/2020

Resumen-
En la actualidad las amenazas cibernéticas abundan a un punto tan alto, que cualquier organización, no importa si es pequeña o grande, internacional o nacional, es un objetivo para estas amenazas. La seguridad es un elemento fundamental con miras a la continuidad del negocio, se debe contemplar siempre. Es un factor el cual involucra a toda la población. Por ende, se debe concientizar el tema entre los colabores de estas.

Al ser necesario tener seguridad, se busca concientizar sobre la importancia de implementar la enseñanza en los colaboradores. Por ello, en este proyecto se busca investigar la importancia de implementar o crear metodologías de instrucción de buenas prácticas de seguridad informática a los colaboradores de una empresa, en Costa Rica. En él se analiza el estado actual de los colaboradores en temas de seguridad, mediante encuestas. También la importancia de las metodologías de instrucción y los factores que implican. Se valora ciertas amenazas a las cuales se pueden enfrentar los colabores en la organización, con ciertas recomendaciones e información relevantes.

En las empresas, los colaboradores constituyen un pilar, debido a esto son uno de los objetivos más fuertes para los atacantes cibernéticos. Es fundamental brindar las medidas necesarias con el fin de estar preparados a la hora en la cual un evento de riesgo como este suceda. No solo mantiene su seguridad, sino la de toda la empresa. La seguridad es responsabilidad de toda la organización, debido a esto se debe estar en un constante ciclo de mejora continua. La concientización y el crear conocimientos sobre buenas prácticas de seguridad disminuye la probabilidad de ser afectado por un evento negativo.

Palabras Claves: *Seguridad, metodología, amenazas, concientización.*

Abstract Context:

Today cyber threats abound to such a high point that any organization no matter if it is small or large, international or national, it will be a target for these threats. Security is a

fundamental element for business continuity, it must always be considered. It is a factor that involves the entire population. Therefore, the same issue must be raised among their collaborators.

Since there is this need for security, it seeks to investigate the importance of implementing it in employees. For this reason, this project seeks to investigate the importance of implementing or creating instructional methodologies of good computer security practices to the employees of a company in Costa Rica. In it, the current status of employees in security issues will be analyzed, through surveys. Also, the importance of instructional methodologies and the factors they involve. Threats that collaborators in the organization may face are assessed, with their recommendations, recommendations and relevant information.

In companies, collaborators are a fundamental pillar, due to this they are one of the strongest objectives that cyber attackers have. It is essential to provide the necessary measures so that they are prepared when a risk event like this happens. You will not only maintain the security of this, but that of the entire company. Security is something that the entire organization is responsible for, because of this it must be in a constant cycle of continuous improvement. Raising awareness and creating knowledge about good security practices decreases the probability of being affected by a negative event.

Keywords: *Security, methodology, threats, awareness.*

organización, "La capacitación no es sinónimo de educación. La capacitación o entrenamiento en las empresas forma parte de la educación y de la formación integral de las personas. En las organizaciones de trabajo, el entrenamiento de los trabajadores debe vincularse y complementarse con otras actividades que contribuyan a su formación.." (p.48). Brinda el conocimiento y herramientas necesarias para que los colaboradores trabajen de manera segura y confiable, es un deber de cada organización. Este debe ser evaluado y considerado siempre, para la mejora de ellos como profesionales y personas.

Se busca poder determinar la importancia de crear metodologías de instrucción o capacitación sobre buenas prácticas de seguridad. Lo anterior con base en análisis y comprensión del estado actual de los colaboradores. Así se puede determinar qué tan bien o mal ellos están respecto del tema. Al igual se busca valorar una cierta cantidad de amenazas o eventos de riesgo los cuales puedan enfrentar en sus días laborales y cotidianos.

Al poder entender el estado actual de los colaborados, se puede tener una idea o imagen de los pasos por seguir como empresa. Entre ellos se busca la concientización sobre la seguridad y lo importante que de cada colaborador tenga conocimientos básicos sobre él. Cuando se crea una cultura, la probabilidad e impacto de una amenaza se reduce drásticamente. Esto a su vez mejora la confianza de los colaboradores, los insta a aprender y tomar mejores decisiones a la hora de materializarse un evento negativo.

I. INTRODUCCIÓN

Según (Cota Olmos, 2002). La importancia de los valores en el desarrollo humano de la

II. ANTECEDENTES DEL PROBLEMA DE ESTUDIO

La información, los procesos de apoyo, los sistemas y las redes, son bienes importantes de las entidades. Debido a esto, requieren protegerse convenientemente frente a amenazas capaces de ponerlos en peligro. Muchos factores como disponibilidad, integridad, confidencialidad de la información, estabilidad de los procesos, niveles de competitividad, imagen corporativa, rentabilidad y legalidad, son aspectos necesarios para alcanzar los objetivos de la organización, son objetivos para estos eventos de riesgo.

Según (Romero Castro, y otros, 2018), en su estudio Introducción a la seguridad informática y el análisis de vulnerabilidades, comenta: la seguridad informática se encarga de la seguridad del medio informático, la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitirla. La seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información. (p. 13) En resumen, quiere decir, se preocupa por casi todo lo relacionado con tecnología de la información, ya sea infraestructura computacional. Eso conlleva a afirmar existen varias diferencias con la seguridad de la información, pero lo más relevante es el universo que maneja cada uno de los conceptos en el medio informático.

Según la Organización Internacional de Normalización o Estandarización (2013) en la normativa ISO 27001, la seguridad de la información es muy extensa, por lo tanto, no es sólo una cuestión técnica, sino supone una responsabilidad de la alta dirección de la empresa, así como de sus directivos. Se debe considerar los sujetos, los procesos y las funciones de negocio para poder garantizar la confidencialidad, integridad y disponibilidad de los datos.

Esto es relevante, pues se puede definir la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas, con el fin de obtener un sistema de información seguro, confiable y, sobre todo, tenga disponibilidad. La seguridad de la información es proteger los datos, indistintamente de su formato, contra cualquier amenaza, de manera que garantice en todo momento la continuidad de las actividades de la empresa. Al comprender el concepto de seguridad informática, es importante conocer aquellas cosas las cuales van por debajo de esta. Entre ellas se encuentra los procesos organizacionales, los sistemas o tecnologías que soportan estos y las personas involucradas en los procesos y los sistemas de la organización. Muchas entidades solo se centran en proteger y dar seguridad a los procesos y a los sistemas de la organización, sin saber que el eslabón más débil son las personas involucradas en estos procesos y sistemas. De acá nace la importancia de crear o implementar metodologías de instrucción de buenas prácticas, así las personas quienes manejan esos procesos realicen sus operaciones de la mejor manera posible, manteniendo la seguridad de la organización.

El crear una cultura de seguridad informática en una organización es fundamental. Las personas son las más vulnerables cuando se enfoca este mundo de la tecnología. La concientización, la instrucción y la educación acerca de la seguridad informática, viene a reducir este problema. Al realizar e implementar metodologías de instrucción se puede aumentar el conocimiento de esto, para poder reducir las posibilidades de eventos de

riesgos donde se involucre los colaboradores de la organización. Se dice reducir, porque es imposible garantizar al 100% su seguridad. Los eventos de riesgos y amenazas van a estar ahí siempre, por eso es importante mitigarlos lo posible, así el nivel de vulnerabilidades y amenazas se reduce.

III. PLANTEAMIENTO DEL PROBLEMA

¿Es importante la creación de metodologías de instrucción respecto de los buenos hábitos de seguridad informática, para la continuidad de negocio en una empresa de Costa Rica con base en un estudio y análisis del personal, así como la valoración de ataques de seguridad durante el año 2020?

IV. JUSTIFICACIÓN

La creación de una cultura de seguridad es uno de los factores más descuidados e importantes en la actualidad. Cómo atacarlos y enfrentarlos es un reto el cual cada empresa debe cubrir hoy en día. En la actualidad se tiene la facilidad de buscar y encontrar información relevante, ella ayuda a garantizar una mejora en estos aspectos. El presente trabajo trata de buscar la importancia de la creación de metodologías para instruir y capacitar a todo el personal, en la mejoría de sus hábitos de seguridad de información, al igual demuestra las mayores amenazas por enfrentar en este mundo de tecnología, su posible impacto en la actualidad y sus recomendaciones.

Lo anterior se puede lograr mediante la recolección de información acerca de los conocimientos actuales de los colaboradores en el área de seguridad, recopilando las amenazas posibles de encontrar para este caso en la empresa investigada, así como las mejores prácticas para mitigarlas, creando una cultura de seguridad informática y ponerla en práctica en la actualidad. Esto es importante con el fin de salvaguardar los sistemas e información propia de la organización, manteniéndolos estables de la mejor manera posible, al hacer conciencia del gran impacto que conlleva, al igual se crea una cultura de seguridad entre la población de la empresa, la cual garantiza una continuidad y contingencia del negocio, y mitiga posibles eventos de riesgos.

El trabajo de investigación se realiza en la organización de Costa Rica, para ver el estado actual de sus colaboradores y encontrar los puntos de mejora necesarios. También busca crear una cultura de seguridad y una concientización sobre el tema por parte de los colaboradores. Además, se brinda más confiabilidad a la hora de efectuar las tareas diarias de dicha institución. Al crear conciencia en los empleados, la seguridad entre ellos crece al igual la de la empresa.

Se pretende realizar este proyecto de analizar la importancia de las metodologías de instrucción a personal sobre los buenos hábitos y prácticas de seguridad informática en el transcurso del año 2020. Es importante abarcar el tema lo más pronto posible, pues a futuro el impacto y el valor generado en los colaboradores va a ser muy grande, por lo tanto, mitiga y previene amenazas a la empresa. No solo el personal se beneficia con nuevos mecanismos y temas de aprendizajes o entendimientos sobre la organización, sino empresa nota un gran impacto en la contingencia, manejo y administración de riesgos. La seguridad siempre va a ser necesaria y no hay un método para garantizar el 100% de la seguridad, pero por lo menos con esto se puede estar más tranquilo al tener

la organización un plan de acción y mitigación de manera adecuada, para así llevar el riesgo de materializar una amenaza en los sistemas.

V. OBJETIVO GENERAL

Analizar la importancia de la creación de las metodologías de instrucción a los colaboradores en los buenos hábitos de seguridad informática para la continuidad de la empresa, mediante la evaluación del personal, valorando los ataques de seguridad en una organización de Costa Rica durante el 2020.

VI. OBJETIVOS ESPECÍFICOS

- Analizar la importancia de la creación de metodologías de instrucción a los colaboradores sobre la seguridad informática, mediante un proceso de evaluación, determinando la relevancia de implementarlas en la empresa.
- Identificar el estado actual de los conocimientos de seguridad informática, mediante encuestas, evaluando que tanto necesitan capacitación en esta área.
- Valorar las distintas amenazas que puede enfrentar en sus días laborales, mediante la explicación de ellas, evaluando su impacto y medios de mitigación.

VII. DELIMITACIÓN, ALCANCE O COBERTURA

Las empresas, ya sea tecnológicas o no, van a estar al margen y siempre son un objetivo para los ataques cibernéticos. No importa qué tan grandes o pequeñas sean, la posibilidad de ser atacadas es muy alta, más en estos tiempos donde todo el mundo está conectado por tecnología, y la mayoría tiene acceso a internet. Por lo tanto, se opta por capacitar al personal, técnico o no técnico, con el fin de que las organizaciones pueden estar más tranquilas en torno a su seguridad.

Hoy en día, la tecnología abunda en todas las empresas, muchas dependen totalmente de ella, es decir, sí la infraestructura tecnológica no está disponible, las pérdidas económicas son gigantes. Debido a lo anterior y a la gran cantidad de ataques presentes, es sumamente importante la capacitación del personal en dichos temas, para así, salvaguardar la empresa y sus sistemas. Tal como lo dicen Arias, Merizalde y Noriega (2013), en su tesis Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audiovisual, la informática de hoy está inmersa en la gestión integral de las empresas, y, por lo tanto, la seguridad es un elemento fundamental, los departamentos de sistemas de cada organización deben dar siempre prioridad a la seguridad de los sistemas de información (p. 1). Esto es más que una realidad, se debe garantizar la seguridad de los departamentos, y así la empresa esté en buen rumbo, en lo referente a temas de seguridad.

Las personas quienes están más integradas en el mundo de la tecnología les es más fácil poner en ejecución las buenas prácticas, para mitigar los ataques en el ambiente, ya sea personal o empresarial. No obstante, si el personal es técnico o no, siempre es un posible blanco para el atacante. Es un reto, pero además de eso, es un deber de quienes tengan el conocimiento, poder trasmitirlo, para ayudar a todos, mitigando los riesgos y amenazas. Así se puede crear un ambiente mucho más confiable, en donde todos conocen los riesgos y amenazas por enfrentar en el camino día a día.

Sí se habla de seguridad informática, es importante evaluar las situaciones que vienen por debajo, entre ellas, los procesos organizacionales, los sistemas o las tecnologías que los soportan y las personas

involucradas. Éstas últimas son el pilar más débil, crean un gran reto para la empresa. Debido a ello es importante mejorar ese pilar, para tener una seguridad informática segura y estable. Acá es donde entran las metodologías de instrucción de seguridad informática, para levantar ese aprendizaje y crear una cultura de seguridad informática la cual beneficie la organización y mantenga la mayor parte salvaguardada. Su creación es relevante, pues da a conocer posibles puntos de mejora, al igual permite identificar sectores o personas quienes necesitan asistencia para realizar su trabajo de manera segura, y minimizar el riesgo de ser infectado por una amenaza, además de mejorar la continuidad del negocio.

VIII. RESTRICCIONES Y/O LIMITACIONES

No se realizó una implementación del sistema de postes multifuncionales propuesto. No se realizó capacitaciones sobre cómo implementar el sistema de postes multifuncionales propuesto. Se limito a la zona geográfica de Cartago para la cobertura de esta investigación y de sus servicios actuales en su cartera en la actualidad.

IX. VIABILIDAD

Es posible llevar a cabo esta investigación tanto en la perspectiva técnica como en la económica, porque, a pesar de que este proyecto va a enfocarse únicamente en una propuesta, se cuenta con los medios y el conocimiento necesarios para la obtención y entendimiento de la información.

a) Punto de Vista Técnico.

El punto de vista técnico para la realización de esta investigación contempla la experiencia en redes y telecomunicaciones, así como el conocimiento en tecnologías de información que poseen los investigadores, ambas necesarias para poder investigar, entender y analizar la información requerida para llevar a cabo esta investigación.

b) Punto de Vista Operativo.

Es importante aclarar para la realización de esta investigación se cuenta con el apoyo de la Municipalidad de Cartago en Costa Rica y que la misma no afectará el funcionamiento normal de la Municipalidad de Cartago en Costa Rica en ninguna de sus áreas de trabajo, ya que al ser esta una propuesta no será necesario consumir recursos de la Municipalidad que afecte el normal accionar de la institución y sobre todo de los funcionarios del Departamento de Tecnologías de Información. A como se expandió en la sección anterior en limitaciones se limita la zona geográfica a la ciudad de Cartago en Costa Rica y a sus servicios disponibles en su cartera.

c) Punto de Vista Económico.

Desde el punto de vista económico, es importante indicar los costos de cada una de las herramientas que se requerirán para la realización de esta investigación con un valor económico de ₡4,713,081.16.

X. MARCO SITUACIONAL METODOLÓGICO

Es importante tomar en cuenta que, estas fuentes son las que están siendo tomadas como marco de referencia para la investigación y las mismas no son definitivas por lo que más fuentes pueden llegar a ser tomadas en cuenta de ser requeridas conforme la investigación avance en su desarrollo. Se entiende como servicio en la nube cómo una "tendencia reciente que mueve los datos lejos de PC de escritorio y las portátiles a grandes centros de datos. Se refiere, básicamente a aplicaciones entregadas como servicios desde Internet." (Dikaiakos, Katsaros, Mehra, Pallis, & Vakali,

2009) El pensamiento de los servicios tecnológicos de la nube, como se menciona en la siguiente cita "… esto requiere una forma muy diferente de pensar, porque está externalizando de manera efectiva infraestructuras completas aparte de la aplicación en sí misma." (Carey, 2018)

De acuerdo con la definición "nube se utiliza como una metáfora de Internet, basado en el dibujo de nubes utilizado en el pasado para representar a la red telefónica, y más tarde para representar a Internet en los diagramas de red de computadoras como una abstracción de la infraestructura subyacente que representa." (FayerWayer, 2012) Como HPE define qué "la nube no es un lugar, sino un método de gestión de recursos de TI que reemplaza las máquinas locales y los centros de datos privados con infraestructura virtual. En este modelo, los usuarios acceden a los recursos virtuales de computación, red y almacenamiento que están disponibles en línea a través de un proveedor remoto. Estos recursos se pueden aprovisionar de manera instantánea, lo que es particularmente útil para las empresas que necesitan escalar verticalmente su infraestructura o reducirla rápidamente en respuesta a una demanda fluctuante." (Hewlett Packard Enterprise, s.f.)

El concepto de una nube pública de acuerdo con la cita a continuación: "servicios informáticos que ofrecen proveedores externos a través de la Internet pública y que están disponibles para todo aquel que desee utilizarlos o comprarlos." (Microsoft, s.f.) A continuación, RedHat define el servicio de una nube pública "que su suscripción sea portátil, de manera que pueda elegir la arquitectura y la infraestructura que mejor se adapten a sus necesidades." (RedHat, s.f.)

Lo principal es definir los sistemas inteligentes, los cuales están basados en programas computacionales que reúnen características similares a la inteligencia humana, estos sistemas inteligentes están basados en el desarrollo de software que utiliza la información de los sistemas multifuncionales a través de las redes de comunicación para prestar los servicios y mejorar el nivel de estos que ayudan a la comunidad en temas como la seguridad en colaboración con la policía, el transporte logrando mejorar los tiempos de traslación de los vehículos y del transporte urbano, así como los servicios basados en tecnología que se le brindan a los ciudadanos. (Arellano & Santoyo, 2009)

d) Definiciones de la investigación

Se entiende servicio en la nube como una "tendencia reciente que mueve los datos lejos de PC de escritorio y las portátiles a grandes centros de datos. Se refiere, básicamente a aplicaciones entregadas como servicios desde Internet." (Dikaiakos, Katsaros, Mehra, Pallis, & Vakali, 2009) El pensamiento de los servicios tecnológicos de la nube, como se menciona en la siguiente cita, "…requiere una forma muy diferente de pensar, porque está externalizando de manera efectiva infraestructuras completas aparte de la aplicación en sí misma. (Computerworld, 2018)" (computerworld.es, 2018)

Asimismo, la nube "se utiliza como una metáfora de Internet, basado en el dibujo de nubes utilizado en el pasado para representar a la red telefónica, y más tarde para representar a Internet en los diagramas de red de

computadoras como una abstracción de la infraestructura subyacente que representa" (FayerWayer, 2012). HPE define que "la nube no es un lugar, sino un método de gestión de recursos de TI que reemplaza las máquinas locales y los centros de datos privados con infraestructura virtual. En este modelo, los usuarios acceden a los recursos virtuales de computación, red y almacenamiento que están disponibles en línea a través de un proveedor remoto. Estos recursos se pueden aprovisionar de manera instantánea, lo que es particularmente útil para las empresas que necesitan escalar verticalmente su infraestructura o reducirla rápidamente en respuesta a una demanda fluctuante" (Hewlett Packard Enterprise, s.f.).

Lo anterior no quiere decir que se exime de responsabilidades a los diseñadores a la hora de la definición la arquitectura, todo lo contrario, sigue siendo una tarea vital para garantizar el éxito de un proyecto, lo que se quiere es aclarar la versatilidad y la mejora con la que se dispone. Finalmente, es importante hacer recomendaciones y conclusiones que permitan aprovechar al máximo el diseño propuesto para sacar el mayor provecho del sistema y aumentar su uso comercial, recuperando lo antes posible su inversión, pero sobre todo para generar ganancias al cliente.

XI. DIAGNÓSTICO DEL ESTADO ACTUAL

Al entender el estado actual de los colaboradores de la empresa, se puede denotar muchos factores los cuales pueden mejorar, y así se beneficia la organización y sus empleados quienes realizan la encuesta. En términos de conocimientos de seguridad informática, se puede determinar: más de la mitad de los empleados tienen un nivel de intermedio ha avanzado en seguridad, igual sucede con los conocimientos en ingeniería social y el impacto que conlleva. No obstante, si hay un buen porcentaje de colaboradores quienes no tienen muy fuertes estas áreas. Las personas con un buen control de estas áreas siempre poseen puntos de mejora y de donde se pueda aprender y mejorar.

Se puede determinar que los colaboradores están interesados en aprender más sobre seguridad informática y buenos hábitos al respecto, y están abiertos a probar metodologías de instrucción para ello. Al igual creen la creación de políticas puede mejorar y ayudar a mantener la seguridad de la empresa, de ellos y sus dispositivos. Se cree que la seguridad, al igual los conocimientos de los empleados pueden mejorar. La creación e implementación de metodologías de capacitación puede garantizar esto sea posible.

La seguridad informática, es una labor la cual debe tener en cuenta cada uno de los colaboradores quien integre una empresa. No importa si no se tiene un departamento dedicado a la seguridad informática, cada empleado debe conocer y ayudar a mantener la seguridad de esta. Otro factor importante observado es: se debe conocer las normas o políticas de la organización, al igual es importante saber cómo está integrada la entidad. Esto con el objetivo de entender y manejar cualquier situación de la mejor manera posible, manteniendo la seguridad de la empresa y de los empleados, mejorando la toma de decisiones. Cada colaborador debe tener claridad respecto de las normas y políticas, sin importar el área en donde labore, siendo la seguridad el beneficio principal de esta práctica. Como resultado, en caso de materializarse un evento de riesgo, la persona pueda realizar los pasos por seguir según el evento presente, minimizando su impacto al no

realizar cosas que puedan empeorar la situación.

En temas de seguridad física de los dispositivos, se debe mencionar un factor importante, una buena parte de la población utiliza dispositivos personales, solo a ciertas personas se les brinda estos. Lo anterior dificulta políticas de implementación de antivirus o VPN's, pues no se puede obligar al usuario a descargar estas herramientas, pero si es posible recomendar e implementar para los casos donde sí apliquen. Estas herramientas son de gran ayuda para mantener la seguridad en los dispositivos, por ejemplo, el antivirus puede usarse para análisis de archivos, detección y corrección de incidentes, mientras las VPN brindadas por una red privada permiten establecer conexión con una o más computadoras de manera segura. A pesar de ser bueno tener esto, no significa se esté totalmente a salvo, siempre se puede estar en riesgo de ser afectado, lo importante es minimizar esa probabilidad de darse.

Esto también hace el uso de los dispositivos posible para cosas no laborales, en sí ese no es el problema. El problema raíz es poder ser afectado por una amenaza al realizar estas acciones y esta impacte la organización y el usuario. Muchas veces se ingresa a sitios o a link sin pensarlo, sin saber que debajo de ello pueden suceder eventos de riesgo. La ingeniería social es un riesgo frecuente en la actualidad. Existen muchos sitios falsos dedicados al robo de información los cuales pueden afectar a los colaboradores. De igual manera se debe tener cuidado con las descargas realizadas en la red. Dichos sitios pueden contener códigos maliciosos y por simples descuidos afectar a toda la organización por eventos los cuales se puede mitigar y prevenir.

Se trata de usar contraseñas fuertes y si es posible implementar doble autentificación para mejorar la seguridad de los dispositivos y de las áreas donde se trabajen. No existen políticas de contraseñas en la organización, pero se puede determinar que la mayoría le toma importancia a esto, como resultado da la prevención de usuario no autorizado y autentificado a los dispositivos o información y actividades de la empresa. Así se disminuye el riesgo de que usuarios sin autorización realicen operaciones en ellos. La información contenida debe protegerse, no importa si es personal o de la empresa. En caso de evento de riesgo se puede corromper o ser comprometida. El uso de respaldos garantiza poder volver a la normalidad si un evento de esos se materializa, al igual es de buena práctica actualizar los respaldos de manera periódica.

XII. PROPUESTA DE CAMBIO

Con el fin de encontrar la importancia de las metodologías de instrucción, se propone analizar los factores que esto conlleva y las distintas maneras de abarcar este proceso, para poder impulsar su implementación en la organización en Costa Rica. Por cuanto las metodologías son una herramienta para compartir conocimientos o aptitudes sobre temas variados y de importancia para la población. Como resultado de su aplicación, se podrá valorar varios beneficios como la sensibilización y capacitación, en este caso sobre temas de seguridad informática y la propia organización. Todo eso fomentará la culturización de la seguridad informática en la empresa. La cultura de seguridad se dará gracias a la concientización y a las metodologías, las cuales al final se trasladará por toda la organización, promoviendo

beneficios y llevando a los empleados a una mejora continua.

Se identificará la mejor manera de poder impartir metodologías de instrucción en la entidad, el fin es estén al alcance de todos los colaboradores, los motive a seguir aprendiendo y a tener un ambiente laboral seguro. Es importante poder brindar este mecanismo a todos los colaboradores sin importar el rango de cada uno, por tanto, la capacitación mejorará los conocimientos de los colaboradores y más sobre seguridad, factor el cual toda la organización debe velar por su continuidad. Hoy en día hay muchas herramientas para facilitar este proceso, como ejemplo está "Saba LMS". Se orienta a la creación de cursos personalizados de manera virtual, que pueden ser accedidos por los empleados, y contener mini exámenes para evaluar el material visto, y asignarse periódicamente para tener una mejora continua, y por supuesto abarcar temas de importancia como la seguridad de la organización, sus políticas, leyes y otros más, según las necesidades y cuanto se busque instruir. Por supuesto es importante tener en cuenta que no se debe sobrecargar los empleados con tantas pruebas o cursos, pero si tener un control en los cuales no se vea como una pérdida de tiempo, sino una manera de mejorar como profesionales, en una ruta donde se mejora la continuidad de la empresa y de los procesos normalmente utilizados.

Con el fin de determinar el entendimiento general sobre los conocimientos actuales de los colaboradores en seguridad informática, se propone realizar una encuesta para cumplir con lo deseado. Para esto se realizará una encuesta de modalidad virtual, con el propósito de acceder a la mayor cantidad de personal posible. Las encuestas son un gran medio de recolecta de información, facilitan este proceso, y mediante herramientas de estadística se puede tener mayor claridad en las cifras o datos correspondientes. En el caso del presente trabajo, las preguntas de la encuesta serán orientadas a seguridad informática y de información, al igual de preguntas sobre la organización, para conocer qué tanto saben los colaboradores sobre estas. Esto apoyara el poder identificar cuáles temas serán importantes de evaluar a la hora de implementar las metodologías de instrucción sobre los colaboradores.

Como insumo complementario al uso de la metodología, se evidencia distintas amenazas a nivel de ciberseguridad en la empresa, las cuales serán señaladas, así como las acciones por ejecutar para su mitigación. Con el objetivo de que estos temas también sean contemplados en las metodologías de instrucción, para se conozcan a nivel organizacional, dándole claridad al tema, y un conocimiento base para poder mitigar los eventos negativos que estos puedan llegar a generar. Orientándose más en la parte de ingeniería social, pues varios estudios como el de la Institución Nacional de Estadística y Censos (INEC) demuestran que en el 2018 hubo 55.296 reportes sobre estafas por internet. Además, se brindará una presentación con un resumen sobre las principales amenazas, su clasificación, información relevante y un diagrama acerca de cómo manejar correos electrónicos, para identificar si son maliciosos o no.

Estas tres propuestas conformarán el trabajo de investigación, y dan la iniciativa para la mejora continua. Se trata de concientizar sobre la importancia de la seguridad informática y lo esencial que es para los colaboradores saber sobre el tema, al igual sobre acerca de la empresa, generando indirectamente una cultura de seguridad. Esta

será cada vez más presente en la organización, fomentando el buen uso de las dispositivos y procesos que se tengan, dando claridad y buena toma de decisiones. A la vez mitigará y minimizará la probabilidad de ser impactados por un evento de riesgo negativo el cual perjudique a toda la población vigente. Es importante no omitir la mejora continua, resulta necesario se esté en una constante actualización de conocimientos, la tecnología y las amenazas cibernéticas avanzan diariamente, debido a esto es esencial estar en constante aprendizaje, en una mejora continua que beneficie a los colaboradores y a la empresa, permita defenderse en todo momento y así mitigar los posibles eventos de riesgo vigentes.

XIII. CONCLUSIONES Y RECOMENDACIONES

El conocimiento es algo fundamental en la actualidad, cada día la tecnología avanza, nuevas técnicas aparecen y otras desaparecen, es importante estar en constante aprendizaje para no estar desactualizado respecto del entorno. Igual sucede con la seguridad informática, por eso es importante entenderla y tenerla contemplada en todo momento. Los colaboradores deben tenerlo muy claro para poder elaborar las tareas diarias de la mejor manera posible, siguiendo los estándares, protocolos o reglas las cuales se tengan para que este se ejecute de manera segura. Los colaboradores son los responsables de mantener la seguridad en la empresa.

Para el objetivo 1. Analizar la importancia de la creación de metodologías de instrucción a los colaboradores sobre la seguridad informática, mediante un proceso de evaluación, determinando la relevancia de implementarlas en la empresa. Se concluye:

- En términos de conocimientos sobre seguridad informática, para este trabajo se determina: en la empresa investigada, la mitad de la población encuestada está en nivel promedio. Esto es positivo, pues se tiene un buen nivel de conocimiento entre un poco más de la mayoría. Sin embargo, hay personas quienes no se encuentran en este nivel, por lo tanto, se recomienda, no importa el nivel que se tenga, se puede mejorar o agregar conocimientos nuevos con metodologías de instrucción. En cuanto a temas de motivación y de interés relacionados con la seguridad, la población considera en la empresa pueden mejorar mucho, siendo ello un factor muy común, pues siempre va a haber puntos de mejora en los cuales se puede trabajar. El personal está interesado o abierto a recibir metodologías de instrucción sobre buenos hábitos de seguridad informática, máxime que se considera este como el primer avance para crear una cultura de seguridad en la organización.

- Por todo lo anterior, se recomienda implementar metodologías de instrucción de manera online, mediante herramientas como Saba LMS, DOCEBO, Sabiorealm, Talent LMS y Litmos LMS, plataformas orientadas a las capacitaciones online de colaborador dentro de la organización, sobre buenas prácticas de seguridad, creando así una cultura de seguridad. Esto genera reducir la probabilidad de materializar un evento de riesgo. Otro beneficio es: el ambiente de trabajo se hace más seguro y ordenado, con un buen entendimiento de lo cuanto se tiene en la empresa y los estándares o protocolos vigentes. De esta manera todo el personal tiene claridad acerca de su empresa y la seguridad que esta conlleva.

- No se tiene un entendimiento claro de cuáles son las normas o políticas de la

empresa, al igual de los pasos por seguir en caso de que un evento de riesgo se materialice. El no saber cuáles son las reglas de la empresa, genera problemas, pues no se tiene una clara idea de lo permitido y lo que no, al igual del impacto que se tiene en caso seguir los procedimientos adecuados, los cuales pueden hacer empeorar la situación. Debido a lo anterior, también es buena práctica retomar estos temas y así los colaboradores tengan una idea de qué se tiene en la propia organización.

Para el objetivo 2. Identificar el estado actual de los conocimientos de seguridad informática mediante encuestas, evaluando qué tanto necesitan capacitación en esta área. Se concluye:

- Gracias al uso de encuestas, se realiza una colecta de información relevante, para ser analizada y poder entender cómo se encuentran los empleados en seguridad informática. Según lo investigado, la mayoría tiene conocimientos promedio e incluso avanzados, sin embargo, se tiene un alto porcentaje de personas quienes no tienen ese nivel, siguen siendo vulnerables sin importar su conocimiento, siempre se puede aprender más, tanto de la empresa como de seguridad informática. Es importante reforzar para mitigar lo más posible dicha situación. Mediante ello se puede determinar que si es necesario implementar metodologías de instrucción. En ellas se recomienda brindar información relevante sobre los diferentes tipos de amenazas las cuales los colaboradores pueden enfrentar en sus días laborales. Muchas de ellas se mencionan a lo largo de este trabajo. Siendo la ingeniería social uno de las más frecuentes en la actualidad.

Para el objetivo 3. Valorar las distintas amenazas que puede enfrentar en sus días laborales, mediante la explicación de ellas, evaluando su impacto y medios de mitigación. Se concluye:

- Es importante los colaboradores conozcan qué se puede enfrentar en sus ambientes de trabajo. Por eso es buena práctica tener un conocimiento base sobre el tipo de malwares existentes, ya sean, virus, gusanos, troyanos, spyware, adwares, ransomware, exploit y muchos más. La lista es larga, sin embargo, resulta bueno tener un entendimiento de cómo se puede ser infectado por uno de estos. Por otro lado, es importante saber cuáles son los pasos por seguir si uno se encuentra con una amenaza de estas y se materializa, qué hacer, cómo manejarlo y cómo minimizar el impacto. Es importante recalcar: toda esta información debe ser contemplada en las metodologías de instrucción, y así el conocimiento se transfiera a los miembros de la organización.

- Se recomienda usar páginas web como "ProWritters" (https://prowritersins.com/cyber-insurance-blog/top-10-cyber-security-threats/), "OWASP" (https://owasp.org/www-project-top-ten/), "Hybrid"(https://www.hybridtp.ie/top-10-cyber-security-vulnerabilities/) y "Cybersecurity Insiders" (https://www.cybersecurity-insiders.com/), pues contienen gran información sobre las principales amenazas que pueden enfrentar los colaboradores, al igual contienen noticias relevantes sobre la seguridad y pueden ser útiles para la organización. Identifican las tendencias en el riesgo cibernético para mantener informada y preparada la población.

- Cuando se tiene un entendimiento de esto, es más fácil a los colaboradores de la empresa poder tomar las medidas correspondientes, según el caso por enfrentar,

estos lo realizarán de manera calmada y con claridad para tener un mejor control. De tal manera se recomienda realizar una especie de examen con el fin de evaluar el conocimiento adquirido por las metodologías de instrucción de seguridad informática. Incorporando los distintos temas evaluados en el trabajo, su estado actual, información de los protocolos, leyes y controles vigentes en la organización y por supuesto, buenas prácticas de seguridad informática, valorando las posibles amenazas las cuales estos puedan enfrentar.

• Otra herramientas posible de usar, según se comenta en el trabajo es ”Phishing Quiz Google” (https://phishingquiz.withgoogle.com/), con el propósito de entrenar a los colaboradores en poder detectar phishing, ya sea en correos o en páginas web, minimizando la probabilidad de que ellos sean afectados, se recomienda trabajar estas habilidades por mecanismos parecidos. La información que se le puede brindar a los colaboradores, como poder identificar phishing, es un factor el cual sin duda mejoría la seguridad de la empresa y la de los empleados. Es importante analizar cada correo recibido para garantizar sean legítimos y confiables. Con ese se creó un diagrama para facilitar dicho análisis. De esta manera se puede tener una base para reducir los ataques de este medio.

XIV REFERENCIAS

Arellano, J., & Santoyo, M. (2009). *Investigar con Mapas Conceptuales Procesos metodológicos.* Madrid: 2009.

Berne, S., Frisén, A., & Berne, J. (2019). Cyberbullying in Childhood and Adolescence: Assessment, Negative Consequences and Prevention Strategies. 141. doi:10.1007/978-3-030-18605-0_10

Carey, S. (2018). Tendencias de nube pública para 2018. *computerworld*. Obtenido de https://www.computerworld.es/tecnologia/tendencias-de-nube-publica-para-2018

Computerworld. (2018). *Tendencias de nube pública para 2018*. Obtenido de https://www.computerworld.es: https://www.computerworld.es/tecnologia/tendencias-de-nube-publica-para-2018

Dikaiakos, M., Katsaros, D., Mehra, P., Pallis, G., & Vakali, A. (2009). Cloud Computing: Distributed Internet Computing for IT and Scientific Research. *IEEE Internet Computing*, 10-13. doi:10.1109/MIC.2009.103

FayerWayer. (2012). *El origen de: El Cómputo en la Nube*. Obtenido de https://www.fayerwayer.com: https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/

Hewlett Packard Enterprise. (s.f.). *¿QUÉ ES LA COMPUTACIÓN EN LA NUBE?* Obtenido de https://www.hpe.com: https://www.hpe.com/mx/es/what-is/cloud-computing.html

Hinduja, S., & Patchin, J. (2008). Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behavior*, 129-156. doi:10.1080/01639620701457816

Li, Q. (2010). Cyberbullying in High Schools: A Study of Students' Behaviors and Beliefs about This New Phenomenon. *Journal of Aggression, Maltreatment & Trauma*, 372-392. doi:10.1080/10926771003788979

McHugh, M., Saperstein, S., & Gold, R. (2018). OMG U #Cyberbully! An Exploration of Public Discourse About Cyberbullying on Twitter. *SAGE Journals*, 97-105. doi:10.1177/1090198118788610

Microsoft. (s.f.). *¿Qué es una nube pública?* Obtenido de https://azure.microsoft.com: https://azure.microsoft.com/es-es/overview/what-is-a-public-cloud/

Ministerio Trabajo Seguridad Social - Costa Rica. (2019). *Ministerio Trabajo Seguridad Social - Costa Rica*. Obtenido de http://www.mtss.go.cr/temas-laborales/salarios/Documentos-Salarios/Lista_Salarios_2019.pdf: http://www.mtss.go.cr/temas-laborales/salarios/Documentos-Salarios/Lista_Salarios_2019.pdf

Noticieros Columbia. (2 de mayo de 2020). *https://www.columbia.co.cr*. Obtenido de https://www.columbia.co.cr/noticias/tecnologia/17054-ciberbullying-el-acoso-que-puede-aumentar-en-cuarentena

Olweus, D., & Limber, S. (2017). Some Problems With Cyberbullying Research. *Current Opinion in Psychology*. doi:10.1016/j.copsyc.2017.04.012

Palladino, B., Nocentini, A., & Menesini, E. (2019). How to Stop Victims' Suffering? Indirect Effects of an Anti-Bullying Program on Internalizing Symptoms. *International Journal of Environmental Research and Public Health*, 2631. doi:10.3390/ijerph16142631

RedHat. (s.f.). *Red Hat Cloud Access*. Obtenido de https://www.redhat.com: https://www.redhat.com/es/technologies/cloud-computing/cloud-access

Sistema Nacional de Acreditación de la Educación Superior. (29 de Agosto de 2019). *SINAES*. Obtenido de https://www.sinaes.ac.cr/index.php/home/sobre-sinaes

Willard, N. (2007). cyberbullying and cyberthreats. Illinois: Research Press.

Woyke, E. (2017). *The Startup Behind NYC's Plan to Replace Phone Booths with 7,500 Connected Kiosks.* Obtenido de https://www.technologyreview.com/s/608281/the-startup-behind-nycs-plan-to-replace-phone-booths-with-7500-connected-kiosks/

www.semal.org. (17 de marzo de 2017). Obtenido de https://www.semal.org/es/component/k2/la-importancia-de-prevenir-el-bullying-y-ciberbullying