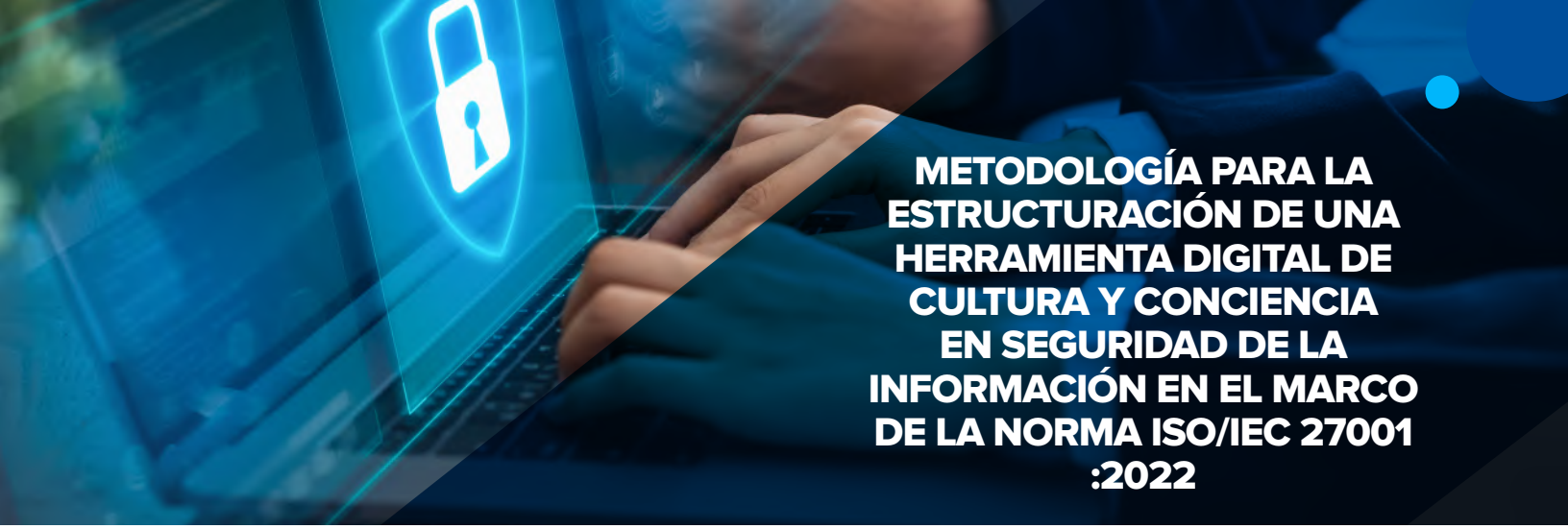


METODOLOGÍA PARA LA ESTRUCTURACIÓN DE UNA HERRAMIENTA DIGITAL DE CULTURA Y CONCIENCIA EN SEGURIDAD DE LA INFORMACIÓN EN EL MARCO DE LA NORMA ISO/IEC 27001 :2022

METHODOLOGY FOR STRUCTURING A DIGITAL TOOL FOR INFORMATION SECURITY CULTURE AND AWARENESS WITHIN THE FRAMEWORK OF ISO/IEC 27001:2022

Maira Alejandra Angel Henriquez [1]
Corporación Tecnológica Industrial Colombiana, TEINCO

Maria Deyanira Perez Vega [2]
Corporación Tecnológica Industrial Colombiana, TEINCO

Lady Johanna Herrera Vargas [3]
Corporación Tecnológica Industrial Colombiana, TEINCO

Manuel Antonio Perez Chaparro [4]
Corporación Tecnológica Industrial Colombiana, TEINCO

John Jairo Sedano Segura [5]
Corporación Tecnológica Industrial Colombiana, TEINCO

RESUMEN

Este capítulo de investigación presenta la creación de la metodología denominada InfoSecurity para el desarrollo de una herramienta digital destinada a fomentar la cultura y conciencia en seguridad de la información, la cual busca sensibilizar a individuos y organizaciones sobre la importancia de la seguridad de la información y ciberseguridad, en línea con numeral 6.3 del Anexo A referente a “Concientización educación y capacitación sobre seguridad de la información” de la norma ISO/IEC 27001 :2022.

La norma cuenta con el Anexo A, el cual dispone de 93 controles, en este anexo se agrupan 4 categorías: organizacional, personas, físico y tecnológico. La categoría de “personas” tiene como identificador Anexo A 6.3, el cual se tomó como referencia para la creación de la metodología InfoSecurity, teniendo en cuenta que la cultura y conciencia en seguridad de la información es un tema que deben aplicarse a la mayoría de controles de la norma, por lo tanto, iniciar con este anexo permitirá a futuro de forma eficiente la implementación de los demás anexos, controles y certificación de la norma, lo cual representaría un valor agregado significativo para TEINCO.

En este contexto, se propone una metodología estructurada en varias etapas clave que incluyen la planificación, investigación, diseño, creación de contenido, personalización, prueba y lanzamiento. Cada una de estas etapas se enfoca en aspectos específicos para garantizar la integridad, disponibilidad y confidencialidad de la herramienta digital y de la información. Por medio de la investigación aplicada con un enfoque cualitativo. Se procede a definir una metodología para que las personas que forman parte de la Corporación Tecnológica Industrial Colombiana - TEINCO u otras personas interesadas implementen

[1] Manuel Fernando García García, director de la División de Investigación Tecnológica Aplicada de la Corporación Tecnológica Industrial Colombiana, TEINCO, Colombia, direccion.investigaciones@teinco.edu.co

[2] Ella Yohanna González Guevara Coordinadora de Investigación Mecatrónica de la Corporación Tecnológica Industrial Colombiana, TEINCO, Colombia

[3] Stephani Muñoz Ávila Coordinadora de Investigación Administración de la Corporación Tecnológica Industrial Colombiana, TEINCO, Colombia

[4] Bueno García Andrés Felipe, estudiante de contaduría pública de la Corporación Tecnológica Industrial Colombiana, TEINCO Colombia, 1003690532@teinco.edu.co

[5] Mendivelso Durán Martha Inés, estudiante de contaduría pública de la Corporación Tecnológica Industrial Colombiana, TEINCO Colombia, 24042549@teinco.edu.co

[6] Urbano Corredor Pablo Enrique, estudiante de contaduría pública de la Corporación Tecnológica Industrial Colombiana, TEINCO Colombia, 1022403733@teinco.edu.co

este tipo de metodología ya que dada su estructura permite su replicabilidad y adaptabilidad en otras instituciones u organizaciones.

Para ilustrar la herramienta digital de la metodología InfoSecurity, se incluirán materiales concretos de video tips, infografías, documentos de interés y juegos, diseñados para abordar diferentes estilos de aprendizaje y promover una comprensión profunda de los conceptos clave en seguridad de la información. Además, se considerará la retroalimentación de especialistas en seguridad de la información para ajustar y mejorar la herramienta digital, asegurando su alineación con los estándares de seguridad y su eficacia en la promoción de una cultura consciente en seguridad de la información.

PALABRAS CLAVE: ciberdelincuente; ciberseguridad; concientización; ISO/IEC 27001 :2002; seguridad de la información.

ABSTRACT

This research chapter presents the creation of the InfoSecurity methodology, a digital tool designed to foster information security culture and awareness. This tool seeks to raise awareness among individuals and organizations about the importance of information security and cybersecurity, in line with section 6.3 of Annex A regarding “Information Security Awareness, Education, and Training” of the ISO/IEC 27001:2022 standard.

The standard includes Annex A, which contains 93 controls. This annex groups four categories: Organizational, People, Physical, and Technological. The “People” category is identified by Annex A 6.3, which was used as a reference for the creation of the InfoSecurity methodology. Considering that information security culture and awareness must be applied to most of the standard’s controls, starting with this annex will allow for efficient future implementation of the standard’s other annexes, controls, and certification, which would represent significant added value for TEINCO.

In this context, a methodology structured into several key stages is proposed, including planning, research, design, content creation, customization, testing, and launch. Each of these stages focuses on specific aspects to ensure the integrity, availability, and confidentiality of the digital tool and its information. Through applied research with a qualitative approach, a methodology is being defined for those working at the Colombian Industrial Technology Corporation (TEINCO) or other interested parties to implement this type of methodology. Its structure allows for its replicability and adaptability to other institutions or organizations.

To illustrate the InfoSecurity methodology’s digital tool, specific materials will be included, including video tips, infographics, relevant documents, and games, designed to address different learning styles and promote a deep understanding of key information security concepts. In addition, feedback from information security specialists will be considered to adjust and improve the digital tool, ensuring its alignment with security standards and its effectiveness in promoting an information security-conscious culture.

KEYWORDS: awareness; cybercriminal; cybersecurity; information security; ISO/IEC 27001:2002.

1. INTRODUCCIÓN

La evolución tecnológica ha tenido un impacto directo e indirecto en la seguridad de la información y la ciberseguridad a lo largo de los años, lo que ha llevado a un aumento en los eventos que comprometen la confidencialidad, integridad y disponibilidad (CID) de la información en el ciberespacio. Tras el cambio de vida impuesto por la pandemia, se ha evidenciado un notable incremento en la ciberdelincuencia, especialmente tras el COVID-19, teniendo en cuenta las siguientes palabras “La crisis propiciada a principios de 2020 por la pandemia del COVID-19 ha puesto de relieve nuestra dependencia de una infraestructura vital que, para la gran mayoría de los ciudadanos, resulta invisible o su existencia pasa prácticamente desapercibida”.(Schwartz 2020. p. 148).

A su vez, Raimondo (2021), “Los ciberataques de – ransomware - están aquí para quedarse, advierto que probablemente se intensifiquen, por lo que insisto a las empresas a que refuercen su seguridad tras los últimos episodios sufridos en el país, lo primero que hay que hacer respecto a los ciberataques es reconocer que esta es la realidad” (Pag.21). Este panorama plantea un alto nivel de preocupación, ya que las organizaciones a menudo se centran en asegurar la tecnología, descuidando otros aspectos críticos como la concientización y capacitación de las personas que interactúan con los sistemas de información, por lo tanto, es fundamental fomentar un pensamiento seguro frente a cualquier evento, riesgo, amenaza o vulnerabilidad que afecte la CID de los datos y de la información.

En la actualidad, actividades cotidianas como pagos electrónicos, compras en línea, uso de redes sociales y videollamadas forman parte de nuestra vida diaria,

exponiendo así nuestra información personal a crecientes amenazas cibernéticas, es ahí cuando los ciberdelincuentes buscan aprovechar las vulnerabilidades de los sistemas y el escaso conocimiento en seguridad por parte de los usuarios para acceder de manera ilegal a nuestros sistemas, dispositivos y datos personales.

En este contexto, es importante adquirir un mayor conocimiento sobre ciberseguridad, como subraya las palabras del coordinador de la maestría en ciencia de los datos y analítica de la Universidad Eafit, Lalinde (2021), quien enfatiza la importancia de que las personas adquieran un mayor conocimiento sobre ciberseguridad para prevenir los ataques cibernéticos en Colombia. Es fundamental que sean conscientes de los riesgos y las implicaciones del uso de la tecnología y la protección de sus datos personales, es por esto que el objetivo de este proyecto es crear una metodología llamada Infosecurity, alineada con numeral 6.3 del Anexo A de la norma ISO/IEC 27001 :2022, con el propósito de reforzar la conciencia en seguridad de la información y ciberseguridad en el caso de estudio TEINCO, una Institución de Educación Superior que ofrece programas académicos en áreas como ingeniería de sistemas, ingeniería mecatrónica, contaduría pública, administración de empresas, entre otros y otras instituciones interesadas en aplicar.

TEINCO actualmente carece de un programa de capacitación en seguridad de la información y ciberseguridad, requisito establecido en la norma ISO/IEC 27001 :2022 (en adelante ISO 27001) en el Anexo A 6.3 Concientización educación y capacitación sobre seguridad de la información de la norma ISO/IEC 27001 :2022. Esta norma internacional cuenta con 93 controles que establecen los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), cuyo objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información (CID).

Es por esto que se busca apoyar esta iniciativa mediante un modelo de simulación de una herramienta digital a través de Google Sites, la cual permite desarrollar el propósito de este capítulo y la cual ya TEINCO tiene debidamente licenciada. Esta metodología emplea una herramienta digital que proporciona acceso a material formativo, infografías, vídeos, juegos, noticias y documentos diseñados para adaptarse al nivel de conocimiento del usuario y promover un pensamiento seguro frente a posibles amenazas que puedan comprometer la seguridad de la información y los datos.

La metodología InfoSecurity aborda el numeral 6.3 del Anexo A “Concientización educación y capacitación sobre seguridad de la información” establecido en la norma ISO/IEC 27001 :2022. Por consiguiente, es importante resaltar que contar con la metodología InfoSecurity permite a la institución proyectarse hacia el futuro para adquirir la certificación en esta norma.

1.1. MARCO CONCEPTUAL

1.1.1. INTRODUCCIÓN AL MARCO TEÓRICO

La seguridad de la información y la ciberseguridad son aspectos críticos en el entorno actual, donde la digitalización y los ciberataques están en constante aumento. Es fundamental concientizar a individuos y organizaciones sobre la importancia de proteger la información sensible.

1.1.2. NORMATIVA INTERNACIONAL Y ISO/IEC 27001 :2022

La norma ISO/IEC 27001 :2022 establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información. El numeral 6.3 de esta norma destaca la sensibilización, educación y formación en seguridad de la información como aspectos fundamentales.

1.1.3. METODOLOGÍA INFOSECURITY

La metodología InfoSecurity se basa en los principios de integridad, disponibilidad y confidencialidad, desglosados en fases como diagnóstico, análisis, diseño e implementación. Su enfoque se centra en la creación de una cultura de seguridad a través de una herramienta digital que promueva la conciencia en seguridad de la información.

1.1.4. SENSIBILIZACIÓN Y EDUCACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La metodología InfoSecurity busca sensibilizar a las personas sobre los riesgos y las implicaciones del uso de la tecnología, fomentando la conciencia en seguridad de la información y ciberseguridad. Esto se alinea con la necesidad de adquirir un mayor conocimiento en ciberseguridad para prevenir ataques cibernéticos.

1.1.5. INVESTIGACIÓN APLICADA Y ENFOQUE CUALITATIVO

El desarrollo de la metodología se basa en una investigación aplicada con enfoque cualitativo, lo que permite comprender las necesidades y percepciones de las personas involucradas. Esta aproximación colaborativa garantiza la relevancia y aplicabilidad de la metodología en diferentes contextos organizativos.

1.1.5.1. BENEFICIOS Y APLICABILIDAD DE LA METODOLOGÍA

La metodología InfoSecurity ofrece un marco sólido para abordar los desafíos en seguridad de la información, promoviendo una cultura de seguridad proactiva. Su implementación a través de una herramienta digital proporciona recursos educativos y prácticos para fortalecer la conciencia en seguridad de la información, alineándose con los estándares de la norma ISO/IEC 27001 :2022.

1.1.6. APORTES DE LA METODOLOGÍA INFOSECURITY AL CASO DE ESTUDIO

La aplicación de la metodología InfoSecurity en el caso de estudio de TEINCO, destaca la importancia de promover una cultura de seguridad sólida y arraigada. La implementación de esta metodología ofrece beneficios tangibles en la protección de la información y la prevención de posibles amenazas cibernéticas.

Este marco teórico proporciona una base conceptual sólida para comprender la importancia de la metodología InfoSecurity en la promoción de la cultura y conciencia en

seguridad de la información, en línea con los estándares internacionales de ciberseguridad.

2. MÉTODO

Se realizó una investigación aplicada con enfoque cualitativo, permitiendo comprender las percepciones, actitudes y comportamientos de las personas en relación con la seguridad de la información y la ciberseguridad. “Comprender los fenómenos, explorándolos desde la perspectiva de los participantes en su ambiente natural y en relación con el contexto” (Sampieri & Mendoza, 2018, p. 390).

A través de la recolección de información mediante encuestas, esta investigación identificó el nivel de conocimiento de las personas en cuanto a seguridad de la información y buenas prácticas. El método de encuestas, respaldado por el enfoque cualitativo, permitió una comprensión detallada y profunda de las percepciones, actitudes y valores de los participantes. Esta profundidad en la comprensión es fundamental para identificar y resaltar los valores individuales, elevando a que se conviertan en valores institucionales que fomenten una cultura y un pensamiento basado en seguridad de la información en el marco de la ISO 27001.

2.1. ESTRATEGIAS METODOLÓGICAS

Considerando la flexibilidad del enfoque cualitativo y la simulación de la herramienta digital, se ha establecido una ruta para el desarrollo de este documento, compuesta por las siguientes fases:

1. Diagnóstico preliminar:

El punto de partida del proyecto fue plantear una pregunta crucial: ¿cómo se puede mejorar o aportar desde el rol ingenieril para reducir la problemática de que Colombia se encuentra como el tercer país con más ataques cibernéticos en Latinoamérica? Este enfoque inicial se alineó con la Norma ISO/IEC 27001, estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema protege la confidencialidad, integridad y disponibilidad de la información. Específicamente, se observó que el numeral 6.3 del anexo de esta norma se centra en la concientización, educación y capacitación sobre seguridad de la información. Con este enfoque cualitativo, se seleccionó a TEINCO como estudio de caso para validar cómo esta institución implementa dicho control.

Para desarrollar esta fase, primero se definió el contexto y la importancia del problema, describiendo brevemente el estado de la ciberseguridad en Colombia y destacando que es el tercer país en Latinoamérica con más ataques cibernéticos. Posteriormente se identificó la relevancia de abordar este problema desde un enfoque ingenieril para contribuir a la protección de la información. Luego, se consultaron los fundamentos de la Norma ISO/IEC 27001 y su objetivo de establecer un SGSI eficaz, detallando cómo el numeral 6.3 del anexo promueve la concientización y la capacitación en seguridad de la información. Finalmente, se justificó la elección de TEINCO como institución para validar la implementación del control de concientización, mencionando que TEINCO, al ser una institución educativa, representa un entorno ideal para estudiar y mejorar las prácticas de seguridad de la información entre estudiantes, profesores y personal administrativo.

2. Diagnóstico:

En esta etapa, se comenzó por identificar cómo TEINCO implementa el control de concientización en seguridad de la información y qué estrategias podrían ser utilizadas para lograr una implementación efectiva. Este diagnóstico se llevó a cabo mediante observación de campo y encuestas.

El proceso de observación de campo en TEINCO se realizó mediante entrevistas informales al personal administrativo, donde se observaron aspectos como las prácticas diarias relacionadas con la seguridad de la información, adicionalmente se identificó que no se contaba con una herramienta o instrumento que ayudará con el cumplimiento del control en la institución.

Simultáneamente, se desarrollaron y administraron encuestas diseñadas para recolectar datos específicos sobre la percepción y prácticas en seguridad de la información. Las encuestas fueron dirigidas a un perfil variado de encuestados, incluyendo estudiantes, profesores y personal administrativo.

El análisis de los resultados del diagnóstico reveló hallazgos clave, destacando las brechas y áreas de mejora. Se identificó una falta de conocimiento general sobre la seguridad de la información y ciberseguridad, una baja percepción del riesgo cibernético y una ausencia de prácticas proactivas de seguridad. Estos resultados subrayaron la necesidad de una estrategia de concientización más robusta y estructurada dentro de TEINCO, lo que guiará las fases posteriores del proyecto.

3. Intervención

Teniendo en cuenta que el diagnóstico reveló que TEINCO no contaba con ninguna herramienta o instrumento que implementara efectivamente el control de concientización en seguridad de la información. En respuesta a esta carencia, se realizó una búsqueda exhaustiva de metodologías o herramientas que pudieran ser aplicadas en instituciones educativas. Durante esta búsqueda se encontraron guías e instructivos sobre recomendaciones generales de seguridad de la información y configuraciones de hardware, se analizaron diversas herramientas disponibles en el mercado y se discutieron sus limitaciones en el contexto educativo.

Por ejemplo, algunas guías revisadas se centraban en recomendaciones generales para la seguridad de la información en entornos corporativos, mientras que otras proporcionaban instrucciones técnicas sobre configuraciones de hardware. Sin embargo, ninguna de estas metodologías ofrecía directrices detalladas para tener una cultura de seguridad en el ámbito educativo, lo que señaló una brecha significativa que necesitaba ser abordada.

La identificación de esta brecha clarificó la necesidad específica que ninguna metodología o herramienta existente cubría, justificando la necesidad de una intervención personalizada, en particular, se observó la falta de directrices detalladas y adaptadas para fomentar la concientización en seguridad de la información dentro de un entorno educativo. Esto llevó al desarrollo de una intervención

diseñada específicamente para responder a las necesidades identificadas en TEINCO.

El diseño de la intervención se basó en los principios de la Norma ISO/IEC 27001, adaptados al contexto educativo, se desarrollaron materiales educativos específicos como videos, infografías y juegos interactivos, diseñados para mejorar la concientización sobre seguridad de la información en el caso de estudio TEINCO. Estos materiales fueron creados para ser accesibles y comprensibles, asegurando que todos los miembros de la institución pudieran beneficiarse de ellos y contribuir a la creación de una cultura sólida de seguridad de la información.

4. Implementación de intervención

A partir de la intervención, surgió la necesidad de crear una metodología específica para la desarrollar una herramienta digital de cultura y conciencia en seguridad de la información alineada con la norma ISO 27001 para el caso de estudio TEINCO y porque no, para otros instituciones o entidades interesadas en replicar. Esta metodología tiene como objetivo mejorar la concientización y las prácticas de seguridad de la información entre los miembros de TEINCO, abarcando tanto a estudiantes como a personal administrativo y profesores.

Para definir los objetivos y el alcance de la metodología, se estableció claramente que su finalidad era fortalecer la cultura y conciencia en seguridad de la información en TEINCO. La metodología debía ser aplicable a diferentes niveles educativos y administrativos, garantizando que todos los miembros de la institución pudieran beneficiarse de ella, ya que esto aseguraría una implementación uniforme y efectiva en toda la organización.

El desarrollo de la metodología siguió un proceso estructurado que incluyó varias fases clave. En la fase de planificación, se identificaron las necesidades específicas de TEINCO y se diseñaron contenidos educativos adecuados. Luego, se llevaron a cabo pruebas piloto con los docentes de apoyo para evaluar la efectividad inicial de los materiales y ajustar su contenido con base a los comentarios recibidos, adicionalmente se integraron los principios de la Norma ISO/IEC 27001 para asegurar que la metodología fuera relevante y efectiva, alineándose con los estándares internacionales de seguridad de la información.

Los componentes de la metodología fueron diversos y adaptados a diferentes estilos de aprendizaje para maximizar la comprensión y retención de información. Se desarrollaron videos educativos, infografías y juegos interactivos que cubrían aspectos esenciales de la seguridad de la información. Estos materiales fueron diseñados para ser accesibles y atractivas, facilitando el aprendizaje y la concientización entre los miembros de TEINCO.

Para evaluar la efectividad de la metodología, se utilizó una rúbrica específica a especialistas en seguridad de la información, la cual permitió realizar una evaluación exhaustiva de cada componente de la metodología, considerando aspectos como la claridad de los contenidos, la relevancia de los temas tratados, la efectividad de las estrategias de enseñanza, el funcionamiento de la herramienta digital, entre otros temas abordados.

Los especialistas proporcionaron retroalimentación detallada sobre cada aspecto evaluado, lo que permitió identificar áreas de mejora y ajustar los materiales y las técnicas de enseñanza en consecuencia. Esta evaluación continua y detallada aseguró que la metodología se mantuviera alineada con los requisitos de la Norma ISO/IEC 27001 y las necesidades específicas de TEINCO, contribuyendo a una mejora continua y sostenible en la cultura y conciencia en seguridad de la información y ciberseguridad de la institución.

2.1.1. POBLACIÓN Y MUESTRA

- Población: personal administrativo, docente y estudiantil de TEINCO.

- Muestra: se realizó el envio de una encuesta por correo electrónico a toda la población de TEINCO, compuesta por aproximadamente mil personas, incluyendo personal administrativo, docente y estudiantil. Sin embargo, solo 124 individuos optaron por responder a la encuesta. Dado que la participación fue voluntaria, esta muestra se caracteriza como un muestreo por conveniencia y no probabilístico. Esta muestra proporcionó una visión significativa de las percepciones y prácticas en seguridad de la información dentro de la comunidad de TEINCO que participó en el estudio.

2.1.2. INSTRUMENTOS DE RECOGIDA DE INFORMACIÓN

Para la recolección de datos que fueron el insumo para el desarrollo de la propuesta metodológica, se usaron los siguientes instrumentos del enfoque cualitativo:

- **Encuesta:**

Se llevó a cabo una encuesta que constaba de 16 preguntas de selección múltiple dirigida a estudiantes, docentes y personal administrativo de TEINCO, con el objetivo de evaluar su nivel de conocimiento y prácticas en seguridad de la información. Esta encuesta se distribuyó tanto de manera presencial como por correo electrónico. De los 124 participantes, aproximadamente el 80% eran estudiantes de Ingeniería de Sistemas, Ingeniería Mecatrónica, Administración de Empresas y Contaduría Pública, mientras que el 20% restante comprendía docentes y personal administrativo. Es relevante destacar que el 80% de los encuestados pertenecían al programa de Ingeniería de Sistemas, lo que ofrece una perspectiva específica sobre ese grupo. Durante la realización de las encuestas presenciales, se observaron prácticas de seguridad y se generaron discusiones adicionales sobre el tema, lo que enriqueció aún más la recolección de datos.

- **Diario de campo:**

El diario de campo fue una herramienta complementaria clave durante la ejecución de las encuestas presenciales. En él se registraron detalladamente las observaciones, experiencias y reflexiones surgidas durante el proceso de recolección de datos. Se destacó la participación activa de los involucrados, así como el interés y las preguntas adicionales que surgieron durante las discusiones sobre el tema de seguridad de la información. Estas observaciones proporcionaron una perspectiva más profunda sobre la interacción de los participantes con el estudio y enriquecieron el análisis de los datos recopilados.

2.1.3. PROCEDIMIENTO

Para el desarrollo de este capítulo se realizó un estudio de caso en TEINCO, una institución que ofrece diversos programas académicos, en la cual se implementó la metodología InfoSecurity como un enfoque integral para abordar los desafíos relacionados con la cultura y conciencia en seguridad de la información y ciberseguridad dentro de la institución. Esta implementación se estructuró teniendo en cuenta las siguientes fases:

Fase 1: Diagnóstico

En la primera etapa de este proyecto, se llevó a cabo la recolección de datos mediante una encuesta realizada a las personas involucradas en nuestro caso de estudio. TEINCO, a través de sus respuestas, se logró obtener una variedad de puntos de vista. Adicionalmente, las encuestas que fueron realizadas de manera presencial fueron cuidadosamente registradas en el diario de campo. Esta recopilación de información no estructurada fue fundamental para la posterior construcción de la propuesta metodológica, proporcionando así una base sólida para el desarrollo del documento.

Fase 2: Análisis del diagnóstico

Tras la recopilación de información a través de encuestas en formularios, se procedió a revisar y organizar los datos en categorías específicas, tales como rol (estudiante, docente, director de programa), carrera y semestre -en el caso de los estudiantes-, así como las respuestas relacionadas con el conocimiento y las prácticas de seguridad implementadas. Con esta información estructurada, se identificaron conceptos desconocidos por las personas encuestadas y prácticas de seguridad que no estaban siendo implementadas, lo que orientó el enfoque del contenido a compartir en la herramienta digital y facilitó el establecimiento de estrategias de formación.

Además, a través del diario de campo se identificó la necesidad de incluir un checklist basado en la norma 27001, con el fin de evaluar la aplicación de controles específicos y promover así una cultura consciente en puntos clave relacionados con la seguridad de la información.

Fase 3: Diseño de la herramienta digital

Basándonos en la experiencia de los autores y en la integración de sitios de seguridad de la información, se propone la adopción de la metodología InfoSecurity para la creación de una herramienta digital utilizando Google Sites, una plataforma debidamente licenciada por TEINCO.

La metodología InfoSecurity se fundamenta en tres pilares clave para la construcción de esta herramienta: 1. Integridad, 2. Disponibilidad, 3. Confidencialidad, los cuales a su vez se desglosan en seis etapas:

a. Planificación.

b. Investigación.

c. Diseño:

El cual estará dividido en las siguientes secciones:

1. Video tips
2. Infografías.
3. Documentos de interés.
4. Juegos.

d. Creación de contenido.

e. Personalización.

f. Prueba y lanzamiento.

Se espera que, al completar todas las fases de esta metodología, se obtenga una herramienta digital que promueva la cultura y conciencia en seguridad de la información y ciberseguridad.

Los pilares de integridad, disponibilidad y confidencialidad mencionados anteriormente son fundamentales debido a su impacto directo en la protección de los datos y la garantía de su correcto funcionamiento.

- La integridad asegura que la información no sea alterada de manera no autorizada, manteniendo su precisión y fiabilidad.
- La disponibilidad garantiza que la información esté siempre accesible para aquellos usuarios autorizados que la necesiten, evitando interrupciones no planificadas en su acceso.
- La confidencialidad se encarga de proteger la información sensible y restringir su acceso únicamente a las personas autorizadas, evitando así filtraciones o accesos no autorizados. Estos pilares son esenciales para garantizar la confianza y seguridad en el manejo de la información, tanto para la organización como para sus usuarios.

Fase 4: Validación de la herramienta

Una vez finalizado el diseño del sitio utilizando la plataforma licenciada por TEINCO, Google Sites, se procedió a la etapa de validación de herramienta. En la Fase 4 se llevó a cabo una evaluación exhaustiva de la herramienta digital mediante la creación y aplicación de una rúbrica. Esta fue diseñada y aplicada en colaboración con expertos certificados en seguridad de la información, con experiencia en la norma ISO 27001, para garantizar que los criterios de evaluación estén alineados con los estándares internacionales de seguridad de la información y que cumple con las necesidades específicas de TEINCO.

La rúbrica servirá como una guía detallada para la evaluación de la herramienta digital, proporcionando un conjunto claro y coherente de criterios para evaluar la calidad y el cumplimiento con los requisitos predefinidos.

Según Lopez (2023), “La aplicación de una rúbrica en proyectos de desarrollo tecnológico proporciona una estructura clara y objetiva para evaluar la calidad y el cumplimiento con los estándares requeridos, esto no solo garantiza la coherencia en la evaluación, sino que también facilita la identificación de áreas de mejora y la toma de decisiones informadas para el desarrollo futuro

del proyecto". (pag. 71). Teniendo en cuenta las palabras de la Especialista en Gestión de Proyectos Tecnológicos, los expertos utilizarán esta rúbrica para realizar una evaluación objetiva y rigurosa de la herramienta digital, identificando áreas de mejora y garantizando su cumplimiento con los estándares de seguridad de la información, puesto que esta permite una evaluación estandarizada y consistente, lo que asegura que el proceso de evaluación sea transparente y libre de sesgos.

Es importante destacar que, al tratarse de un estudio de caso en TEINCO y considerando que la herramienta digital se ha desarrollado dentro del dominio de la corporación utilizando Google Sites, el acceso estará restringido a aquellas personas que dispongan de un correo institucional autorizado. Esta medida garantiza la confidencialidad y seguridad de la información, en línea con los pilares fundamentales de integridad, disponibilidad y confidencialidad establecidos en la metodología InfoSecurity, por lo tanto, para la realización de esta rúbrica fue necesario realizar una sesión virtual.

Fase 5: Implementación algoritmo conceptual mediante IA

Ante la imperativa necesidad de robustecer los principios y la cultura institucional de seguridad de la información en la Corporación Tecnológica Industrial Colombiana - TEINCO, se plantea la introducción de un modelo comprensivo basado en el Modelo de Cadena de Valor (MCV). Este modelo, meticulosamente diseñado para satisfacer las exigencias del ámbito educativo y productivo del país, se enfoca primordialmente en el desarrollo del numeral 6.3 del Anexo A de la norma ISO 27001:2022, conocido como Conciencia de Seguridad de la Información, Educación y Formación.

Para llevar a cabo esta innovadora iniciativa, se busca el apoyo de la inteligencia artificial (IA), aprovechando su capacidad para analizar datos, generar matrices y sugerir acciones específicas que se alineen con los objetivos del proyecto. Esta fase, que se llevará a cabo durante la futura implementación de la herramienta digital, posibilitará la simulación de su desempeño y la evaluación de su eficacia en entornos controlados, garantizando así su coherencia con los estándares de seguridad y las necesidades particulares de TEINCO.

La integración de la Inteligencia Artificial en la implementación del Modelo de Cadena de Valor (MCV) representaría una aportación sustancial a la metodología, debido a que la capacidad analítica y predictiva de la inteligencia artificial facilita una evaluación más precisa de los datos recopilados durante la simulación de la herramienta digital, lo que permite la identificación más efectiva de patrones, tendencias y áreas de mejora, optimizando así el proceso de toma de decisiones. Además, al utilizar la IA para generar matrices y proponer acciones específicas en consonancia con los objetivos del proyecto, se aseguraría una mayor eficiencia y efectividad en la implementación de las estrategias de seguridad de la información.

En resumen, la incorporación de la Inteligencia Artificial en la metodología InfoSecurity fortalecería su capacidad para adaptarse de manera dinámica a los cambios y desafíos del entorno, asegurando la excelencia en la gestión de la seguridad de la información en TEINCO.

3. RESULTADOS Y DISCUSIÓN

3.1. METODOLOGÍA INFOSECURITY

Se propone la metodología InfoSecurity para la estructuración de una herramienta digital de cultura y conciencia en seguridad de la información alineada al numeral 6.3 del anexo A de la ISO 29001, en el caso de estudio TEINCO, promueve un pensamiento seguro y actuar oportuno frente a posibles amenazas que puedan comprometer la seguridad de la información y los datos.

Esta metodología, como marco principal en el abordaje de la cultura y la conciencia en seguridad de la información en TEINCO, se fundamenta en tres pilares esenciales: integridad, disponibilidad y confidencialidad. Estos pilares fueron cuidadosamente seleccionados debido a su crucial importancia en la protección de datos sensibles y la promoción de prácticas seguras en el manejo de la información. Como afirman Smith y Johnson (2019), "la integridad, la disponibilidad y la confidencialidad son los pilares fundamentales sobre los cuales se basa la seguridad de la información en cualquier organización" (p. 45).

La metodología InfoSecurity se compone de seis (3) pilares:

1. **Integridad:** la integridad, primer pilar de la metodología, garantiza que la información no sea alterada de manera no autorizada, manteniendo su precisión y fiabilidad. Este aspecto es crucial para preservar la confianza en los datos y su utilidad para la toma de decisiones. Según Jones (2020), "la integridad de los datos es esencial para garantizar su valor y utilidad para la organización" (p. 67).

2. **Disponibilidad:** el segundo pilar, la disponibilidad, asegura que la información esté siempre accesible para aquellos usuarios autorizados que la necesiten, evitando interrupciones no planificadas en su acceso. Como señala Brown (2018), "la disponibilidad de la información es fundamental para garantizar la continuidad del negocio y la eficiencia operativa" (p. 32).

3. **Confidencialidad:** finalmente, la confidencialidad, tercer pilar de la metodología, se encarga de proteger la información sensible y restringir su acceso únicamente a las personas autorizadas, evitando así filtraciones o accesos no autorizados. De acuerdo con García (2019), "la confidencialidad es esencial para proteger la información sensible y preservar la privacidad de los individuos" (p. 21).

Estos pilares fueron seleccionados, no solo por su importancia intrínseca en la seguridad de la información, sino también por su capacidad para garantizar la confianza y seguridad en el manejo de los datos y de la información tanto para la institución como para sus usuarios.

Con estos pilares definidos a continuación se exponen las fases de la metodología Infosecurity:

1. **Fase 1. Diagnóstico:**

En la Fase 1, nos sumergimos en el proceso inicial y fundamental del diagnóstico en TEINCO, con el propósito

de identificar con precisión las necesidades y desafíos en materia de seguridad de la información como podemos ver a continuación:

- **Identificación de la necesidad**

En este paso, se llevó a cabo un proceso de recolección de información crucial para comprender el panorama actual de TEINCO con relación a la seguridad de la información. Se realizaron entrevistas informales con la alta dirección y otros líderes clave de la institución, con el objetivo principal de obtener una visión clara sobre el estado actual de la seguridad de la información, así como conocer las expectativas y desafíos relacionados con la concientización en este ámbito dentro de TEINCO.

Se tuvo en cuenta preguntas como:

I. ¿En algún momento ha existido un programa o un plan relacionado con seguridad de la información para concientizar a las personas de TEINCO en estos temas?

II. ¿Se ha contemplado la posibilidad de adquirir la certificación en la norma ISO 27011?

III. ¿Considera importante que en TEINCO haya un plan de concientización en Seguridad de la Información?

Estas preguntas permitieron identificar las experiencias pasadas, las expectativas futuras y las áreas de interés clave para la alta dirección y los líderes de TEINCO con relación a la seguridad de la información. Los datos recopilados en esta etapa proporcionó una base sólida para el desarrollo de estrategias y planes de acción futuros relacionados con la concientización en seguridad de la información en la institución.

2. Fase 2. Análisis de diagnóstico:

En esta etapa crucial del proceso de mejora de la seguridad de la información en TEINCO, se lleva a cabo un análisis del diagnóstico realizado en la fase anterior. El objetivo principal de esta fase fue profundizar en los hallazgos obtenidos durante el diagnóstico inicial, identificando las brechas existentes, las oportunidades de mejora y definiendo las estrategias y acciones específicas necesarias para fortalecer la concientización en seguridad de la información en la institución.

Durante este análisis, se examinó detenidamente los resultados obtenidos de las entrevistas con la alta dirección y otros líderes clave, así como cualquier información recopilada mediante investigaciones de documentos relacionados con seguridad de la información y ciberseguridad en Google Academy. Este proceso de análisis permitió comprender la situación actual de TEINCO con relación a la seguridad de la información, identificando áreas de fortaleza y áreas de mejora.

Además, en esta fase se presta especial atención al cumplimiento del numeral de concientización en seguridad de la información establecido en la norma ISO 27001, asegurando que todas las acciones planificadas estén alineadas con este requisito internacionalmente reconocido.

Lo que motivó a implementar la metodología para crear una herramienta digital de cultura y conciencia en seguridad de la información. Esta herramienta no solo proporciona recursos asociados a la seguridad de la información, sino que también desempeña un papel crucial en la sensibilización de los usuarios sobre este tema tan importante, ya que al centralizar y organizar el material educativo, facilita la difusión de información relevante y actualizada, lo que contribuye significativamente a optimizar los esfuerzos de concientización.

3. Fase 3. Diseño:

Esta fase representa un paso crucial en la implementación de la metodología de seguridad de la información en TEINCO, ya que se establecieron los fundamentos para la creación de la herramienta digital que desempeñaría un papel central en el fortalecimiento de la conciencia y la cultura de seguridad entre los docentes, administrativos y estudiantes de la institución.

Esta se divide en varias etapas y se enfocó en la planificación, investigación, diseño, creación de contenido y personalización de la herramienta digital, asegurando así su alineación con los objetivos y necesidades específicas de TEINCO, así como podemos evidenciar a continuación:

a. Etapa 1. Planificación

En esta etapa inicial, se establecieron los objetivos y alcances del proyecto, definiendo claramente los resultados esperados. Adicionalmente, se identificaron los recursos necesarios, tanto humanos como tecnológicos, así como los plazos de ejecución.

Se identificaron los requisitos de la norma ISO 27001 que se interrelacionan con la concientización y con el numeral 6.3 del Anexo A y en los cuales aplicará un plan de acción de concientización como se puede observar a continuación:

- Requisito de ISO 27001:2022: 4.2 Comprensión de las necesidades y expectativas de las partes interesadas:

- Requisito de ISO 27001:2022: 5.2 - Política de Seguridad de la Información:
- Requisito de ISO 27001:2022: 6.1.1 - Acciones para abordar riesgos y oportunidades:
- Requisito de ISO 27001:2022: 7.3 - Toma de Conciencia:
- Requisito de ISO 27001:2022: 8.2 - Responsabilidad de la Dirección:
- Requisito de ISO 27001:2022: 8.3 - Roles y Responsabilidades:
- Requisito de ISO 27001:2022: 8.4 - Conciencia, formación y competencia:

Adicionalmente, se realizó una evaluación de riesgos para anticipar posibles obstáculos y se diseñó un plan de acción detallado que guio el desarrollo de las siguientes etapas como se evidencia en la Tabla 3. Esta fase fue crucial para asegurar que el proyecto avanzara de manera estructurada y eficiente, garantizando su éxito a largo plazo.

Tabla 3. Evaluación de riesgos

NO.	IDENTIFICACIÓN DE RIESGO	EVALUACIÓN DE RIESGO	MITIGACIÓN DE RIESGO	MONITOREO Y CONTROL (FUTURA IMPLEMENTACIÓN)
1	Cambios en el entorno tecnológico	Impacto: Alto	Realizar análisis de impacto y pruebas de compatibilidad antes de implementar cambios tecnológicos significativos	Monitorear regularmente los avances en tecnología y evaluar su impacto en el proyecto
2	Escasez de recursos humanos	Impacto: Medio	Contratación de personal adicional o capacitación del personal existente	Establecer un sistema de seguimiento del personal para identificar cualquier necesidad de refuerzo
3	Retrasos en la adquisición de equipos	Impacto: Alto	Diversificar proveedores y establecer acuerdos de nivel de servicio (SLA)	Supervisar de cerca el proceso de adquisición y establecer fechas límite claras
4	Cambios en el entorno legal/ regulatorio	Impacto: Medio	Mantenerse actualizado sobre las regulaciones y adaptar los procesos en consecuencia	Asignar un responsable para monitorear los cambios en el entorno legal/regulatorio
5	Fallas en la comunicación interna	Impacto: Medio	Establecer canales de comunicación claros y reuniones periódicas de seguimiento	Realizar encuestas de satisfacción del equipo para identificar posibles problemas de comunicación
6	Interrupciones en la conectividad de red	Impacto: Alto	Implementar redundancia en la infraestructura de red y servicios en la nube	Realizar pruebas de resiliencia de red periódicas y mantener un plan de contingencia actualizado

Nota: Esta tabla presenta una estructura clara para identificar, evaluar, mitigar y monitorear los riesgos asociados al proyecto.

Fuente: Elaboración propia

Cada riesgo se acompaña de medidas específicas para abordarlo y se establece un proceso de monitoreo para garantizar una gestión efectiva a lo largo del proyecto. Esta identificación de riesgos es fundamental para gestionar de manera efectiva los riesgos asociados con el proyecto, lo que contribuye a su éxito al identificar y abordar los posibles obstáculos de manera anticipada y planificada.

b. Etapa 2. Investigación

Durante esta etapa, se llevó a cabo un análisis para recopilar información relevante sobre las necesidades y características del público objetivo en TEINCO, así como las mejores prácticas en seguridad de la información.

a. Se realizaron encuestas a personal administrativo, docente y estudiantil para identificar sus percepciones, conocimientos y prácticas en cuanto a seguridad de la información. Este proceso de investigación proporcionó información valiosa que sirvió de base para diseñar estrategias efectivas y personalizadas de concientización en seguridad de la información.

En las encuestas que se realizaron a toda la población de TEINCO que son aproximadamente mil personas, de las cuales respondieron 124 personas, se preguntaron aspectos como:

I. Si utilizan el doble factor de autenticación o 2FA.

II. Qué hacen cuando reciben un link o archivo mediante correo electrónico o SMS.

III. Si utilizan la misma contraseña para varias cuentas en línea.

IV. Con qué frecuencia cambian las contraseñas de sus aplicaciones.

V. Si alguna vez ha sido víctima de un ataque cibernético.

VI. Si utiliza un software antimalware/antivirus en tus dispositivos.

VII. Con qué frecuencia actualizan el software de seguridad de los dispositivos normalmente (computador, celular, tablet).

VIII. Si realizan copias de seguridad de la información.

IX. Si se conectan a redes Wi-Fi públicas.

X. Alguna vez ha recibido alguna formación o capacitación sobre Seguridad de la Información.

Es aquí cuando observamos la importancia de implementar la herramienta digital con contenido orientado a reforzar y garantizar que se aborden de manera integral las necesidades y desafíos en materia de seguridad de la información.

b. Se definió un diario de campo cuando se realizaron las encuestas de manera presencial, lo cual tuvo el resultado que se puede observar en la Tabla 4.

Tabla 4. Diario de Campo

Fecha: 24 de abril del 2024	**Lugar:** TEINCO
Responsable: Maira Angel & Deyanira Perez	
Participantes: Personal administrativo, docente y estudiantil de TEINCO	
Descripción: durante esta fase de investigación, se realizaron encuestas presenciales al personal de TEINCO, incluyendo administrativos, docentes y estudiantes. El objetivo fue identificar percepciones, conocimientos y prácticas en seguridad de la información. La encuesta abordó temas relevantes como el uso de doble factor de autenticación (2FA), la gestión de enlaces y archivos recibidos por correo electrónico o SMS, el manejo de contraseñas, entre otros aspectos relacionados con la seguridad cibernética.	
Resultados: durante la realización de las encuestas presenciales, se recopiló información valiosa sobre las prácticas de seguridad de los participantes. Se observó que un porcentaje significativo de encuestados no utiliza el doble factor de autenticación y utiliza contraseñas similares para varias cuentas en línea. Además, se identificó una falta de conciencia sobre la importancia de realizar copias de seguridad de información de manera regular y de actualizar el software de seguridad en dispositivos.	
Implicaciones: los resultados obtenidos de las encuestas presenciales resaltan la necesidad de implementar estrategias efectivas de concientización en seguridad de la información en TEINCO. La falta de prácticas seguras identificadas subraya la importancia de diseñar contenido educativo y de capacitación específico para abordar las áreas de vulnerabilidad. La herramienta digital propuesta deberá centrarse en ofrecer información relevante y práctica que ayude a mejorar las prácticas de seguridad cibernética en la institución.	
Conclusión: las encuestas presenciales realizadas durante esta fase proporcionaron una visión detallada del estado actual de la seguridad de la información en TEINCO. Los resultados obtenidos servirán como base para el diseño y desarrollo de estrategias efectivas de concientización en seguridad de la información, con el objetivo de fortalecer la cultura de seguridad de la información y ciberseguridad en la institución.	

Fuente: Elaboración propia

c. Etapa 3. Diseño:

El diseño de la herramienta digital se dividió en varias secciones para abordar de manera integral las necesidades de los usuarios, se crearon secciones como: video tips, infografías, documentos de interés y juegos.

Cada sección se desarrolló con base en los hallazgos de la fase de investigación, asegurando su relevancia y utilidad para el público objetivo. El diseño se realizó con un enfoque centrado en el usuario, buscando ofrecer una experiencia

intuitiva y atractiva que fomentará la participación y el aprendizaje, y promoviendo los pilares de integridad, disponibilidad y confidencialidad en el manejo de la información.

Para la fase del diseño se utilizó Google Sites como plataforma para desarrollar la herramienta digital ya que proporciona una solución robusta, flexible y segura que cumple con los requisitos del proyecto en TEINCO. Su facilidad de uso, capacidad de colaboración en tiempo real y acceso desde cualquier lugar lo convierten en una opción ideal para promover una cultura de seguridad de la información en la institución.

Esta herramienta digital cuenta con beneficios significativos, como, por ejemplo:

I. Facilidad de uso: Google Sites es conocido por su interfaz intuitiva y fácil de usar, lo que permite a los usuarios crear y editar contenido de manera sencilla sin necesidad de tener habilidades técnicas avanzadas.

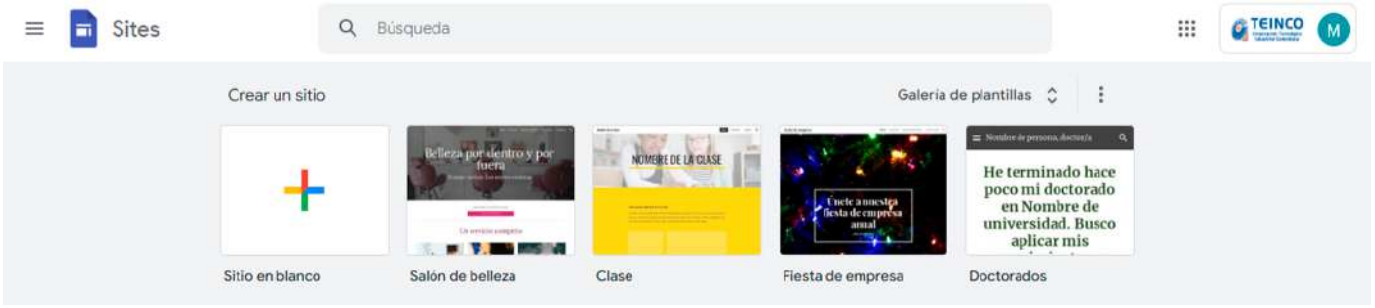
II. Esto facilita la colaboración entre diferentes equipos y garantiza una curva de aprendizaje suave para los usuarios, así como se observa en la Figura 5.

Figura 5. Ejemplo interfaz de sitio en Google Sities

Fuente: Elaboración propia

Acceso desde cualquier lugar: como parte del conjunto de herramientas de Google Workspace, Google Sites está completamente integrado con otras aplicaciones de Google, lo que permite a los usuarios acceder y editar el contenido desde cualquier dispositivo con conexión a Internet. Esto brinda flexibilidad y facilita el acceso remoto, lo que es especialmente útil en entornos educativos y corporativos como TEINCO, tal como se evidencia en la Figura 6.

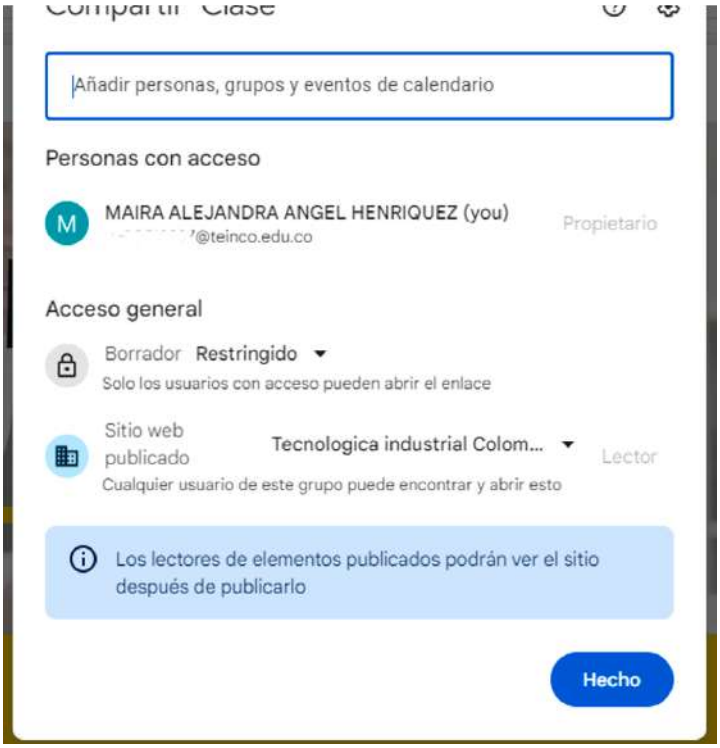
Figura 6. Primer paso para crear la herramienta digital en Google Sites



Fuente: Elaboración propia

III. Colaboración en tiempo real: Google Sites permite la colaboración en tiempo real entre múltiples usuarios, lo que significa que varias personas pueden trabajar en el mismo sitio al mismo tiempo. Esto promueve la colaboración y la productividad al facilitar la comunicación y la edición simultánea del contenido como se puede observar a continuación en la Figura 7.

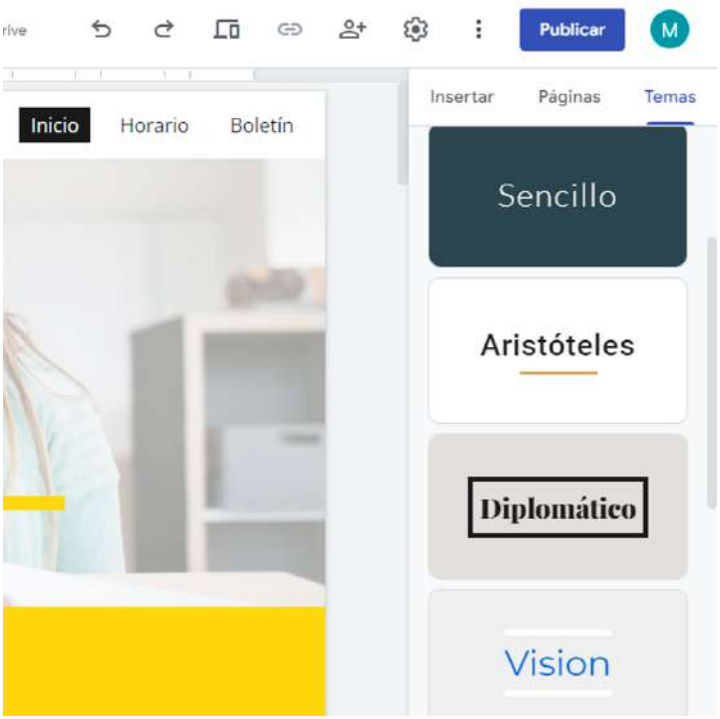
Figura 7. Ejemplo de cómo se puede compartir la herramienta digital



Fuente: Elaboración propia

IV. Personalización y diseño flexible: aunque Google Sites ofrece plantillas prediseñadas para facilitar el proceso de creación, también permite una gran flexibilidad en cuanto al diseño y la personalización del sitio. Los usuarios tienen la capacidad de personalizar la apariencia y la estructura del sitio según sus necesidades específicas, lo que garantiza que la herramienta digital se adapte perfectamente a los requisitos del proyecto como se puede evidenciar en la Figura 8.

Figura 8. Ejemplo de cómo configurar y personalizar los temas en la herramienta digital



Fuente: Elaboración propia

V. Seguridad y fiabilidad: Google Sites ofrece altos estándares de seguridad y fiabilidad respaldados por la infraestructura de Google. Los datos almacenados en Google Sites están protegidos mediante cifrado y medidas de seguridad avanzadas, lo que garantiza la privacidad y la integridad de la información.

La implementación de la herramienta digital de la metodología InfoSecurity, en el caso de estudio TEINCO, se llevó a cabo de la siguiente manera:

Se seleccionaron cuidadosamente diversas categorías para el material mediante el cual se transmitió la información sobre cultura y conciencia en seguridad de la información y ciberseguridad. Esta elección se fundamentó en la efectividad de cada formato para alcanzar y comprometer a la audiencia objetivo. Según un estudio realizado por la Universidad de los Andes en Colombia, "La tecnología ha cambiado drásticamente la forma en que aprendemos y procesamos la información. El 65% de los estudiantes considera que el contenido visual facilita la comprensión de los conceptos difíciles" (pag.76).

Es por esto que los materiales escogidos fueron los siguientes:

1. **Video Tips:** los Video Tips fueron seleccionados debido a su capacidad para ofrecer información de manera visual y dinámica, lo que facilita la comprensión de conceptos complejos en un formato accesible y atractivo. Dale (2021) desarrolló la "Cone of Experience" (Cono de la Experiencia), que muestra que recordamos el 10% de lo que leemos, el 20% de lo que escuchamos, el 30% de lo que vemos, y hasta el 90% de lo que simulamos o hacemos nosotros mismos. Esto respalda la idea de que el contenido audiovisual, como los videos, puede ser una forma muy efectiva de aprendizaje.

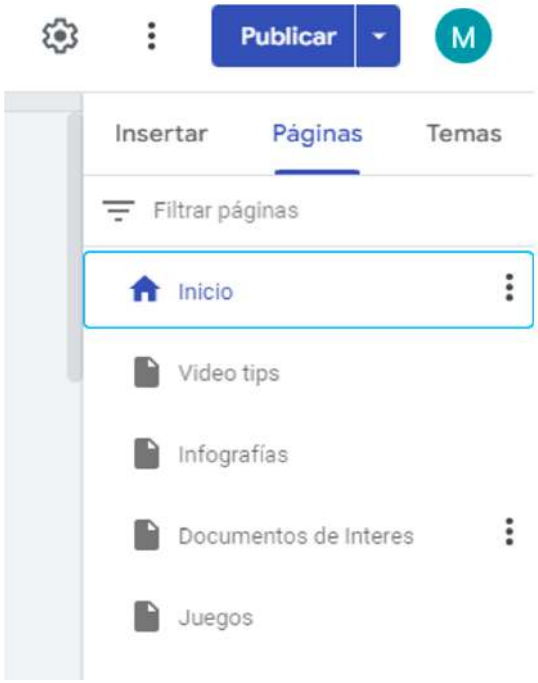
2. **Infografías:** fueron incluidas por su capacidad para condensar información compleja en un formato visualmente atractivo y fácil de digerir. Según estudios de 3M Corporation (2022), "los seres humanos procesan imágenes 60,000 veces más rápido que el texto", lo que subraya la eficacia de las infografías para captar la atención y mejorar la retención de la información.

3. **Documentos de Interés:** estos se consideraron esenciales para proporcionar recursos adicionales y en profundidad sobre temas específicos relacionados con la seguridad de la información. Como dijo Angelou (2020)"cuando sabes mejor, haces mejor", lo que sugiere que la educación continua a través de documentos detallados puede empoderar a las personas para tomar decisiones más informadas (pag.93).

4. **Juegos:** se integraron como una forma lúdica y entretenida de involucrar a los usuarios y reforzar los conceptos de seguridad de la información de manera interactiva. De acuerdo con McGonigal (2022), "los juegos nos ofrecen la oportunidad de concentrarnos, aprender y socializar". (pag.67), lo que destaca el potencial de los juegos como herramienta para el compromiso y el aprendizaje experiencial.

Ya definidas estas secciones, se procedió a crear las secciones en la herramienta digital, como se puede observar en la Figura 9.

Figura 9. Ejemplo de cómo configurar, personalizar y colocar en secciones las páginas en la herramienta digital



Fuente: Elaboración propia

d. Etapa 4. Creación de contenido:

Durante la Fase 4 del proyecto, el contenido se creó utilizando la plataforma Canva, como se puede evidenciar en la figura 10, que permitió diseñar materiales visuales atractivos y profesionales. Estos recursos se enfocaron en los temas identificados como mejoras en las investigaciones y según los resultados de las fases anteriores. Además, se tuvo en cuenta los controles de seguridad de la información que requieren acciones de concientización, según lo establecido en el numeral 6.3 del anexo A de concientización de la norma ISO 27001.

De esta manera, el contenido creado abordó de manera específica los aspectos clave relacionados con la seguridad de la información y se alineó con los requisitos de la norma internacional. Los temas abordados incluyeron:

I. Gestión de contraseñas seguras.

II. Protección contra ataques de phishing.

III. Uso adecuado de redes Wi-Fi públicas.

IV. Importancia de las actualizaciones de software y antivirus.

V. Realización de copias de seguridad de la información.

VI. Identificación y prevención de amenazas cibernéticas.

VII. Buenas prácticas en el manejo de datos sensibles.

VIII. Sensibilización sobre políticas de seguridad de la información.

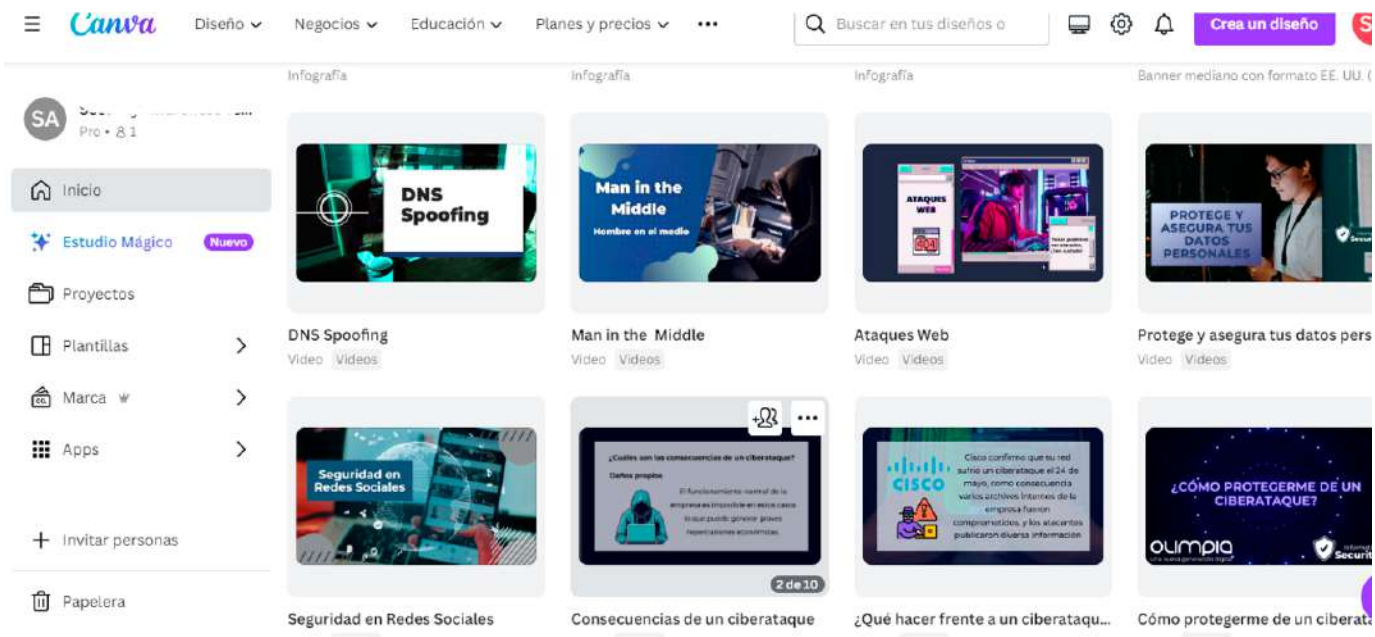
IX. Concientización sobre el uso adecuado de dispositivos móviles y almacenamiento externo.

X. Uso consciente de redes sociales.

XI. Promoción de una cultura de seguridad informática en el entorno personal y educativo.

Estos temas, entre muchos otros, fueron seleccionados cuidadosamente para abordar las áreas críticas de seguridad de la información y promover prácticas seguras entre el personal administrativo, docente y estudiantil de TEINCO.

Figura 10. Creación de contenido audiovisual en Canva



Fuente: Elaboración propia

e. **Etapa 5. Personalización:**

En esta etapa, se ajustó y personalizó la herramienta digital para adaptarla a las características y preferencias de TEINCO y su comunidad. Se establecieron mecanismos de seguimiento y control para garantizar que la herramienta cumpliera con los estándares de calidad y seguridad establecidos.

Esta personalización no solo permitió adecuar la herramienta a las necesidades cambiantes del entorno institucional, sino que también reforzó los pilares de integridad, disponibilidad y confidencialidad en la gestión de la información.

En la personalización de la herramienta se tuvo en cuenta la identidad de marca, la organización de cada una de las secciones y el contenido a publicar de la siguiente manera:

- **Identidad de marca:**

  En la personalización de la herramienta digital, se prestó especial atención a la identidad de marca de TEINCO. Los colores seleccionados fueron cuidadosamente escogidos para reflejar fielmente la imagen corporativa de la institución, se aseguró que los tonos y combinaciones elegidos estuvieran en línea con los estándares visuales establecidos por TEINCO, garantizando una integración coherente con la marca y una experiencia de usuario consistente, así como se puede visualizar en la Figura 11.

Figura 11. Personalización de la identidad de marca de TEINCO en Google Sites

Fuente: Elaboración propia

- **Organización de cada sección:**

  Cada sección de la herramienta fue meticulosamente organizada para proporcionar una navegación intuitiva y fluida a los usuarios.

  Se priorizó la coherencia y consistencia en la presentación del contenido, asegurando que cada sección estuviera claramente identificada y accesible, adicionalmente se implementaron jerarquías visuales y estructuras de navegación claras para facilitar la ubicación y el acceso a la información relevante como se puede ver un poco en la Figura 12.

Figura 12. Ejemplo de organizaciones de secciones en Google Sites

Fuente: Elaboración propia

- **Contenido a publicar:**

  En cuanto al contenido, se seleccionaron cuidadosamente materiales relevantes y de alta calidad que abordaron los temas clave y que de acuerdo a las fases anteriores, se identificó la necesidad de reforzar en seguridad de la información y ciberseguridad.

  Se incluyeron videos tips, infografías informativas, documentos de interés y juegos interactivos. Esta selección se basó en los resultados de la fase de investigación y en las necesidades específicas de la comunidad de TEINCO.

  El objetivo fue ofrecer información útil y prácticas que contribuyan al fortalecimiento de la cultura de seguridad digital en la institución y dieran cumplimiento al objetivo de esta metodología.

  El contenido en cada una de las secciones se realizó de la siguiente manera:

  1. **Inicio:**

     En el inicio de la herramienta digital se añadió información acerca de TEINCO y temas de seguridad como el cifrado de la información, el MA (Multiple Factor de Autenticación) y la protección de datos personales, come se puede ver en la Figura 13. Esto se consideró crucial para proporcionar a los usuarios una comprensión clara de los principales aspectos relacionados con la seguridad de la información desde el principio de su interacción con la plataforma, sin embargo, se espera que estos temas se actualicen periódicamente de acuerdo con la información relevante que deba compartirse debido a los avances en tecnología, cambios en las regulaciones de seguridad y otras actualizaciones pertinentes. Esta práctica garantiza que los usuarios estén al tanto de las últimas tendencias y mejoren prácticas en seguridad digital, manteniéndolos informados y preparados para enfrentar los desafíos emergentes en el ámbito de la seguridad de la información y ciberseguridad.

Figura 13. Contenido de la página principal

Fuente: Elaboración propia

2. **Video Tips:**

En la sección de Video Tips, se incluyeron una serie de videos educativos diseñados para abordar temas específicos relacionados con la seguridad de la información y la ciberseguridad. Estos videos fueron cuidadosamente seleccionados y producidos con el objetivo de ofrecer información clara, concisa y fácil de entender para los usuarios de TEINCO.

Cada video abordó un tema relevante como amenazas principales para la seguridad de la información, qué es un ataque cibernético, qué hacer frente a un ciberataque, proteger datos personales, seguridad en dispositivos móviles, seguridad en redes sociales y demás conceptos presentados para facilitar su comprensión. Además, se integraron ejemplos prácticos y casos de estudio para ilustrar los conceptos presentados y facilitar su comprensión. Los Videotips se basaron en los resultados de la fase de investigación y en las necesidades específicas identificadas por la comunidad de TEINCO, asegurando así su relevancia y utilidad para los usuarios. Esta sección proporciona una forma efectiva y accesible de aprender sobre seguridad digital, complementando otras estrategias de concientización implementadas en la plataforma.

Los Videotips se basaron en los resultados de la fase de investigación y en las necesidades específicas identificadas por la comunidad de TEINCO, asegurando así su relevancia y utilidad para los usuarios. Esta sección proporciona una forma efectiva y accesible de aprender sobre seguridad digital, complementando otras estrategias de concientización implementadas en la plataforma como se puede evidenciar en la Figura 14.

Figura 14. Contenido sección de Videotips

Fuente: Elaboración propia

3. **Infografías:**

En la sección de infografías, se abordaron diversos temas fundamentales para la seguridad cibernética y la protección de la información, estos incluyen aspectos como la identificación de los ciberdelincuentes y sus objetivos, así como consejos prácticos para utilizar de manera segura las redes sociales. También se exploraron temas más técnicos, como los ataques DDoS y las medidas de autenticación de dos pasos en redes sociales. Las infografías proporcionaron orientación sobre cómo configurar la privacidad en las redes sociales y promover buenas prácticas para proteger la información sensible. Además, se ofrecieron recomendaciones sobre cómo mejorar la seguridad y privacidad en dispositivos móviles, así como la importancia de realizar copias de seguridad, adicionalmente, se incluyeron consejos útiles para identificar aplicaciones falsas y se discutió el riesgo de exposición de datos personales en línea. Estas infografías se diseñaron para ofrecer información clara y concisa, ayudando a los usuarios a comprender mejor los desafíos de seguridad en el mundo digital y adoptar medidas preventivas adecuadas como se puede observar en la Figura 15.

Figura 15. Contenido sección de Infografías

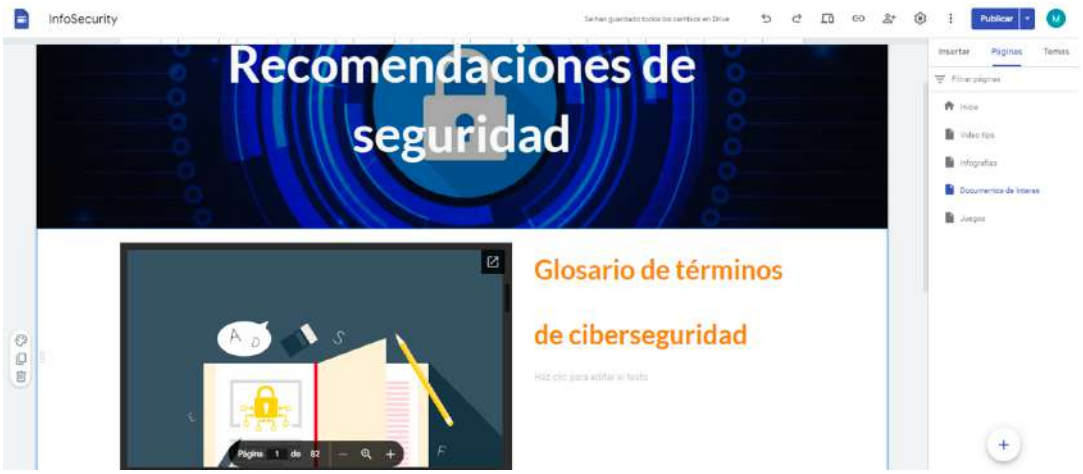
Fuente: Elaboración propia

4. **Documentos de interés:**

En la sección de “Documentos de interés”, se proporcionaron recursos valiosos relacionados con la seguridad de la información y la ciberseguridad. Estos documentos abarcan una variedad de temas relevantes para la comunidad de TEINCO, incluyendo un glosario de términos de ciberseguridad y directrices para proteger los datos personales de manera efectiva. Además, se incluyeron materiales educativos sobre prácticas recomendadas para mejorar la seguridad.

Estos documentos fueron seleccionados cuidadosamente para proporcionar información relevante y práctica que ayudará a los usuarios a fortalecer su postura de seguridad digital y a proteger sus datos de manera más efectiva en un entorno en constante evolución como se puede evidenciar en la Figura 16.

Figura 16. Contenido sección de Recomendaciones de Seguridad



Fuente: Elaboración propia

5. **Juegos:**

En la sección de “juegos”, se incluyen actividades interactivas diseñadas para educar y concienciar a la comunidad de TEINCO sobre temas clave relacionados con la seguridad de la información y la ciberseguridad. Estos juegos ofrecieron una forma divertida y dinámica de aprender sobre conceptos importantes, se desarrollaron juegos que permitieron a los usuarios practicar habilidades específicas frente a seguridad de la información. Estas actividades lúdicas no solo proporcionaron un enfoque interactivo para el aprendizaje, sino que también ayudaron a reforzar los conocimientos adquiridos a través de otros recursos como videos, infografías y documentos de interés. Al incorporar juegos en la herramienta digital, se promovió la participación activa de los usuarios y se fomenta un mayor compromiso con los principios de seguridad digital como se puede evidenciar en la Figura 17.

Figura 17. Contenido sección de Juegos

Fuente: Elaboración propia

f. Etapa 6. Prueba y lanzamiento:

En esta etapa crucial del proyecto, nos preparamos para poner a prueba la simulación de la herramienta digital desarrollada y lanzarla oficialmente para su evaluación y futura implementación en TEINCO. Para garantizar su efectividad y éxito potencial, seguimos un proceso riguroso que involucra pruebas exhaustivas y una estrategia de lanzamiento cuidadosamente planificada descrita a continuación:

- **Pruebas de funcionalidad:** antes del lanzamiento oficial, llevamos a cabo pruebas exhaustivas de funcionalidad para asegurarnos de que todas las características de la herramienta funcionen correctamente. Esto incluye verificar la navegación, la interactividad de los elementos, la reproducción de videos, la visualización de infografías, la descarga de documentos y el funcionamiento de los juegos simulados.

- **Pruebas de compatibilidad:** también realizamos pruebas de compatibilidad para asegurarnos de que la simulación funcione correctamente en diferentes dispositivos y navegadores web. Se verificó su rendimiento en computadoras de escritorio, portátiles, tabletas y dispositivos móviles, así como en navegadores populares como Chrome, Firefox, Safari y Edge.

- **Pruebas de seguridad:** dado que la seguridad de la información es una prioridad, se realizaron pruebas exhaustivas de seguridad para identificar y abordar posibles vulnerabilidades en la simulación. Se aseguró de que la simulación cumpla con los estándares de seguridad establecidos y que los datos simulados de los usuarios estén protegidos de manera adecuada.

- **Plan de lanzamiento:** para el lanzamiento oficial de la simulación, desarrollamos un plan que incluye la fecha y hora de lanzamiento, la comunicación y las actividades de promoción.

4. Fase 4. Validación herramienta:

La validación de la herramienta digital es una etapa crítica en el proceso de implementación, donde se verifica que la solución diseñada cumpla con los estándares de calidad y requisitos establecidos. En esta fase, nos enfocamos en realizar pruebas exhaustivas y obtener retroalimentación de expertos en seguridad de la información certificados en la norma ISO 27001 para asegurar la efectividad y la confiabilidad de la herramienta. El proceso de validación se llevó a cabo de la siguiente manera:

- **Pruebas de funcionabilidad y seguridad:** antes de compartir la herramienta digital con los expertos en seguridad de la información, se realizaron pruebas detalladas para evaluar la funcionalidad y la seguridad de la herramienta digital, se verificaron aspectos como la navegación, la interactividad de los elementos, la protección de datos y la integridad de la información, se identificaron posibles vulnerabilidades y se tomaron medidas correctivas para garantizar la robustez de la herramienta frente a posibles amenazas de seguridad.

- **Rúbrica con especialistas en seguridad de la información:** se desarrolló una rúbrica específica en colaboración con dos especialistas certificados en seguridad de la información y con experiencia en la norma ISO 27001. Esta rúbrica se utilizó como guía para evaluar diferentes aspectos de la herramienta, como su alineación con los estándares de seguridad, la claridad y precisión de la información proporcionada, la usabilidad y la experiencia del usuario, entre otros criterios relevantes.

- **Evaluación y retroalimentación:** los especialistas en seguridad de la información llevaron a cabo una evaluación exhaustiva de la herramienta digital utilizando la rúbrica establecida. En esta se revisaron cada una de las secciones y características de la herramienta y se proporcionó retroalimentación detallada sobre áreas de mejora y aspectos destacados. Esta retroalimentación fue fundamental para identificar posibles puntos ciegos y oportunidades de optimización antes del lanzamiento oficial.

La rúbrica específica utilizada en este ejercicio fue desarrollada en colaboración con dos especialistas certificados en seguridad de la información y con amplia experiencia en la norma ISO 27001. Estos especialistas aportaron una perspectiva valiosa y un profundo conocimiento en el área de la seguridad de la información.

El Especialista 1 es Ingeniero de Sistemas y Especialista de Seguridad de la Información, con 12 años de experiencia en el campo de la tecnología. Graduado de TEINCO, cuenta con experiencia en controles técnicos, continuidad del negocio y ha desempeñado roles como Auditor interno ISO 27001, 9001 y 20000. Además, ha ejercido como Especialista de seguridad de la información en Olimpia IT, lo que le ha brindado una perspectiva práctica y aplicada en el ámbito de la seguridad de la información como se puede ver en la Tabla 5.

Tabla 5. Rúbrica realizada al primer especialista

ASPECTOS A EVALUAR	CALIFICACIÓN			
	EXCELENTE	BUENO	REGULAR	INSUFICIENTE
1. RELEVANCIA DEL CONTENIDO:				
¿El contenido proporcionado es relavante y útil para el público objetivo?	Cumple completamente con los criterios y supera las expectativas.	Cumple la mayoría de los criterios de manera satisfactoria.	Cumple algunos criterios pero presenta áreas de mejora siginificativas.	No cumple con la mayoría de los criterios y requiere una revisión completa.
¿Aborda adecuadamente los conceptos clave de seguridad de la información y ciberseguridad?	Sí, los conceptos relacionados a seguridad de la información y ciberseguridad son abordados de manera adecuada.	Aborda algunos conceptos relevantes y permite entender los temas relacionados.	Algunos conceptos no son claros y generan confusión al momento de interpretar el contenido. Existen oportunidades de mejora.	En la mayoría de los conceptos se tiene ausencia de claridad, se debe evaluar y reestructurar.
2. VARIEDAD DE MATERIALES:				
¿La herramienta ofrece una variedad de materiales, como videos, infografías, documentos y juegos, para adaptarse a diferentes niveles de aprendizaje y preferencias de los usuarios?	Sí, la herramienta cuenta con una metodología práctica agradable y de fácil manejo para el usuario final.	La herramienta muestra variedad de materiales de fácil entendimiento para gran parte de los usuarios objetivo.	El material empleado en la herramienta tiene alcance a una parte de la población objetivo de acuerdo con la diferencia de niveles de aprendizaje.	El material utilizado en la herramienta, se encuentra destinado a público con experiencia en los temas tratados, complicando el desarrollo para otras personas.
¿Los contenidos están diseñados de manera atractiva y son fáciles de entender?	El contenido está definido y diseñado para fácil entendimiento y desarrollo de las actividades por parte de los diferentes actores.	El contenido refiere a los temas de interés con un poco de complejidad para su entendimiento.	El contenido presenta inconsistencias en su desarrollo y dificulta el entendimiento.	El contenido no está relacionado en su totalidad con los temas SI y Ciberseguridad.
3. INTERACTIVIDAD Y PARTICIPACIÓN:				
¿La herramienta fomenta la interacción activa de los usuarios a través de sus actividades?	Sí, la herramienta es interactiva y muy interesante para los usuarios.	La herramienta tiene actividades con interacción amigable pero limitada.	La herramienta es presenta algunas actividades con poco interés para los usuarios.	Es importante considerar mejoras en las actividades buscando el interés del usuario.
¿Permite a los usuarios participar activamente en el proceso de aprendizaje y comprender mejor los conceptos presentados?	Sí, fomenta la participación activa y el interés de aprender gracias a su contenido.	Genera interés y participación en algunos de sus puntos.	Algunos usuarios se limitan en la participación por la complejidad del contenido.	La participación es muy baja por temas de complejidad de entendimiento frente a sus contenidos.
4. ACCESIBILIDAD Y USABILIDAD:				
¿La herramienta es fácil de acceder y usar para todos los usuarios autorizados de TEINCO?	Sí, la herramienta muestra facilidad en su acceso y funcionalidad sin importar el nivel de conocimiento del usuario.	La herramienta facilita el acceso y uso siempre y cuando el usuario presente cierto nivel de conocimientos.	El acceso y uso de la herramienta genera confianza para algunos usuarios, pero funciona.	El acceso y funcionalidad no son muy amigables para todo público.
¿La herramienta digital es accesible desde una variedad de dispositivos y plataformas?	Accesibilidad completa desde una amplia gama de dispositivos y plataformas.	Accesibilidad aceptable, pero con restricciones.	Accesibilidad limitada a ciertos dispositivos o plataformas.	Accesibilidad a dispositivos específicos.
¿Está diseñado de manera intuitiva y presenta una navegación clara y sencilla?	Sí, todos los usuarios sin importar su nivel de conocimiento podrán usar y navegar en la herramienta sin inconvenientes.	La herramienta está diseñada para público con experiencias frente a este tipo de contenidos.	El uso y navegación son complicados sin tener acompañamiento de alguien con experiencia.	La herramienta está sujeta a una experiencia previa frente a otras herramientas.

5. IMPACTO Y EFECTIVIDAD:				
¿La herramienta logra su objetivo de sensibilizar y educar a los usuarios sobre seguridad de la información y ciberseguridad?	Sí, los usuarios aplican los conocimientos brindados.	Los participantes aplican un gran porcentaje de los conocimientos adquiridos.	Algunos temas no son de fácil entendimiento y aplicación.	Los temas relacionados en la herramienta, no generan impacto en el público objetivo.
¿Se observa un cambio positivo en el conocimiento y las prácticas de seguridad de los usuarios después de interactuar con la herramienta?	Sí, la se evidencia aumento de participación en debates y charlas por parte de los usuarios.	Los usuarios aplican el pensamiento seguro y preventivo en el uso de la tecnología.	Algunos temas son aplicados y fomentados en su entorno con un alcance mínimo por su complejidad.	Pocas personas aplican y usan los conocimientos adquiridos.
6. ADAPTABILIDAD Y ACTUALIZACIÓN:				
¿La herramienta puede adaptarse fácilmente para incluir nuevas actualizaciones y contenidos relevantes sobre seguridad de la información?	Sí, al ser una herramienta digital, permite estar en constante actualización.	La herramienta permite actualización sujeta a temas específicos.	La herramienta se limita con relación al proceso de actualización y o cambio.	El proceso de actualización es muy lento y limitado.
¿Se tienen planes para mantener y actualizar periódicamente la herramienta con el tiempo?	Sí, los contenidos y/o materiales se mantienen de acuerdo con el avance y actualización mundial.	Gran parte de los temas son actualizados de acuerdo a cronogramas, lo anterior sujeto a cambios por disponibilidad.	El proceso de actualización está sujeto a disponibilidad del personal y el acceso a los contenidos y/o materiales.	El plan de actualización es muy lento y con pocos recursos.
PUNTUACIÓN:	80%			

Fuente: Elaboración propia

El Especialista 2 también es Ingeniero de Sistemas y Especialista de Seguridad de la Información, con 15 años de experiencia en tecnología. Su experiencia se centra en áreas como gestión de riesgos, continuidad de negocio y auditoría interna ISO 27001, 9001 y 20000. Actualmente, se desempeña como oficial de s eguridad asignado en Sofka Technologies, lo que le ha permitido estar al tanto de las últimas tendencias y desafíos en seguridad de la información como se puede ver en la Tabla 6.

Tabla 6. Rúbrica realizada al segundo especialista

ASPECTOS A EVALUAR	CALIFICACIÓN			
	EXCELENTE	BUENO	REGULAR	INSUFICIENTE
1. RELEVANCIA DEL CONTENIDO:				
¿El contenido proporcionado es relavante y útil para el público objetivo?	Cumple completamente con los criterios y supera las expectativas.	Cumple la mayoría de los criterios de manera satisfactoria.	Cumple algunos criterios pero presenta áreas de mejora siginificativas.	No cumple con la mayoría de los criterios y requiere una revisión completa.
¿Aborda adecuadamente los conceptos clave de seguridad de la información y ciberseguridad?	Sí, los conceptos relacionados a seguridad de la información y ciberseguridad son abordados de manera adecuada.	Aborda algunos conceptos relevantes y permite entender los temas relacionados.	Algunos conceptos no son claros y generan confusión al momento de interpretar el contenido. Existen oportunidades de mejora.	En la mayoría de los conceptos se tiene ausencia de claridad, se debe evaluar y reestructurar.
2. VARIEDAD DE MATERIALES:				
¿La herramienta ofrece una variedad de materiales, como videos, infografías, documentos y juegos, para adaptarse a diferentes niveles de aprendizaje y preferencias de los usuarios?	Sí, la herramienta cuenta con una metodología práctica agradable y de fácil manejo para el usuario final.	La herramienta muestra variedad de materiales de fácil entendimiento para gran parte de los usuarios objetivo.	El material empleado en la herramienta tiene alcance a una parte de la población objetivo de acuerdo con la diferencia de niveles de aprendizaje.	El material utilizado en la herramienta, se encuentra destinado a público con experiencia en los temas tratados, complicando el desarrollo para otras personas.

¿Los contenidos están diseñados de manera atractiva y son fáciles de entender?	El contenido está definido y diseñado para fácil entendimiento y desarrollo de las actividades por parte de los diferentes actores.	El contenido refiere a los temas de interés con un poco de complejidad para su entendimiento.	El contenido presenta inconsistencias en su desarrollo y dificulta el entendimiento.	El contenido no está relacionado en su totalidad con los temas SI y Ciberseguridad.
3. INTERACTIVIDAD Y PARTICIPACIÓN:				
¿La herramienta fomenta la interacción activa de los usuarios a través de sus actividades?	Sí, la herramienta es interactiva y muy interesante para los usuarios.	La herramienta tiene actividades con interacción amigable pero limitada.	La herramienta es presenta algunas actividades con poco interés para los usuarios.	Es importante considerar mejoras en las actividades buscando el interés del usuario.
¿Permite a los usuarios participar activamente en el proceso de aprendizaje y comprender mejor los conceptos presentados?	Sí, fomenta la participación activa y el interés de aprender gracias a su contenido.	Genera interés y participación en algunos de sus puntos.	Algunos usuarios se limitan en la participación por la complejidad del contenido.	La participación es muy baja por temas de complejidad de entendimiento frente a sus contenidos.
4. ACCESIBILIDAD Y USABILIDAD:				
¿La herramienta es fácil de acceder y usar para todos los usuarios autorizados de TEINCO?	Sí, la herramienta muestra facilidad en su acceso y funcionalidad sin importar el nivel de conocimiento del usuario.	La herramienta facilita el acceso y uso siempre y cuando el usuario presente cierto nivel de conocimientos.	El acceso y uso de la herramienta genera confianza para algunos usuarios, pero funciona.	El acceso y funcionalidad no son muy amigables para todo público.
¿La herramienta digital es accesible desde una variedad de dispositivos y plataformas?	Accesibilidad completa desde una amplia gama de dispositivos y plataformas.	Accesibilidad aceptable, pero con restricciones.	Accesibilidad limitada a ciertos dispositivos o plataformas.	Accesibilidad a dispositivos específicos.
¿Está diseñado de manera intuitiva y presenta una navegación clara y sencilla?	Sí, todos los usuarios sin importar su nivel de conocimiento podrán usar y navegar en la herramienta sin inconvenientes.	La herramienta está diseñada para público con experiencias frente a este tipo de contenidos.	El uso y navegación son complicados sin tener acompañamiento de alguien con experiencia.	La herramienta está sujeta a una experiencia previa frente a otras herramientas.
5. IMPACTO Y EFECTIVIDAD:				
¿La herramienta logra su objetivo de sensibilizar y educar a los usuarios sobre seguridad de la información y ciberseguridad?	Sí, los usuarios aplican los conocimientos brindados.	Los participantes aplican un gran porcentaje de los conocimientos adquiridos.	Algunos temas no son de fácil entendimiento y aplicación.	Los temas relacionados en la herramienta, no generan impacto en el público objetivo.
¿Se observa un cambio positivo en el conocimiento y las prácticas de seguridad de los usuarios después de interactuar con la herramienta?	Sí, la se evidencia aumento de participación en debates y charlas por parte de los usuarios.	Los usuarios aplican el pensamiento seguro y preventivo en el uso de la tecnología.	Algunos temas son aplicados y fomentados en su entorno con un alcance mínimo por su complejidad.	Pocas personas aplican y usan los conocimientos adquiridos.
6. ADAPTABILIDAD Y ACTUALIZACIÓN:				
¿La herramienta puede adaptarse fácilmente para incluir nuevas actualizaciones y contenidos relevantes sobre seguridad de la información?	Sí, al ser una herramienta digital, permite estar en constante actualización.	La herramienta permite actualización sujeta a temas específicos.	La herramienta se limita con relación al proceso de actualización y o cambio.	El proceso de actualización es muy lento y limitado.
¿Se tienen planes para mantener y actualizar periódicamente la herramienta con el tiempo?	Sí, los contenidos y/o materiales se mantienen de acuerdo con el avance y actualización mundial.	Gran parte de los temas son actualizados de acuerdo a cronogramas, lo anterior sujeto a cambios por disponibilidad.	El proceso de actualización está sujeto a disponibilidad del personal y el acceso a los contenidos y/o materiales.	El plan de actualización es muy lento y con pocos recursos.
PUNTUACIÓN:	72%			

Fuente: Elaboración propia

Con base en la rúbrica desarrollada en colaboración con los especialistas en seguridad de la información, se llevaron a cabo los ajustes necesarios en la herramienta digital propuesta. Estos ajustes se realizaron considerando la retroalimentación proporcionada por los especialistas, quienes ofrecieron comentarios y sugerencias para mejorar diversos aspectos de la herramienta. Su experiencia y conocimiento permitieron identificar áreas de oportunidad y fortaleza en el diseño y funcionalidad de la herramienta, lo que contribuyó significativamente a su mejora y optimización.

Las recomendaciones recibidas fueron evaluadas cuidadosamente y se implementaron aquellas que contribuyeron a garantizar una mayor alineación con los estándares de seguridad, así como a mejorar la claridad, precisión, usabilidad y experiencia del usuario. El proceso de retroalimentación por parte de los especialistas en seguridad de la información desempeñó un papel crucial en la evolución y refinamiento de la herramienta, asegurando que cumpliera con los más altos estándares de calidad y eficacia en términos de seguridad de la información.

- **Ajustes y mejoras:** con base en la retroalimentación recibida de los especialistas en seguridad de la información, se realizaron ajustes y mejoras en la herramienta digital. Se corrigieron errores identificados, se refinaron los contenidos y se optimizó la usabilidad para garantizar una experiencia óptima para los usuarios finales. Además, se realizaron actualizaciones en función de las recomendaciones proporcionadas por los especialistas para asegurar la alineación con los estándares de seguridad y las mejores prácticas en el campo de la seguridad de la información.

- **Validación final:** una vez completados los ajustes y mejoras, se llevó a cabo una validación final de la herramienta digital para verificar que todas las modificaciones implementadas hayan sido efectivas y que la solución cumpla con los requisitos establecidos. Se realizaron pruebas adicionales para confirmar la estabilidad y el rendimiento de la herramienta antes de su lanzamiento oficial.

En resumen, la Fase 4 de Validación de la Herramienta Digital es fundamental para asegurar la calidad y confiabilidad de la solución desarrollada. A través de pruebas exhaustivas, la colaboración con especialistas en seguridad de la información y la implementación de ajustes y mejoras basados en retroalimentación experta, nos aseguramos de que la herramienta esté lista para futura implementación en TEINCO y contribuya de manera efectiva a fortalecer la cultura de seguridad de la información en la institución.

5. Fase 5. Implementación de algoritmo conceptual mediante I.A.

En la Fase 5 de la metodología InfoSecurity aplicada en TEINCO, se llevará a cabo la implementación algoritmo conceptual mediante I.A. Esta fase ayuda a fortalecer la seguridad de la información en la institución en la futura implementación de la herramienta digital, se basa en el Modelo de Cadena de Valor (MCV) como guía estratégica. Dicho modelo adaptado a las necesidades del sector educativo y productivo, establece una serie de procesos estratégicos (PE), misionales (PM), de apoyo (PA) y de evaluación (PV), cada uno con sus respectivos sistemas de información (SI) necesarios para su ejecución.

La implementación de la Inteligencia Artificial (IA) se integra en esta fase para aprovechar su capacidad analítica y predictiva. Así, se espera que la IA facilite la toma de decisiones, optimice la gestión de la seguridad de la información y garantice la alineación con los estándares ISO 27001: 2022. La relación entre los procesos del MCV y los SI es clave para el éxito de esta iniciativa. Por ejemplo, los procesos estratégicos (PE) se vinculan con sistemas como el banco de proyectos y estadísticas (SI1) o la gestión de acuerdos institucionales (SI6).

Del mismo modo, los procesos misionales (PM) y de apoyo (PA) cuentan con sistemas específicos para su ejecución, como el registro y control académico (SIa) o la gestión del talento humano (SIe). Esta interacción dinámica entre procesos y sistemas garantiza una implementación efectiva de la IA, contribuyendo así a fortalecer la cultura de seguridad de la información en TEINCO.

En resumen, la Fase 5 se presenta como un paso crucial hacia la mejora continua en la gestión de la seguridad de la información, aprovechando el potencial de la Inteligencia Artificial en un contexto educativo y productivo, teniendo en cuenta los siguientes pasos:

- Paso 1: se inicia asignándole un rol a la IA, por ejemplo:

  Rol-1: Implementador y auditor líder en sistemas de gestión basados en las normas ISO con especial atención y manejo de ISO/NTC 21001:2015, ISO/IEC/NTC 9001:2015 e ISO/IEC/NTC 27001:2022.

- Paso 2: posteriormente se le da un contexto a la IA, por ejemplo:

  “La Institución de Educación Superior Corporación Tecnológica Industrial Colombiana (en adelante TEINCO) desarrolla desde hace más de 37 años en el territorio colombiano aportes en la educación bajo programas propedéuticos para formar profesionales en el campo técnico, tecnológico y profesional con el propósito de contribuir a la formación integral de los estudiantes respondiendo a las exigencias del sector productivo del país.

  TEINCO, consciente de la necesidad de mejoramiento continúo, ha logrado las siguientes certificaciones que mantiene vigentes: a) ISO 9001: Sistema de gestión de calidad. Sello otorgado por la Entidad certificadora ICONTEC con el registro SC-CER393049; este sello se acompaña con la certificación otorgada por IQNet Certified Management System con registro CO-SC-CER393049, b) ISO21001: Esta norma impulsa la excelencia educativa y la satisfacción de los estudiantes para lograr una educación de calidad. Sello otorgado por ICONTEC con registro SGOE-CER958748; este sello se acompaña con la certificación otorgada por IQNet Certified Management System con registro CO-SGOE-CER958748.

  TEINCO, en su proceso de excelencia extendido a toda la comunidad institucional, se interesa en desarrollar el requisito de concientización en seguridad de la información indicado en ISO/IEC27001:2022. En consecuencia, y aun cuando su prioridad inmediata no se centra en certificarse en esta norma, si desea fortalecer los siguientes aspectos en pro de formar una excelencia

en la cultura y principios institucionales: a) Protección de datos sensibles, b) Cumplimiento normativo, c) Reputación y confianza, d) Prevención de incidentes de seguridad de la información, e) Preparación de la comunidad institucional en la sociedad digital, entre otras.

- Paso 3: se le indica el objetivo del modelo

  Centrar todos los esfuerzos y la atención en desarrollo del numeral 6.3 del Anexo A de la norma ISO 27001:2022, titulado "Concientización educación y capacitación sobre seguridad de la información" y su interrelación con las normas ISO 9001:2015 e ISO 21001:2018.

- Paso 4: se le indica una descripción general del Modelo de Cadena de Valor (MCV), por ejemplo, en este caso utilizaremos un MCV que puede ser aplicado a TEINCO como marco de referencia como se puede evidenciar en la Figura 14.

Figura 18. Procesos del MCV, (sugerido para entidades como TEINCO), creada a partir de la información suministrada por la IA

Fuente: Elaboración propia adaptado de ChatGPT.

Entradas (E)

E1: Requisitos y expectativas de la sociedad.

E2: Mejoramiento curricular de la formación profesional en todos sus ciclos propedéuticos.

E3: Alternativas de articulación con a) la media, b) industria y empresas productivas, c) Ejes de investigación y cultura, dEjes de conciencia crítica.

Procesos Estratégicos (PE):

PE1: Direccionamiento Institucional.

PE2: Desarrollo de la comunidad académica e institucional.

PE3: Relaciones Institucionales e internacionales.

PE4: Comunicación y relaciones públicas.

Procesos Misionales (PM):

PM1: Investigación técnica, tecnológica y profesional aplicada.

PM2: Ejes de formación académica y curricular (presencial y sincrónica).

PM3: Fidelización, extensión y actualización profesional (estudiantes, egresados, docentes, administrativos).

Procesos de apoyo (PA):

PA1: Bienestar y sociedad universitaria.

PA2: Gestión del talento humano.

PA3: Gestión de recursos de investigación, servicios bibliotecarios.

PA4: Gestión de laboratorios y semilleros.

PA5: Gestión de sistemas de información y transformación digital tecnológica.

PA6: Gestión administrativa y financiera.

PA7: Gestión jurídica.

PA8: Gestión de seguridad social y ambiente de trabajo.

Procesos de Evaluación (PV):

PV1: Evaluación, medición, control y mantenimiento.

Salidas (S):

S1: Sociedad; cumplimiento a sus necesidades y expectativas.

S2: a) Profesionales en formación, b) Profesionales egresados.

S3: a) Articulaciones; programas de interrelación con la sociedad y otras instituciones de educación media y superior, b) Asesorías y consultorías técnicas, científicas, artísticas, culturales y sociales.

A continuación, en la Figura 19, te daré una descripción general de los Sistemas de información (SI) requeridos para el cumplimiento de los objetivos del MCV:

Figura 19. Procesos del MCV, (sugerido para entidades como TEINCO) creada a partir de la información suministrada por la IA

Fuente: Elaboración propia adaptado de ChatGPT.

SI1: Banco de proyectos, presupuestos y estadística.

SI2: Registro y control de donaciones, becas, subsidios y benefactores.

SI3: Registro y gestión de programas SNIES, acreditación, pares académicos.

SI4: Participación de la comunidad académica e institucional (PQR, Votaciones, consultas).

SI5: Gestor y sensor de indicadores corporativos (balanced scorecard).

SI6: Control y gestión de acuerdos institucionales y contractuales.

SI7: Control y gestión de relaciones internacionales y de investigación.

SI8: Comunicaciones y relaciones con la comunidad (redes sociales, medios de comunicación, radio digital).

SI9: Gestión de investigaciones.

SIa: Registro y control académico (Admisiones, notas, pensum, Pruebas TyT y Saber Pro).

SIb: Control y gestión de egresados (Actualizaciones, bolsa de empleo, convocatorias).

SIc: Gestión de innovación, propiedad intelectual, registro de patentes.

SId: Gestión de programas de bienestar universitario.

SIe: Gestión y control de recurso humano (Hojas de vida, escalafón, nóminas).

SIf: Gestión de investigaciones y control de recursos de bibliotecas.

SIg: Registro, control y seguimiento de semilleros y proyectos de investigación.

SIh: Control de licenciamiento de software, mantenimientos a la red, actualizaciones a sistemas de información, plataformas y suite de educación (Classroom, Meet, OneDrive).

SIi: Registro contable y producción de resultados financieros, control de pagos fiscales y parafiscales, pagos y gestión de cobros.

SIj: Gestión y control jurídico (litigios, registros de patentes y marca, atención de recursos (apelación, reposición, tutelas, demandas).

SIk: Gestión de seguridad y salud en el trabajo, seguridad industrial.

SIl: Gestión de auditorías, medición de indicadores, producción estadística de progreso.

A continuación, se establece la relación de MCV con SI. El indicativo de relación se hará con el siguiente carácter: “=”.

PE1 = SI1, SI2, SI3, SI4.

PE2 = SI5.

PE3 = SI6, SI7.

PE4 = SI8.

PM1 = SI9.

PM2 = Sia,

PM3 = SIb, SIc.

PA1 = SId.

PA2 = SIe.

PA3 = SIf.

PA4 = SIg.

PA5 = SIh.

PA6 = SIi.

PA7 = SIj.

PA8 = SIk.

PV1 = SIj, SIk, SIl.

- Paso 5: en este paso procedió a realizarle solicitudes puntuales a la I.A.

Las siguientes preguntas están diseñadas para orientar y estructurar el proceso de implementación del Modelo de Cadena de Valor (MCV) en TEINCO, específicamente en lo que respecta a la integración de los Sistemas de Información (SI) necesarios para alcanzar los objetivos del modelo. Estas solicitudes abordan aspectos clave, como la relación entre los procesos del MCV y los SI requeridos, la identificación de requisitos de concientización según la norma ISO27001:2022, así como la elaboración de planes de concientización y proyectos de implementación.

Cada solicitud realizada a la I.A. proporcionó una guía detallada para garantizar la efectividad y la coherencia en el desarrollo de las estrategias de seguridad de la información en TEINCO, asegurando así el cumplimiento de los estándares y requisitos establecidos, como podemos evidenciar a continuación:

a. Plan de necesidades de concientización: temas, campañas y relación del numeral 6.3 del anexo A de la ISO/IEC 27001:2022 con MVC orientada al estudio de caso TEINCO y segmentado a las partes interesadas como podemos visualizar en la Tabla 7.

Tabla 7. Plan de necesidades de concientización, (sugerido para entidades como TEINCO) creada a partir de la información suministrada por la IA

TEMAS CONCIENTIZACIÓN	CAMPAÑAS	MODELOS INTERACTIVOS	DOCUMENTACIÓN	ESTUDIANTES	PROFESORES	ADMINISTRATIVOS	DIRECTIVOS	PROCESOS MCV ASOCIADOS
Importancia del Cumplimiento Normativo	"Cumplimiento en la Práctica"	Simulaciones de Escenarios de Cumplimiento	Políticas de Cumplimiento. Procedimientos	Conciencia sobre políticas de seguridad. Responsabilidad	Revisión y Comprensión de la Política de Seguridad de la Información	Procedimientos para cumplir con los requisitos normativos	Liderazgo en la implementación y supervisión del cumplimiento normativo	PE1, PM2, PM3, PA2
Revisión y Comprensión de la Política de Seguridad de la Información	"Conoce tu Política de Seguridad"	Videos interactivos sobre la Política de Seguridad	Política de Seguridad de la Información, manuales	Comprensión de la política de seguridad, responsabilidad	Enseñanza de la política de seguridad y su relevancia en el aula	Aplicación de la política de seguridad en las operaciones diarias	Implementación y supervisión de la política de seguridad	PE1, PM2, PM3, PA2
Identificación y mitigación de riesgos	"Gestión de Riesgos en Acción"	Juegos de Roles para Identificar Riesgos	Análisis de riesgos, planes de mitigación	Identificación de riesgos en entornos educativos	Gestión de riesgos en proyectos de investigación y enseñanza	Evaluación de riesgos en la administración de datos	Estrategias de mitigación de riesgos a nivel institucional	PE1, PM1, PM3, PV1
Importancia de la seguridad de la información	"Seguridad es Responsabilidad de Todos"	Juegos de preguntas y respuestas sobre seguridad	Folletos informativos, carteles	Conciencia sobre la responsabilidad individual en la seguridad	Integración de la seguridad de la información en el currículo	Cumplimiento de las políticas de seguridad en todas las actividades	Liderazgo en la promoción de una cultura de seguridad	PE1, PM2, PM3, PA1
Liderazgo en Seguridad de la Información	"Liderando con Seguridad"	Simulaciones de Escenarios de Liderazgo en Seguridad	Guías de liderazgo, casos de estudio	Desarrollo de habilidades de liderazgo en seguridad	Liderazgo en la enseñanza y promoción de la seguridad	Liderazgo en la implementación y gestión de la seguridad de la información	Liderazgo estratégico en la seguridad de la información	PE1, PM2, PM3, PA1, PA8
Descripción de roles y responsabilidades	"Claves para el éxito en la organización"	Herramientas Interactivas de Identificación de Roles	Descripciones de puestos, organigramas	Conocimiento de roles y responsabilidades en el uso de la información	Definición de roles y responsabilidades en la gestión	Asignación clara de roles y responsabilidades en la administración	Claridad en los roles y responsabilidades de liderazgo	PA2
Formación en Seguridad de la Información	"Fortaleciendo tus Conocimientos"	Plataformas de Capacitación Interactivas	Cursos en línea, webinars, materiales didácticos	Formación básica en seguridad de la información	Desarrollo profesional en seguridad de la información	Capacitación en políticas y procedimientos de seguridad	Formación ejecutiva en liderazgo y gestión de seguridad	PE1, PM2, PM3, PA1, PA2

Fuente: Elaboración propia adaptado de ChatGPT.

b. Programa de concientización: como se puede observar en la Tabla 8, allí se plantea un programa de concientización que se puede implementar en la aplicación futura de la metodología InfoSecurity en el caso de estudio TEINCO.

Tabla 8. Programa de concientización, (sugerido para entidades como TEINCO) creada a partir de la información suministrada por la IA

TEMAS CONCIENTIZACIÓN	CAMPAÑAS	MODELOS INTERACTIVOS	DOCUMENTACIÓN	MÓDULOS INTERACTIVOS POSIBLES	PERIODICIDAD	INTENSIDAD HORARIA	REGISTRO DE DATOS	MÉTODO DE EVALUACIÓN
Importancia del Cumplimiento Normativo	"Cumplimiento en la Práctica"	Simulaciones de Escenarios de Cumplimiento	Políticas de Cumplimiento. Procedimientos	Reforzamiento de la autenticación de doble factor. Importancia de las copias de seguridad y backup. Actualizaciones y parches de seguridad.	Anual	2 horas	Si	Prueba de Conocimientos
Revisión y Comprensión de la Política de Seguridad de la Información	"Conoce tu Política de Seguridad"	Videos interactivos sobre la Política de Seguridad	Política de Seguridad de la Información, manuales	Importancia de la gestión de contraseñas, cómo identificar correos electrónicos de phishing. Actualización de software.	Anual	1.5 horas	Si	Evaluación del Comportamiento
Identificación y mitigación de riesgos	"Gestión de Riesgos en Acción"	Juegos de Roles para Identificar Riesgos	Análisis de riesgos, planes de mitigación	Educación sobre ataques de malware y ransomware, protección de datos sensibles, identificación de vulnerabilidades.	Semestral	2 horas	Si	Examen Práctico
Importancia de la seguridad de la información	"Seguridad es Responsabilidad de Todos"	Juegos de preguntas y respuestas sobre seguridad	Folletos informativos, carteles	Importancia de las actualizaciones de software, uso seguro de redes Wi-Fi públicas, protección de datos personales.	Semestral	1 hora	Si	Encuesta de Satisfacción
Liderazgo en Seguridad de la Información	"Liderando con Seguridad"	Simulaciones de Escenarios de Liderazgo en Seguridad	Guías de liderazgo, casos de estudio	Importancia de la gestión de incidentes, estrategias de concientización, cumplimiento de las normas de privacidad de datos.	Anual	2 hora	Si	Evaluación de actitudinal y comportamental

Fuente: Elaboración propia adaptado de ChatGPT.

c. Modelo de gobierno de seguridad de la información: los roles, responsabilidades claras, la actuación del Comité de Dirección de Seguridad Institucional y un resumen de cómo establecer e implementar el proceso formal de concientización en riesgos y seguridad de la información alineado al numeral 6.3 del anexo A de la ISO 27001:2022 como podemos observar en la Tabla 9.

Tabla 9. Matriz implementación modelo de gobierno alineado al requisito 6.3 de la ISO 27001

ASPECTO	DESCRIPCIÓN
Roles y Responsabilidades	Comité de Dirección de Seguridad Institucional (CDSI): Responsable de definir la estrategia de seguridad de la información y supervisar su implementación. Incluye representantes de la alta dirección, el equipo de seguridad de la información y otros departamentos relevantes. Equipo de Seguridad de la Información (ESI): Encargado de implementar y mantener las medidas de seguridad de la información, incluida la Concientización.
Flujo a Seguir	1. El CDSI establece la política de seguridad de la información y define los objetivos de Concientización en riesgos y seguridad de la información. 2. El ESI desarrolla un plan de concientización basado en los objetivos definidos y los resultados de la matriz de la Solicitud-10. 3. Se asignan responsabilidades claras a los diferentes niveles de la institución para la implementación del plan. 4. Se realizarán actividades de concientización y se monitoreará su efectividad. 5. El ESI reporta al CDSI sobre el progreso y los resultados de las actividades de Concientización.
Proceso formal de concientización	• Identificar las necesidades de concientización: Analizar los riesgos y las necesidades específicas de concientización de la institución. • Desarrollar un plan de concientización: Basado en los resultados de la matriz de la Solicitud-10, diseñar un plan detallado con objetivos, actividades y recursos necesarios. • Implementar actividades de concientización: Ejecutar las actividades planificadas, como campañas, capacitaciones y simulacros. • Evaluar la efectividad: Medir el impacto de las actividades de concientización y realizar ajustes según sea necesario. • Mantener y mejorar: Continuar con actividades periódicas de concientización y actualizar el plan según los cambios en los riesgos y las necesidades de la institución.

Fuente: ChatGPT

Esta matriz proporciona una visión clara de los aspectos relevantes y el flujo a seguir para establecer e implementar un modelo de gobierno de seguridad de la información, centrándose en el numeral 6.3 del anexo A de ISO 27001: 2022.

Al concluir esta fase, ya se podrá avanzar con confianza hacia las próximas etapas del proyecto, con la certeza de que se cuenta con una base sólida y una estrategia innovadora para proteger los activos digitales de TEINCO en un entorno tecnológico en constante evolución.

4. CONCLUSIONES

La metodología InfoSecurity para la estructuración de una herramienta digital de cultura y conciencia en seguridad de la información, en el marco de la norma ISO/IEC 27001: 2022, representa un enfoque integral y sistemático para abordar los crecientes desafíos en ciberseguridad y la protección de la información.

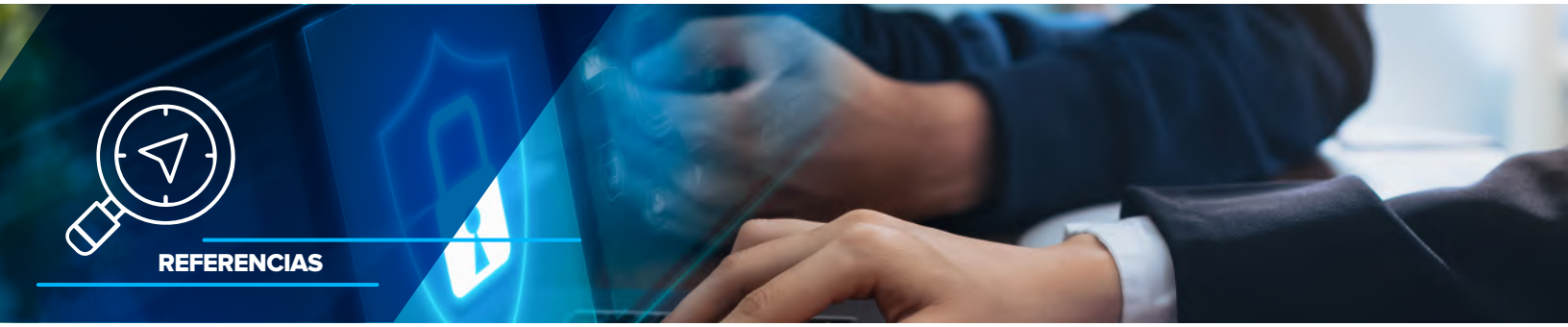
En un entorno donde los ciberataques están en aumento y la digitalización de las actividades cotidianas es cada vez más omnipresente, la necesidad de concienciar a las personas sobre la importancia de la seguridad de la información se vuelve imperativa. La falta de conocimiento en este ámbito expone a individuos y organizaciones a diversas amenazas cibernéticas, subrayando la importancia de promover una cultura de seguridad sólida y arraigada.

La investigación aplicada con un enfoque cualitativo ha permitido definir una metodología que puede ser implementada, tanto por los miembros de TEINCO como por otras organizaciones interesadas. Este enfoque inclusivo y colaborativo garantiza que la metodología sea relevante y aplicable en diversos contextos organizativos.

La metodología propuesta se basa en los principios y directrices establecidos por la norma ISO/IEC 27001: 2022, en particular en el numeral 6.3 del Anexo A, que aborda la sensibilización, educación y formación en materia de seguridad de la información. Al enfocarse en este control, la metodología busca establecer una base sólida para la implementación efectiva de los demás controles de la norma, lo que eventualmente podría conducir a la certificación y proporcionar un valor agregado significativo para TEINCO. Además, se puede considerar la integración de la ISO/IEC 27002:2022, que ofrece una guía holística y permite un mayor alcance. Adicionalmente, la metodología podría incorporar el Top 10 de OWASP para ampliar su enfoque.

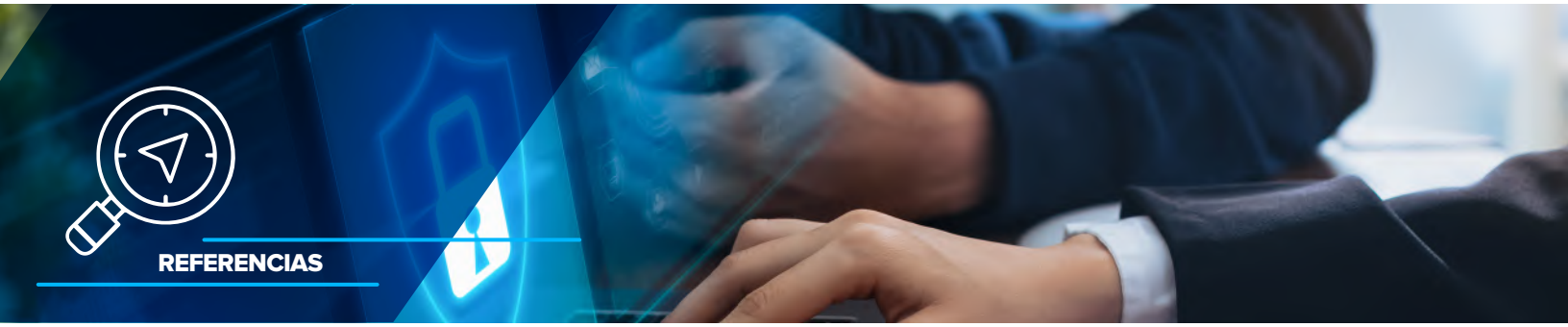
La implementación de la herramienta digital propuesta proporciona una plataforma para la difusión de información clave relacionada con la seguridad de la información y la ciberseguridad, al ofrecer recursos educativos, prácticos y de fácil acceso. La herramienta contribuye a fortalecer la cultura y conciencia en seguridad de la información, alineándose con el numeral 6.3 del Anexo A de la norma ISO/IEC 27001: 2022.

En conclusión, la metodología InfoSecurity ofrece un marco sólido y coherente para abordar los desafíos actuales en seguridad de la información al promover una cultura de seguridad proactiva y proporcionar herramientas prácticas para su implementación, esta metodología representa un paso significativo hacia la protección y resiliencia de la información en TEINCO y más allá.



REFERENCIAS

- ***Agencia Nacional de Seguridad Cibernética (ANSC). (2020). Política Nacional de Ciberseguridad.***
- ***Cardona, E., & Rivera, W. (2018). Seguridad de la información en Colombia: un enfoque desde las normas ISO 27001. Editorial Universidad del Rosario***
- ***Castrillón, C., & Giraldo, M. (2021). Estrategias pedagógicas para la formación en competencias digitales en estudiantes de ingeniería. Revista Educación en Ingeniería, 16(31), 65-78.***
- ***Duque, J., & Patiño, J. (2018). Ciberseguridad: Retos y desafíos en Colombia. Editorial Universidad de La Salle.***
- ***Escobar, J. (2020). La importancia de la concientización en seguridad de la información en el contexto colombiano.12(25),31-45.***



REFERENCIAS

- *Gaviria, A., & Horta, D. (2021). Implementación de Google Sites en la Universidad de la Costa CUC: una experiencia exitosa en la enseñanza virtual durante la pandemia. Revista Iberoamericana de Educación a Distancia, 24(1), 209-226.*
- *Giraldo, A., & Hernández, L. (2020). Aproximación cualitativa a la inclusión de la tecnología en la enseñanza universitaria en Colombia. Entramado, 16(2), 134-151.*
- *Gómez, A., & López, J. (2021). Experiencias de formación docente en entornos virtuales: estrategias implementadas en Colombia durante la emergencia sanitaria por COVID-19. Revista Electrónica Educare, 25(2).*
- *Gutiérrez, M., & Galindo, D. (2020). Estrategias de enseñanza-aprendizaje en entornos virtuales: una mirada desde la educación superior en Colombia. Revista Educación y Humanismo, 22(39), 234-252.*
- *Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta (Vol. 1).*
- *Horta, D., & Gaviria, A. (2020). Uso de Google Sites en la educación superior: una experiencia de la Universidad de la Costa CUC. Revista de Tecnología Educativa, 31(2), 57-70.*
- *ISO/IEC 27001:2022. Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.*
- *Lalinde, J. (2021). Maestría en Ciencia de Datos y Analítica. Universidad EAFIT.*
- *Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2020). Estrategia Nacional de Ciberseguridad 2020-2022.1.*
- *Rincón, M., & López, D. (2019). Implementación de políticas de concientización en seguridad de la información en empresas colombianas. Revista de Investigación, Desarrollo e Innovación, 10(1), 21-3*
- *Ríos, C., & Gómez, P. (2020). Experiencias de aprendizaje colaborativo mediado por Google Sites en la educación superior: un estudio de caso en la Universidad Nacional de Colombia. Revista Investigación y Desarrollo Educativo, 10(2), 187-202.*
- *Rivera, W., & Cardona, E. (2019). Análisis de la ciberseguridad en Colombia en el contexto de la infraestructura crítica de información.*
- *Rodríguez, M. (2018). "Estrategias para la concientización en seguridad de la información en pequeñas y medianas empresas en Colombia" [Archivo PDF].*
- *Sánchez, D., & Torres, E. (2021). Investigación cualitativa en la enseñanza de la tecnología: perspectivas desde Colombia. Revista de Investigación en Educación, 19(2), 241-260.*
- *Schwartz, P. M. (2020). Ciberseguridad para principiantes: conceptos básicos y prácticas esenciales para protegerse en la era digital. Ediciones Granica.*
- *Universidad de Antioquia (2019). "Concientización en seguridad de la información en organizaciones colombianas: Una mirada desde la perspectiva de los empleados" [Archivo PDF]. Repositorio Institucional Universidad de Antioquia*
- *Universidad de La Salle (2019). Impacto de las campañas de concientización en seguridad de la información: Un estudio de caso en empresas colombianas.*
- *USTA (2022). Concientización en seguridad de la información en empresas colombianas: Un enfoque desde la perspectiva de los usuarios finales. Proyecto de Investigación Universidad Santo Tomás,54(2),12-54.*