República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

Facultad de Estudio de Posgrados

Tesis en opción al título de Magister en:

Sistemas de Información Gerencial

Tema:

ANÁLISIS Y DESARROLLO DE UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE IDIOMAS BUCKINGHAM ENGLISH CENTER S.A.

Autor:

Ing. Carlos Ernesto Mora Farfán

Directora de Tesis:

Lcda. Grace Viteri Guzmán, MSc.

MARZO - 2021

Guayaquil – Ecuador

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta tesis de Maestría me corresponde exclusivamente, y el patrimonio intelectual del mismo a la “UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL - UTEG”

Ing. Carlos Ernesto Mora Farfán

CI. 091832588-7

DEDICATORIA

El presente trabajo va dedicado a Dios, mis abuelos, mis padres y a mi novia. A Dios por darme la fortaleza de seguir adelante, a mis abuelos Hugo Humberto Farfán Miranda, que desde el cielo me cuida y Cruz Violeta Paredes Egas, que con mucho cariño ha velado por mi bienestar, a mis padres Alfonso Gerardo Cabrera Flores y Leova Margarita Farfán Paredes, que con mucho amor me guiaron por el sendero correcto de la vida dándome apoyo incondicional en cada instante de mi vida, a mi novia Estrella Mariby Cantos Merelo, que con su amor, comprensión y permanencia a mi lado en todo supo darme aliento para poder llegar a la meta final lograda. Es por ello y mucho más que lo que soy ahora se los debo a ellos, los amo.

AGRADECIMIENTO

Los resultados del presente trabajo, son gracias a todas aquellas personas que de alguna forma, fueron parte de su inicio, desarrollo y culminación. Los sinceros agradecimientos están dirigidos en primer lugar a Dios por darme la fortaleza de haber terminado esta meta, en segundo lugar a todas las autoridades de la Universidad Tecnológica Empresarial de Guayaquil “UTEG”. Por último a mis abuelos, a mis padres y a mi novia, a los docentes que impartieron su valioso conocimiento y a mi asesora de proyecto de tesis quien me ayudó en todo momento con su apoyo, MSc. Grace Viteri Guzmán.

RESUMEN

El presente estudio se orientó al análisis y desarrollo de un modelo de gestión de seguridad de la información para el Centro de Idiomas Buckingham English Center S.A, justificándose su desarrollo en la importancia de garantizar que la información de su plataforma para la enseñanza de idiomas y demás sistemas informáticos se encuentre segura, garantizando su confidencialidad, integridad y disponibilidad, evitando con ello vulnerabilidades que provocan la insatisfacción de los usuarios externos, deterioro de la imagen en el mercado e incluso demandas. Por tal motivo se plantea el diseño de este modelo, del cual carece actualmente el centro, desarrollándose según la normativa ISO 27001. La metodología para su desarrollo involucró como tipos de investigación la documental y de campo, con alcance descriptivo y enfoque mixto, a través del cual se consultaron a clientes del centro y al personal del Área de Tecnologías de Información y Comunicación. El desarrollo de encuestas y entrevistas hizo posible detectar debilidades y amenazas del sistema, las cuales deben corregirse para reducir las vulnerabilidades en la seguridad de la información, entre ellas la información no respaldada de usuarios, firewall desactivados, falta de protocolos HTTP, entre otros, a los cuales se suman experiencias negativas de los usuarios externos con la plataforma, con quejas y reclamos sobre los cuales no ha existido respuesta. Identificados los riesgos y las limitaciones se procedió al diseño del modelo de gestión de la seguridad de la información en donde se definieron las políticas, el alcance del modelo, se analizó el riesgo y se gestionó mediante controles orientados a minimizar las amenazas detectadas, finalizando con la presentación de un detalle respecto a cómo obtener la aprobación y autorización para implementarlo en el Centro de Idiomas Buckingham English Center S.A.

Palabras claves: Seguridad, información, modelo, tecnologías, sistema.

ABSTRACT

This study was oriented to the analysis and development of an information security management model for the 'Buckingham English Center S.A.' Language Center, justifying its development on the importance of ensuring that the information on its language teaching and other Computer systems platform are secure, guaranteeing their confidentiality, integrity and availability, thus avoiding vulnerabilities that cause the dissatisfaction of external users, deterioration of the image in the market and even lawsuits. For this reason, this model design which the center currently lacks is being proposed, being developed according to the ISO 27.001 standard. The methodology for its development involved documentary and field types of research, with a descriptive scope and a mixed approach, through which the center clients and the Information and Communication Technologies Area personnel were consulted. The surveys and interviews development made it possible to detect weaknesses and threats in the system, which must be corrected to reduce vulnerabilities in information security, including unsupported information from users, disabled firewalls, lack of https protocols, among others, to which negative experiences of external users with the platform are added, having faced complaints and claims on which there has been no response. Once the risks and limitations were identified, the information security management model was designed along with the scope model, where the policies were defined and the risk was analyzed being managed through controls aimed at minimizing the threats detected, ending with the presentation of a detail regarding how to obtain approval and authorization to implement it in the 'Buckingham English Center SA' Language Center.

Key words: Security, information, model, technologies, system.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO DE TÉRMINOS

CESAE: Consejo Superior de Administración Electrónica de España

COBIT: Control Para las Tecnologías de la Información y Relacionadas

IEC: Comisión Electrotécnica Internacional

ISO: Organización Internacional de Normalización

ITIL: Biblioteca de Infraestructura de Tecnologías de Información

MAGERIT: Metodología de Análisis y Gestión de Riesgo de Sistemas de la Información

OCTAVE: Evaluación de vulnerabilidades, activos y amenazas operativamente críticas

OGC: Ministerio de Comercio Británico

SGSI: Sistema de Gestión de la Seguridad de la Información

TIC: Tecnología de Información y Comunicación

INTRODUCCIÓN

Dentro de las empresas se toman decisiones encaminadas a alcanzar el éxito de las operaciones. Pérez y Fol (2016) expresan que, con este fin, “una empresa debe requerir de información que haga posible evaluar su desenvolvimiento y sirva de juicio para estimar su comportamiento” (p.3). Es decir, obtener información que ayude a diagnosticar la realidad de la empresa para tomar decisiones que aporten a su óptimo desenvolvimiento, respaldando además que su importancia no depende de la cantidad de ésta, sino de las circunstancia alrededor de ella.

Con ello se defiende que la información debe ser relevante, además de comprensible, confiable y estar disponible, de forma íntegra y confidencial, cuando se la requiera, para la toma de decisiones. La Segunda Cohorte del Doctorado en Seguridad Estratégica en Guatemala (2018) destaca la importancia de la seguridad de la información para evitar que sea vulnerada, indicando que “implica un conjunto de medidas reactivas y preventivas de las organizaciones, incluyendo sistemas tecnológicos, los cuales se orientan a resguardar y proteger la información” (p.100). Con su implementación es posible garantizar que información útil esté disponible cuando se requiera, además de protegerla ante riesgos potenciales como robo, destrucción o alteración.

Como tal, su finalidad es mantenerla en carácter confidencial, además de su integridad y disponibilidad. No debe confundirse con la seguridad informática, ya que la seguridad de la información se extiende mucho más allá de estas plataformas electrónicas, pudiendo encontrarse información en diferentes medios y formas. Así se evita que pueda divulgarse, ser borrada, robada y saboteada, lo cual afectaría su disponibilidad y confiabilidad, generando un perjuicios para las organizaciones e incluso, ocasionar sanciones cuando la información vulnerada exponga a terceros.

Entre ellas está la información de los clientes que, en sistemas vulnerables, podría caer en manos de los competidores o volverse pública de forma no autorizada, provocando que la empresa pierda credibilidad, negocios, surjan

demandas legales e incluso culmine con su quiebra o clausura. De esta forma se destaca la importancia de la seguridad de la información, no solo como una necesidad en las empresas para la toma de decisiones acertadas que aporten a su supervivencia en un mercado competitivo, sino también para evitar sanciones y pérdida de credibilidad en su público objetivo.

Con lo expuesto, el proyecto se orienta a analizar y desarrollar un modelo de gestión de seguridad de la información en el Centro de Idiomas Buckingham English Center S.A, el cual brinde confianza a sus clientes y proyecte mayor credibilidad ante su público. Este establecimiento carece de un Sistema de Gestión de Seguridad de la Información que brinde mayores garantías respecto a la confidencialidad, disponibilidad e integridad de la información de sus clientes, usuarios de su plataforma para el aprendizaje del idioma inglés. Debe tenerse en consideración que cualquier problema en la plataforma que vulnere la información, influiría en el servicio que el cliente recibe del centro, deteriorando la calidad percibida del mismo.

El desarrollo del estudio consta de un Capítulo I en donde se aborda el marco teórico conceptual, el cual contiene una descripción del problema, los objetivos que se esperan alcanzar, además de otros aspectos que respaldan la investigación. A su vez, concluye con el marco de referencia en donde se expone información bibliográfica que aporta a la fundamentación teórica y permite aproximarse a la realidad del estudio.

Seguido de esto, se presenta el Capítulo II que aborda el marco metodológico, mostrando los parámetros para la recolección de datos necesarios para conocer la realidad del problema, respecto a la seguridad de la información dentro del centro objeto de estudio. Una vez establecido estos parámetros e iniciada la recolección de datos, en el Capítulo III se presentan los resultados y discuten, detallando así los principales hallazgos. Con los resultados se procede a diseñar y presentar el modelo de sistema de gestión de la seguridad de la información propuesto, cumpliendo así el objetivo trazado.

CAPÍTULO I. MARCO TEÓRICO CONCEPTUAL

1.1. Antecedentes de la investigación

En este apartado se realizó la consulta de estudios previos, tanto nacionales como extranjeros, que guardan relación al tema. Entre los proyectos realizados en el exterior se encuentra el de Sánchez y Rebolledo (2017) quienes se enfocaron en “el diseño de un modelo para la gestión de la seguridad de la información en la Secretaría de Educación de Colombia, específicamente en su área de talento humano” (p.7). Como base al problema destaca que la institución no posee una política de seguridad definida a pesar de realizar procesos críticos en el campo de la calidad educativa tales como la vigilancia de establecimientos, la atención a ciudadanos, manejo de recursos, evaluación de resultados académicos, entre otros.

El objetivo se orienta en el diseño del modelo aplicándose una metodología basada en la norma ISO 27001 basada en la seguridad de la información, empleándose como instrumentos la observación y el análisis documental. Con ello se evidencia que los riesgos comprenden la pérdida de documentos, ingresos no autorizados a los sistemas informáticos, deterioro de expedientes, instalación de sistemas sin autorización, infraestructura física que no brinda protección a los equipos, entre otros. Basado en los hallazgos, el proyecto concluye con el diseño del modelo expresando que en la sociedad moderna es esencial que las empresas protejan su información, misma que permita guiar su conducta en el alcance de sus objetivos organizacionales.

Otro estudio se realizó en Perú teniendo como enfoque el modelo de gestión de riesgos de seguridad de la información en pequeñas y medianas empresas de este país. García y Huamani (2019) indicaron que todas las empresas deben dar importancia a la información como un activo vital; sin embargo, mencionaron que es común su desaprovechamiento y con ello se generan pérdidas. Estas pérdidas, expresan los autores que no solo surgen de esta falta de aprovechamiento, sino también a vulnerabilidades que ponen en riesgo la integridad de la información.

Por tales efectos expresaron que en las instituciones deben existir modelos para minimizar el riesgo a la información desarrollándose un modelo basado en la ISO 27005. Como metodología, se utilizó un enfoque cualitativo a través del cual se identificaron los riesgos existentes y se desarrolló un modelo enfocado en las necesidades de estas entidades, constando además de controles e indicadores para mejorar la gestión del riesgo. Esta gestión resulta relevante en las empresas y su seguimiento evita que existan problemas ligados a la pérdida de información.

Entre los estudios nacionales se encuentra aquel direccionado al diseño de un modelo para la gestión de la seguridad de la información, este para el sistema académico de una universidad del país. Conforme (2018) expresó que esta entidad es la Universidad Estatal del Sur de Manabí justificando el tema en “la necesidad respecto al uso de los sistemas de información, especialmente en esta entidad, que ayuden a acceder a información en tiempo real para los usuarios, agilizando procesos académicos y dando mayores facilidades a los estudiantes” (p.11). De esta forma, se vincula su aprovechamiento a la óptima satisfacción del público y por ende, a una mejora en la calidad que perciben del servicio.

Por otra parte, tiene claro que resulta además esencial que exista seguridad en estos sistemas, lo cual garantiza que la información se mantenga íntegra, confidencial y disponible para los usuarios y demás personas autorizadas, no disponiendo de un modelo que aporte a la gestión de la seguridad de la información. La metodología usada se sustenta en la ISO 27002 arrojando el análisis que los riesgos se orientan a la falta de políticas y que fomentan incidentes de seguridad, mismos que afectan la confidencialidad e integridad de la información, diseñando el modelo sustentando en esta norma.

Un segundo estudio en Ecuador se realizó como parte de un modelo de gestión de seguridad de la información en instituciones del sector público. Rocha (2019) indicó que “el modelo fue desarrollo en sustento a la ISO 27.000, constituyéndose en una herramienta que se adapta a los objetivos estratégicos de toda institución y los requerimientos de seguridad para el resguardo de la información” (p.2). De esta manera, la información de los ciudadanos y, de las

instituciones, se mantendría íntegra, confidencial y disponible mediante una adecuada prevención del riesgo.

Se indica que las plataformas E-Learning del Ministerio de Finanza del Ecuador, incluyendo todas las demás, se encuentran expuestas a intrusiones y amenazas, planteando el estudio métricas claras, simples y objetivas sobre las vulnerabilidades de estos sistemas, proponiendo controles que minimicen las amenazas. La metodología se concentró en un estudio de caso, con enfoque cuantitativo y cualitativo, arrojando como resultado que en la institución, si bien se ha implementado un modelo de gestión, aún no se logra garantizar la seguridad de la información por completo, diseñándose un modelo que ayude a fortalecerla.

1.2. Planteamiento del problema de investigación

Partiendo de la importancia de la seguridad de la información para una empresa, lo cual ha sido mencionado en puntos anteriores, el estudio toma como referencia al Centro de Idiomas Buckingham English Center S.A. La entidad dispone de una plataforma informática que permite brindar su servicio al cliente, este en relación a la enseñanza de inglés, donde los clientes crean un usuario, avanzan en el aprendizaje por módulos y todo se registra en la plataforma.

Esta institución se encuentra ubicada en la ciudad de Guayaquil, estando comprometida a la mejora en la experiencia del usuario, llevando a cabo desde el año 2018 la ampliación de salas informática, hasta la implementación de la red inalámbrica de internet y el sistema cerrado de cámaras de seguridad, además de TIC´s al interior de las aulas para utilizarse como una herramienta didáctica y de apoyo en el proceso de aprendizaje. Sin embargo, en relación a su ambiente educativo virtual, carece de un modelo que favorezca a la gestión de la seguridad de la información.

Esta carencia pone en riesgo la información de los usuarios, quienes incluso pueden ver vulnerados sus datos, deteriorándose así su experiencia en el uso de la plataforma que registra sus avances en los módulos, avances que pueden

perderse y con ello, provocar la insatisfacción del cliente. Para superar esta problemática se considera idóneo disponer de un modelo de gestión de la seguridad de la información que permita lograr un adecuado balance entre control y usabilidad, e incorporar en forma exitosa las nuevas tecnologías de seguridad que ayuden a mitigar las amenazas más importantes sin perder facilidad de uso.

De acuerdo a Chicano (2018) “los incidentes de seguridad que pueden presentarse en los sistemas son robo y borrado de información, accesos no autorizados a la plataforma, códigos maliciosos, mal uso de los recursos tecnológicos, entre otros” (p.4). Como puede observarse, cada uno de ellos pone en riesgo la información y afecta a su integridad, evitando que sea útil para la toma de decisiones organizacionales.

Dicho esto, el modelo debe ir orientado a prevenir estos riesgos en la plataforma de la entidad, evitando así que deba responder ante demandas legales que afecten su imagen en el mercado y deterioren el nivel de satisfacción de los usuarios externos. La ISO 27001 abarca los Sistemas de Gestión de Riesgos y Seguridad, teniendo como objetivo “asegurar la confidencialidad e integridad de los datos e información, incluso de los sistemas que la procesan, componiéndose de siete fases que van desde identificar los activos de información hasta el plan de tratamiento del riesgo” (Organización Internacional de Normalización, 2020, pág. 1). Con lo descrito, el estudio utilizará este modelo para la propuesta de un Sistema de Gestión de Seguridad de la Información.

Dicho sistema, va orientado al Centro de Idiomas Buckingham English Center S.A evitando la vulneración de su plataforma, lo cual podría provocar daños en la imagen que se proyecta al público y deteriorar la confianza de sus clientes actuales. De esta forma, el modelo a presentar para la gestión de la seguridad de la información en ambientes educativos virtuales podría convertirse en una herramienta de gestión que permitiría conocer, gestionar y minimizar los riesgos que atentan contra la seguridad de la información de los cursos virtuales. Además, ayudará a analizar y ordenar la estructura del ambiente educativo

virtual, así como facilitar la definición de procedimientos de trabajo para mantener la integridad de la información.

1.2.1. Formulación del Problema

¿Cómo desarrollar un modelo de gestión de seguridad de la información para la plataforma virtual del centro de idiomas?

1.2.2. Sistematización del problema de investigación

- ¿Cómo determinar la situación actual sobre la gestión de seguridad de la información aplicada a la plataforma virtual de Buckingham?

- ¿Cómo identificar las amenazas a las que está expuesto la plataforma virtual de Buckingham?

- ¿Cómo proveer un modelo de gestión de seguridad de la información para el apoyo personal del departamento de TIC´s de Buckingham?

- ¿Cómo proteger la plataforma virtual de Buckingham de las amenazas informáticas identificadas?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Proponer un modelo de sistema de gestión de la seguridad de la información de la plataforma del centro de idiomas.

1.3.2. Objetivos específicos

- Determinar la situación actual de la plataforma virtual del centro de idiomas.

- Identificar las amenazas a las que está expuesta la plataforma virtual de Buckingham.

- Proveer un modelo de gestión de seguridad de la información como apoyo al personal del departamento de TIC´s de Buckingham.

- Exponer alternativas orientadas a la protección de la plataforma contra amenazas informáticas identificadas al personal del departamento de TIC´s de Buckingham.

1.4. Justificación de la investigación

El estudio sienta sus bases en establecer el proceso mediante el cual se desarrollaría un modelo de sistema de gestión de la seguridad de la información en el centro de estudios Buckingham. Desde una perspectiva teórica, el proyecto se justifica al consultar teorías relacionadas al tema, a partir de fuentes fiables, enfocándose en la norma ISO 27001 enfocada en la Gestión de la Seguridad de la Información.

Desde un punto de vista metodológico, el desarrollo de este modelo partirá de la evaluación de los riesgos de la entidad bajo un enfoque cualitativo, lo cual permita describirlos y plantear acciones de respuesta a fin de minimizar dichos riesgos, tomando como referencia lo indicado en la norma ISO 27001 para su diseño. Finalmente, el proyecto se justifica de forma práctica, al enfocarse en brindar una solución viable a un problema que atraviesa el centro de idiomas Buckingham English Center S.A, el cual carece de un modelo para la gestión de la seguridad de la información, incrementando el riesgo de su plataforma respecto a ser vulnerada por terceras personas e incluso, exponer la información de sus clientes a pérdida o robo, generando una experiencia negativa en el mercado que podría traducirse en graves problemas económicos.

Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo y Castillo (2018) expresaron que:

> La seguridad de la información debe sustentarse en tres pilares que son la confidencialidad, es decir que solo personas autorizadas podrán acceder a ella, la integridad que implica que no se pierda información ni se vea afectada,

cerrando con la disponibilidad que implica la medida en la cual puede consultarse con rapidez por la persona autorizada. (p.22)

Con lo expuesto, el modelo a proponer es pertinente para la empresa ya que se fundamenta en estos tres pilares, haciendo posible que utilice esta información para la toma de decisiones, en forma rápida, mientras que los usuarios externos sientan que están protegidos y que la organización se preocupa por su seguridad, evitando así demandas legales, pérdida de clientes y cese de operaciones.

1.5. Marco de referencia de la investigación

1.5.1. La información

Para Bravo, Valdivieso y Arregui (2018) “la información es considerada un recurso estratégico de gran importancia para las organizaciones, puesto que contar con la necesaria, crea posibilidades de tomar mejores decisiones” (p.46). Como tal, se vuelve un recurso estratégico porque la empresa hará uso de ella para responder de forma efectiva ante problemas que surjan, e incluso anticiparse a ellos, sin poner en riesgo su competitividad.

Por este motivo, las organizaciones deben implementar sistemas de información como una prioridad, especificando que serán válidos si aportan a disponer de información óptima para las operaciones, de forma oportuna y actualizada sobre su entorno y la empresa. Dentro de las entidades se considera a la información como “el pilar fundamental para poder generar conocimientos, que ayuden a innovar en base a las nuevas tecnologías, permitiendo la identificación de nuevas oportunidades, mejoras y cambios” (Serrano, Señalin, Vega, & Herrera, 2018, pág. 4). Esto se debe a lo antes expuesto, ya habiéndose indicado que la información es útil para la toma de decisiones y anticiparse al riesgo.

Sin embargo, el éxito también depende de cómo es acogida, procesada y transmitida a todos los sectores de manera oportuna y, que en base a esta, se asuman las responsabilidades individuales. A su vez, el manejo de la información

dentro de las organizaciones ayuda a facilitar que el personal cumpla con sus responsabilidades en menor tiempo, demostrando eficiencia en el desarrollo de sus funciones.

Para esto, la entidad debe manejar sistemas de información dirigidos a producir informes sobre la gestión, la realidad financiera y el cumplimiento de las normas. En relación a Monterrosa y Ospino (2018) puede definirse a la información como “un dato o conjunto de datos, que han sido procesados para que el receptor pueda mejorar la toma de decisiones” (p.5). Así, los sistemas deben garantizar que la obtención de datos con significado para los interesados y que, una vez sean procesados, se transformen en información útil para la toma de decisiones.

En ocasiones, los términos datos e información son utilizados como sinónimos, lo cual es un error ya que los datos son hechos sin analizar, teniendo poca utilidad para los gerentes sin una debida interpretación. Para Ramírez y Perusquia (2019) “la información es un conjunto de datos ordenados y procesados que proporcionan conocimiento a la empresa, constituyendo la base de los sistemas de información” (p.1). Es este conocimiento el que agrega valor para las operaciones y se utiliza como referencia para el fortalecimiento de las operaciones y logro de los objetivos trazados.

Generalmente, dicho análisis está basado en tecnologías digitales y en red, que una organización pone a disposición para facilitar la producción y el consumo de datos. Como tal, la información se concibe como un recurso sustancial para la sociedad, como se muestra en las distintas civilizaciones y etapas históricas de las culturas sociales.

Esta se utiliza para “sostener un hecho, transmitir conocimiento y comunicarse, mientras que, desde el punto de vista empresarial, es un recurso crítico que puede concretar el éxito de una organización cuando se maneja de manera eficiente” (Suárez, Cruz, & Pérez, 2015, pág. 73). Dicho manejo eficiente se verá reflejado en el acceso a información útil y suficiente para dar soporte a la toma de decisiones.

Así gana relevancia la gestión de la información, siendo actividades que se ejecutan con la finalidad de obtener, procesar, guardar y recuperar la información que se crea o se recibe en una organización y que permite el desarrollo de su actividad. Para Rodríguez (2015) la información vista como un recursos, “se encuentra muy involucrada en la toma de decisiones, mencionando que esta última maneja un carácter informacional” (p.154). Así, su utilización resulta importante porque fundamenta la toma de decisiones en las organizaciones, convirtiéndose en el activo más valioso dentro de las empresas, siendo las mismas quienes le han dado prioridad por la forma de ordenar los datos indispensables para el funcionamiento de éstas.

Su administración necesita de estrategias que sean llevadas a cabo por la alta dirección en las organizaciones, indicando Vite, Molina y Dávila (2018) que “su óptimo aprovechamiento hará posible cumplir la planificación estratégica, estando alineada directamente al logro de los objetivos trazados por una entidad” (p.29). Es esto lo que motiva a que la información, incluso en la ISO/IEC 27001, tenga un valor estratégico para la organización y se establezca un enfoque hacia garantizar su continuidad dentro de la empresa.

1.5.2. Seguridad de la información en la empresa

La seguridad de la información basada en la norma ISO 27001 se sustenta en “la conservación de su confidencialidad, disponibilidad e integridad, además de todos los sistemas incluidos en su tratamiento, dentro de la organización” (ISO Tools Excelence, 2015, pág. 1). De esta forma, su implantación en cualquier establecimiento irá orientada a salvaguardar la información, evitando que se deteriore y ello perjudique la toma de decisiones eficaces para fortalecer las operaciones.

Para garantizar la seguridad de la información, en primer lugar debe ser gestionada correctamente, utilizando un proceso sistemático, documentado y conocido por toda la organización, desde una perspectiva de riesgo empresarial. ISO Tools Excelence (2015) expone que “la información, los procesos y los

sistemas de los que hace uso el sistema de gestión de seguridad de la información son considerados activos muy importantes de la empresa". De esta manera, no solo resulta relevante garantizar la seguridad de la información como tal, sino de todo aquello que se involucra en la recolección, almacenamiento y procesamiento de datos que hacen posible obtenerla, además de los medios por los cuales se difunde a personas autorizadas.

Así se destacan tres pilares u objetivos de los sistema de gestión de la seguridad de la información, siendo la confidencialidad, integridad y disponibilidad de la información, considerándolos indispensables para mantener altos niveles de rentabilidad, competitividad, conformidad legal e imagen empresarial. Con su cumplimiento, el público percibirá que la entidad protege su información y así podrá gozar de confianza, empleando también esta información para guiar la toma de decisiones y asegurar el beneficio económico.

Por otro lado, hay que recordar que "la seguridad que brindan por sí mismos los medios técnicos es insuficiente, debiéndose contar además con la presencia y participación de todos quienes están dentro de la organización, partiendo desde la gerencia que debe estar al frente del proyecto" (Vite, Molina, & Dávila, 2018, pág. 30). Así determina que, siempre será necesario el elemento humano que supervise y participe en el proceso que hará posible obtener información mediante los datos, debiendo estar capacitados y tener conocimientos suficientes sobre el manejo de los sistemas y otros activos.

Según Vite, Molina y Dávila (2018) "la ISO/IEC 27001 permite administrar la seguridad de la información dentro de las organizaciones y consolidar los activos de información" (p.31). La cantidad de información dentro de las organizaciones requiere el uso de medidas tecnológicas que posibiliten la gestión necesaria, tomando en cuenta los datos, de acuerdo a la actividad económica donde se desarrolle.

Es importante tener en cuenta que la información debe ser analizada y puesta en buen recaudo mediante la aplicación de políticas que permitan su control adecuado. Por otra parte, la implementación de la norma ISO 27001 requiere la

ejecución de un proceso de evaluación de riesgo que permita tasar los activos y su importancia dentro de la gestión de la información, para luego identificar sus vulnerabilidades y amenazas de manera integral.

1.5.3. Objetivos de la seguridad de información

La seguridad de la información tiene relación con las medidas de prevención aplicadas con la finalidad de proteger la información bajo la confidencialidad, disponibilidad e integridad. Dicho esto, “las organizaciones deben acoger y adaptar métodos para proteger los archivos y registros, mantener en funcionamiento una infraestructura tecnológica adecuada, misma que sirva para la custodia y salvaguardia de la información” (Solarte, Enríquez, & Benavides, 2015, pág. 497). Cabe destacar que la información es vista constantemente como el núcleo de la organización, debiendo considerar medidas de protección para ésta.

Debe tenerse en consideración que, “si el proceso informativo es continuo, los procesos se realizarán de manera óptima; pero si hay interferencia, la organización puede verse perjudicada, lo cual se convierte en un riesgo de seguridad de la información” (Cárdenas, Martínez, & Becerra, 2016, pág. 932). Dicho riesgo se deriva de los problemas en el flujo continuo de información entre quienes intervienen en los procesos, lo cual puede impedir que se ejecuten con eficiencia.

La seguridad de la información ha tenido transformaciones, desde la seguridad física, pasando por la seguridad de sistemas y redes de tecnologías, a centrarse en la gestión de alto nivel por medio de políticas, procedimientos y controles basados en las personas. Valencia y Orozco (2017) explican que “la seguridad de la información está asociada a las TIC, teniendo como propósito mantener bajos niveles de riesgo en la integridad de la información, y de los dispositivos tecnológicos que ayudan a su recolección, procesamiento y almacenamiento” (p.74). De esta manera será posible que, la información utilizada como base para la toma de decisiones, agregue valor ajustándose a las necesidades de los interesados.

Cabe señalar que los sistemas de seguridad se concentran en garantizar la confidencialidad, integridad y disponibilidad de la información. Es importante indicar que, “a partir de la creación de las normas ISO, se refleja la gran importancia que ha tomado la seguridad de la información, presentando un crecimiento exponencial, de empresas certificadas con esta norma” (Valencia & Orozco, 2017, pág. 74). Ello supone que existen empresas que han logrado implementar sistemas de este tipo, los cuales resultan seguras y minimizan el riesgo a vulneraciones de su información.

Como tal, su objetivo es garantizar niveles adecuados de protección de la información empresarial para la toma de decisiones, y el diseño de estrategias competitivas que distinguen una organización de otra. Desde este punto de vista, se protege la información como recurso importante, por lo que debe precautelarse también los medios por los cuales se genera, almacena, procesa y transforma en un recurso de utilidad para los negocios. Valencia y Orozco (2017) explican que los objetivos son:

> Preservar la confidencialidad, de forma que la información no esté disponible ni debe ser mostrada a ciertos individuos, entidades o procesos que no se encuentren autorizados; la Integridad ya que se debe especificar la exactitud y la complejidad de la información; y la disponibilidad que es el acceso y la utilización de la información por parte de los individuos, entidades o procesos que se encuentren autorizados. (p.83)

Es importante delimitar los dos tipos de objetivos que contempla la seguridad de la información que son los objetivos generales del sistema y los objetivos de control resultantes del análisis y valoración de riesgos. Para poder implementar un sistema de gestión de seguridad de información se deben definir los objetivos generales, articulándolos con las políticas y dentro del alcance previsto.

1.5.4. Gestión de riesgos en la empresa

El riesgo es “la probabilidad de que cierta amenaza se materialice explotando las vulnerabilidades de un activo o grupo de activos, causándole daños o pérdidas a la organización” (Arévalo, Cedillo, & Moscoso, 2017, pág. 32). Basadas en sus efectos, los riesgos pueden dividirse en tres categorías que son daños a las operaciones, daños a la reputación y daños legales de la organización.

En relación a los elementos del riesgo, Arévalo, Cedillo y Moscoso (2017) indicaron que son cuatro, descritos a continuación:

> El primero corresponde a los activos de Información y que hacen referencia a cualquier elemento que contenga información, y que deben clasificarse según el nivel de criticidad o sensibilidad de dicha información contenida. Seguido de esto, se encuentran las amenazas, entendidas como vulnerabilidades de un activo y que pueden explotarse por una o más causas potenciales de un incidente, dañando o alterando la información. El tercer elemento son las vulnerabilidades, entendidas como activos que están expuestos a una serie de amenazas, existiendo una alta probabilidad de que estas se hagan realidad, degradando el activo que contiene la información. Finalmente, como cuarto elemento, está el impacto y que se ubica como un indicador de aquello que puede suceder cuando ocurren las amenazas, permitiendo medir el daño causado cuando la amenaza se materializa. (p.32)

Dicho esto, un sistema de seguridad de la información debe estar orientado a minimizar las amenazas y vulnerabilidades que puedan ocasionar la pérdida o daños a información valiosa para la empresa, anticipándose al riesgo mediante una correcta gestión de los activos que la contienen. García y Vidal (2016) mencionan que:

> Los asuntos relacionados a la seguridad de las tecnologías de información son vistos de forma distinta en dependencia de la posición de cada cual, de forma que los directivos esperan que los procesos de la organización no se

> vean interferidos, y que las aplicaciones y servicios que utilizan no se detengan. (p.32)

Si bien, pueden existir fallas, las mismas deben ser estimadas con el sistema, esperando que el personal encargado de la seguridad reaccione de forma oportuna evitando que el impacto sea significativo, evitando el robo de equipos, la fuga de información y demás amenazas. García y Vidal (2016) determinan que "la seguridad de la información también se enfoca en proteger las computadoras de los virus y otros programas maliciosos, siendo su objetivo evitar el acceso del personal a sitios inadecuados, aunque la seguridad es mucho más que lo descrito" (p.51). Se evitan los virus y demás programas porque pueden crear aperturas para que personas no autorizadas ingresen al sistema y acceda a información valiosa, e incluso pueden provocar su destrucción.

De esta manera, puede indicarse que se encuentra orientada a la protección de la infraestructura computacional en donde se almacena la información y demás medios, aunque no sean electrónicos, para lo cual existen normas, herramientas y leyes creadas que minimizan los riesgos. Hay tres principios o aspectos fundamentales vinculados que son la confidencialidad, la integridad y la disponibilidad, describiéndose a continuación según García y Vidal (2016):

> La confidencialidad es la condición que asegura que la información no pueda estar disponible o ser descubierta por personas, entidades o procesos no autorizados; la integridad es la condición que garantiza que la información solo puede ser modificada, incluyendo su creación y borrado, por el personal autorizado; y la disponibilidad significa que el sistema funciona de forma eficiente y que es capaz de recuperarse rápidamente en caso de que falle. (p.51)

Con lo expuesto, resulta esencial que el sistema dentro del establecimiento estudiado garantice esto tres aspectos, garantizando la seguridad de la información en beneficio, no solo de la entidad, sino también de sus clientes. Para la gestión se riesgo, "el primer paso involucra el generar una Matriz de Riesgo Inicial (MRI) de los activos de información con las variables: Valor del

activo, probabilidad de ocurrencia de una amenaza, valor del impacto y el riesgo del activo" (Paillacho, 2015, pág. 42). Esta puede ser aplicada y adaptada a cualquier organización, arrojando en qué medida la entidad se encuentra vulnerable ante determinados eventos donde la información se vería afectada.

Al momento de la valoración del riesgo, se evalúa cada activo, diferencian las amenazas y vulnerabilidades, determinando y priorizando el tratamiento de los riesgos, teniendo como resultado la MRI valorada con el estado del riesgo de acuerdo al criterio de valoración del riesgo. Paillacho (2015) explica que "las principales amenazas de la seguridad de la información son el hacktivismo, siendo movimientos que dan a conocer su ideología haciendo uso no adecuado de herramientas informáticas para conseguir objetivos políticos, sociales, etc." (p.3). Estos proclaman la libertad de acceso a la información, oponiéndose a restricciones de acceso a la información, catalogándose así como el principal reto y amenaza para la ciberseguridad.

1.5.5. Sistema de gestión de la seguridad de información SGSI

Tomando como referencia a García (2015) "existen estándares internacionales y metodologías orientadas a fortalecer la seguridad de la información en las empresas, gestionando sus riesgos como pilar fundamental" (p.17). Entre ellas destaca la norma ISO 27.001 como estándar internacional para la seguridad de la información; COBIT que aborda el control, gobernabilidad, información, entre otras; ITIL que corresponde a una norma sobre mejores prácticas para administrar los servicios de Tecnologías de Información; OCTAVE que se orienta al análisis del riesgo informático a partir del riesgo operacional; MAGERIT cuyo objetivo es mitigar riesgos en la medidas de seguridad para generar confianza en medios tecnológicos.

1.5.5.1. ISO 27001

Como primer sistema se encuentra el expresado en la norma internacional ISO 27001 "enfocándose en la seguridad de la información, la cual pretende garantizar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la tratan" (Universidad

Internacional de La Rioja UNIR, 2019, pág. 1). La misma, fue creada por la Organización Internacional de Normalización y por la Comisión Electrotécnica Internacional.

La norma define cómo se planifica, instaura, comprueba y controla un SGSI, partiendo de un análisis de riesgos y de la planificación e implantación, siendo así que toda empresa puede implementar un SGSI siguiendo este estándar. Se conoce como SGSI al conjunto de políticas y procedimientos que sirven para administrar la información de una empresa u organismo cumpliendo una serie de requisitos, garantizando su confidencialidad, integridad y disponibilidad, por medio de una gestión de los riesgos que considera a las personas, procesos y sistemas relacionados con la misma.

La norma está alineada con la ISO 27002, que fija un conjunto de buenas prácticas de gestión de la seguridad de la información para todos los responsables. Dicha norma, "especifica el sistema de controles que pueden emplearse a la seguridad de la información ajustados a la norma ISO/IEC 27001 en cada dominio y proceso" (Solarte, Enríquez, & Benavides, 2015, pág. 497).

Esta norma es la guía de funcionamiento de los controles aplicables a la seguridad de la información en forma de políticas y procedimientos, incluyendo: La disposición estándar, la valoración y procedimiento del riesgo, el régimen de seguridad y su gestión, los aspectos de la seguridad de la información, la gestión de activos, la seguridad ligada al talento humano, la seguridad física y seguridad de los equipos, la gestión de comunicaciones y operaciones, la defensa frente a código malicioso y descargable, las copias de seguridad, la gestión de la seguridad de las redes, la manipulación de los soportes, el tráfico de información, la gestión de usuarios, el control de la red, el control de acceso al sistema operativo, a las aplicaciones y a la información, la seguridad de los archivos de sistema, entre otros aspectos.

Su propósito es la instalación de los mecanismos para la confidencialidad, integridad y disponibilidad de la información en medio de un conjunto de estándares determinados para estimar la seguridad, evidenciando cada activo y

persona que apoya los sistemas informáticos, además de examinar los controles de seguridad que permitan incluirlos a las políticas y procedimientos para disminuir los riesgos encontrados. De acuerdo a Solarte, Enríquez y Benavides (2015) “dentro de los activos informáticos existen dos categorías para diferenciarlos de acuerdo a su naturaleza y existencia física, agrupando la primera categoría los activos intangibles y la segunda los activos tangibles” (p.498). Dentro de los activos intangibles están los bienes inmateriales como las bases de datos, las herramientas tecnológicas, el conocimiento y la experiencia, y los procesos operativos.

Se consideran bienes tangibles a los equipos informáticos, hardware de redes, equipos de protección eléctrica, cableado estructurado, teléfonos y plantas telefónicas, entre otros. La empresa y sus Sistemas de Gestión de Seguridad de la Información están propensos a un alto número de amenazas, tales como robos de información mediante espionaje, o fraude aprovechándose de alguna vulnerabilidad. Algunos ejemplos son los virus informáticos, el *hacking*, pero también se consideran riesgos el sufrir accidentes de seguridad de la información ocasionado de forma voluntaria o involuntaria por en la propia organización.

Figura 1. Modelo para la implantación de un sistema de Gestión de la Seguridad de la Información

Elaborado por: *Norma ISO (2020)*

De acuerdo al sitio web Norma ISO (2020) “la metodología para implantar un SGSI parte de la identificación de los activos de la información y sus responsables, lo cual implica comprender que los activos pueden ser soportes físicos, intelectuales o informativos” (p.1). En ello pueden almacenarse datos que posteriormente se convertirán en información. Posteriormente se identifican las vulnerabilidades de estos activos, siendo aquellas que pueden volverlo susceptible a sufrir daños o ataques.

Posteriormente señala el Identificar las amenazas, es decir los hechos que pueden ocurrir y así dañar el activo de la información. Una vez conocidas, se identifican los requisitos legales y contractuales que la organización debe cumplir ante sus clientes, proveedores y socios, evitando que el sistema lo vulnere, e incluso diseñarlo de tal forma que refuerce el cumplimiento de la entidad hacia estos compromisos (Norma ISO, 2020). También se identificarán los riesgos, en este caso el nivel de probabilidad para la ocurrencia de amenazas o vulnerabilidades antes descritas, además de su impacto en la organización.

Así se podrán identificar los riesgos prioritarios, teniendo que ser calculados. Finalmente, se presenta el plan de tratamiento de riesgo, lo cual supone establecer políticas para reducir estos riesgos y responder a ellos de forma eficiente si llegasen a ocurrir.

1.5.5.2. COBIT

Luc (2017) explicó el nombre de este marco de referencia se deriva del inglés *Control Objetives for Information and Related Technologies* que traducido al español se entiende como Control Para las Tecnologías de la Información y Relacionadas, indicando que “permite auditar y evaluar los servicios informáticos que una organización posee, valorando su rendimiento y robustez en relación a la seguridad y conformidad” (p.28). Con ello, hace posible controlar el conjunto de operaciones relacionadas a la información, mientras facilita a los responsables el entender y gestionar los riesgos informáticos.

El COBIT se encuentra en su quinta versión, teniendo su inicio en los años 90 al ser desarrollado por la asociación americana ISACA. Tomando como referencia Venegas y Esparza (2018) “el COBIT5 es un marco de referencia que fue desarrollado a fin de ayudar a las empresas a sacar el máximo provecho de sus tecnologías de información TI” (p.11). Es importante tener en consideración que puede aplicar cualquier empresa, sin importar su tamaño o sector, a fin de satisfacer las necesidades de creación de valor mediante TI, ya sean dichas necesidades de interesados externos o internos.

Se caracteriza porque su gestión es holística, es decir completa e integral, de extremo a extremo, trayendo una serie de beneficios según Venegas y Esparza (2018), los cuales involucran “el uso efectivo e innovador de las TI, además del logro de los objetivos estratégicos; optimizar los gastos en TI; apoya a que la empresa cumpla leyes, acuerdos, reglamentos y políticas; y gestión eficaz de los riesgos de TI” (p.11). De esta manera se busca mejorar el rendimiento del negocio, protegiendo la información y disminuyendo vulnerabilidades.

Ante lo planteado, la adopción de este marco de referencia ayudaría a que la plataforma del Centro de Idiomas Buckingham English Center S.A. opere sin riesgos en la información de los clientes, fortaleciendo la seguridad. Venegas y Esparza (2018) explican que el COBIT posee cinco principios que son:

> “Satisfacer las necesidades de las partes interesadas, lo cual implica definir y vincular los objetivos de la organización con los de las TI; Cubrir la organización de forma integral, orientándose a modificar la visión en las instituciones, considerando a las TI no como un costo, sino como un activo valioso; Aplicar un solo marco integrado, el cual se oriente a que las organizaciones brinden un valor óptimo a sus recursos y activos TI; Habilitar un enfoque holístico considerando que el COBIT incluye siete habilitadores, los cuales deben tenerse en cuenta al implementarse este marco de referencia, involucrando políticas; marcos; principios, la cultura; los procesos; la gente; y la información; y separar el gobierno de la administración”. (p.23)

Cabe señalar que la empresa debe disponer de un gobierno de TI (GEIT) cuyos procesos deben orientarse al alcance de los objetivos mediante la evaluación de las necesidades de todos los interesados, tomando decisiones, estableciendo las directrices, monitoreando el desempeño, cumplimiento y progreso del marco de referencia. Con los resultados del GEIT, la directiva de la empresa y el mismo GEIT deben planear, crear, realizar y monitorear las actividades para así alcanzar los objetivos trazados.

En relación a los procesos identificados dentro de este marco, Santacruz, Vega, Pinos y Cárdenas (2017) explican se encuentran "el Planificar y Organizar PO; Adquirir e implementar (AI); Proveey Soportar (DS); y Monitorear y Evaluar (ME)" (p.67). Es importante señalar que estas áreas se derivan de las responsabilidades tradicionales que implican planificar, construir, ejecutar y monitorear.

1.5.5.3. ITIL

Luc (2017) expuso que el nombre se deriva del inglés *Information Technology Infraestructure Libray* y que traducido al español se entiende como Biblioteca de Infraestructura de Tecnologías de Información, mencionando que “hace referencia a un conjunto de libros que abordan el tema de la infraestructura de las TI, con buenas prácticas para la gestión de los sistemas informáticos" (p.29). De esta forma, también podría ser aplicada como una forma de fortalecer la seguridad de la plataforma del Centro de Idiomas Buckingham English Center S.A. y brindar un mejor servicio al cliente.

Fue generada y es de propiedad intelectual de la *Office of Governmeten Commerce OGC*, siendo el Ministerio de Comercio Británico. Como tal, no es un estándar ni tampoco una norma, basándose en la experiencia y generando así buenas prácticas concretas para el suministro de servicios informáticos. Sus bases iniciales fueron creadas en 1988.

De acuerdo a Luc (2017) “está compuesta de tres módulos que comprenden publicaciones principales, publicaciones adicionales y artículos de internet”

(p.30). Las publicaciones principales se agrupan en cinco libros que tratan de la estrategia del servicio, transición del servicio, diseño del servicio, explotación del servicio, y la mejora continua del servicio. Cada libro describe las buenas prácticas enfocadas a cada fase del ciclo de vida de los servicios.

Por otra parte, las publicaciones adicionales conforman una biblioteca viviente donde constantemente se suman artículos y libros escritos por expertos. Finalmente, incluye artículos que pueden consultarse en internet y que se encuentran en sitios web, pero su calidad varía.

Entre las características que Santacruz, Vega, Pinos y Cárdenas (2017) exponen respecto al ITIL se encuentra "el estar orientado a la mejora del servicio al cliente, brindando buenas prácticas para la gestión de las TI, además el no ser rígido, lo cual facilita su implementación y adaptación" (p.68). Esto hace que los cambios sean fáciles de manejar, mejorando el uso de los recursos y disminuyendo los costos, aunque esto no podría ser visible en la medida que la empresa no tome el tiempo necesario ni dedique el esfuerzo suficiente para su implementación.

Cuervo y Bejarano (2020) determinaron que "se encuentra en su cuarta versión, siendo publicada el año 2019 en donde aparece el término sistema de valor del servicio" (p.16). Como tal, pretende ver al valor del servicio y al ciclo de vida del servicio, no como procesos, sino como una estructura o sistema de valor, enfocándose en su mejora continua.

El ITIL debe desarrollarse en función a siete principios que son "enfoque de valor; empezar donde se está; progresar iterativamente con retroalimentación; pensar y trabajar holísticamente; mantenerlo simple y práctico; y Optimizar y automatizar" (p.18). En base a cada principio, se presenta a continuación una interpretación de cada uno:

- Enfoque de valor, partiendo de que su implementación debe orientarse a crear valor para los clientes, ya sea creando valor para ellos, para la organización como tal, o para otros interesados.

- Empezar donde se está, lo cual implica emplear aquello que está disponible en la empresa, en lugar de iniciar desde cero, realizándose un diagnóstico para luego identificar qué puede ser útil para la creación de valor.

- Progresar iterativamente con retroalimentación, haciendo referencia a evitar la búsqueda de todo en un solo momento, sino dividir el trabajo para hacerlo más manejable y, en la medida que se avance, realizar la retroalimentación.

- Pensar y trabajar holísticamente, lo que implica realizar un trabajo integral, en donde cada actividad en la empresa se oriente a la entrega de valor.

- Mantenerlo simple y práctico, simplificando los métodos de trabajo, disminuyendo su complejidad. Esto parte de identificar y eliminar procesos o pasos innecesarios que no agregan valor.

- Optimizar y automatizar el trabajo que realiza el equipo humano, en la medida de lo posible, para que exista una mínima intervención humana.

1.5.5.4. OCTAVE

Giménez (2017) expuso que “hace referencia a las siglas Operationally Critical Threat, Asset and Vulnerability Evaluation que traducido al español se refiere a Evaluación de vulnerabilidades, activos y amenazas operativamente críticas, siendo desarrollado por la Universidad de Caregie Mellon” (p.93). Este queda definido como un conjunto de criterios para la implementación de métodos más flexibles en las empresas identificándose el OCTAVE original, El OCTAVE-S direccionado a pequeñas empresas y el OCTAVE-Allegro centrado en los activos de información.

Entre los criterios considerados para su implementación están el que las medidas se adapten a las necesidades; que el proceso de análisis se encuentre definido, sea continuo y disponga de una visión a futuro; y finalmente que el

proceso se enfoque en un conjunto reducido de riesgos catalogados como críticos. De acuerdo a Giménez (2017) “los resultados se dividen en tres faces que son la organizativa, la tecnológica y la estratégica” (p.93). Dicho esto, se presenta a continuación un detalle de cada una:

- Fase organizativa que involucra desarrollar un perfil de las amenazas de los activos críticos, requerimientos y prácticas de seguridad.

- Fase tecnológica que se direcciona a identificar las vulnerabilidades y los componentes clave.

- Fase estratégica donde se desarrolla el plan de seguridad y mitigación, a fin de protegerse y afrontar posibles riesgos.

Dicho esto, el presente método permitiría, en estas tres etapas, identificar los riesgos potenciales del sistema, para luego llevar a cabo un plan con acciones orientadas a mitigarlos. Al criterio de Hurtado (2018) queda definido como "una técnica de evaluación de riesgos desarrollada por el Software Enginnering Institute de Estados Unidos conocido como SEI, presentando sus fases cierto grado de complejidad en relación otras metodologías” (p.3). Como se explica, se enfoca en el riesgo, más no en las tecnologías que una empresa disponga, disminuyendo así su eficacia en lo que respecta a sistemas informáticos.

Su éxito requiere que el equipo humano, especialmente de áreas operativas, tecnologías y otras, trabajen de manera conjunta en función de las necesidades de seguridad que existan, apoyándose también de especialista. Hurtado (2018) indica que “fue ideada para empresas con más de 300 empleados, a diferencia de otras que pueden aplicarse en cualquier organización” (p.4). Esto motiva que sea descartada entre los modelos potenciales que podrían implementarse dentro del Centro de Idiomas Buckingham English Center S.A. para favorecer a la gestión de la seguridad de la información.

1.5.5.5. MAGERIT

De acuerdo a Giménez (2017):

> Es una metodología que responde al acrónimo Metodología de Análisis y Gestión de Riesgo de Sistemas de la Información, siendo desarrollada por el Consejo Superior de Administración Electrónica de España CESAE creada en función de la alta dependencia que la sociedad mantiene en las TIC para alcanzar sus objetivos. (p.8)

Se determina que el uso de estas tecnologías proporciona una serie de beneficios y, en consecuencia, también expone a la organización a una serie de riesgos que deben ser mitigados mediante la implantación de medidas de seguridad que brinden confianza.

Esta confianza no solo será en los usuarios internos quienes manejan la estructura, sino también en los usuarios externos quienes verán que su información está protegida. De esta manera, puede deducirse que es posible implementarlo en el Centro de Idiomas Buckingham English Center S.A. al responder al objetivo de fortalecer la seguridad de la información en su plataforma para la enseñanza de idiomas.

Giménez (2017) explica que "fue creada en 1997 y se encuentra en su segunda versión compuesta de seis que involucran definir el alcance; identificar los activos; identificar amenazas; identificar vulnerabilidades y salvaguardas; evaluar el riesgo; y tratar el riesgo” (p.9). En relación a cada fase, se presenta un detalle a continuación:

- Definir el alcance del estudio, es decir en qué aspecto o áreas estratégicas se procedería a revisar y mejorar la seguridad.

- Establecer los activos relevantes, lo cual conlleva evaluar el valor de aquellos que contienen la información, determinando en qué medida podría perderse de materializarse una amenaza.

- Identificar las amenazas, es decir aquellas vulnerabilidades o riesgos a los cuales están expuestos los activos que contienen la información.

- Identificar vulnerabilidades y salvaguardas. La cuarta fase implica conocer los planes de contingencia o salvaguardias que ayudarán a contrarrestar las amenazas.

- Evaluar el riesgo, determinando en este caso el impacto que su ocurrencia podría causar y en qué medida amenazaría el activo.

- Tratar el riesgo, esto con el fin de reducir la probabilidad de ocurrencia de las amenazas de podrían afectar al activo. Con ello deberían tomarse tres decisiones que pueden ser aceptar el riesgo si la probabilidad de que ocurra es baja; transferir el riesgo si su probabilidad es media; y evitar el riego si su ocurrencia es alta.

Rosales, Martelo y Franco (2020) explican que "se encuentra en su tercera versión, orientándose a la evaluación del riesgo en la seguridad de la información, basándose en el área informática y además, resulta compatible con la norma ISO 27.001" (p.229). Cabe señalar que, sobre su objetivo, determinar que corresponde a mitigar los riesgos durante la implantación y manejo de las TI, direccionando inicialmente a instituciones públicas.

CAPÍTULO II. MARCO METODOLÓGICO

2.1. Tipo de diseño, alcance y enfoque de la investigación

El estudio se desarrolló considerando los tipos de investigación, la documental y de campo. Galeano (2018) expuso que la investigación documental comprende la consulta de fuentes referenciales a fin de obtener información que sirva de sustento teórico. Con su implementación se tomaron libros, sitios webs y demás fuentes referenciales, incluyendo aquella relacionada a los modelos de gestión de seguridad de la información.

Por otra parte, la investigación de campo, permitió recopilar información exclusiva del objeto de estudio, siendo el Centro de Idiomas Buckingham English Center S.A. a fin de identificar sus limitaciones en la seguridad de la información, permitiendo diseñar el modelo que aporte a su fortalecimiento en beneficio de la empresa y sus clientes externos. Muñoz (2015) explicó que esta investigación involucra la consulta de fuentes primeras para recolectar datos o información directamente de la realidad del entorno o problema de interés, es decir de los hechos y cómo ocurren.

En relación al alcance, el estudio es descriptivo por centrarse en la descripción de la realidad del Centro de Idiomas Buckingham English Center S.A, esto en relación a la seguridad de la información que brinda su ambiente educativo virtual, siendo una plataforma para el aprendizaje de inglés. Este alcance es definido por Merino, Pintado, Sánchez y Grande (2015) indicando que se enfoca es describir una situación, problema o fenómeno, exponiendo sus características en un momento determinado.

Respecto al enfoque, este correspondió al mixto, involucrando tanto el cualitativo como cuantitativo. Anselm (2016) define al cualitativo como la recolección de datos no cuantificables sin que intervengan procedimientos estadísticos, orientándose a describir una realidad, problema o situación de interés mediante el uso de técnicas basada en dicho enfoque. Dicho esto, es cualitativo por centrarse en recopilar información mediante procesos no estadísticos, involucrando teorías, además del talento humano del Centro de

Idiomas Buckingham English Center S.A. a fin de identificar si existen problemas o limitaciones en la seguridad de la información dentro de la plataforma virtual, las acciones para fortalecer dicha seguridad, y demás información relevante.

En relación al cuantitativo, Galeano (2020) indicó que describe una realidad trabajando con datos que pueden ser cuantificables y expresados numéricamente, recopilados mediante procedimientos estadísticos. En este caso, se consideró a clientes del Centro de Idiomas Buckingham English Center S.A., evidenciando cómo perciben la seguridad de su información en la plataforma.

2.2. Método de investigación

La investigación se desarrolló considerando como método el analítico sintético, siendo un razonamiento lógico que aporta a la generación de nuevo conocimiento. A través del analítico se profundiza en cada una de las partes del tema, para luego integrarse mediante el método sintético, presentando un análisis condensado para comprender la realidad y fortalecer los hallazgos (Bernal, 2016). Dicho esto, se profundizó en la seguridad de la información y modelos para la gestión de la seguridad de la información, realizando posteriormente un análisis integral para proponer un modelo adaptado a la situación del Centro de Idiomas Buckingham English Center S.A.

Así se pretende, no solo brindar un beneficio para los clientes quienes contratan el servicio, garantizando que su información esté protegida, sino también a la empresa que evitará posibles demandas, además de la pérdida de clientes por la desconfianza que genera la vulneración de su plataforma.

2.3. Unidad de análisis, población y muestra

Como población se consideró al talento humano del Centro de Idiomas Buckingham English Center S.A. y a sus clientes, recolectando información respecto a sus perspectivas sobre la seguridad de la información en la plataforma virtual, misma que permite proporcionar el servicio al público.

Para el talento humano de la empresa, considerando que el enfoque en este grupo fue cualitativo, se aplicó un muestreo no probabilístico por conveniencia, no realizándose cálculos estadísticos para determinar el número de individuos a consultar, sino seleccionándose en función de su accesibilidad para el investigador (Otzen & Manterola, 2017).

En función a lo explicado, se seleccionaron para el enfoque cualitativo, aplicándose un muestreo no probabilístico por conveniencia a:

- 5 Personas.

Miembros del equipo humano involucrados en el funcionamiento y seguridad de la información que la plataforma debe proporcionar, entre ellos el encargado del departamento de sistema y su personal de apoyo.

Se seleccionaron para el enfoque cuantitativo, aplicándose un muestreo no probabilístico para determinar el número de individuo a consultar a:

- 10.000 Personas.

La cartera de clientes, según comentarios de los directivos. Dicho esto, se presenta a continuación el cálculo:

$$n = \frac{Z^2 * N * p * q}{\left(e^2\ (N-1)\right) + (Z^2 * p * q)}$$

N: Hace referencia a la población de estudio, siendo 10.000 clientes del Centro de Idiomas Buckingham English Center S.A.

p y q: Probabilidad de éxito y fracaso, asignándose a cada una un 50% o 0,5%.

Z: Hace referencia al valor Z, asignándose con frecuencia un valor de 1,96 y que se refiere a un 95% de nivel de confianza.

e: Corresponde al margen de error, valorándose en 5% o 0,05 en aquellos casos cuando el nivel de confianza asciende al 95%.

$$n = \frac{1{,}96^2 * 10.000 * 0{,}5 * 0{,}5}{\left(0{,}05^2 (10.000 - 1)\right) + (1{,}96^2 * 0{,}5 * 0{,}5)}$$

$$n = \frac{9.604}{24{,}9975 + 0{,}9604}$$

$$n = \frac{9.604}{25{,}9579}$$

$$n = 370$$

Del total de clientes, el muestreo probabilístico arrojó la necesidad de consultar a 370, identificando sus perspectivas en torno a la seguridad que proporciona la plataforma y su funcionamiento.

2.4. Variables de la investigación, Operacionalización

Atendiendo al tema y el objetivo de estudio se pudieron identificar las variables de la investigación, siendo descritas a continuación:

- Variables Independientes: Modelo de sistema de gestión de la seguridad de la información.
- Variables Dependientes: Seguridad de la información de los usuarios externos.

Bajo este razonamiento, la seguridad de la información de los usuarios externos en la plataforma virtual del Centro de Idiomas Buckingham English Center S.A va a depender del modelo de gestión que se diseñe, el cual irá orientado a fortalecerlo y minimizar sus vulnerabilidades.

2.5. Fuentes, técnicas e instrumentos para la recolección de información

El estudio recurrió a fuentes primarias y secundarias para la recolección de datos. Las primarias son aquellas fuentes exclusivas que permiten conocer la realidad del entorno o problema, en el contexto donde se producen, mientras las secundaria son aquellas referenciales que fortalecen la aproximación teórica

(Martínez, 2015). Con las fuentes primarias se accedieron a opiniones de informantes claves y sus perspectivas sobre la seguridad de la información en el establecimiento de interés, mientras que el uso de fuentes secundarias ayudó a definir una serie de términos que guardaron relación al tema.

Para la consulta de fuentes primarias, las cuales guardan afinidad con la investigación de campo, se utilizaron como técnicas de investigación la entrevista y la encuesta. Martínez (2015) expuso que la entrevista se encuentra enfocada en obtener información interactuando con otra persona, conociendo así sus opiniones, actitudes o comportamientos en función a un tema, caracterizándose por ser un individuo con amplio conocimiento o experiencia en el ámbito de estudio. El instrumento empleado fue el cuestionario de entrevista, compuesto de preguntas dirigidas al talento humano del establecimiento (VER ANEXO 5)

Sobre la encuesta, Merino, Pintado, Sánchez y Grande (2015) la ubican como una técnica de investigación de campo para la recolección de datos primarios, aplicándose a una muestra representativa de una población, obteniendo información estructurada y homogénea que permita realizar conclusiones numéricas. El instrumento implementado fue el cuestionario de encuesta dirigido a los clientes del Centro de Idiomas Buckingham English Center S.A. (VER ANEXO 6), permitiendo conocer sus perspectivas en relación a la seguridad de la información de la plataforma virtual.

2.6. Tratamiento de la información

La información obtenida, tras la implementación de las entrevistas al talento humano del Centro de Idiomas Buckingham English Center S.A, se redactó para presentar un análisis condensado de los hallazgos por pregunta. Por otra parte, las encuestas se tabularon para la presentación resumida de los datos, utilizando tablas y gráficos estadísticos, facilitando su interpretación. Una vez presentados los resultados, se desarrolló un análisis general de los hallazgos.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1. Análisis de la situación actual

En este apartado se presenta un detalle de la situación actual del Centro de Idiomas Buckingham English Center S.A, esto en función de los hallazgos de la recolección de datos, teniendo en cuenta que se aplicaron entrevistas al personal y encuestas a clientes.

3.1.1. Resultados de entrevistas a talento humano.

Este instrumento se aplicó a miembros del talento humano del centro, mismos que se encontraban involucrados en el funcionamiento y seguridad de la plataforma para la enseñanza de idiomas. El número de personas consultadas ascendió a cinco, constando el Director de Tecnologías de Información y Comunicación TIC´s y cuatro individuos que pertenecen a su equipo de trabajo.

Dicho esto, se presentan a continuación las respuestas a cada pregunta, tanto del director como de sus asistentes o personal de apoyo dentro del departamento de sistemas:

Identificación de activos

1. ¿Qué activos de información posee la empresa donde se soporta información de los clientes, según los siguientes criterios?

Director: Los Soportes físicos son el Firewall (CPU), discos sólidos extraíbles y Computadoras para el fin apropiado; mientras que los soportes informáticos comprenden el S.O. Windows 10, S.O. Pfsense, Plataforma PhP, Plataforma Moodle, Hosting y Dominio.

Apoyo 1: Entre los soportes físicos puedo mencionar los discos duros extraíbles, además de dispositivos USB y discos compactos. Respecto a los soportes electrónicos se encuentran el correo electrónico, información subida en la nube y en el mismo sistema operativo

Apoyo 2: Los soportes físicos involucran discos duros extraíbles, el CPU de las computadoras, información que se encuentra grabada en discos compactos; mientras que los soportes electrónicos e informáticos corresponden a la plataforma por la cual se proporciona el servicio al cliente, además de los correos electrónicos institucionales, información almacenada en la nube, entre otras similares

Apoyo 3: Los soportes físicos de la información involucran las carpetas físicas con información de clientes, discos extraíbles y dispositivos USD. Al contrario, los soportes informáticos comprenden el propio sistema que permite brindar el servicio al cliente, información en la nube, etc.

Apoyo 4: Entre los soportes físicos pueden mencionarse los discos compactos, discos duros extraíbles, el CPU, información que se encuentra en informes y archivos impresos de clientes, entre otros. Por otra parte, los soportes informáticos comprenden el correo institucional en donde existe información de los clientes, la información en la nube, el mismo sistema operativo, entre otros.

Análisis: A criterios de los consultados podrían indicarse que, dentro del establecimiento, existen soportes físicos e informáticos que contienen información respecto al cliente y que, dentro del establecimiento, debe garantizar su seguridad, evitando que sean accesibles para personas no autorizadas o, en su defecto, sean robados, alterados, o borrados. De ocurrir aquello, se generaría un perjuicio para el establecimiento y sus clientes, deteriorando la imagen del centro al público.

2. ¿Quiénes son los responsables de la gestión de estos activos?

Director: Personal área de TIC’s, desarrolladores de contenido.

Apoyo 1: Generalmente los responsables son el personal que se encuentra dentro del departamento de sistemas, siendo en primera línea el director del área.

Apoyo 2: Como principal responsable se encuentra el director de tics, siendo quien lidera el departamento de sistemas y, a su vez, también su personal de apoyo.

Apoyo 3: Los responsables de la gestión de estos activos son el personal dentro del área de sistemas, figurando como máxima autoridad al director de TIC´s.

Apoyo 4: La responsabilidad recaería sobre el área de sistemas

Análisis: En base a los criterios de los consultados es posible mencionar que la entidad posee un equipo responsable de la gestión de los activos de la información, siendo en este caso todo el departamento de sistemas y que se encuentra compuesto por un director y a su equipo de apoyo. Este personal opera y debe comprometerse a garantizar la seguridad de estos activos, permitiendo que la información sea accesible solo para personal autorizado, no se vea alterada ni deteriorada, y puede consultarse en el momento que se requiera.

Amenazas y vulnerabilidades de la plataforma

3. ¿Con qué frecuencia se realiza en la entidad un análisis para identificar y corregir debilidades y/o amenazas relacionadas a la seguridad de la información en la plataforma virtual?

Director: Cada 15 días.

Apoyo 1: Esto suele realizarse cada 15 días.

Apoyo 2: Se realiza pasando quince días.

Apoyo 3: Quincenalmente suelen realizarse estos análisis.

Apoyo 4: Pasando 15 días se llevan a cabo estos análisis.

Análisis: Las respuestas del personal dentro del departamento de sistemas permiten corroborar que cada quien días se realizan análisis que permitan identificar y corregir debilidades, las cuales influyen negativamente en la seguridad de la información de su plataforma. De esta manera se garantiza que no sea vulnerada, provocando la pérdida o el deterioro de la información de los clientes, afectando a la imagen que percibe el público en relación al Centro de Idiomas Buckingham English Center S.A y los servicios ofrecidos.

4. ¿Qué debilidades y/o amenazas posee la plataforma virtual y que la vuelve susceptible a ataques o daños?

Director: Falta de protocolo https para plataforma y páginas web; además, no suelen realizarse copias de seguridad para contenido y datos de usuario.

Apoyo 1: Pérdida de contenidos externos, son archivos adjuntos que se utilizan para la creación de un módulo de estudio.

Apoyo 2: Cifrado de dispositivos nulos, los equipos están activos con el sistema operativo libremente.

Apoyo 3: Spam/Correos no deseados, a pesar que los correos institucionales son seguros, hay un 3% de probabilidad de recibir estos contenidos con virus de red y más.

Apoyo 4: Firewall Gateway desactivado, afectaría a equipos y redes de manera directa con dispositivos externos.

Análisis: Los resultados reflejan que existen una serie de debilidades que se deben intervenir para evitar problemas en la seguridad de la información. Entre ellos están la pérdida de contenidos externos y el no respaldo sobre determinados datos que, al perderse, pueden influir en la experiencia del usuario. A ello se suma la exposición a virus de red, los cuales pueden afectar el funcionamiento del sistema y provocar el deterioro y pérdida de información.

5. En relación a las debilidades y/o amenazas ¿Cuáles considera usted que tienen altas probabilidades para ocurrencia y pueden afectar el funcionamiento y seguridad de la plataforma?

Director: Considero que las mencionadas son aquellas que poseen mayor nivel de ocurrencia y pueden afectar a la plataforma.

Apoyo 1: La principal, que ya ha ocurrido, es la pérdida de contenidos para los módulos de estudios. Esto afectó de manera directa a nuestros usuarios, razón por la cual se controla más mediante copias de seguridad.

Apoyo 2: El uso de dispositivos externos en los equipos del instituto ya ha dejado casos de ello, pero se ha solucionado antes de que afecte a la plataforma de manera directa.

Apoyo 3: Firewall a pesar que no presenta fallas mediante software, falta de mantenimiento en hardware por su uso constante, debería tener un dispositivo preparado para el reemplazo de este.

Apoyo 4: Correos no deseados, a pesar que esto solo es de uso administrativo debería contener parámetros para la descarga de archivos dañinos mediante E-mail y proteger, tanto el equipo, la red y la plataforma.

Análisis: Los consultados exponen algunas de las desventajas y/o amenazas previamente mencionadas, Entre ellas destaca las debilidades en la realización de las copias de seguridad en donde se excluyen datos, cuya pérdida influirá directamente en el servicio que se brinda al usuario. También se encuentra el Firewall que provoca la vulnerabilidad del sistema, sin excluir el hardware, no teniendo equipos de reemplazo que permitan actuar ante cualquier avería.

Tratamiento del riesgo

6. ¿Qué acciones se han desarrollado en la entidad a fin de minimizar las amenazas y vulnerabilidades para la plataforma virtual del centro de estudio?

Director: Revisión de datos y contenidos dentro del sistema creando un respaldo fuera de la plataforma y eliminándolo con el fin de tener espacio de almacenamiento controlado.

Apoyo 1: En primer lugar, están los controles quincenales, a lo cual también incluimos los respaldos de la información de los clientes.

Apoyo 2: A fin de garantizar la seguridad de la información se realizan respaldo de los datos de clientes y luego se eliminan de la fuente.

Apoyo 3: Llevamos a cabo los controles, sumando a esto los respaldos de la información de los clientes.

Apoyo 4: El contenido dentro de la plataforma se respalda y luego se elimina del origen.

Análisis: Las respuestas obtenidas permiten conocer que la información dentro del sistema se respalda y se elimina, lo cual no solo permite disponer de mayor espacio, sino también evita que cualquier ataque o problema con la plataforma provoque la pérdida de un gran volumen de datos valiosos para la entidad. A las acciones para minimizar el riesgo se suman los análisis quincenales, los cuales ayudarían a detectar debilidades y amenazas que pongan en riesgo la seguridad de la plataforma.

7. ¿Cómo estas acciones han garantizado la disponibilidad, confidencialidad e integridad de la plataforma para la seguridad de la información del cliente?

Director: Manteniendo los datos de los usuarios por un tiempo determinado en la plataforma, no presentándose hasta la fecha irregularidades en cuanto a seguridad.

Apoyo 1: Al respaldar la información del sistema y luego eliminarla de la plataforma se ha garantizado que dicha información se mantenga de manera confidencial e integra en otros soportes.

Apoyo 2: La información en el sistema se mantiene temporalmente ya que luego se respalda en otros soportes, evitando que dentro de la plataforma exista un gran volumen de información que pueda ser borrada o deteriorada por alguien más

Apoyo 3: Como se mencionó anteriormente, en el sistema existe un gran volumen de información, permitiendo su respaldo que permanezca por un corto tiempo expuesto en la plataforma.

Apoyo 4: En este caso, como se respalda la información no existe el riesgo a que la información en la plataforma se deteriore o se pierda gran volumen de datos, esto al colocarse en otros soportes

Análisis: Los comentarios de los consultados permiten evidenciar que la empresa toma como medida de seguridad el respaldo de la información en otros soportes; sin embargo, no se evidencia ningún tipo de control respecto a la información respaldada de la plataforma y cómo se controla que esté disponible e íntegra cuando se la requiera. A su vez, se podría sobreentender que los controles quincenalmente también irían orientados a garantizar la seguridad de la información que permanece en el sistema, evitando su robo, deterioro o algún tipo de modificación no autorizada, detectando debilidades o amenazas para su intervención.

8. ¿Qué problemas se han presentado en la entidad respecto a la seguridad de la información del cliente y funcionamiento de la plataforma virtual? Indique la frecuencia con la que ocurren

Director: Ninguna

Apoyo 1: No hemos tenido ningún problema por el momento.

Apoyo 2: No se han detectado.

Apoyo 3: Ninguno por el momento.

Apoyo 4: No se han presentado.

Análisis: Los consultados exponen que la entidad no ha presentado ningún tipo de problema en la seguridad de la información; sin embargo, existen debilidades y amenazas que la ponen en riesgo, debiendo ser corregidas para evitar ataques a la plataforma.

9. Indique las razones que han impedido la adopción de un modelo de gestión para la seguridad de la información en la empresa

Director: No se han manifestado irregularidades hasta la actualidad. Se han seguido protocolos ya establecidos para mantener los datos de los usuarios seguros.

Apoyo 1: Aunque existen debilidades, no se ha implementado un modelo porque las irregularidades han mantenido una nula ocurrencia.

Apoyo 2: Porque no ha ocurrido ninguna irregularidad.

Apoyo 3: Las irregularidades son nulas y con ello, la implementación de un modelo de este tipo no ha sido considerada necesaria.

Apoyo 4: Esto puede obedecer a que no existe ninguna irregularidad reportada en relación al sistema.

Análisis: En la empresa no existe una cultura fuertemente orientada a la prevención del riesgo, evidenciándose que no existe un modelo de gestión de la seguridad de la información que permita prevenir el riesgo a su plataforma, esto porque no se han experimentado irregularidades. Si bien, existen debilidades y amenazas, se ha prácticamente descartado la implementación de estos modelos porque aún no se han concretado.

De esta forma, la ocurrencia de algún problema podría provocar la pérdida de información valiosa, considerando que un modelo no solo previene riesgos, sino también brinda pautas para afrontarlo y reducir los efectos que puedan causar en la organización.

10. De presentarse un modelo de gestión para la seguridad de la información ¿Qué aspectos consideraría para su implementación?

Director: Moodle es la plataforma base y su lenguaje es abierto. Lo que debería controlarse es el hosting y dominios que siguen expuestos a amenazas, tanto de información de usuarios y contenidos de la institución, ya sea cuando el personal de TIC's está ausente o algún otro motivo.

Apoyo 1: Actualización constante del firewall ya sea en red y en computadoras.

Apoyo 2: Copias de seguridad de plataforma y archivos de administración en una sola base de datos.

Apoyo 3: Revisar punto por punto la red de todos los equipos con el fin de evitar un virus infeccioso que por medio de internet afecte la plataforma.

Apoyo 4: Realizar bitácoras y horarios fijos para mantenimiento de cada componente ya sea mantenimiento, creación o edición de contenidos, conocer a

fondo el uso de otras plataformas añadidas a la nuestra con el fin de conocer los riesgos que pueden causar.

Análisis: Como puede observarse, los aspectos a considerar para su implementación involucran una serie de recomendaciones orientadas a fortalecer la seguridad de la información. Entre ellas se encuentran la actualización del firewall y que se constituye en una desventaja actual para el centro, además de las copias de seguridad, revisión de la red para evitar vulnerabilidades frente a virus, y por último establecer horarios fijos para la intervención del sistema, a lo cual también debería sumarse el mantenimiento del hardware.

3.1.2. Resultados de las encuestas al talento humano.

Se aplicaron encuestas a clientes de la empresa, siendo una muestra de 370 personas que figuran como usuarios de la plataforma orientada a la enseñanza de ingreso en el Centro de Idiomas Buckingham English Center S.A. Una vez aplicadas, se presentan a continuación los hallazgos:

Información del cliente

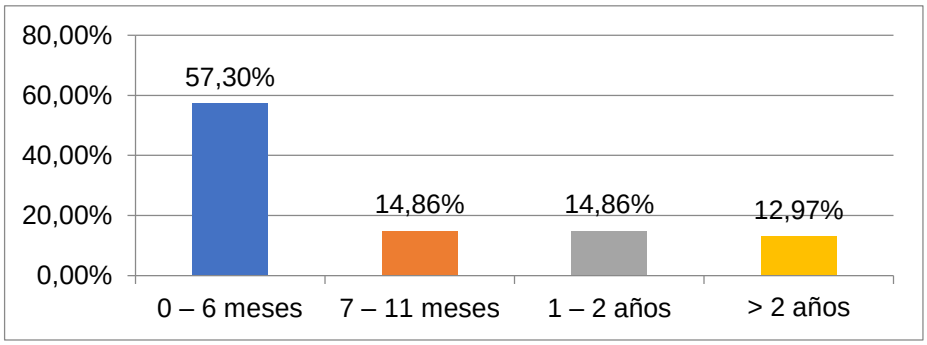
1. ¿Cuánto tiempo lleva como cliente del Centro de Idiomas Buckingham English Center S.A?

Tabla 1. Tiempo que lleva como cliente

Tiempo como cliente	Frecuencia absoluta	Frecuencia relativa
0 – 6 meses	212	57,30%
7 – 11 meses	55	14,86%
1 – 2 años	55	14,86%
> 2 años	48	12,97%
TOTAL	**370**	100,00%

Elaborado por: *El autor*

Figura 2. Tiempo que lleva como cliente



Elaborado por: *El autor*

La encuesta se remitió de manera aleatoria a los clientes, lo cual permite suponer que la institución posee más clientes con una trayectoria no mayor al año. Es decir, que su experiencia contratando el servicio es temprana, pero ello no evita que puedan exponer sus criterios en torno a la seguridad que perciben como clientes, en relación a la plataforma.

Además, al existir una alta concentración de clientes con una antigüedad inferior a los 12 meses, esto también refleja que es muy probable que finalicen su contrato en el corto plazo y abandonen el aprendizaje del idioma bajo la tutela de los docentes en el centro. Esto se sustenta al indicar que apenas 103 clientes superaron el año contratando el servicio, lo cual equivale al 27,83%. Cabe señalar que este valor se obtuvo sumando la tercera y cuarta opción de respuesta dentro de la encuesta.

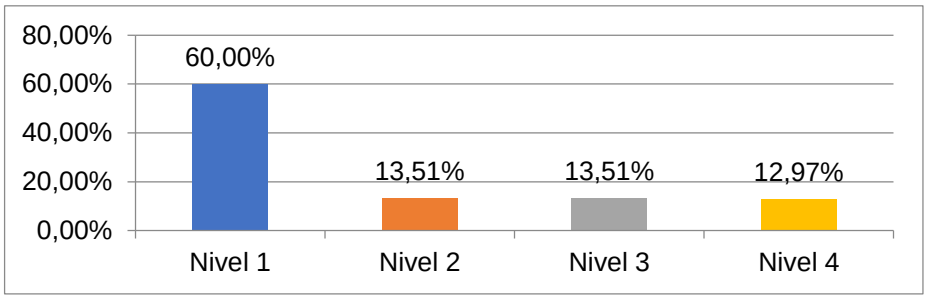
2. ¿En qué módulo de aprendizaje se encuentra actualmente?

Tabla 2. ***Módulo de aprendizaje que se encuentra cursando***

Aprendizaje	Frecuencia absoluta	Frecuencia relativa
Nivel 1	222	60,00%
Nivel 2	50	13,51%
Nivel 3	50	13,51%
Nivel 4	48	12,97%
TOTAL	**370**	100,00%

Elaborado por: *El autor*

Figura 3. Módulo de aprendizaje que se encuentra cursando



Elaborado por: *El autor*

A mayor nivel en el módulo, se supone que el cliente posee más conocimiento del idioma. La mayor concentración en el nivel 1 puede obedecer a la existencia de clientes con una trayectoria no superior al año dentro del centro.

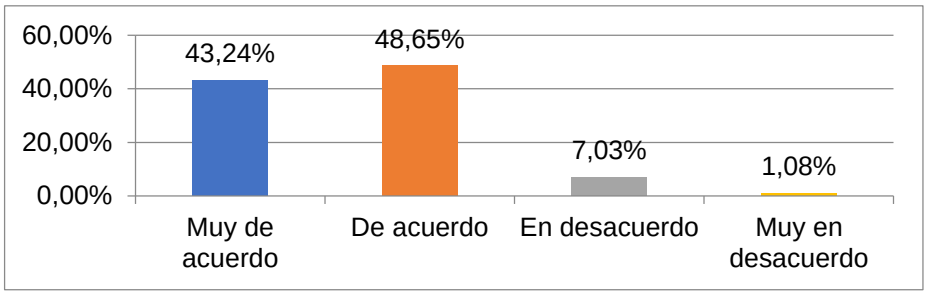
3. ¿Considera que la plataforma virtual aporta a su aprendizaje del idioma?

Tabla 3. Aporte de la plataforma a su aprendizaje

Aporte al aprendizaje	Frecuencia absoluta	Frecuencia relativa
Muy de acuerdo	160	43,24%
De acuerdo	180	48,65%
En desacuerdo	26	7,03%
Muy en desacuerdo	4	1,08%
TOTAL	**370**	**100,00%**

Elaborado por: *El autor*

Figura 4. Aporte de la plataforma a su aprendizaje



Elaborado por: *El autor*

Los clientes encuestados indicaron que perciben un gran aporte de la plataforma para el aprendizaje del inglés. Sin embargo, existe un grupo mínimo de consultados que mantiene una percepción contraria, mostrando estar "en desacuerdo" y "muy en desacuerdo", en un 7,03% y 1,08% respectivamente. Es decir que existe una alta probabilidad en este grupo minúsculo de clientes en abandonar el servicio.

Adicionalmente, a pesar de percibir que la plataforma apoya al aprendizaje del idioma, la antigüedad de clientes no es amplia, lo cual determina que existen otras razones que motivan al abandono temprano del curso.

Amenazas y vulnerabilidades

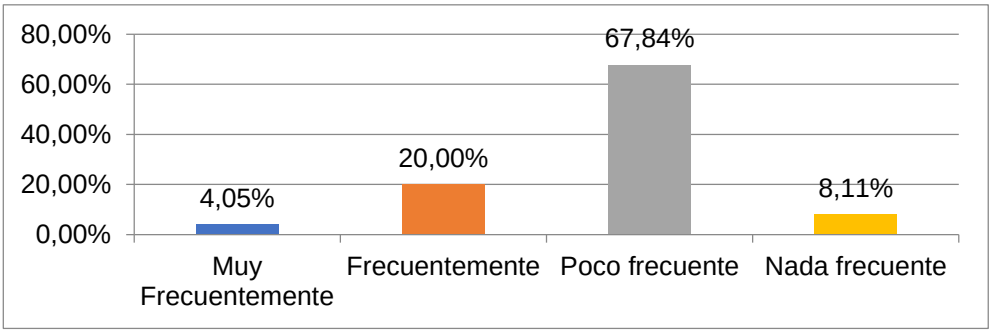
4. ¿Con qué frecuencia usted ha percibido que su información como cliente no ha estado segura en la plataforma del establecimiento?

Tabla 4. Percepción de inseguridad en su información

Confidencialidad	Frecuencia absoluta	Frecuencia relativa
Muy Frecuentemente	15	4,05%
Frecuentemente	74	20,00%
Poco frecuente	251	67,84%
Nada frecuente	30	8,11%
TOTAL	**370**	**100,00%**

Elaborado por: *El autor*

Figura 5. Percepción de inseguridad en su información



Elaborado por: *El autor*

Respecto a la percepción de inseguridad en su información dentro de la plataforma, lo cual guarda relación a la confidencialidad, los clientes indicaron que, en su mayoría, no es frecuente que existan anomalías. Sin embargo, existen clientes que indicaron percibir inseguridad frecuentemente y muy frecuentemente, correspondiendo al 20,00% y 4,05% respectivamente.

El total de estos clientes asciende a 89, los cuales no sienten que el centro mantenga su información confidencial, pudiendo esto influir en el abandono temprano del curso y deterioro de su imagen en el mercado.

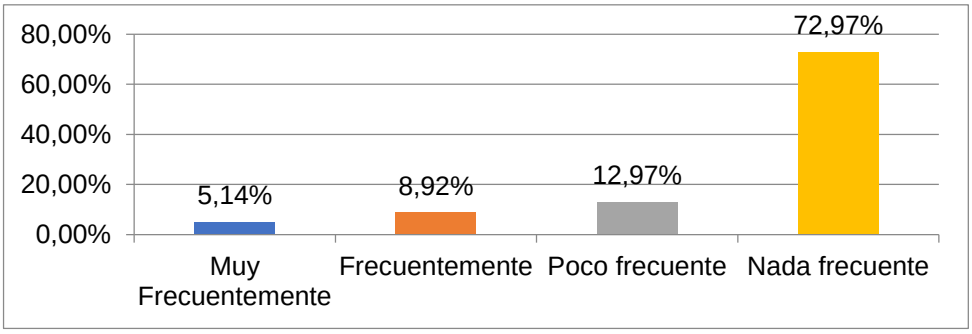
5. ¿Con qué frecuencia usted ha percibido que su progreso en los módulos de aprendizaje ha sido alterado y le genera un perjuicio?

Tabla 5. Percepción de alteraciones en su progreso dentro de la plataforma

Integridad	Frecuencia absoluta	Frecuencia relativa
Muy Frecuentemente	19	5,14%
Frecuentemente	33	8,92%
Poco frecuente	48	12,97%
Nada frecuente	270	72,97%
TOTAL	**370**	**100,000%**

Elaborado por: *El autor*

Figura 6. Percepción de alteraciones en su progreso dentro de la plataforma



Elaborado por: *El autor*

Respecto a percibir si su progreso en los módulos ha sido alterado, los consultados indicaron que es nada y poco frecuente, equivalentes al 72,97% y 12,97% respectivamente. El saldo restante, y que correspondería al 14,06% considera que estas alteraciones son frecuentes y muy frecuentes, influyendo negativamente en su experiencia como clientes.

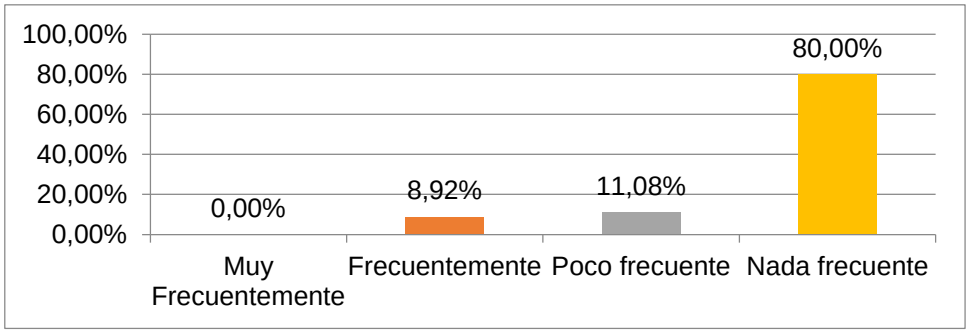
6. ¿Qué tan frecuente suele denegarse o impedirse el acceso a la plataforma sin previo aviso?

Tabla 6. Problemas en el acceso a la plataforma

Accesibilidad	Frecuencia absoluta	Frecuencia relativa
Muy Frecuentemente	0	0,00%
Frecuentemente	33	8,92%
Poco frecuente	41	11,08%
Nada frecuente	296	80,00%
TOTAL	**370**	**100,00%**

Elaborado por: *El autor*

Figura 7. Problemas en el acceso a la plataforma



Elaborado por: *El autor*

En relación a la frecuencia con la cual los clientes experimentan problemas con el acceso a la plataforma, se pudo evidenciar que resultan nada y poco frecuentes en un 80,00% y 11,08% respectivamente. Si bien, no existen registros de clientes que perciban estos problemas en forma muy frecuente, sí indican que son frecuentes en un 8,92%, deteriorando así su satisfacción en el servicio.

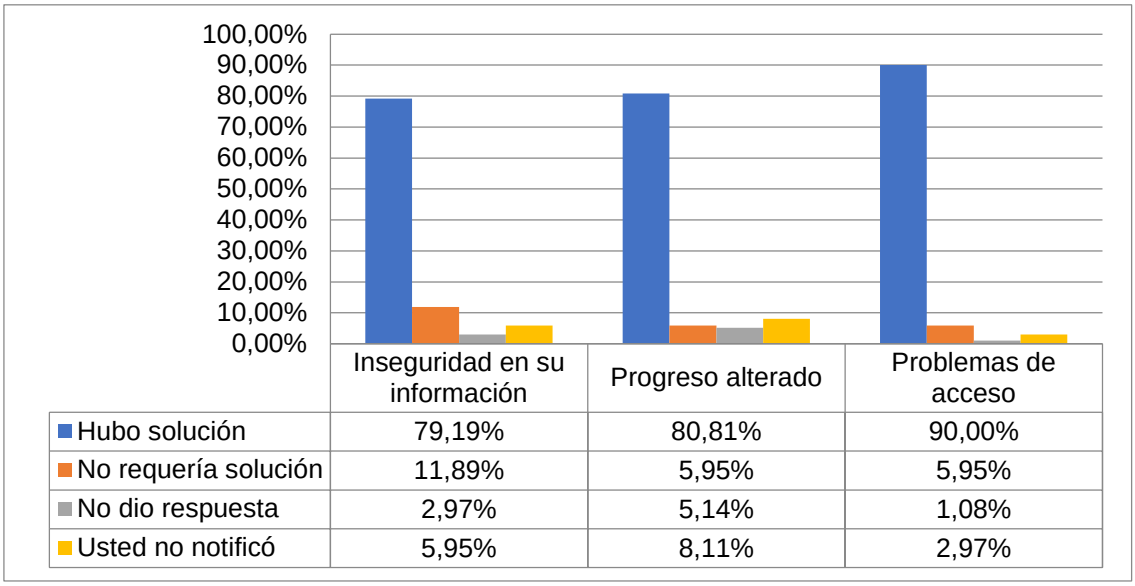
7. ¿Qué acción ha tomado la empresa ante los incidentes de vulnerabilidad reportados?

Tabla 7. Acciones de la empresa frente a los incidentes de vulnerabilidad

Incidente	Hubo solución	No requería solución	No dio respuesta	Usted no notificó	Total
Inseguridad en su información	293	44	11	22	370
Progreso alterado	299	22	19	30	370
Problemas de acceso	333	22	4	11	370

Elaborado por: *El autor*

Figura 8. Acciones de la empresa frente a los incidentes de vulnerabilidad



	Inseguridad en su información	Progreso alterado	Problemas de acceso
Hubo solución	79,19%	80,81%	90,00%
No requería solución	11,89%	5,95%	5,95%
No dio respuesta	2,97%	5,14%	1,08%
Usted no notificó	5,95%	8,11%	2,97%

Elaborado por: *El autor*

Conociendo que existen clientes que han experimentado problemas con la confidencialidad, accesibilidad e integridad de su información dentro de la plataforma, se les consultó de qué forma la empresa había respondido a estas anomalías. Si bien, se evidencia un alto índice de reportes de estos eventos que han sido solucionados por el centro, existe un porcentaje de clientes que no los ha dado a conocer. Es decir, continúan experimentando inseguridad y esto podría influir en la cancelación del contrato y deterioro de la imagen que percibe del centro.

También existen ocasiones en las cuales el cliente notificó a la empresa pero no recibió ninguna respuesta. Esto puede obedecer a que las observaciones son recientes y aún siguen procesándose, ya que el centro comunica cuando los problemas no requieren ser solucionados y es solo una duda o confusión por parte del usuario.

En este caso, las limitaciones principales corresponden a aquellos casos en los cuales el cliente no recibe respuesta o no notifica, lo cual significa que aún sigue experimentando el problema, siendo mayor en las situaciones cuando su progreso ha sido alterado, seguido de inseguridad en su información ingresada en la plataforma y finalmente, problemas con el acceso al sistema.

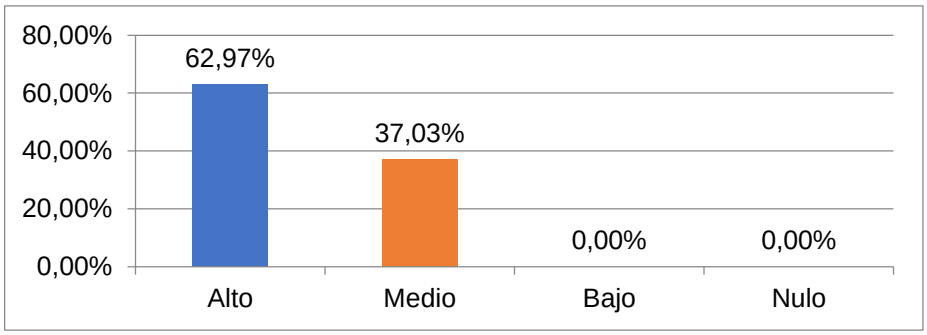
8. En función a su experiencia como cliente ¿Cómo califica el nivel de seguridad de su información en el centro?

Tabla 8. Calificación de la seguridad de su información

Percepción de seguridad	Frecuencia absoluta	Frecuencia relativa
Alto	233	62,97%
Medio	137	37,03%
Bajo	0	0,00%
Nulo	0	0,00%
TOTAL	**370**	**100,00%**

Elaborado por: *El autor*

Figura 9. Calificación de la seguridad de su información



Elaborado por: *El autor*

Respecto a la seguridad de la información que el cliente percibe, una vez conocidas las limitaciones en la confidencialidad, integridad y accesibilidad, puede evidenciarse que es alta y media con el 62,97% y 37,03% respectivamente. Sin embargo, debe tenerse en cuenta que existen limitaciones que pueden influir en su percepción negativa en la calidad del servicio que perciben y motivar al cierre de temprano de contratos.

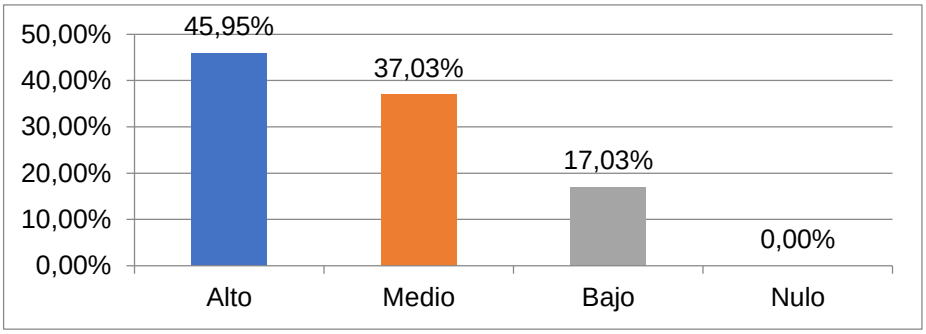
9. ¿Cómo evalúa usted su nivel de satisfacción global como cliente de este centro?

Tabla 9. Nivel de satisfacción global como cliente

Satisfacción como cliente	Frecuencia absoluta	Frecuencia relativa
Alto	170	45,95%
Medio	137	37,03%
Bajo	63	17,03%
Nulo	0	0,00%
TOTAL	**370**	**100,00%**

Elaborado por: *El autor*

Figura 10. Nivel de satisfacción global como cliente



Elaborado por: *El autor*

Sobre los niveles de satisfacción, existe un grupo significativo de clientes que mantienen un nivel de satisfacción alto y medio, mientras un 17,03% indicó que era bajo. Si bien, no existe una satisfacción nula, debe indicarse que el servicio ofrecido por la entidad no cubre en su mayoría las expectativas de los clientes, lo cual puede deteriorar la imagen que perciben del centro.

Tratamiento del riesgo

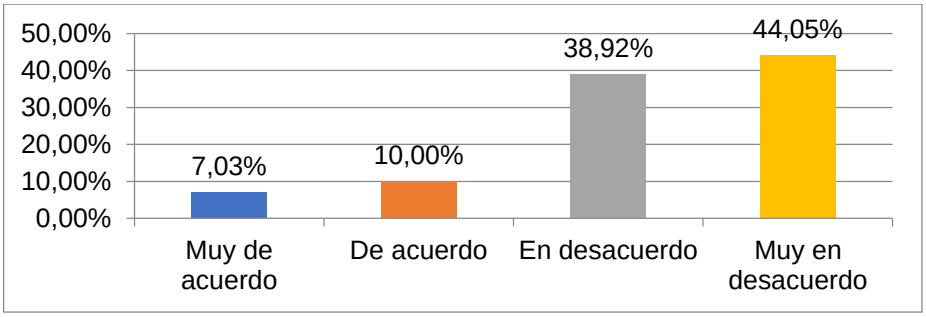
10. ¿Conoce usted las acciones realizadas por la empresa para fortalecer la seguridad de la plataforma virtual que usted utiliza?

Tabla 10. Conocimiento de acciones realizadas por la empresa para fortalecer la seguridad

Conocimiento de acciones	Frecuencia absoluta	Frecuencia relativa
Muy de acuerdo	26	7,03%
De acuerdo	37	10,00%
En desacuerdo	144	38,92%
Muy en desacuerdo	163	44,05%
TOTAL	**370**	**100,00%**

Elaborado por: *El autor*

Figura 11. Conocimiento de acciones realizadas por la empresa para fortalecer la seguridad



Elaborado por: *El autor*

En las entrevistas se evidenció que el centro realiza controles cada 15 días para fortalecer la seguridad de la información, además de respaldar los datos. A fin de evidenciar si los clientes conocen estos controles, se formuló esta pregunta, obteniéndose como respuesta que mantiene un amplio desconocimiento sobre estas acciones. Cabe señalar que, el difundirlas podría contribuir a reducir la inseguridad que los clientes lleguen a percibir, y que incluso no obedece a problema alguno, sino a confusión o error del propio usuario.

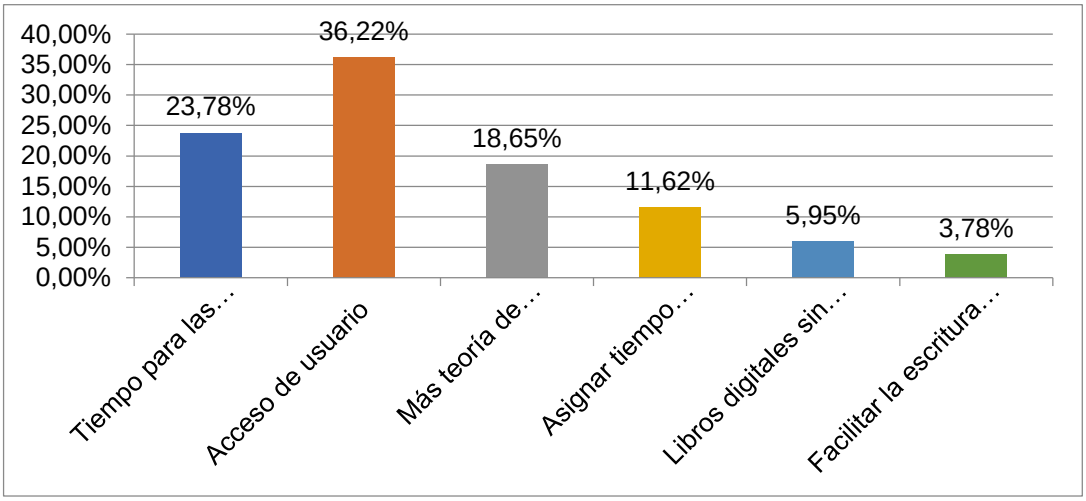
11. ¿Qué recomendaciones usted daría para mejorar su experiencia como usuario de la plataforma virtual, relacionadas o no a la seguridad?

Tabla 11. Recomendaciones para mejorar su experiencia como usuario

Recomendaciones	Frecuencia absoluta	Frecuencia relativa
Tiempo para las evaluaciones	88	23,78%
Acceso de usuario	134	36,22%
Más teoría de contenido	69	18,65%
Asignar tiempo según los ejercicios	43	11,62%
Libros digitales sin costo	22	5,95%
Facilitar la escritura de caracteres	14	3,78%
Total	370	100,00%

Elaborado por: *El autor*

Figura 12. Recomendaciones para mejorar su experiencia como usuario



Elaborado por: *El autor*

En esta pregunta se evidenciaron una serie de recomendaciones que los clientes consideran que deberían ser aplicadas por el centro para una mayor satisfacción. En primer lugar está el acceso del usuario a la plataforma, existiendo complicaciones respecto al método de contraseñas y que puede influir

a que la accesibilidad sea catalogada como deficiente, esto a pesar que no exista riesgo alguno a accesos no autorizados.

En segundo lugar está el tiempo para las evaluaciones, ya que los clientes no logran cumplir todos los ejercicios en el tiempo actual. Esto guarda relación con otra de las recomendaciones, la cual comprende el asignar tiempo según los ejercicios, ya que perciben que son muchos y no logran completarlos todos.

Seguido de esto, se encuentra el incrementar la teoría, además de incluir a la plataforma libros digitales gratuitos que podrían fortalecer su aprendizaje del idioma. Finalmente mencionaron el facilitar la escritura de caracteres, considerando que el inglés requiere el uso de apóstrofes, entre otros signos cuya escritura no está configurada en todos los teclados, dificultando así el desarrollo de ejercicio y perjudicando al estudiante.

3.2. Análisis comparativo, evolución, tendencias y perspectivas

Con los resultados obtenidos tras la recolección de datos, pudo evidenciarse que en el Centro de Idiomas Buckingham English Center S.A se realizan controles para garantizar la seguridad de la información del cliente, involucrando controles quincenales en donde se identifican debilidades y amenazas que serán corregidas, además de realizarse respaldos de los datos evitando que gran volumen de información se pierda o deteriore en la plataforma.

Aunque no han existido problemas de seguridad, sí existen debilidades que pueden poner en riesgo la información. Sin embargo, contrario a esto, en la entidad no se ha implementado un modelo de gestión que contribuya a minimizar tal riesgo, demostrándose que existe una débil cultura hacia la prevención. Además, los controles que aplica el departamento de sistemas actualmente son desconocidos por los clientes, lo cual incrementa su percepción de inseguridad.

Además, se refleja que los clientes suelen percibir, aunque en baja frecuencia, problemas de confidencialidad, accesibilidad e integridad de la información, los

cuales son corregidos en su mayoría por la empresa, existiendo casos que no han sido solucionados o que incluso no han sido reportados por los clientes.

Esto impide mejorar su experiencia y puede provocar la cancelación del contrato, reduciendo así los ingresos del establecimiento. Por tal motivo, existen usuarios con un bajo nivel de satisfacción, quienes recomiendan una serie de mejoras, entre las cuales figura el hacer más sencillo el acceso a la plataforma para los clientes, evitando confusiones y una percepción negativa en relación al servicio.

De esta manera, la adopción de un modelo de gestión para la seguridad de la información debe orientarse a fortalecer los controles en la plataforma, corrigiendo las debilidades existentes, además de acompañarse de mejoras a la experiencia del cliente y así incrementar su satisfacción, permitiendo fidelizarse y evitar que cancelen sus contratos en el corto plazo.

CAPÍTULO IV. PROPUESTA

4.1. Justificación

En relación a los datos recolectados en la entidad, es posible determinar que la empresa no ha implementado un sistema de gestión de la seguridad de la información, existiendo de esta manera mayor riesgo a problemas en la confidencialidad, integridad y disponibilidad de su información. Los hallazgos muestran que, si bien no han ocurrido problemas, existen debilidades respecto al tratamiento de los datos, además de percepciones negativas de los usuarios externos respecto a cómo la empresa gestiona su información y la seguridad que le brinda.

Adicionalmente, consideran que han surgido anomalías respecto a sus avances en los módulos dentro de la plataforma y el acceso a la misma que, si bien han sido en su mayoría corregidos por la empresa, algunas de ellas no tuvieron respuesta. A su vez, existen casos en los cuales el cliente prefiere no notificar alguna novedad, quedando con la incertidumbre sobre si es en realidad un problema de la plataforma, de su equipo o por mal uso del mismo.

Todo ello influye a que existan clientes que denotan un bajo nivel de satisfacción, recomendando mejoras en el acceso a la plataforma, mejorar los tiempos para realizar las evaluaciones y facilitar la escritura para los usuarios de la plataforma. Por otra parte, el personal encargado de la plataforma destaca la necesidad de una mejor planificación en el mantenimiento y otras medidas como evitar problemas con la seguridad de los datos, tales como fortalecer medidas para prevenir correos no deseados, incluir cifrado de dispositivos y activar el Firewall Gateway a fin de evitar consecuencias negativas en los equipos y redes, lo cual podría causar pérdida de información, daños en la plataforma y así deteriorar el servicio al cliente

Ante esta situación, el estudio presentará un modelo de gestión de seguridad de la información como apoyo al personal del departamento de TIC´s de Buckingham, modelo que se estructuraría en función de la Norma ISO 27001, la cual define cómo se planifica, instaura, comprueba y controla un SGSI, teniendo

en cuenta que hace referencia a un conjunto de políticas y procedimientos orientados a administrar la información en una entidad, garantizando que esta sea confidencial, íntegra y se encuentre disponible cuando se requiera.

4.2. Propósito general

Como propósito, la propuesta responderá al tercer objetivo específico, el cual indica el proveer un modelo de gestión de seguridad de la información como apoyo al personal del departamento de TIC´s de Buckingham. De esta manera se terminaría de cumplir el objetivo general y que obedece al desarrollo de este modelo.

4.3. Desarrollo

4.3.1. Definir la política

Dentro de esta sección se establece cómo está conformado el comité de seguridad de la información, además de todo lo relacionado a la declaración y notificación e incidentes para el Centro de Idiomas Buckingham English Center S.A. También se presentan las políticas que formarán parte de SGSI y que se derivan de los hallazgos de la recolección de datos y otros aspectos que tendrían que considerarse.

4.3.1.1. Comité de Seguridad de la Información

Para el Centro de Idiomas Buckingham English Center S.A, a fin de garantizar que exista apoyo y dirección de la gerencia para brindar soporte al sistema de gestión de la seguridad de la información, garantizando el compromiso en la organización, el uso de recursos de forma apropiada, la aplicación correcta de controles de seguridad de la información, incluyendo la forma comunicación de políticas y de su mantenimiento.

Dicho esto, el comité dentro del centro debe estar conformado por:

- Director General Administrativo.

- Director del talento humano.

- Director del área comercial.

- Director de Tecnologías de Información y Comunicación TIC´s.

- Personal de apoyo para la dirección de Tecnologías de Información y Comunicación TIC´s.

Entre sus funciones se encuentran:

- Asegurar la implementación del modelo de gestión de la seguridad de la información de forma coordinada.

- Ordenar el diagnóstico y revisar el estado de la seguridad de la información dentro del centro de idioma Buckingham English Center S.A

- Realizar el acompañamiento, además de impulsar el desarrollo de proyectos para la seguridad dentro de la entidad.

- En relación a acciones que permitan alcanzar un ambiente de seguridad en la empresa, serán los responsables de coordinarlas y dirigirlas, de tal manera que logren las metas y los objetivos del centro.

- De ser requeridas, aprobar el empleo de metodologías y procesos orientados a garantizar la seguridad de la información.

- Participar activamente en la formulación y evaluaciones de planes que tengan como finalidad mitigar y/o eliminar riesgos

- Revisar periódicamente el sistema de gestión de la seguridad de la información en un periodo mínimo de dos veces al año y, en base a los resultados, definir acciones enfocadas a fortalecerla.

- Promover prácticas orientadas a garantizar la seguridad de la información dentro del centro.

- Comunicar y poner a disposición de la gerencia información respecto a situaciones que puedan provocar un impacto negativo a la seguridad dentro del centro

4.3.1.2. Comité de gestión de incidentes

Se determinó la necesidad de un comité de gestión de incidentes, ordenándose su creación. Estará encabezado por el Director de Tecnologías de Información y Comunicación TIC´s y su equipo de trabajo quienes actualmente se encargan de garantizar que la plataforma opere de forma óptima, además están en la responsabilidad de dar solución a quejas y reclamaciones de los clientes.

Entre sus funciones pueden destacarse:

- La detección de todo tipo de incidentes relacionados a la seguridad, llevando para ello un monitoreo y verificación de la plataforma y los activos de la información.

- Atención y resolución de incidentes.

- La recolección y el análisis de todo tipo de evidencia digital que soporte los incidentes ocurridos para llevar un registro de estos.

- Comunicar, respecto a los incidentes de seguridad, al responsable de primera línea, siendo el Director de Tecnologías de Información y Comunicación TIC´s. A su vez, este se encargará de comunicar a la gerencia de ser necesario, y el Comité de Seguridad de la Información.

- Llevar a cabo la auditoría y trazabilidad de la seguridad informática dentro del centro, verificando que los equipos de trabajo funciones de manera óptima y, respecto la plataforma, analizar las debilidad, amenazas y las brechas de seguridad.

- Calificación de los productos informáticos utilizados por la empresa a fin que se mantengan ajustados a los requerimientos mínimos de seguridad informática. Además, deben configurarlos y administrarlos de tal manera que funcionen de forma eficiente.

- Investigación y desarrollo, lo cual comprende la búsqueda de nuevos productos informáticos, los cuales hagan posible fortalecer las operaciones del área, brindando mayor protección a los clientes y reduciendo las brechas de seguridad como una forma de garantizar, en mayor medida, la seguridad de la información.

4.3.1.3. Declaración y notificación de incidentes

Se establecieron los parámetros a fin de declarar y notificar todo tipo de incidentes, respondiendo a cada uno de ellos de una manera sistemática. Cabe señalar que esto debe también ir orientado a reducir su ocurrencia, utilizándose esta información como punto de partida para el diseño de acciones de prevención y responder de manera efectiva, con rapidez, si llegaran a ocurrir como una forma de minimizar su impacto y el riesgo a la pérdida de información.

En relación a la notificación de incidentes, deben seguirse los siguientes pasos:

1. Un usuario interno o externo que perciba la materialización de un incidente relacionado a la seguridad deberá notificarlo al área y personal encargado de esta función, siendo el Área de Tecnologías de Información y Comunicación TIC´s. Esto puede ser mediante un correo, contacto telefónico o por medio de la plataforma del centro.

2. El personal del área verificará el tipo de incidente que se reporta a fin de darle solución. De esta manera indicará si efectivamente es un problema con la plataforma o ya corresponde a la infraestructura propia del cliente.

3. De comprobarse que corresponde a un problema del centro, se dará solución a aquello en forma inmediata.

4. En estos casos, para evitar que el cliente indique no haber recibido respuestas a su requerimiento, es importante que cada uno de ellos responda y, en caso de requerir mayor tiempo para su solución, mencionarle que se encuentra en proceso de gestión. Esto demostrará al usuario externo que existe compromiso en brindar un servicio de calidad y que el Centro de Idiomas Buckingham English Center S.A. se preocupa por ellos.

5. Sobre la solución del incidente, luego de evaluarlo se determinarán las acciones para corregirlo y, una vez gestionado, es importante emitir un reporte como una forma de soportar la existencia de este problema y prevenir futuras reclamaciones de otros usuarios.

4.3.1.4. Políticas de seguridad

Las políticas se encuentran orientadas a garantizar que en la empresa se eviten todo tipo de incidentes y problemas relacionados a la seguridad de la información. Como objetivo de esta sección se plantea:

Mostrar con claridad las políticas de seguridad que deben ser cumplidas por los directivos del Centro de Idiomas Buckingham English Center S.A. y demás personal, sin importar el puesto que desempeñe.

El alcance de las políticas involucra:

Su cumplimiento es obligatorio para el personal, especialmente los que hagan uso directamente de las Tecnologías de Información y Comunicación, al igual que los activos de información.

En relación a las políticas, estas se describen a continuación:

1. La información contenida en los equipos, demás soportes y respaldos, es de carácter confidencial. Por ende, ningún trabajador podrá hacer uso de ella para fines personales ni tampoco facilitará su acceso o difusión, sin la debida autorización de la gerencia.

2. Los equipos que se hayan designado al personal, especialmente al Área de TIC´s, son de uso exclusivo y solo podrán hacer uso de ellos con fines laborales.

3. De provocar daños a los equipos o cualquier otro soporte a la información, deberán asumir los costos que ello implica.

4. Todo uso indebido de la información y los equipos será motivo de sanción e incluso despido del personal responsable de comprobarse faltas gravísimas que generen un perjuicio para la empresa.

5. El mantenimiento de la plataforma debe realizarse cada 15 días llevando una bitácora para el control de novedades. Para tales efectos, la fecha de su ejecución sería cada 15 y fin de mes, cuatro horas antes de que finalice la jornada laboral. De resultar estos días no laborables, se realizará en el día laborable próximo.

6. El mantenimiento de los equipos informáticos se realizará mensualmente, evidenciando cómo funcionan y si requieren alguna intervención en su hardware o software.

7. Todo incidente de seguridad que el usuario externo o interno reporte, debe quedar documentado y realzar el debido seguimiento hasta su solución. De

ser un usuario externo, se le indicará por qué experimenta el problema y, de requerir la intervención del centro, se le indicaría en qué momento se gestionaría el trámite, en un plazo no superior a las 48 horas. Cuando los problemas obedezcan al mal uso de la plataforma o de la infraestructura propia del usuario, se le darán pautas respecto a cómo corregirla, evitando su insatisfacción.

8. Semanalmente se revisarán los incidentes que se hayan reportado, identificando cuáles se han generado con mayor frecuencia a fin de utilizarlos como pautas para el desarrollo de planes de acción que fortalezcan la seguridad de la información.

4.3.2. Definir el alcance del SGSI

El sistema de gestión de la seguridad de la información se orienta a gestionar y minimizar el riesgo en la seguridad de la información en el Centro de Idiomas Buckingham English Center S.A, evitando que los clientes vean vulnerados sus datos y que su experiencia en el uso de la plataforma para la enseñanza del idioma inglés se vea deteriorada, siendo dicha plataforma el principal servicio que ofrece el establecimiento.

4.3.3. Análisis de riesgos

En este punto se procedió a realizar la identificación de los riegos relacionados a la gestión de la seguridad de la información. Cabe señalar que previamente se llevó a cabo la recolección de datos mediante entrevistas y encuestas como una forma de detectar problemas que puedan percibirse en torno a este aspecto. De esta manera, utilizando la información recabada, se describen a continuación cada uno de los riesgos:

- Existen clientes que no notifican incidentes en la plataforma respecto a inseguridades percibidas a la seguridad, confidencialidad y disponibilidad de su información.

- Existen controles quincenales en la plataforma virtual para detectar y corregir debilidades y amenazas en la seguridad de la información; sin embargo, no se establecen con claridad cómo se programan

- Falta de protocolo https. para la plataforma y páginas web; lo cual resta seguridad a la conexión entre el servidor y los usuarios, exponiéndolos a amenazas que pueden provocar el robo y pérdida de información.

- No suelen realizarse copias de seguridad para contenido y datos de los usuarios. De esta manera, en caso que se borren, no existiría ningún tipo de respaldo.

- Pérdida de contenidos externos, específicamente aquellos utilizados para la creación de módulos de estudio.

- El cifrado de dispositivos nulos, lo cual implica los equipos están activos con el sistema operativo libremente, haciendo más fácil el robo de información y acceso no autorizado a éstos

- Firewall Gateway desactivado, lo cual afecta a equipos y redes de manera directa con dispositivos externos.

- El mantenimiento del hardware no se encuentra planificado.

- No se observan equipos informáticos de reemplazo que permitan sustituirla, total o parcialmente, en caso de alguna falla o daño.

- Las copias de respaldo no mantienen un almacenamiento lógico que permita identificar rápidamente información necesaria para su consulta.

- El acceso a la plataforma presenta dificultades, lo cual genera insatisfacción del cliente.

- Deficiencia en el control de códigos maliciosos o malware.

Si bien, los resultados mostraron que el centro no ha sufrido ningún tipo de problemas de seguridad de la información y el funcionamiento de la plataforma, sus declaraciones denotan que han sufrido pérdida de información del cliente, además de existir una serie de debilidades que incrementan el riesgo a sufrir algún problema de confidencialidad, seguridad y/o disponibilidad de la información.

Debe añadirse que incluso el cliente percibe inseguridad, lo cual denota la necesidad de mejorar la gestión de la seguridad de la información, concentrándose en los riesgos antes descritos.

4.3.4. Gestión del riesgo y selección de controles a implementar

A fin de minimizar estos riesgos y evitar la ocurrencia de problemas relacionados a la seguridad de la información en el centro de idiomas se plantean los siguientes puntos:

4.3.4.1. Responsabilidades de la alta gerencia

Teniendo en cuenta que el involucramiento de la alta gerencia es uno de los principales puntos a considerar dentro del Sistema de Gestión de la Seguridad de la Información según la norma ISO 27001, garantizando que la gestión del negocio no presente mayores problemas, se establecen sus responsabilidades para alcanzar el éxito en la implementación.

También debe fomentarse la idea de que la gestión de la seguridad de la información no es un tema meramente tecnológico ni responsabilidad de los directivos, sino también de todos los trabajadores, quienes deben asegurar que los soportes físicos y virtuales de la información funcionen en forma óptima

Por otra parte, deben mostrar compromiso en implementar, operar, monitorear, mantener, revisar y mejorar el Sistema de Gestión de Seguridad de la Información ejecutando las siguientes iniciativas:

- Promover la adopción de las políticas orientadas a garantizar la seguridad de la información.

- Garantizar que se cumplan los objetivos y planes descritos para el Sistema de Gestión de la Seguridad de la Información, además de comunicar a todo el equipo humano la importancia de cumplirlos.

- Ordenar que se lleven a cabo revisiones periódicas al sistema de gestión de seguridad de la información cada fin de mes, debiendo realizar una revisión profunda al menos dos veces al año

- Proporcionar todos los recursos económicos que se requieran para fortalecer la seguridad de la información, y por ende la protección de los datos de los clientes, incluyendo todos los desembolsos que se requieran en cada etapa del sistema.

- Monitorear la implementación del sistema de gestión.

4.3.4.2. Asignación de los recursos

Es importante que, a fin de lograr cumplir todos los aspectos descritos en el Sistema de Gestión de la Seguridad de la Información, se designen los recursos necesarios, debiendo garantizarlos la alta gerencia para:

- Lograr que todos los procedimientos relacionados a la seguridad de la información vayan acorde a los requerimientos del negocio.

- Disponer de equipos informáticos de respaldo que hagan posible continuar las operaciones en caso de algún problema o avería de los utilizados.

- Fortalecer la seguridad de la información en el centro, previa comprobación de la necesidad.

- Implementar y mejorar el Sistema de Gestión de la Seguridad de la Información.

4.3.4.3. Formación y concienciación

Para lograr el éxito con la implementación del Sistema de Gestión de la Seguridad de la Información se requiere que exista una correcta formación y concienciación en el centro de estudios Buckingham. Para tales efectos, la alta gerencia en coordinación con el Director de Tecnologías de Información y Comunicación TIC´s debe garantizar que cada trabajador posea responsabilidades definidas de manera coherente, mismas que deben ser correctamente asignadas en el Sistema de Gestión de Seguridad de la Información. Dicho esto deberán:

- Determinar en forma clara qué competencias requiere cada trabajador para desarrollar tareas que se le asignarán. Deberá prestarse mayor atención al Área de Tecnologías de Información y Comunicación en donde cada miembro del equipo de apoyo a la dirección debe tener responsabilidades respecto a garantizar la Seguridad de la Información.

- Fortalecer el conocimiento del personal mediante planes de formación debidamente programados, especialmente dirigidos al personal del área de TIC´s.

- Evaluar la eficiencia del trabajador mediante el cumplimiento de sus funciones de forma óptima y en los parámetros acordados, permitiendo considerar si el personal seleccionado es idóneo, debe ser reemplazado o capacitado.

- Llevar un registro de todos los trabajadores, dando énfasis a los estudios realizados, experiencias laborales previas, formación recibida y habilidades que posea.

Cabe señalar que es obligación de la gerencia y del director del área de TIC´s que los trabajadores se involucren y hagan conciencia en la importancia de la seguridad de la información en el centro, a fin que participen activamente en el alcance de los objetivos del Sistema de Gestión de Seguridad de la Información.

4.3.4.4. Revisión del Sistema de Gestión de la Seguridad de la Información

Como principal responsabilidad de la gerencia y la dirección del área de tecnologías de información y comunicación TIC´s está el garantizar que el sistema de gestión de la seguridad de la información sea eficaz, eficiente y adecuado en función a la entidad. Por tal motivo es esencial que, como mínimo dos veces al año, se proceda a su revisión, centrándose en los siguientes aspectos para la toma de decisiones:

- Un análisis de las amenazas y vulnerabilidades que continúan manteniéndose dentro del centro a pesar de las mejoras aplicadas.

- Nuevas amenazas y vulnerabilidades detectadas, detallando sus causas.

- Resultados de las revisiones periódicas realizadas al sistema para comprobar su eficacia.

- Listado de problemas que hayan ocurrido una vez implementado el sistema, estos relacionados a la seguridad de la información.

- Efectividad de las acciones preventivas y correctivas aplicadas para prevenir y dar solución a los problemas.

- Recomendaciones de mejoras que haya realizado el Comité de Gestión de Incidentes a fin de fortalecer la seguridad de la información.

- El estado de todos los equipos dentro de la entidad, entre otros activos de la información.

- Detalle de quejas y reclamos realizados por los usuarios de la plataforma de la empresa, identificando si existen nuevas, y en qué medida se han reducido las anteriores.

La revisión del sistema debe permitir a los responsables:

- Fortalecer la eficiencia del Sistema de Gestión de la Seguridad de la Información a fin de minimizar en mayor medida los riesgos.

- Actualización de las acciones encaminadas al tratamiento de los riesgos, pudiendo identificar hasta otros que no hayan sido detectados con anterioridad.

- Modificar los procedimientos y controles que afecten a la seguridad dentro del centro.

- Fortalecer y mejor el cómo se mide la eficiencia de los controles, para lo cual debe considerarse el grado de ocurrencia de problemas relacionados a la seguridad de la información.

4.3.4.5. Compromisos del Comité de Seguridad de la Información

Como parte de su compromiso está el garantizar que este sistema se implemente de una forma óptima, además de realizar las evaluaciones que permitan detectar las vulnerabilidades existentes, además de las oportunidades respectos a la mejora en el centro de la seguridad de la información.

Cabe destacar que resulta también imprescindible que lideren el proceso relacionado a la gestión de los incidentes de seguridad que llegasen a ocurrir, identificando las causas, responsables y las recomendaciones que permitan evitarlos y mejorar la seguridad de la información. Por tal motivo, también es importante que se transmita a todo el equipo de trabajo la importancia de la

seguridad de la información, además de proporcionarles una mayor preparación y capacitación, sumando a la selección personal idóneo.

Esto permitiría no solo garantizar que el equipo humano está calificado para desempeñar sus funciones, sino también que se encuentran comprometidos a la seguridad de la información en el centro.

4.3.4.6. Selección de los controles para el tratamiento de los riesgos

Los controles para el tratamiento de los riesgos, mismos que fueron previamente descritos, son planteados en la presente sección con la finalidad de mitigarlos. El objetivo de este apartado es presentar instrucciones que sirvan para el cumplimiento y concientización sobre el correcto uso de los equipos y demás activos de información, entre otros aspectos claves del sistema de gestión de la seguridad de la información.

Como parte del alcance, es importante destacar que su cumplimiento es obligatorio por parte de todo el talento humano del centro, especialmente el área de Tecnologías de Información y Comunicación TIC´s. Cabe señalar que el Comité de Seguridad de la Información garantizará el cumplimiento de estos controles y revisará periódicamente cada uno de ellos, determinando si se deberán realizar ajustes para responder a nuevas amenazas que se susciten.

4.3.4.6.1. Control de las políticas

- Se publicará en la intranet del Centro de Idiomas Buckingham English Center S.A., difundiéndose además por otros medios de comunicación internos, lo cual permita que los empleados las conozcan y las implementen para minimizar el riesgo en la seguridad de la información.

- El área de Tecnologías de Información y comunicación se encargará de su difusión, además de revisarlas cada tres meses, a fin que se modifiquen o actualicen de ser el caso.

- Para fortalecer la adopción de las políticas es esencial que los empleados reciban instrucciones apropiadas sobre el uso correcto de los sistemas de información, además de sus recursos y la importancia en garantizar dicha seguridad.

- Es importante monitorear al personal, especialmente los que tengan a su disposición equipos informáticos y otros activos de información, garantizando que cumplan las normas sobre su utilización y tratamiento de los datos.

- Las actividades que se realicen, a fin de garantizar la seguridad de la información, deben ser coordinadas por el Director de Tecnologías de Información y Comunicación.

- La información que los aspirantes a los cargos proporcionen a la empresa debe ser validada a fin de cubrir esas vacantes. A su vez, previa a la ocupación del cargo, debe explicarse al interesado todo lo referente al puesto, sus responsabilidades, políticas existentes y las consecuencias por su incumplimiento

- Los trabajadores firmarán documentos de confidencialidad en donde el trabajador se obligará a la no divulgación de los datos.

- Cuando un trabajador cese sus funciones, el documento de compromiso de confidencialidad firmado tendría una vigencia de doce meses a partir de la fecha en la cual se confirme su desvinculación del cargo.

- Los usuarios internos deben ser correctamente inducidos respecto a sus responsabilidades, especialmente aquellos que involucren en manejo de equipos informáticos y demás activos de información.

- Los usuarios externos, es decir los clientes, deben ser correctamente inducidos respecto al uso de la plataforma para la enseñanza de idiomas.

De esta forma, estará totalmente capacitado y se reducirá la incertidumbre en la seguridad de la información por el desconocimiento en su uso.

4.3.4.6.2. Controles de activos

- Todos los activos de información en la empresa deben ser inventariados, ordenándose de forma cronológica y por tipo, a fin de garantizar que se ubique rápidamente información cuando sea requerida.

- Todo trabajador que reciba un equipo informático o cualquier otro activo de soporte de información deberá firmar un acta en donde declara que lo recibe en óptimas condiciones y se compromete a su devolución en las mismas condiciones una vez deje de utilizarlo. En caso de equipos informáticos cuyo deterioro obedezca al uso propio del mismo, el trabajador responsable deberá informar para la reparación o sustitución del mismo hasta su devolución posterior.

- El inventario de los activos de información y equipos informáticos se realizará cada cuatro meses, en donde se evaluará el estado de cada uno de ellos. Cabe señalar que, en el caso de los equipos informáticos, la revisión para el mantenimiento preventivo se desarrollará el primer día laborable de cada mes, evidenciando que funcionen adecuadamente y la información que contienen se encuentra segura.

- En caso de evidenciarse un deterioro por mal uso del activo, se informará al Director de Tecnologías de Información y Comunicación para que ordene la sanción correspondiente al caso.

- Cuando se identifique el mal funcionamiento de un equipo informático, ya sea por indicación del usuario interno o durante la revisión del mismo, se procederá a gestionar su reparación de ser el caso. En caso que requiera sustitución, se gestionará firmando una nueva carta de compromiso sobre recibir el equipo en condiciones óptimas para su uso.

- Los activos que se encuentren y sobre los cuales no exista un registro o no pertenezcan al centro, serán revisados para verificar si contienen información confidencial del negocio. De poseerla, será borrada y se ubicará al dueño del mismo. En caso de no contar con esa información, se devolverá a quien indique ser su propietario, sin perjuicio de que el dueño sea otro, salvo haya sido autorizado para ello.

- Cuando los trabajadores devuelvan activos, llenarán un formulario de devolución del mismo, indicando que se encuentran en la misma condición en la que lo recibió. Para asegurar aquello serán revisados y, de encontrarse anomalías, se aplicaran las medidas correspondientes.

- Deben existir equipos informáticos que sirvan de respaldo en caso del deterioro de aquellos que se encuentran en uso. Para ello, debe ordenarse la compra de al menos dos equipos de repuestos completos para su funcionamiento y, de utilizarse, se gestionará una nueva compra para disponer de la misma cantidad de respaldo inicial. Dicha recompra será realizada si el activo que fue sustituido no puede ser reparado y tendrá que desecharse.

4.3.4.6.3. Control de los recursos humanos

- El director del talento humano debe garantizar que todos los trabajadores tengan clara sus funciones y que las responsabilidades están acorde a sus roles. Igual compromiso tendrá el Director de Tecnologías de Información y de Comunicación frente a su equipo de trabajo.

- El director del talento humano y de tecnologías de la información y comunicación validarán que la información que los aspirantes al cargo sea verás. Además, se contactará a empleadores previos, de presentar experiencias laborales, para consultar cómo fue su desempeño en otras instituciones.

- Los trabajadores, especialmente aquellos que tengan a su cargo equipos informáticos y demás activos que soporten información, recibirán una inducción respecto a la importancia de proteger la información y el activo que le será entregado por medio de un acta de compromiso, además de explicarse las sanciones que podrían aplicarse por su mal uso.

4.3.4.6.4. Controles frente a amenazas informáticas

- Todos los mantenimientos que se realicen sobre la plataforma y demás sistemas del centro deben ser documentados y comunicados al Comité de la Seguridad de la Información, especialmente si se detectaron debilidades y amenazas que deben ser corregidas.

- El área de tecnologías de información y comunicación deberá detectar e informar todo intento no autorizado e intención de vulnerar la seguridad de la información, tanto interno como externo. De observarse que hubo acceso no autorizado y vulneración de la información, se bloqueará el acceso a todos los sistemas y se corregirá, identificando luego el origen de la vulnerabilidad y si es posible encontrar al responsable.

- De ser una vulneración voluntaria del personal interno se procederá al despido del mismo con visto bueno y, de ser gravísimas, enfrentará una demanda para indemnización de los daños causados.

- Es importante que durante la revisión de la plataforma, proceso que se ha programado quincenalmente, también se realice la comprobación de las redes, antivirus y del firewall, para su actualización de ser el caso.

- Todo virus o malware detectado será documentado previa eliminación, detallando un informe. En caso de infección reiterada deberá considerarse la sustitución del antivirus y comprobación de la causa de dicha infección, verificando los sitios en los cuales navega el responsable del equipo en donde se detecta el problema.

- Las copias de seguridad que se realicen sobre la plataforma deben ser cargadas a la nube o en una sola base de datos, de manera ordenada para su consulta, con las respectivas medidas de seguridad para garantizar su acceso no autorizado. Dentro de este respaldo se incluirá el contenido y datos que los usuarios externos tengan en la plataforma.

- Deben realizarse pruebas periódicas a los métodos de respaldo de la información para garantizar que no se pierda información en el proceso. Además, se revisarán los respaldos anteriores en un intervalo mensual para comprobar que la información sigue íntegra.

- La documentación sobre el sistema se almacenarán en los servidores del centro y el acceso autorizado será único del Director de Tecnologías de la Información y Comunicación.

- El director del área de tecnologías de la información y comunicación será el responsable de implementar medidas para proteger la mensajería electrónica del centro frente a correo no deseado/spam.

- Toda falla que se presente en la plataforma y otros sistemas será tratada con un incidente de seguridad y se llevará a cabo el proceso descrito para la resolución.

- Se implementarán protocolo https. para la plataforma y páginas web a fin de garantizar la seguridad a la conexión entre el servidor y los usuarios.

- Los equipos informáticos del centro estarán cifrados y su acceso será exclusivo de su custodio, salvo los equipos para el director del área de tecnologías de información y comunicación que tendrá acceso a ello, tanto dentro o fuera del área del área a su cargo.

- El director de tecnologías de información y de comunicación, en conjunto a su equipo de trabajo, verificará los privilegios de acceso de los usuarios al

sistema, revisando sus contraseñas de acceso, validando mediante un informe el cumplimiento de esta gestión.

- El área de tecnologías de información y de comunicación debe garantizar a cada usuario una cuenta única mediante la cual pueda loguear en la plataforma y acceder a ella. Además, expondrá todas las precauciones a los usuarios, funcionamiento de la plataforma y todos los requerimientos mínimos para que pueda operar adecuadamente.

- Se prohíbe la instalación de programas sin autorización. De demostrarse aquello y de comprobarse que esto provocó un daño o problema en los sistemas que pudo o puso en riesgo la seguridad de la información, será motivo de desvinculación del responsable.

- Todo trabajador está en la obligación de informar, en caso de identificar algún incidente, debilidad o amenaza que ponga en riesgo la seguridad de la información en el momento que la detecte. Esto se realizará de manera formal al director del área de tecnologías de información y comunicación o su equipo de trabajo de ser el caso.

4.3.5. Obtener la aprobación de la dirección sobre los riesgos residuales propuestos

Esta aprobación deberá ser solicitada formalmente a la gerencia del centro quien además deberá evaluar el modelo propuesto junto al Director de Tecnologías de Información y Comunicación.

4.3.6. Obtener autorización de la dirección para implementar y operar el Sistema de Gestión de Seguridad de la Información

La autorización para la puesta en marcha del Modelo de Gestión de la Seguridad de la información en el Centro de Idiomas Buckingham English Center S.A. será obtenida tras la evaluación de la gerencia y la dirección de TIC´s, quienes indicarán cuándo podrán iniciarse con las gestiones.

CONCLUSIONES

El estudio permitió evidenciar la situación actual de la plataforma virtual del centro de idiomas, realizando controles quincenales para garantizar la seguridad de la información. Sin embargo, existen situaciones cuando el usuario externo percibe inseguridad en su información, motivo por el cual suele comunicar al centro para obtener una solución al problema. Si bien, existe una alta capacidad de la empresa en la solución del problema, existen casos en los cuales el usuario no notifica o no recibe solución al problema, incrementando su insatisfacción. Por otra parte, se registran eventos que, a pesar de ser notificados, no son un verdadero problema y surgen de la duda del usuario, motivadas por su desconocimiento en el manejo de la plataforma.

Se identificaron los riesgos, amenazas y debilidades del centro en su seguridad de la información. Entre ellas está el no respaldo completo de la información del cliente, firewall desactivado y falta de protocolo https, además de no existir una planificación óptima respecto al mantenimiento de los equipos informáticos ni repuestos, entre otros detalles que, si bien mencionan que no han provocado problemas, suponen un riesgo que deben ser corregidos para garantizar la eficiencia de las operaciones y altos niveles de seguridad de la información-

Ante esta problemática y la carencia de un sistema para la gestión de la seguridad de la información, se presentó un modelo tomando como referencia la norma ISO 27001 en donde se definieron las políticas, el alcance del modelos, se analizó el riesgo y se gestionó mediante controles orientados a minimizar las amenazas detectadas, finalizando con la presentación de un detalle respecto a cómo obtener la aprobación y autorización para implementarlo en el Centro de Idiomas Buckingham English Center S.A.

En el proyecto, tomando como base las recomendaciones y demás hallazgos en la recolección de datos, se plantearon alternativas orientadas a garantizar en mayor medida la seguridad de la información del centro, especialmente su plataforma, presentes en políticas y cuatro tipos de controles.

RECOMENDACIONES

De acuerdo a los resultados obtenidos mediante las muestras, los puntos importantes y de prioridad son los controles programados, el mantenimiento correspondiente a la información y esto debe ser informado con un día de anticipación a los usuarios externos para su conocimiento a fin de informar que si experimentan problemas, se debe a este tipo de gestión que garantizará la seguridad de la información.

La organización, en función de su estado actual, diseñará un presupuesto para cubrir cada una de las gestiones que se detalla dentro del modelo para la gestión de la seguridad de la información. Todos los gastos e inversiones derivadas del modelo deben estar soportadas con documentos que comprueban los movimientos monetarios para la respectiva declaración de impuesto y como soporte de que fueron utilizados adecuadamente.

Las mejoras planteadas que se ubican dentro de los controles y políticas deben ser implementadas y evaluadas, describiendo la situación antes de implementar el modelo y luego de su ejecución. De no evidenciarse mejorías, es importante que se intervenga el sistema de gestión de la seguridad de la información, detectando si es pertinente, requiere mejoras o no se está implementado adecuadamente.

Resulta conveniente la evaluación anual del usuario externo a fin de calificar su experiencia con el servicio brindado por el centro, determinando si existen mejorías, si perciben que sus requerimientos están siendo atendidos adecuadamente y que su información está realmente segura, dando a conocer que los requerimientos por seguridad y problemas por parte de los usuarios ha disminuido. Una respuesta positiva, en mejores niveles que la obtenida en el diagnóstico realizado en el presente proyecto, significará que la implementación del modelo ha tenido resultados favorables.

REFERENCIAS BIBLIOGRÁFICAS

Anselm, J. (2016). Bases de la investigación cualitativa: Técnicas y procedimientos para desarrollar la teoría fundamentada. Medellín: Universidad de Antioquia.

Arévalo, F., Cedillo, P., & Moscoso, S. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. Revista Killkana Técnica, 1(2), 31-42.

Bernal, C. (2016). Metodología de la investigación. Administración, economía, humanidades y ciencias sociales. Bogotá: Pearson Educación.

Bravo, C., Valdivieso, P., & Arregui, R. (Diciembre de 2018). Los sistemas de información en la toma de decisiones gerenciales en las empresas comerciales de Portoviejo. Scielo, 9(2), 45-54.

Cárdenas, L., Martínez, H., & Becerra, L. (Noviembre de 2016). Gestión de seguridad de la información: revisión bibliográfica. El profesional de la información, 25(6), 931-948.

Carpentier, J. (2016). La seguridad informática en la PYME: Situación actual y mejores prácticas. Barcelona: Eni Ediciones.

Chicano, E. (2018). Gestión de incidentes de seguridad informática. IFCT0109. Málaga: IC Editorial.

Conforme, C. (20 de Noviembre de 2018). Universidad Internacional SEK. Obtenido de Diseño de un modelo de gestión de seguridad de la información para el sistema académico de la Universidad Estatal del Sur de Manabí: https://repositorio.uisek.edu.ec/bitstream/123456789/3222/1/Proyecto-TesisCarlosConforme-Act%20%281%29.pdf

Cuervo, J., & Bejarano, M. (2020). Universidad Santo Tomás. Obtenido de Formular acciones de mejora utilizando las buenas prácticas de ITIL v4, para mejorar la gestión de solicitudes e incidentes de la universidad Santo Tomás sede principal en Bogotá.:

https://repository.ucc.edu.co/bitstream/20.500.12494/20192/5/2020_Formular_acciones_Itil.pdf

Galeano, M. (2018). Estrategias de investigación social cualitativa: El giro en la mirada. Medellin: FCSH.

Galeano, M. (2020). Diseño de proyectos en la investigación cualitativa. Medellín: Fondo Editorial Universidad EAFIT.

García, G., & Vidal, M. (2016). La informática y la seguridad. Un tema de importancia para el directivo. Medigraphic, 22(1), 47-58.

García, J., & Huamani, S. (18 de Junio de 2019). Universidad Peruana de Ciencias Aplicadas. Obtenido de Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú: https://repositorioacademico.upc.edu.pe/handle/10757/625905

García, Y. (13 de Mayo de 2015). Escuela Politécnica Nacional. Obtenido de Modelo de gestión de la seguridad de información en los procesos críticos de las áreas financieras universitarias. Caso PUCE: https://bibdigital.epn.edu.ec/handle/15000/10537?locale=de

Giménez, J. (2017). Seguridad en equipos informáticos. IFCT0510. Málaga: IC Editorial.

Hurtado, M. (15 de Mayo de 2018). Universidad Piloto de Colombia. Obtenido de Gestión de riesgo metodologías Octave y Magerit: http://35.227.45.16/bitstream/handle/20.500.12277/2965/00004420.pdf?sequence=1&isAllowed=y

ISO Tools Excelence. (28 de Enero de 2015). ISO Tools Excelence. Obtenido de ISO 27001: Gestión de Seguridad de la Información mediante el modelo de pirámide: https://www.isotools.org/2015/01/28/iso-27001-gestion-seguridad-informacion-mediante-modelo-piramide/

Luc, J. (2017). ITIL V3: preparación para la certificación ITIL Foundation V3 : más de 400 preguntas - respuestas. Barcelona: ENI.

Martínez, J. (2015). Marketing en la actividad comercial. Madrid: Paraninfo.

Merino, M., Pintado, T., Sánchez, J., & Grande, I. (2015). Introducción a la investigación de mercados. Madrid: ESIC.

Monterrosa, I., & Ospino, M. (Abril de 2018). Los sistemas de información gerencial en empresas cartageneras. Revista Observatorio de la Economía Latinoamericana, 1(1), 1-26.

Muñoz, C. (2015). Metodología de la investigación. México: Oxford University Press.

Norma ISO. (2020). Norma ISO. Obtenido de ISO 27001 SEGURIDAD DE LA INFORMACIÓN: https://www.normas-iso.com/iso-27001/

Organización Internacional de Normalización. (2020). Normas ISO. Obtenido de ISO 27001 SEGURIDAD DE LA INFORMACIÓN: https://www.normas-iso.com/iso-27001/

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. Scielo, 35(1), 227-232.

Paillacho, S. (Marzo de 2015). Escuela Politécnica Nacional. Obtenido de Modelo de un proceso de la gestión del riesgo de la Seguridad de la Información en Entidades Gubernamentales: https://bibdigital.epn.edu.ec/bitstream/15000/10653/1/CD-6286.pdf

Pérez, J., & Fol, R. (2016). Contabilidad electrónica y su envío a través del Portal del SAT 2016. México: Tax Editores Unidos.

Ramírez, M., & Perusquia, J. (2019). El Sistema de Información de Marketing como modelo de gestión basado en la comunicación organizacional. Revista Espacios, 40(27), 1-6.

Rocha, C. (2019). Universidad Tecnológica de Israel. Obtenido de Modelo de gestión de seguridad de la información para el sector público: http://repositorio.uisrael.edu.ec/bitstream/47000/1863/1/UISRAEL-EC-MASTER%20-%20TELEM-378.242-2019-001.pdf

Rodríguez, Y. (2015). Gestión de Información y del Conocimiento para la toma de decisiones organizacionales. Dialnet, 11(11), 150-163.

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Alicante: 3 Ciencias.

Rosales, E., Martelo, R., & Franco, D. (30 de Junio de 2020). Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit. Aglala Revista Virtual, 11(1), 227-245. Obtenido de http://revistas.curnvirtual.edu.co/index.php/aglala/article/view/1579

Sánchez, E., & Rebolledo, F. (2017). Institución Universitaria Politécnico Grancolombiano. Obtenido de Diseño de un modelo de gestión de la seguridad de la información en el área de talento humano de la Secretaría de Educación: http://repository.poligran.edu.co/bitstream/handle/10823/1039/DISE%c3%91O%20DE%20UN%20MODELO%20DE%20GESTI%c3%93N%20DE%20LA%20SEGURIDAD%20DE%20LA%20INFORMACI%c3%93N%20EN%20EL%20%c3%81....pdf?sequence=1&isAllowed=y

Santacruz, J., Vega, C., Pinos, L., & Cárdenas, Ó. (2017). Sistema cobit en los procesos de auditor´ıas de los sistemas informáticos. Journal of Science, 2(8), 65-68.

Segunda Cohorte del Doctorado en Seguridad Estratégica en Guatemala. (2018). Seguridad de la información. Guatemala: Universidad de Guatemala.

Serrano, P., Señalin, L., Vega, F., & Herrera, J. (2018). El control interno como herramienta indispensable para una gestión financiera y contable eficiente en las empresas bananeras del cantón Machala (Ecuador). Revista Epacios, 39(3), 1-13.

Solarte, F., Enríquez, E., & Benavides, M. (Diciembre de 2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica Espol, 28(5), 492-507.

Suárez, A., Cruz, I., & Pérez, Y. (2015). La gestión de la información: herramienta esencial para el desarrollo de habilidades en la comunidad estudiantil universitaria. SciELO, 7(2), 72-79.

Universidad Internacional de La Rioja UNIR. (11 de Diciembre de 2019). Universidad Internacional de La Rioja. Obtenido de ¿Qué es la certificación ISO 27001 y para qué sirve?: https://www.unir.net/ingenieria/revista/iso-27001/

Valencia, F., & Orozco, M. (Junio de 2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Revista lbérica de Sistemas y Tecnologías de Información, 22(6), 73-88.

Venegas, L., & Esparza, F. (2018). Guía metodológica para la evaluación técnica informática de la implementación de educación y capacitación virtual - COBIT 5. Alicante: 3 Ciencias.

Vite, H., Molina, B., & Dávila, J. (Julio de 2018). Gestión de la Información en las Instituciones de Educación Superior (IES) con base a la norma ISO 27001. Revista Informática y Sistemas, 4(1), 29-34.

ANEXOS

ANEXO 1. Matriz auxiliar de operación

TÍTULO	**PLANTEAMIENTO DEL PROBLEMA**	**FORMULACIÓN DEL PROBLEMA**	**OBJETIVO**	**VARIABLES DEPENDIENTES**	**VARIABLES INDEPENDIENTES**
ANÁLISIS Y DESARROLLO DE UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE IDIOMAS BUCKINGHAM ENGLISH CENTER S.A.	La entidad carece de un modelo que favorezca a la gestión de la seguridad de la información poniendo en riesgo la información de sus usuarios, pudiendo ver vulnerados sus datos y afectándose así su satisfacción como clientes.	¿Cómo desarrollar un modelo de gestión de seguridad de la información para la plataforma virtual del centro de idiomas? **SISTEMATIZACIÓN DEL PROBLEMA DE INVESTIGACIÓN** • ¿Cómo determinar la situación actual sobre la gestión de seguridad de la información aplicada a la plataforma virtual de Buckingham? • ¿Cómo identificar las amenazas a las que está expuesto la plataforma virtual de Buckingham? • ¿Cómo proteger la plataforma virtual de Buckingham de las amenazas informáticas identificadas? • ¿Cómo proveer un modelo de gestión de seguridad de la información para el apoyo personal del departamento de TIC´s de Buckingham?	Desarrollar un modelo de sistema de gestión de la seguridad de la información de la plataforma del centro de idiomas. • Determinar la situación actual de la plataforma virtual del centro de idiomas. • Identificar las amenazas a las que está expuesta la plataforma virtual de Buckingham. • Plantear alternativas orientadas a la protección de la plataforma contra amenazas informáticas identificadas. • Establecer los lineamientos para un modelo de gestión de seguridad de la información como apoyo al personal del departamento de TIC´s de Buckingham.	Seguridad de la información de los usuarios externos	Modelo de sistema de gestión de la seguridad de la información

Elaborado por: *El autor*

ANEXO 2. Antecedentes bibliográficos

AUTORES	METODOLOGÍA	MODELO	DESCRIPCIÓN	FASES DE LA METODOLOGÍA	DESCRIPCIÓN
(Galeano, 2018)	Investigación Documental	Revisión documental	Obtención de datos que se analizan para convertirse en información, preveniente de fuentes secundarias o bibliográficas.	Recopilación de fuentes bibliográficas.	Búsqueda de fuentes referenciales relacionadas al tema
				Identificación de información relevante.	Selección de contenido que aporte al estudio
				Interpretación de la información	Parafraseo de la información obtenida
				Exposición de hallazgos.	Análisis del contenido
(Muñoz, 2015)	Investigación de campo	Cuestionario	Recopilan datos directamente del entorno donde se desarrolla el problema.	Determinación de los objetivos.	Justificación del estudio de campo
				Identificación de sujetos de interés.	Selección de los individuos a quienes se consultará
				Diseño de instrumentos para la recolección de datos.	Planteamiento de preguntas que conformen el instrumento
				Presentación y análisis de la información.	Redacción de respuestas e interpretación

Elaborado por: *El autor*

ANEXO 3. Marco teórico seleccionado

METODOLOGÍA	MODELO	FASES DE LA METODOLOGÍA	VARIABLE DEPENDIENTE	VARIABLE INDEPENDIENTE
Investigación de campo	Entrevistas y encuestas	Determinación de los objetivos.	Seguridad de la información de los usuarios externos.	Modelo de sistema de gestión de la seguridad de la información.
		Identificación de sujetos de interés.		
		Diseño de instrumentos para la recolección de datos.		
		Presentación y análisis de la información.		

Elaborado por: *El autor*

ANEXO 4. Marco Operacionalización

MODELO	VARIABLE DEPENDIENTE	DEFINICIÓN	VARIABLE INDEPENDIENTE	DEFINICIÓN	INDICADOR
Entrevistas y encuestas	Seguridad de la información de los usuarios externos	La seguridad de la información pretende que los activos que la contiene no sean vulnerables garantizando su disponibilidad, integridad y confidencialidad (Carpentier, 2016).	Modelo de sistema de gestión de la seguridad de la información	Su propósito es la instalación de los mecanismos para la confidencialidad, integridad y disponibilidad de la información en medio de un conjunto de estándares determinados para estimar la seguridad (Solarte, Enríquez, & Benavides, 2015).	Activos de información disponibles Amenazas identificadas de la plataforma Vulnerabilidades identificadas de la plataforma Frecuencia de análisis de amenazas y vulnerabilidades Acciones para prevención de riesgos Problemas para la seguridad de la información Nivel de riesgo percibido por el cliente

Elaborado por: *El autor*

ANEXO 5. Modelo de cuestionario de entrevista a talento humano del Centro de Idiomas Buckingham English Center S.A.

Identificación de activos

1. ¿Qué activos de información posee la empresa donde se soporta información de los clientes, según los siguientes criterios?

Soportes físicos:

Soportes informáticos:

2. ¿Quiénes son los responsables de la gestión de estos activos?

Amenazas y vulnerabilidades de la plataforma

3. ¿Con qué frecuencia se realiza en la entidad un análisis para identificar y corregir debilidades y amenazas relacionadas a la seguridad de la información en la plataforma virtual?
4. ¿Qué debilidades y/o amenazas posee la plataforma virtual y que la vuelve susceptible a ataques o daños?
5. ¿Cuáles considera usted que tienen altas probabilidades para ocurrencia y pueden afectar el funcionamiento y seguridad de la plataforma?

Tratamiento del riesgo

6. ¿Qué acciones se han desarrollado en la entidad a fin de minimizar las amenazas y vulnerabilidades para la plataforma virtual del centro de estudio?
7. ¿Cómo estas acciones han garantizado la disponibilidad, confidencialidad e integridad de la plataforma para la seguridad de la información del cliente?
8. ¿Qué problemas se han presentado en la entidad respecto a la seguridad de la información del cliente y funcionamiento de la plataforma virtual? Indique la frecuencia con la que ocurren

9. Indique las razones que han impedido la adopción de un modelo de gestión para la seguridad de la información en la empresa
10. De presentarse un modelo de gestión para la seguridad de la información ¿Qué aspectos consideraría para su implementación?

ANEXO 6. Modelo de cuestionario de encuesta a clientes del Centro de Idiomas Buckingham English Center S.A.

Información del cliente

1. ¿Cuánto tiempo lleva como cliente el Centro de Idiomas Buckingham English Center S.A?

0 – 6 meses		1 – 2 años	
7 – 11 meses		> 2 años	

2. ¿En qué módulo de aprendizaje se encuentra actualmente?

_____

3. ¿Considera que la plataforma virtual aporta a su aprendizaje del idioma?

Muy de acuerdo		En desacuerdo	
De acuerdo		Muy en desacuerdo	

Amenazas y vulnerabilidades

4. ¿Con qué frecuencia usted ha percibido que su información como cliente no ha estado segura en la plataforma del establecimiento?

Muy Frecuentemente		Poco frecuente	
Frecuentemente		Nada frecuente	

5. ¿Con qué frecuencia usted ha percibido que su progreso en los módulos de aprendizaje ha sido alterado y le genera un perjuicio? Explique

Muy Frecuentemente		Poco frecuente	
Frecuentemente		Nada frecuente	

6. ¿Qué tan frecuente suele denegarse o impedirse el acceso a la plataforma sin previo aviso?

Muy Frecuentemente		Poco frecuente	
Frecuentemente		Nada frecuente	

7. ¿Qué acciones ha tomado la empresa ante los incidentes de vulnerabilidad reportados?

Incidente	**Hubo solución**	**No requería solución**	**No dio respuesta**	**Usted no notificó**
Inseguridad en su información				
Progreso alterado				
Problemas de acceso				

8. En función a su experiencia como cliente ¿Cómo califica el nivel de seguridad de su información en el centro?

Alto		Bajo	
Medio		Nulo	

9. ¿Cómo evalúa usted su nivel de satisfacción global como cliente de este centro?

Alta		Baja	
Media		Nula	

Tratamiento del riesgo

10. ¿Conoce usted las acciones realizadas por la empresa para fortalecer la seguridad de la plataforma virtual que usted utiliza?

Muy de acuerdo		En desacuerdo	
De acuerdo		Muy en desacuerdo	

11. ¿Qué recomendaciones usted daría para mejorar su experiencia como usuario de la plataforma virtual, relacionadas o no a la seguridad?

_____

_____