REVISTA ELECTRÓNICA SOBRE TECNOLOGÍA, EDUCACIÓN Y SOCIEDAD
ISSN: 2448 - 6493
CTES

Artículos científicos

Aplicación de buenas prácticas, un camino hacia la cultura de la seguridad informática en las instituciones públicas

Application of good practices, a path towards the culture of computer security in public institutions

Araceli Romero Romero*
Universidad Autónoma del Estado de México, México
aromeroruaemex@gmail.com
https://orcid.org/0000-0002-0328-0525

Michael Esperanza Gasca Leyva
Universidad Autónoma del Estado de México
michellegasley@yahoo.com.mx
https://orcid.org/0000-0002-4906-5628

Mayela Anita García Palmas
Universidad Autónoma del Estado de México, México
gmayela8107@gmail.com
http://orcid.org/0000-0001-7364-8199

Alejandro Hernández Suárez
Universidad Autónoma del Estado de México, México
ahsuaemex37@gmail.com
http://orcid.org/0000-0003-3958-5272

Resumen

García-Cervigón y Alegre (2011, p. 26) afirman que la seguridad Informática es una parte esencial dentro de las instituciones, la información es uno de los activos primordiales que puede llegar a tener un valor incalculable y por lo tanto se necesita ejercer su protección.

La presente investigación trasciende en hacer conciencia y darle el lugar de importancia que le corresponde a la cultura de seguridad de la información en las instituciones, si esto se logra, como consecuencia se va a contemplar su fortalecimiento, por esa razón se pretende fortalecer la cultura de la seguridad de la información a través de buenas prácticas que pueda ser aplicado en distintas organizaciones. Por lo tanto, beneficiar a las instituciones que quieran fortalecer su cultura de seguridad de la información, de primer momento a la organización pública en la cual se va a realizar el estudio, pero podrá ser aplicado por otras instituciones, adecuándolo a sus necesidades y tiene implicaciones trascendentes para poder resolver problemas prácticos.

Las empresas necesitan tener una infraestructura informática segura, que minimice los riesgos asociados con la seguridad. Los elementos que la seguridad de la información busca proteger son la información, los equipos que la soportan y las personas que la utilizan. Las personas son una parte esencial en la cadena de seguridad de la información, por tal motivo es importante que los empleados tomen conciencia sobre el manejo de la información de forma segura, siendo que de nada sirve cualquier sistema de seguridad, por complejo y completo que este sea, si los empleados llegan a compartir su usuario y contraseña con otras personas y con esto dejan abierta la puerta a posibles ataques o filtraciones de información.(Dussan, 2006)

Un instrumento que mide las dimensiones de la cultura de la seguridad de la información sostenidas en el trabajo de Alnatheer, autor que dio su autorización, instrumento basado el estándar ISO/IEC 27001:2013, además de aspectos importantes de COBIT 5 e ISO/IEC 17769 para el diagnóstico.

Para el presente trabajo se precisó el tamaño de la muestra, a través de la fórmula para realizar un muestreo aleatorio simple, proponiendo casos para un estudio cuantitativo de tipo descriptivo.

Con base a la información y resultados obtenidos, proporciona hallazgos que muestran fortalecimiento de la cultura de seguridad de la información mediante la aplicación de buenas prácticas, en este se desarrolla cada una de sus fases, entre las cuales se encuentran las estrategias y líneas de acción, derivadas del diagnóstico.

Palabras clave: *Seguridad informática, buenas prácticas, estándares de calidad*.

Abstract

García-Cervigón and Alegre (2011, p. 26) affirm that Computer security is an essential part within institutions, information is one of the primary assets that can have incalculable value and therefore it is necessary to exercise its protection.

The present investigation transcends in raising awareness and giving it the place of importance that corresponds to the culture of information security in the institutions, if this is achieved, as a consequence its strengthening will be contemplated, for that reason it is intended to strengthen the culture of information security through good practices that can be applied in different organizations. Therefore, to benefit the institutions that want to strengthen their information security culture, from the first moment to the public organization in which the study is going to be carried out, but it can be applied by other institutions, adapting it to their needs and has important implications for solving practical problems.

Companies need to have a secure computing infrastructure that minimizes the risks associated with security. The elements that information security seeks to protect are the information, the equipment that supports it, and the people who use it. People are an essential part of the information security chain, for this reason it is important that employees become aware of the safe handling of information, since any security system is useless, no matter how complex and complete it may be. that is, if the employees come to share their username and password with other people and with this they leave the door open to possible attacks or leaks of information. (Dussan, 2006)

An instrument that measures the dimensions of the information security culture sustained in the work of Alnatheer, author who gave his authorization, instrument based on the ISO/IEC 27001:2013 standard, in addition to important aspects of COBIT 5 and ISO/IEC 17769 for diagnosis.

For the present work, the size of the sample was specified, through the formula to carry out a simple random sampling, proposing cases for a descriptive quantitative study.

Based on the information and results obtained, it provides findings that show strengthening of the information security culture through the application of good practices, in which each of its phases is developed, among which are the strategies and lines of action. , derived from the diagnosis.

REVISTA ELECTRÓNICA SOBRE TECNOLOGÍA, EDUCACIÓN Y SOCIEDAD
ISSN: 2448 - 6493
CTES

Keywords: *Computer security, good practices, quality standards.*

Fecha Recepción: Diciembre 2022 **Fecha Aceptación:** Julio 2022

Introducción

Actualmente la tecnología sigue creciendo y cambiando de una manera exorbitante, al igual que los incidentes en seguridad, en los últimos días hemos escuchado términos como malware, ingeniería social, ransomware entre otros, dichos delitos cibernéticos tienen como elemento de entrada el factor humano.

Las tecnologías de la información están evolucionando constantemente en periodos de tiempo muy cortos, pero no podemos decir que vaya evolucionando de la misma manera la seguridad en el manejo de la tecnología. Los investigadores de ESET (Enjoy Safer Technology) en su trabajo Tendencias 2017: La seguridad como Rehén, mencionan que los tipos de amenazas han tenido una evolución y han cambiado con el tiempo, pero tienen como factor común al usuario como punto de entrada, nos dice que "los atacantes siguen encontrando en el comportamiento inocente y en muchos casos irresponsable de los usuarios la posibilidad de comprometer la seguridad de un sistema".

La importancia y el valor que tiene la información tanto para las instituciones, profesionales y ciudadanos. Las instituciones preocupadas por la seguridad de su información han implantado sistemas de seguridad física y lógica, pero han dejado de lado el factor humano, el cual muchos autores refieren como el eslabón más débil de la cadena.

La investigación presenta el tema "cultura de la seguridad de la información", permite fortalecer la cultura de la seguridad de la información y con esto robustecer la seguridad de la información en un organismo público.

Un universo de estudio de 400 empleados mientras la muestra se calculó a través de la fórmula para realizar un muestreo aleatorio simple, considerando un nivel de confianza del 95% y un margen de error del 6.69%, proponiendo 140 casos del universo como tamaño mínimo de muestra para un estudio cuantitativo de tipo descriptivo. El instrumento de medición que se utilizó en el presente trabajo de investigación, contiene reactivos manejados en los trabajos de ALNATHEER (2012) para medir la cultura de la seguridad de la información.

Aunado a lo mencionado, en esta investigación se tratará de dar respuesta al problema de cómo fortalecer la cultura de seguridad de la información a través de la aplicación de buenas prácticas en un organismo público.

Seguridad de la información

La seguridad es "un estado de bienestar, es la ausencia de riesgo por la confianza que existe en alguien o algo". Lo que busca la seguridad es gestionar los riesgos para realizar acciones con la finalidad de evitar o prevenir situaciones de la mejor forma. (Romero Castro et al., 2018, p. 13)

ESET (Enjoy Safer Technology) compañía de seguridad informática explica que la seguridad no es solamente la implantación de soluciones tecnológicas si no que hay que poner atención en el componente humano, por lo cual el foco debe dirigirse a la concientización de usuarios, siendo que los atacantes aprovechan la falta de conocimiento de los usuarios para obtener sus ganancias.

La información es un activo que tiene valor para los procesos de negocio de la empresa ya que ayuda a satisfacer sus objetivos y es crítica para su desempeño y subsistencia. (Miguel Pérez, 2015, p. 236) "La información se considera como el oro de la seguridad informática, es lo que se debe de proteger, es el principal activo". (Romero Castro et al., 2018, p. 14)

La seguridad de la información puede ser definida como "el conjunto de medidas preventivas y reactivas que las instituciones deberán generar y aplicar: políticas, normas, procedimientos, evaluar el riesgo, planes de contingencias, entre otras medidas, con el objetivo de mantener y asegurar la confidencialidad, integridad y disponibilidad de la información"(Sampedro Guamán, Carlos Roberto, Machuca Vivar, Silvio Amable, Palma Rivera, Diego Paúl, & Carrera Calderón, Franks Alberto, 2019, p. 421)

"La seguridad no es un producto, es un proceso; por tanto, la seguridad no puede comprarse, pero puede gestionarse." (Miguel Pérez, 2015, p. 242)

“La Seguridad de la Información tiene una significativa relevancia corporativa porque tiene como objeto proteger un activo extremadamente importante y porque existe una amplia regulación que obliga a las compañías a proveer Seguridad de la Información”(Parra, 2010, p. 7) por lo tanto no pueden ser cumplidos los objetivos del Gobierno Corporativo sin proteger la información de la perdida, la alteración no autorizada y de la revelación inapropiada. (Parra, 2010, p. 4)

Es importante evaluar la seguridad informática continuamente ya que "a medida que cambian los factores internos y externos, controles que una vez resultaron idóneos y efectivos pueden dejar de ser adecuados". (Piattini Velthuis & Peso Navarro, 2001, p. 42)

Los principales pilares de la seguridad de la información son: integridad, disponibilidad y confidencialidad, si alguno de estos pilares se debilita se perdería la seguridad o usabilidad, si falta alguno de los lados, la organización queda expuesta a ataques. (Romero Castro et al., 2018, p. 25) como lo son: la confidencialidad, integridad y disponibilidad.

Cuando se habla de la seguridad de la información, poco se escucha mencionar acerca de la cultura de la seguridad de la información, diferentes autores mencionan que las fuerzas o aquello que se genera a través de la cultura es algo muy poderoso, que nos ayuda a definir a que le debemos prestar atención, cómo se puede reaccionar a ello y las acciones que debemos tomar, por lo tanto esta inquietud me lleva a estudiar los beneficios que nos puede dar el generar por medio del fortalecimiento de la cultura de seguridad de la información en las instituciones, el minimizar los riesgos en la seguridad de la información, por ejemplo, el generar que a una persona de una organización, al llegarle un correo fraudulento o estar en riesgo de atentar contra la seguridad, a través de la creación de esa fuerza generada por la cultura de seguridad de la información, sea capaz de prestar atención, poder reaccionar a ello y actuar de una manera adecuada, además de ir generando esas historias compartidas.

En algunas instituciones he podido observar, que el personal no es tomado en cuenta en el plan de seguridad de la información, si es que existiera uno, y si es tomado en cuenta, solo es para memorizar respuestas con la finalidad de cumplir con una auditoria, en esta era donde la tecnología va evolucionando constantemente y a su vez va evolucionando la delincuencia informática, es un riesgo ignorar todo lo que está sucediendo a nuestro alrededor y no implementar acciones para minimizar los riesgos en la seguridad de la información, por tal motivo es conveniente realizar esta investigación, porque va a ayudar a confirmar el valor que tiene la toma de decisiones de las personas en la seguridad de la información en la organización, lo que lleva al estudio de la importancia de fortalecer la cultura de seguridad de la información y dar una respuesta a como poder fortalecerla a través de buenas prácticas.

Por otro lado, un sistema de gestión de la seguridad de la información SGSI es el encargado de mantener la confidencialidad, integridad y disponibilidad de la información, entregando confianza a las partes interesadas. (Norma ISO 27001:2013)

"La norma ISO 27001 proporciona una guía para construir un SGSI sólido, estable y reconocido a escala internacional". (Miguel Pérez, 2015, p. 255)

Los elementos básicos del estándar son: las cláusulas de requisitos y los controles de seguridad. Consideran controles que se aplican previo a los incidentes, elementos proactivos

para mantener la continuidad del negocio, la seguridad ofensiva, como la gestión de vulnerabilidades y enfoques reactivos referente a la gestión de incidentes.

"COBIT 5 para seguridad de la información", es un documento dentro de la familia COBIT, especializado en la seguridad de la información, en el plantea la seguridad de la información como una disciplina transversal, lo cual quiere decir que esta se debe tomar en cuenta en cada actividad y proceso desempeñado.(COBIT para la seguridad en las instituciones, 2015)

La cultura de la seguridad de la Información positiva, es una estrategia para guiar el comportamiento de seguridad de los empleados en las instituciones. (Nasir, Arshah, & Hamid, 2019, p. 55),

Como se cita en "Conceptualización de una Estrategia de Ciberseguridad para la Seguridad Nacional de México" Romero (2018) la ciberseguridad se define como "la colección de herramientas, políticas, conceptos de seguridad, salvaguardas, guías, enfoques de gestión de riesgos, acciones, entrenamiento, mejores prácticas, seguridad y tecnologías, que pueden ser usadas para proteger los activos de la organización y de los usuarios dentro del ciberespacio"

El cibercrimen son los delitos cometidos a través de internet como el "robo de identidad, las estafas online, el scareware, el fraude fiscal, el robo de negocios, la extorsión, el robo de datos de clientes, el espionaje industrial y el robo de propiedad intelectual", entre otros. (Jiménez, 2020). Estos son dirigidos principalmente a sujetos privados. (Villamil, Jara, Venegas, & Aguilar, 2020)

Las políticas de seguridad "son los documentos que respaldan los compromisos adquiridos, prácticas a ejercer, o bien las normas que determinan la conducta y comportamiento de los miembros de las instituciones con la relación al manejo y cuidado de los datos". ("Guías, procedimientos y otros componentes de las políticas de seguridad", 2016)

"Las políticas se enfocan hacia resultados deseados y no hacia la manera de lograrlos. Deben orientarse al qué y no al cómo". ("Guías, procedimientos y otros componentes de las políticas de seguridad", 2016)

Se debe tomar en cuenta que "el proceso de formulación de políticas de seguridad debe centrarse en el comportamiento de los empleados. Un profesional de seguridad debe recordar que el desempeño de los empleados está orientado a objetivos". (Zinatullin, 2016, p. 68)

Después de la breve revisión de algunos conceptos indispensables, es necesario resaltar la importancia de la cultura en la seguridad de la información, y como dice Sampedro Guamán, Carlos Roberto et al. (2019, p. 423) "La seguridad de la información es una prioridad en esta

era digital. Así mismo, es relevante concienzar a los involucrados en el uso correcto de este sistema integral".

Cultura de la Seguridad de la Información en una Institución Pública

"La cultura es una abstracción, pero las fuerzas que se crean en situaciones sociales y organizativas derivadas de la cultura son poderosas." (Schein, 2010, p. 7)

Schein (2010, p. 18) define la cultura de un grupo como "un patrón de supuestos básicos compartidos, aprendido por un grupo al resolver sus problemas de adaptación externa e interna, integración que ha funcionado lo suficientemente bien como para ser considerada válida y, por tanto, que se les enseñe a los nuevos miembros la forma correcta de percibir, pensar y sentir en relación con esos problemas".

La ampliación del dominio cultura organizacional se debe a que las ocupaciones son más técnicas y complejas, por lo tanto las culturas ocupacionales son más diferenciadas y es más complicado coordinarlas en una organización; también se debe a que la tecnología está en constante cambio y ha ayudado a crear redes en el mundo, lo cual ha impactado en las formas de trabajo, esto implica un cambio en la interacción humana, otro motivo es la globalización que ha permitido la interacción entre varias macroculturas en una organización. (Schein, 2010, p. 4)

Por tal motivo un área de oportunidad es medir la cultura de la seguridad de la información en la dependencia de Gobierno, con la finalidad de dar un diagnóstico y tener la posibilidad en base a buenas prácticas fortalecer la cultura de la seguridad de la información. "Ser consiente del valor que tiene tu información es el primer paso para comenzar a protegerla". ("Redes sociales", 2018)

Nasir, Arshah, & Hamid (2019, p. 57) en su trabajo "A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions", citan a la Cultura de la Seguridad de la Información como "un patrón compartido de valores, modelos mentales y actividades que se intercambian entre los miembros de una organización utilizados a lo largo del tiempo, afectando la seguridad de la información", otra definición es "el conjunto de percepciones, actitudes, valores, supuestos y conocimientos que guían a los seres humanos al interactuar con los activos de información en una organización con el objetivo de influir en el comportamiento de los empleados para preservar la seguridad de la información".

La cultura de la seguridad de la información es una cultura que enfatiza sobre la seguridad de los activos de información, mejorando el comportamiento de seguridad de la información de los empleados y promoviéndolo, por lo tanto, contribuye al logro de los objetivos generales de la organización. (Nasir et al., 2019, p. 56)

Para los usuarios las políticas de seguridad son sólo actividades engorrosas que interrumpen su productividad, por lo tanto, ellos sienten un impacto negativo hacia estas, porque los mecanismos agotan su tiempo y esfuerzo, por lo tanto, si esto afecta al cumplimiento de su tarea principal siempre van a justifica el riesgo. (Zinatullin, 2016, p. 66)

"El uso de herramientas tecnológicas es un proceso cultural, en el sentido que las personas desconocen los riesgos que vienen de su uso. De hecho las fallas de seguridad o la pérdida de información, la mayoría de las veces obedecen al desconocimiento de los riesgos que conlleva el uso inadecuado de las mismas por parte de los mismos operadores de la organización" (Velasco Melo, 2008, p. 353)

Un “Plan” es definido como un “escrito en que sumariamente se precisan los detalles para realizar una obra”, también lo define como un “modelo sistemático de una actuación pública o privada, que se elabora anticipadamente para dirigirla y encauzarla”. (ASALE & RAE, s/f)

De acuerdo a Martínez (2001, p. 284) plan estratégico es “un conjunto de elementos y/o conceptos que orientan, unifican, integran y dan coherencia a las decisiones que dan rumbo y destino a una organización, departamento o unidad.

Actualmente, en el tema de seguridad, en una dependencia de gobierno resulta ser robusta en cuanto a seguridad perimetral robusta, ya que cuenta con equipos de marcas reconocidas a nivel mundial, configuraciones de seguridad en sus equipos de alta gama, tiene implementados antivirus en los equipos de los usuarios, elaboraron un documento de políticas y lineamientos para los equipos de cómputo, servicios de red, internet y correo electrónico.

Se manejan cuentas de correo institucionales con un proveedor de talla mundial, en dicha plataforma se tienen configuradas políticas para protección de correo, pero solo un porcentaje de los servidores públicos tienen una cuenta institucional, los demás utilizan cuentas gratuitas de correo electrónico para realizar sus labores, por tal motivo esas políticas solo blindan a cierto porcentaje de la población, dicho esto, es necesario generar un cultura en la seguridad de la información que les permita a los usuarios tener las precauciones necesarias en el uso de herramientas tecnológicas y no estar siempre a expensas de que venga el blindaje por el área de Tecnologías de la información.

En muchas ocasiones, los empleados no son conscientes de que sus acciones tienen un impacto directo en la seguridad de la información, esto puede solucionarse si se logra influenciar el comportamiento de los empleados para cumplir con la política de la seguridad. (Alnatheer, 2012, p. 61)

El cumplimiento de la seguridad es posible mejorarla a través de programas de concientización de seguridad donde también puedan los empleados comprender los posibles riesgos, la participación de la alta gerencia con conciencia y educación, la evaluación del cumplimiento leyes y regulaciones aplicables, un monitoreo constante. (Alnatheer, 2012, p. 61)

Derivado de las incidencias solventadas por el equipo de soporte técnico como: los restablecimientos de contraseña, recuperación de información, virus, suplantación de correo electrónico, phishing, entre otras, se pretende analizar y estudiar la mitigación de los riesgos de seguridad a través de la cultura.

Metodología

El enfoque elegido para esta investigación es el enfoque cuantitativo, el cual se basa en investigaciones previas, y consiste en la medición de variables de investigación, se utiliza para consolidar las creencias y establecer con exactitud patrones de comportamiento de una población. (Hernández, 2014, p. 10).

El alcance de la investigación es el descriptivo, cuyo objetivo es indagar para especificar propiedades y características de algún fenómeno (Hernández, 2014, p. 92,93), por lo tanto se pretende medir y recoger información de las dimensiones de la variable cultura de la seguridad de la información, en un organismo público en el Estado de México, con la finalidad de diagnosticarlo y poder establecer un plan estratégico que fortalezca la cultura de la seguridad de la información a través de buenas prácticas.

El diseño de la investigación es no experimental, ya que no se va a realizar alguna manipulación en las variables, solo se va a observar los fenómenos en su ambiente natural. (Hernández, 2014, p. 185), será de tipo transeccional o transversal puesto que la recolección de datos se realizará en un solo momento. (Hernández, 2014, p. 187)

Se utilizaron como técnicas de recolección de datos la revisión bibliográfica, y la recolección de datos a través de un instrumento de medición aplicado en el lugar de estudio.

La revisión y actualización de la política de la seguridad de la información se debe de contemplar mediante un ciclo de vida para elaboración y actualización de la política de la seguridad de la información además de la integración de políticas de conducta ética.

Para la implementación de la política de seguridad de la información, es de vital importancia tener el apoyo de la Alta Dirección.

El Gerente de la seguridad de la información (ISM) tendrá la responsabilidad de que se haga la revisión y actualización de la política de seguridad de la información.

El Equipo de investigación y desarrollo en seguridad de la información (EIDSI) con base en su conocimiento revisa y actualiza la política.

Se debe tener el compromiso administrativo y organizativo para su implementación.

Es necesarios realizar una revisión y adecuación de la política de seguridad de la información.

En la política se debe incluir:

1. Las personas que aprueban la política, se sugiere que sea la Alta dirección, el Comité de Gerentes de unidad.
2. Las consecuencias de no cumplir la política.
3. La manera de cómo se medirá el cumplimiento de la política.
4. Agregar políticas de conducta ética.

Apoyo Documental

Para la actualización de las políticas es conveniente revisar el ISO 27001:2013 en su apartado "Anexo A OBJETIVO DE CONTROL Y CONTROLES"

Elementos que deben tomar en cuenta al revisar y actualizar la política:

- La política debe estar adecuada al propósito de la organización.
- La política de incluir los objetivos de la organización en cuanto a seguridad de la información.
- Debe centrarse en el comportamiento de los empleados.
- Se tienen que considerar las necesidades del usuario.
- Evitar implementar controles innecesarios que entorpezcan las actividades de las personas en la organización.
- Tomar en cuenta aspectos internos de la organización en los que existan riesgos en los que participan los empleados.
- Proporcionar en la implementación de una política valores y prioridades de los empleados.

- Contemplar que las políticas que se generen no afecten al cumplimiento de sus tareas principales, es decir llegar a un equilibrio de seguridad de la información evitando el entorpecimiento de las tareas diarias de cada persona
- En caso de ser necesarias, proporcionar las herramientas necesarias para cumplir con la política de la seguridad.
- Considerar agregar políticas de conducta ética, donde se establezcan claramente las acciones que son éticas y las que no son éticas.
- Se debe crear una visión compartida y una comprensión de cómo se usarán diversos controles.

Ciclo de vida de la política

La política de seguridad debe de tener un ciclo de mejora continua permanente. A continuación, se muestra una propuesta del ciclo de vida de la política y las partes interesadas que participan en cada etapa.

Procedimiento de recolección de datos

La muestra se define como un "subgrupo del universo o población del cual se recolectan los datos y que debe ser representativa de ésta" (Hernández, 2014, p. 206), su aplicación nos ayuda a economizar tiempo y recursos, la población se debe delimitar para poder generalizar resultados y establecer parámetros. (Hernández, 2014, p. 171)

Se realizó una muestra de clase probabilística la cuál es esencial en los diseños de investigación transeccional descriptivo. (Hernández, 2014, p. 177). Los tipos de muestra dependen del tamaño de la muestra y el proceso de selección. Las unidades de análisis deben ser seleccionados siempre de manera aleatoria, para que cada elemento tenga la probabilidad de ser elegido (Hernández, 2014, p. 216),

Para el presente trabajo de investigación se precisó el tamaño de la muestra, de un universo de estudio de 400 empleados. La muestra se calculó a través de la fórmula para realizar un muestreo aleatorio simple, considerando un nivel de confianza del 95% y un margen de error del 6.69%, proponiendo 140 casos del universo como tamaño mínimo de muestra para un estudio cuantitativo de tipo descriptivo. (Hernández, 2014, p. 178-179 y 184)

Con el diagnostico que se realizó se pudo concluir que existe una amplia área de oportunidad en fortalecer los componentes que influyen en la cultura de seguridad de la información, como lo es el apoyo y compromiso de la alta dirección, en cada una de las etapas como lo es

la generación de políticas, proveer los recursos necesarios (humanos y materiales), apoyar en los programas de concienciación y capacitación, dar el ejemplo de cultura hacia todo el personal, entre otros. La política de seguridad es una pieza importante en la cultura, tanto la elaboración, actualización, como la comunicación de esta hacia el personal, de acuerdo a los hallazgos encontrados, es necesario actualizar la política y comunicarla de una manera adecuada, pues se encontró un gran porcentaje del personal que no tiene conocimiento de esta. También se encontró que un alto porcentaje del personal se siente responsable de proteger su información, pero aún no son conscientes y no saben que ellos también deben conocer y aplicar técnicas de seguridad de la información y no solo el área de tecnologías; también se encontró un alto porcentaje del personal que no cuenta con conocimientos básicos en seguridad de la información o temas actuales en seguridad de la información, lo cual se reafirma porque se encontró que no se han realizado programas para concientizar, capacitar y dar a conocer la política, lo cual lo convierte en un área de oportunidad.

El instrumento de medición que se utilizó en el presente trabajo de investigación, contiene reactivos manejados en los trabajos de ALNATHEER (2012) para medir la cultura de la seguridad de la información; para la medición de la seguridad de la información, se elaboraron reactivos basados en los estándares ISO 27001 e ISO 17769.

Análisis y resultados

Para el presente trabajo se propone el indicador 1 e indicador 2, tomado del trabajo de ALNATHEER (2012), el indicador 3 se agregó y adecuo para conocer la aplicación y conocimiento de algunas buenas prácticas base en seguridad de la información, a continuación, se realiza la descripción de las dimensiones e indicadores:

Tabla 1. Tabla de dimensiones e indicadores

DIMENSIONES	INDICADORES
Dimensión 1 Grado de Cultura de la Seguridad de la Información	Indicador 1 Grado de conocimiento en los factores que constituyen la cultura de la seguridad de la información: Conciencia de la seguridad, Cumplimiento de la Seguridad, Propiedad de la seguridad.
	Indicador 2 Grado de conocimiento en los factores que influyen en la cultura de la seguridad de la información: Alta dirección en la seguridad de la información, Aplicación de la política de la seguridad de la información, Mantenimiento de las políticas, Entrenamiento y capacitación en la seguridad de la información, Políticas de conducta ética.
	Indicador 3 Grado de conocimiento en la aplicación de seguridad de la información en base a los estándares ISO 27001 e ISO 17769.

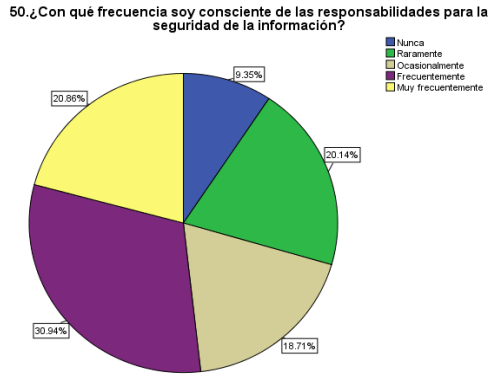
Fuente: Elaboración propia 2021

Los factores que constituyen la cultura de la seguridad de la información son la conciencia de la seguridad, cumplimiento de la seguridad y la propiedad de la seguridad.

Con respecto a la variable cultura de la seguridad de la información, en su dimensión conocimiento de la cultura de la seguridad de la información de la dependencia de gobierno, Indicador 1, que se refiere a los factores que constituyen la cultura de la seguridad de la información se encontró lo siguiente:

Con respecto a la *conciencia de la seguridad*, el 30.94% de las personas frecuentemente son conscientes de las responsabilidades para la seguridad de la información, el 20.86% dice que muy frecuentemente, el 18.71% ocasionalmente, por otro lado, el 20.14% raramente y el 9.35% nunca es consciente.

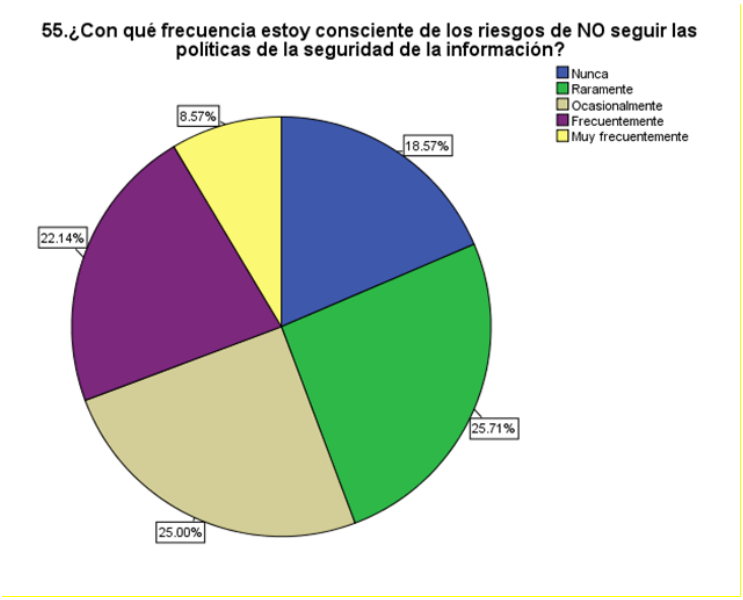
Gráfica 1. Conciencia de la seguridad



Fuente: Elaboración propia 2021

Al preguntarles acerca de que tan frecuente están conscientes de los riesgos de no seguir las políticas de la seguridad de la información el 25.71% raramente está consciente, el 18.57% comenta que nunca esta consciente, el 25% ocasionalmente, tan solo el 8.57% muy frecuentemente y el 22.14% frecuentemente está consciente.

Gráfica 2. Frecuencia de Consiencia de riesgos



Elaboración propia 2021

Con respecto al cumplimiento de la seguridad de la información y preguntarles a las personas la frecuencia con la que se adhieren a las políticas de seguridad de la información, el 31.43% contestaron que frecuentemente, solo el 15% lo hace muy frecuentemente, por otra parte, el 23.57% dice que raramente lo hace, 15.71% dice que nunca lo hace y el 14.29% ocasionalmente.

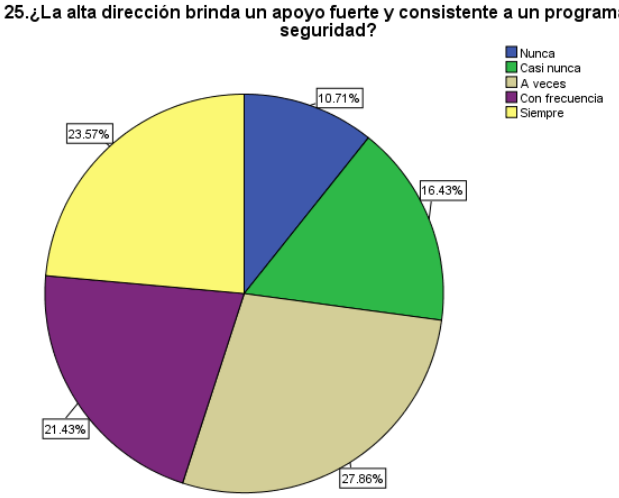
Más del 50% de las personas están conscientes de su responsabilidad en el tema seguridad de la información, pero al cuestionarlas acerca de su nivel de consciencia en cuanto políticas de seguridad, hubo una reducción en el porcentaje. También se observa que existe un área de oportunidad en la liberación de un programa de concientización en el tema de seguridad de la información, para que esa conciencia de responsabilidad que ya tienen las personas, pueda ser cumplido, y aquellas que aún no lo tienen o es menor, encuentren su nivel de responsabilidad y consciencia.

Gráfica3. Cumplimiento de la Seguridad de la Información

Fuente: Elaboración propia 2021

Analizando los ítems relacionados a la alta dirección en la seguridad de la información se encontró que el 23.57% considera que la alta dirección siempre brinda un apoyo fuerte y consciente en un programa de seguridad, el 21.43% piensa que, con frecuencia, el 27.86% dice que a veces, el 16.43% casi nunca y el 10.71% nunca.

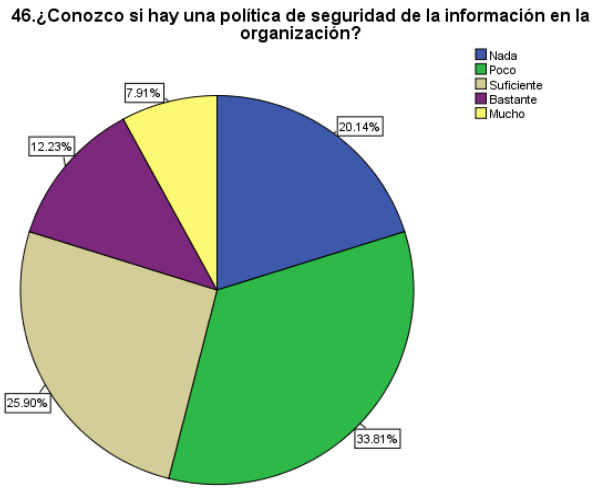
Gráfica 4. Alta dirección en la seguridad de la información



Fuente: Elaboración propia 2021

Entre los ítems que se refieren a la aplicación de la política de la seguridad de la información se preguntó si conocían si hay una política de seguridad de la información en la organización el 20.14% no conocen, el 33.81% conocen poco, el 25.90% suficiente, el 12.23% conocen bastante y el 7.91% mucho.

Gráfica 5. Aplicación de la política de la seguridad de la información



Fuente: Elaboración propia 2021

Existe un área de oportunidad para poder generar una cultura positiva de la seguridad de la información y así fortalecer la seguridad. Considerando los resultados obtenidos en el tema de conciencia, se puede trabajar en concientizar al personal en el tema de seguridad de la información, realizando un plan estructurado que pueda traspasar esa conciencia para que el personal pueda actuar con un alto grado de conciencia al realizar sus tareas diarias y encausar

a que se realice de una manera natural. Una ventaja que se encontró es que las personas tienen esa pertenencia de proteger la información posiblemente por la naturaleza de la dependencia, o el tipo de información que se maneja.

A partir de los resultados arrojados, se sugirió determinar los objetivos para fortalecer la cultura de la seguridad de la información a través de buenas prácticas en la dependencia de gobierno estudiada; para la elaboración de este plan estratégico se tomó como base el marco de trabajo COBIT 5, la norma ISO 27001:2013.

Como se mencionó anteriormente los factores que influyen a la cultura de la seguridad de la información son la Alta dirección en la seguridad de la información, Aplicación de la política de la seguridad de la información, Mantenimiento de las políticas, Entrenamiento y capacitación en la seguridad de la información y Políticas de conducta ética.

La alta dirección es factor esencial para contribuir en la cultura, como área de oportunidad se encuentra el apoyo para ofrecer un programa en el cual se considere una buena formación de seguridad de la información incluyendo el conocimiento de la política de la seguridad de la información, considerando a la totalidad del personal, así como el supervisar para garantizar el cumplimiento.

Se encontró en cuanto al tema de responsabilidad en los aspectos de seguridad de la información, es posible que un grupo alto de personas no se consideran ellas mismas dentro de esas personas apropiadas responsables para ejecutar aspectos específicos en la seguridad de la información, ya que un alto porcentaje de las personas consideran que existía un programa efectivo de concientización para la seguridad de la información, pero a la vez un porcentaje muy alto no conocen la política.

Es esencial considerar la concientización de las personas, a través del entrenamiento y capacitación de la seguridad de la información, el conocimiento de las políticas de seguridad, para que conozcan sus responsabilidades y de qué manera ellos pueden proteger la información y de esta manera llegar al cumplimiento.

Discusión

La aplicación de buenas prácticas en un organismo público, logrado a partir del diagnóstico generado a través del instrumento que fue aplicado, el cual contiene las dimensiones que constituyen e influyen la cultura de seguridad de la información, mismo que sirvió para localizar las estrategias que se deben emplear para lograr la misión y visión del plan estratégico, teniendo estas estrategias, y con certeza fue posible desarrollar la línea de acción con base a buenas prácticas, como lo son del estándar ISO 27001 y el marco de trabajo COBIT 5, que son elementos internacionales que apoyan de forma estandarizada al cumplimiento del objetivo.

La finalidad de estas estrategias es que los empleados lleguen a un estado de conciencia "Inconscientemente-Competente", y una apropiación de la seguridad de la información y cumplimiento.

Conclusiones

La propuesta emanada de esta presente investigación puede tomarse como base y adecuarse para ser utilizado en otras Instituciones. Se debe mencionar, que el instrumento de medición ayudó a diagnosticar la cultura de seguridad de la información, por lo tanto se puede aplicar en otras organización para realizar su diagnóstico, y se recomienda en el indicador "aplicación de seguridad de la información en base a los estándares ISO27001 e ISO 17769", adecuar los ítems con temas que se requiera que conozca el personal de la organización acerca de los controles de seguridad de la información o amenazas en seguridad nuevas en el mercado, y apoyado de esta información poder adecuar la política y el programa de concienciación, capacitación y entrenamiento.

Las estrategias que fueron desarrolladas se basan en crear una estructura, con personal que cuente con los conocimientos necesarios para poder realizar las tareas en seguridad; otra estrategia es actualizar la política añadiendo políticas de conducta ética y considerando su actualización de forma permanente continua; y la última estrategia realizar un programa de concienciación, capacitación y conocimiento de la política, todo esto debe ser apoyado por la alta dirección.

Futuras Investigaciones

La cultura de seguridad de la información nos lleva a pensar en lo importante que es que las instituciones concienticen y dé herramientas al personal que labora con ellos siendo que esto conlleva a implantar poder implementar un programa en busca del fortalecimiento. Siendo el objetivo que las instituciones tengan una infraestructura informática segura mediante estrategias como el proteger la información, los equipos donde se soportan y las personas que los van a utilizar por ello siempre será necesario seguir investigando acerca del tema desde la estructura de la institución y sus roles, así como hacer mejoras en las estrategias de capacitación del personal y llevarlos a la práctica, generando conciencia sobre el buen manejo de la información de forma segura.

Referencias

Alnatheer, M. A. (2012). Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia.

ASALE, R.-, & RAE. (s/f). Plan | Diccionario de la lengua española. Recuperado el 26 de septiembre de 2021, de «Diccionario de la lengua española»—Edición del Tricentenario website: https://dle.rae.es/plan

COBIT para la seguridad en las organizaciones. (2015, agosto 4). Recuperado el 26 de septiembre de 2021, de WeLiveSecurity website: https://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

Dussan, C. A. (2006). Políticas de seguridad informática. Entramado, 2(1), 86–92.

El ciclo de vida de las políticas de seguridad. (2014, agosto 18). Recuperado el 4 de febrero de 2020, de WeLiveSecurity website: https://www.welivesecurity.com/la-es/2014/08/18/ciclo-de-vida-de-las-politicas-de-seguridad/

García-Cervigón Hurtado, A., & Alegre Ramos, M. del P. (2011). Seguridad informática Sistemas microinformáticos y redes: [Informática y comunicaciones. Madrid: Paraninfo.

Guías, procedimientos y otros componentes de las políticas de seguridad. (2016, febrero 3). Recuperado el 4 de febrero de 2020, de WeLiveSecurity website: https://www.welivesecurity.com/la-es/2016/02/03/guias-procedimientos-politicas-de-seguridad/

Hernández, S. R., Fernández, C. C. y Baptista, L. P. (2014). *Metodología de la Investigación*. (6a ed.). México: McGraw-Hill.

ISO27001:2013 “Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos”

Jiménez, D. L. (2020). Recensión. Derecho de daños tecnológicos, ciberseguridad e Insurtech. PAAKAT: revista de tecnología y sociedad, (19). Recuperado de https://www.redalyc.org/journal/4990/499069742008/

Nasir, A., Arshah, R. A., & Hamid, M. R. A. (2019). A dimension-based information security culture model and its relationship with employees’ security behavior: A case study in Malaysian higher educational institutions. Information Security Journal: A Global Perspective, 28(3), 55–80. https://doi.org/10.1080/19393555.2019.1643956

Martínez, T. E. A. (2001). Metodología para elaborar un plan estratégico y rediseño organizacional de una unidad de producción agropecuaria. Revista Mexicana de

Agronegocios, V(9). Recuperado de https://www.redalyc.org/articulo.oa?id=14100903

Miguel Pérez, J. C. (2015). Protección de datos y seguridad de la información: Guía práctica para ciudadanos y empresas. Madrid: Ra-Ma.

Parra, C. F. R. (2010). Seguridad De La Información: Estrategia Para Fortalecer El Gobierno Corporativo. Revista de Derecho Privado, (43), 3–24.

Piattini Velthuis, M. G., & Peso Navarro, E. del. (2001). Auditoría informática: Un enfoque práctico. México D.F.; Madrid Ra-Ma: Alfaomega ;

Redes sociales: El valor de la información personal y la responsabilidad de los usuarios. (2018, marzo 21). Recuperado el 31 de enero de 2020, de WeLiveSecurity website: https://www.welivesecurity.com/la-es/2018/03/21/redes-sociales-valor-informacion-responsabilidad-usuarios/

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., … Castillo Merino, M. A. (2018).Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Científica 3Ciencias.

Sampedro Guamán, Carlos Roberto, Machuca Vivar, Silvio Amable, Palma Rivera, Diego Paúl, & Carrera Calderón, Franks Alberto. (2019). Percepción de seguridad de la información en las pequeñas y medianas empresas en santo domingo. 40, 421–428.

Schein, E. H. (2010). Organizational culture and leadership (4th ed). San Francisco: Jossey-Bass.

Velasco Melo, A. H. (2008). El derecho informático y la gestón de la seguridad de la información una perspectiva con base en la norma iso27001. Revista de derecho, (No. 29), 366.

Villamil, X. A. C., Jara, M. L. B., Venegas, J. C. P., & Aguilar, J. A. Q. (2020). Ciberseguridad y ciberdefensa en Colombia: Un posible modelo a seguir en las relaciones cívico-militares. Revista Científica General José María Córdova, 18(30), 357–377.

Zinatullin, L. (2016). The psychology of information security: Resolving conflicts between security compliance and human behaviour. Recuperado de http://www.books24x7.com/marc.asp?bookid=112006