Herramienta web para capacitación y sensibilización de seguridad de la información en el ámbito administrativo de la Universidad CESMAG con alineación a la norma ISO/IEC 27001

David Esteban Pantoja Estrada, ✉ depantoja.5964@unicesmag.edu.co

Universidad CESMAG
Facultad de Ingeniería
Ingeniería de sistemas
Pasto – Nariño
2025

Herramienta web para capacitación y sensibilización de seguridad de la información en el ámbito administrativo de la Universidad CESMAG con alineación a la norma ISO/IEC 27001

David Esteban Pantoja Estrada, ✉ depantoja.5964@unicesmag.edu.co

Trabajo de grado para optar al título de ingeniero de sistemas

Asesor:

Mg: Luis Arnoby Escobar Hernández

Co-asesor

Mg: Jairo Andrés Casanova Caicedo

Universidad CESMAG
Facultad de Ingeniería
Ingeniería de sistemas
Pasto – Nariño
2025

Nota de Aceptación

_____

_____

_____

_____

_____

Página de exclusión de responsabilidad intelectual

"El pensamiento que se expresa en esta obra es exclusiva responsabilidad de sus autores y no compromete la ideología de la Institución Universitaria CESMAG"

DEDICATORIA

Quiero expresar principalmente esta dedicatoria a Dios, ya que él me ha permitido durante estos 5 años poder cursar mi carrera donde junto a mi madre Ana Lucia Estrada han guiado mi camino tanto para ser un profesional como para ser una gran persona.

Dedico enaltecida mente este trabajo de grado a mi madre que ha sido mi apoyo y soporte de mi vida desde pequeño, donde a pesar de las dificultades que se han suscitado nunca ha soltado mi mano y con su mayor esfuerzo será quien disfrute de los frutos de mi ser profesional.

A mis abuelos Alonso Estrada y Carmen Obando que desde el cielo me han apoyado constantemente a no rendirme y seguir adelante, alentándome así cada vez mas a ser un profesional.

A mi abuelita Mariana Pantoja que durante 4 años también me motivo en este sueño que a día de hoy se siente más cerca que nunca.

A mi familia que siempre estuvo apoyándome y viendo como me formaba como profesional y ser humano en la universidad.

Y por último agradezco a todos los docentes que hicieron parte de este proceso formativo desde primer semestre hasta el último, donde aportaron su conocimiento, dedicación y saber en mí. Especialmente agradezco a mi querido asesor Luis Arnoby Escobar Hernández y a mi co-asesor Jairo Andrés Casanova Caicedo que hicieron posible con ideas y apoyo para este proyecto de grado.

David Esteban Pantoja Estrada

AGRADECIMIENTOS

Principalmente quiero expresar mi mas profundo agradecimiento al primer amor de mi vida que es mi madre, por el gran esfuerzo que hizo incesantemente para que haya podido cursar semestre tras semestre, donde junto siempre tomando su mano he podido llegar hasta el día donde estoy hoy, tanto como persona y como ya casi un profesional.

Agradezco primordial y totalmente su apoyo en todos los sentidos, por que día tras día me ha demostrado ser mi padre y madre. Pero más aun mi ejemplo a seguir, por su responsabilidad, compromiso, dedicación, honestidad y, sobre todo el amor que tiene a su profesión.

Agradezco a Dios, al universo y la vida por haberme dado la mejor madre de este mundo por todo su amor y cariño, la vida que tengo hoy para lograr y culminar este proceso formativo.

Extiendo mi agradecimiento a mis familiares que tengo hoy en día y que me han apoyado de manera incondicional, agradezco a mis familiares que no se encuentran en este plano por que desde el reino de los cielos siempre están velando por mí. Por último, a todas las personas que han pasado por mi vida para lograr este momento.

Como ultimo agradecimiento es dirigido a la facultad de Ingeniería de Sistemas de la universidad CESMAG, por aportar su conocimiento y herramientas con sus excelentes docentes para formarme como profesional y persona en este mundo.

A ti madre, gracias de corazón.

David Esteban Pantoja Estrada

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

ANEXOS

RESUMEN ANALÍTICO DE ESTUDIO

Facultad	Ingeniería
Programa	Ingeniería de Sistemas
Fecha de elaboración	2025
Autores de la investigación	David Esteban Pantoja Estrada
Asesor de la investigación	Mg. Luis Arnoby Escobar Hernández
Sub-Asesor de la investigación	Mg. Jairo Andrés Casanova Caicedo
Título de la investigación	Herramienta web para capacitación y sensibilización de seguridad de la información en el ámbito administrativo de la Universidad CESMAG con alineación a la norma ISO 27001
LÍNEA DE INVESTIGACIÓN	Seguridad de la información
SUB LÍNEA DE INVESTIGACIÓN	Seguridad informática

DESCRIPCIÓN

El presente proyecto busca capacitar y sensibilizar al personal administrativo de la Universidad CESMAG en el manejo seguro de la información, conforme a los lineamientos de la norma ISO 27001. La iniciativa surge ante la creciente amenaza de ataques cibernéticos y la falta de preparación del personal para enfrentar estos riesgos, lo que compromete la confidencialidad, integridad y disponibilidad de los datos institucionales.

La capacitación se fundamente en una herramienta web interactiva, diseñada para fortalecer el conocimiento en seguridad informática; abordará temas como el robo de datos, ransomware y otras amenazas digitales. Además, permitirá planificar cursos, evaluar avances y establecer una cultura de seguridad de la información dentro de la institución.

Como objetivo principal, se plantea desarrollar una plataforma de formación para el personal administrativo, permitiendo optimizar la gestión de riesgos y cumplir con estándares internacionales. Entre los objetivos específicos se incluyen caracterizar el nivel actual de conocimiento, construir la herramienta web, y evaluar el progreso en la adopción de buenas prácticas.

CONTENIDO

El proyecto final de grado se realizó de la siguiente manera:

Capítulo 1:

Se presenta la problemática central, identificando acciones para prevenir amenazas y fallas relacionadas con el personal universitario. Se establece un objetivo general, tres específicos y la justificación del proyecto, destacando la necesidad de capacitar y sensibilizar continuamente al personal, dado que el factor humano es el eslabón más débil en la cadena de seguridad. El proyecto tiene una duración de 12 meses, desde 2024 hasta 2025.

Capítulo 2:

Se exponen antecedentes internacionales, nacionales y locales, junto con estudios y ejemplos similares que evidencian la importancia y pertinencia del proyecto.

Capítulo 3:

Se describe la metodología con un enfoque positivista, detallando la población, muestra y técnicas de recolección de datos que sustentan la investigación y el desarrollo del proyecto.

Capítulo 4:

Se presentan los resultados del proyecto, mostrando cómo se capacitó al personal y evidenciando avances en conocimientos y sensibilización.

Capítulo 5:

Se analizan y discuten los resultados obtenidos, incluyendo los métodos de recolección de datos antes y después de la implementación del proyecto.

CONCLUSIONES

El proyecto fortaleció la seguridad institucional al capacitar al personal y reducir riesgos asociados al factor humano.

RECOMENDACIONES

Continuar con las capacitaciones periódicas y ajustar las estrategias según las necesidades del personal.

PALABRAS CLAVE

Seguridad de la información, seguridad y tratamiento de los datos, capacitación, ISO 27001, sensibilización, personal administrativo, Universidad CESMAG, ley normativa 1581

INTRODUCCIÓN

El presente trabajo de investigación tiene como objetivo capacitar y sensibilizar al personal administrativo de la Universidad CESMAG en el tratamiento adecuado de los datos, conforme a las normativas vigentes aplicables a cualquier organización. Este personal cumple un papel clave, ya que gestiona información de diversa naturaleza, lo que lo expone a riesgos y amenazas que pueden comprometer la seguridad institucional.

En la era digital, la protección de datos es una necesidad urgente. La información circula por múltiples medios, cada uno con vulnerabilidades específicas. Por ello, se busca que el personal sea plenamente consciente de las amenazas existentes y de las consecuencias de una gestión inadecuada. La formación abordará buenas prácticas y medidas preventivas que permitan evitar brechas de seguridad.

Más allá de la capacitación técnica, el proyecto pretende generar conciencia sobre la importancia de proteger los datos personales y confidenciales de estudiantes y personal universitario. Se abordarán temas como el robo de información, el ransomware y otras amenazas cibernéticas que pueden afectar la integridad y reputación institucional.

El enfoque del proyecto no será únicamente teórico; incluirá ejercicios prácticos y simulaciones de escenarios reales, permitiendo al personal aplicar los conocimientos adquiridos. Para ello, se desarrollará una herramienta virtual, orientada a fortalecer el conocimiento sobre confidencialidad, integridad y disponibilidad de los datos. Esta plataforma facilitará la planificación de cursos para el personal administrativo y docente, y permitirá evaluar el progreso en la apropiación de los conceptos de seguridad de la información. La iniciativa se ajustará a los lineamientos de la norma ISO 27001, proporcionando un marco sólido de gestión de seguridad. Se combinarán sesiones teóricas y prácticas con herramientas interactivas que favorezcan el aprendizaje y aplicación de los conocimientos. Además, se implementarán mecanismos de control y seguimiento para garantizar la adopción efectiva de políticas y procedimientos, contribuyendo a una mejora continua en la protección de los datos sensibles de la universidad.

I. PROBLEMA DE INVESTIGACIÓN

A. Objeto o Tema de Investigación.

Fortalecimiento de la gestión y protección de la información en el personal administrativo de la Universidad CESMAG, mediante procesos de optimización, capacitación y sensibilización, en cumplimiento con los estándares de la norma ISO/IEC 27001 y la ley normativa 1581 del 2012 enfocada en el tratamiento de datos.

B. Línea de investigación.

Seguridad Información

La seguridad de la información es un campo de la ingeniería de sistemas que se enfoca en la protección de datos, abarcando tanto conceptos teóricos como prácticas y riesgos fundamentales para garantizar la seguridad de la información en cualquier ámbito, ya sea empresarial, gubernamental, de salud o personal. Esta área contempla estándares, protocolos, métodos, reglas, herramientas y leyes, con el objetivo de minimizar, controlar y mitigar posibles riesgos dentro de las estructuras de información establecidas[1]. Por lo cual, el proyecto se enfoca en la capacitación y sensibilización del personal administrativo para mejorar las prácticas de seguridad de la información y datos personales en la Universidad CESMAG.

C. Sublínea de investigación.

Seguridad Informática

Enmarca métodos y controles tecnológicos que se pueden implementar para mitigar y prevenir los riesgos latentes que se encuentran en el internet, también conocidos como amenazas cibernéticas donde pueden comprometer la privacidad, integridad o confidencialidad y que se integran en la norma ISO/IEC 27001.

D. Planteamiento del problema.

La seguridad informática se ha convertido en un pilar fundamental en el entorno digital actual, especialmente para instituciones educativas como la Universidad CESMAG, que gestionan

información sensible y confidencial. La creciente sofisticación de las amenazas cibernéticas, junto con el limitado conocimiento del personal administrativo sobre prácticas adecuadas de protección de datos, incrementa significativamente los riesgos de seguridad. Esta carencia de capacitación expone a la universidad a incidentes como el robo de información, ataques de ransomware y otras vulnerabilidades, comprometiendo la confidencialidad, integridad y disponibilidad de los datos, así como afectando negativamente la reputación institucional[2].

Al manejar grandes volúmenes de datos personales y académicos, la institución se convierte en un objetivo atractivo para los atacantes. La falta de una cultura sólida de seguridad y de capacitación continua en buenas prácticas de protección de datos genera un entorno vulnerable, donde los riesgos pueden pasar desapercibidos o no mitigarse adecuadamente, elevando la probabilidad de brechas y pérdidas significativas[3].

La Universidad CESMAG carece de herramientas específicas para capacitar adecuadamente en seguridad de la información. Esta limitación se refleja en la preparación insuficiente del personal administrativo para identificar y gestionar riesgos cibernéticos [4], lo que incrementa la vulnerabilidad institucional ante posibles amenazas. Como consecuencia, se pone en riesgo tanto la protección de los datos como la confianza y seguridad de toda la comunidad universitaria.[4]

E. Formulación del problema.

¿Cómo optimizar procesos de capacitación y sensibilización en seguridad de la información para el personal administrativo de la Universidad CESMAG, garantizando conocimientos y buenas prácticas basadas en la norma ISO/IEC 27001?[5].

F. Objetivos.

1 General

Desarrollar una herramienta web de capacitación de Seguridad de la información para el recurso humano de la parte administrativa de la Universidad CESMAG de acuerdo a los lineamientos y practicas concertadas en norma ISO/IEC 27001.

2 Específicos

- Caracterizar el conocimiento en seguridad de la información al personal administrativo de la Universidad CESMAG.
- Construir una herramienta web interactiva que permita la capacitación en: confidencialidad, integridad y disponibilidad de la información a partir de la norma ISO 27001.
- Evaluar el progreso en el entendimiento y aplicación de los conocimientos sobre seguridad de la información a lo largo del tiempo.

G. Justificación.

La Universidad CESMAG enfrenta desafíos significativos en materia de seguridad informática, debido al creciente número de incidentes de suplantación de identidad, robo de información y otros actos maliciosos en su entorno digital. El personal administrativo, al ser responsable de gestionar información confidencial, se encuentra especialmente expuesto a estas amenazas, principalmente por la falta de capacitación y conciencia en prácticas adecuadas de seguridad[6]. Las instituciones educativas, al manejar grandes volúmenes de datos sensibles, se han convertido en objetivos prioritarios para los ciberdelincuentes. Por ello, resulta fundamental implementar una plataforma de capacitación continua y actualizada que fomente una cultura institucional orientada a la seguridad de la información. Esta iniciativa no solo busca proteger la confidencialidad, integridad y disponibilidad de los datos, sino también garantizar el funcionamiento eficiente de la universidad. [7].

Al fortalecer las competencias del personal administrativo en el conocimiento de la gestión de riesgos cibernéticos, el proyecto contribuirá a aumentar la confianza y seguridad dentro de toda la comunidad universitaria. Además, la adopción de una herramienta digital alineada con los estándares internacionales de la norma ISO/IEC 27001 evidencia el compromiso de la Universidad CESMAG con la excelencia en la gestión de la seguridad de la información, promoviendo un entorno digital seguro y confiable[8].

Asimismo, la propuesta impulsará una cultura organizacional orientada a la seguridad informática, promoviendo la conciencia y la responsabilidad en el manejo de la información.[9]. A través de

módulos de formación en una plataforma educativa interactiva y accesible, se facilitará la comprensión de conceptos clave en ciberseguridad, permitiendo al personal aplicar eficazmente estos conocimientos en sus tareas cotidianas. De esta manera, se refuerza la capacidad institucional para enfrentar los desafíos del entorno digital actual[10].

H. Delimitación.

El proyecto se realizará en la Universidad CESMAG, ubicada en Pasto, Nariño, Colombia[15]. Durante el periodo comprendido entre mayo de 2024 y junio de 2025, la investigación se centra en el personal administrativo y docente de la Universidad CESMAG, con el objetivo de desarrollar herramientas tecnológicas para su capacitación y sensibilización en la norma ISO/IEC 27001. Este marco temporal permitirá ejecutar las etapas de diagnóstico, diseño, implementación y evaluación de dos módulos de formación en una plataforma educativa adaptada a sus necesidades, fortaleciendo así el conocimiento y la cultura institucional de seguridad de la información.

II. MARCO TEÓRICO

A. Antecedentes

1 Internacionales

Según EUD ACADEMY (Egresados Universidad Distrital) la página de certificaciones internacionales la cual busca formar profesionales con estándares de calidad y mejorando prácticas que rigen a las empresas, la seguridad de la información es fundamental debido a los riesgos que conlleva tener sistemas hoy en día, explica el por qué es importante gestionar factores de riesgo y proteger la seguridad de las empresas para no incurrir en costos por ataques. Apuesta por abordar las amenazas de una manera estratégica teniendo un paso adelante por cualquier incurrencia y así crear un esquema de procesos efectivos y eficientes para la correcta seguridad de la información. Considera aportar herramientas a todas aquellas empresas para que participen activamente en el monitoreo resguardo del activo de los datos donde las empresas puedan aplicar un modelo de seguridad estandarizado el cual genere una concientización y desarrolle el conocimiento de controlar la información[16].

Para ISACA (Information Systems Audit and Control Association) una asociación que certifica internacionalmente a auditores y profesionales que controlen lo sistemas de información las empresas apuestan a tecnología generando una armonía en las TI, pero no obstante no generan la inversión necesaria en la protección y prevención de los datos donde consideran inevitable la protección de los recursos por encima de la información que puede componer a la empresa. “Aquellas empresas grandes consideradas que tienen estándares de calidad altos es porque pueden prevenir, proteger, detectar y responder a los ataques cibernéticos lo cual puede representar una problema para las empresas pequeñas“[17].

El verdadero desafío implica acatar las recomendaciones básicas para las empresas pequeñas puesto que su seguridad es mínima y en algunas casi nula donde al haber una brecha, fuga o incidente se puede acoger a sanciones legales debido que la empresa no proporciona las medidas

mínimas para mantener sus activos de información protegidos de ciertos ataques maliciosos los cuales los hagan pasar un “mal rato”.

La FTC (Federal Trade Comission) sugiere estándares para la protección de información del cliente, garantiza que entidades cubiertas por la norma puedan certificar a la empresa para salvaguardar de manera óptima la información del cliente. Se rige a medida que la tecnología se actualice manteniendo día a día la escalabilidad de la protección de los datos donde se aplique la regla la regla y así mismo refleje los principios básicos de la seguridad de la información. Los artículos publicados sirven como guía para las empresas pequeñas que manejan volúmenes de datos aceptando y acatando la regla en general dentro de instituciones financieras donde deben desarrollar un programa que implemente y mantenga a salvo la información personal no pública[18].

Para ENISA (La Agencia de Ciberseguridad de la Unión Europea) la mejora constante de la confidencialidad de los datos aumenta la confianza de productos, servicios y procesos con las TIC dentro de las empresas, contempla los desafíos cibernéticos como una oportunidad para la sensibilización y la ampliación del conocimiento en la sociedad donde por la hiperconexion que ha sufrido el mundo se debe impulsar la resiliencia para mantener digitalmente seguras a las personas debido que los ciberdelincuentes han tomado ventaja de esta situación para corresponder a sus fines maliciosos y de esta manera ellos puedan sacar provecho según los intereses. ENISA propone estandarizar a toda empresa que se constituya con un volumen de tecnología e información debido a las conexiones físicas y sistemáticas que puedan tener [19].

2 Nacionales

Los autores, Ospina, M., y Sanabria, P. (2020) en su artículo “Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia” abordan sobre los diferentes amenazas cibernéticas donde al igual que el avance tecnológico ha progresado, tiene serios problemas en su seguridad, donde aplicaciones, transacciones, archivos entre otros han generado peligros y vulnerabilidades en la información que son llevados (por personas u organizaciones inescrupulosas) que se aprovechan de empresas/individuos y/o gobiernos de cualquier índole

(nacional, dptal, municipal) donde la situación toma gran relevancia a la frecuencia que se van desarrollando este tipo de situaciones. Considera los bancos de datos de empresas que se encuentran en la nube siendo este el principal objetivo para los ciberdelincuentes donde se encuentra la información de las rutinas del día a día de las empresas donde se contempla información de correos, contraseñas, direcciones, inventarios, cuentas de banco, archivos que sufran daños o perdida por cuenta de estas acciones y así perjudicando de manera legal y monetaria a las empresas involucradas[20].

Los autores, Jiménez, G y Enrique, D (2023) con su artículo "Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia" de la Revista Ibérica de Sistemas e Tecnologías de Informação, sostienen la seguridad integral para combatir los ciberataques y proteger la información de la ciudadanía a través de las normativas más relevantes donde destaca la importancia de la educación y la capacitación de la población en la seguridad de la información y debido a la frecuencia con la que se interactúa con dispositivos electrónicos incluyendo las empresas son sus TI puede ser vulnerable generado daños irreparables a este tipo de empresas. El articulo aprecia sobre lo prioritario que se ha convertido el tema de la ciberseguridad en Colombia donde busca implementar políticas de seguridad integral de esta manera buscando la protección no solo de los sistemas de información de las empresas sino también procesos, personas y recursos de una organización y empresa[21]

La autora, Cano, J (2022) en su artículo "Prospectiva de ciberseguridad nacional para Colombia a 2030" contempla que la ciberseguridad es un factor fundamental que agrupa y articula esfuerzos de entidades gubernamentales las cuales pueden garantizar un entorno de confianza digital para las personas que hacen uso de las tecnologías mediante actividades de la vida diaria y así mismo apalancar iniciativas en nuestro contexto para generar mayor prosperidad y bienestar en la sociedad. Propone activamente en establecer referentes básicos para la prevención, educación dando así una respuesta y visión a base de las prácticas de seguridad y riesgos que pueden ejercer mediante estos medios.

El articulo propone la iniciativa de explorar, tomar y modificar tendencias internacionales para la seguridad de la información lo cual hará posible implementar los planes de acción correspondientes

a la amenaza generada por las fugas analizando los retos que se tienen pendientes por combatir buscando así los resultados en el ejercicio del aprendizaje y practico[22].

3 Regionales

La fundación FEPROPAZ oriunda de Nariño considera que tanto aplicaciones móviles que solicitan permisos para acceso a la información personal hasta los ciberataques que se proporciona a lo largo de las horas comprometen la seguridad de la información y los datos de las personas donde la falta de privacidad y seguridad representan dificultades a la seguridad considerando ya ser una amenaza, donde entra en juego la confianza de los clientes, personal y recursos pertenecientes a las empresas pueden arruinar de manera profunda la integridad de la información, puesto que la entidad presente afrontar los desafíos en la seguridad de la información de manera directa y concisa de esta manera protegiendo la dignidad de usuarios como de la empresa.

El autor Casanova, A (2016) en su artículo “Modelo de Evaluación Cuantitativa de Riesgos en Seguridad Informática” expresa sobre la evaluación cuantitativa de los riesgos donde se puede estimar por alternativas o estrategias que permitan minimizar los riesgos que pueden encontrar los profesionales de la seguridad informática en estos días, puesto que las estrategias pueden ser por experiencias propias o de hechos conocidos o cercanos a los profesionales. Las estrategias se realizan con el fin de minimizar los riesgos existentes o potenciales acatando y respetando el orden de las estrategias o metodologías propuestas así estimando la probabilidad de ocurrencia. Propone el principio de medir y controlar los riesgos eventuales en la seguridad de la información donde todas las acciones que están propuestas y orientadas a la reducción del impacto de las mismas.[23]

Los autores, Villalba Romero, J. J., Jiménez Toledo, R. A., & Torres Burbano, Álvaro R. (2016) en su artículo “Evaluación de la seguridad de la información en la Clí-nica Hispanoamérica de Pasto, basada en la norma ISO/IEC 27001” exponen que desde el nacimiento del internet las compañías han presentado incidentes de seguridad en la información debido a la deficiente seguridad e inadecuado uso del manejo de la información presentadas por la falta de experiencia y poca actualización en las normas como la ISO/IEC 27001, generan pérdidas millonarias buscando alternativas que puedan combatir contra los incidentes. Recalcan que las empresas pequeñas se

convierten en un blanco vulnerable para personas o agencias con fines delictivos. Expresan fuertemente sobre la complicidad del personal donde en ciertas ocasiones los trabajadores ingresan a portales no permitidos y así se ve mira afectada la red [24].

B. Supuestos teóricos de investigación

1 Seguridad de la información

La seguridad de la información, en el contexto institucional de la Universidad CESMAG, se refiere a la implementación de prácticas, protocolos y políticas orientadas a proteger los datos académicos, administrativos y personales frente a accesos no autorizados, alteraciones, pérdida o interrupciones. Este enfoque busca garantizar los principios fundamentales de confidencialidad, integridad y disponibilidad de la información[25].

En concordancia con la norma ISO/IEC 27001, la seguridad de la información se convierte en un componente estratégico, cuya comprensión y correcta aplicación por parte del personal administrativo es esencial. La herramienta de capacitación propuesta en este proyecto tiene como objetivo fortalecer ese conocimiento, promoviendo una cultura organizacional que priorice la gestión adecuada de los riesgos asociados al manejo de la información institucional[26].

a) La triada de la seguridad de la información

Existen 3 conceptos claves dentro de la seguridad de la información los cuales permiten de manera activa y efectiva que la seguridad de la información pueda mantener una escalabilidad evolutiva permanente de acuerdo a los nuevos riesgos que se puedan ir generando al paso del tiempo. La CIA o CID (Confidencialidad, Integridad, Disponibilidad) como se la conoce hace referencia a la seguridad de los datos[27].

b) Confidencialidad:

Es uno de los pilares fundamentales de la seguridad de la información. Se refiere a la protección de datos e información para que solo las personas autorizadas puedan acceder a ellos y

utilizarlos. La confidencialidad asegura que la información sensible no sea revelada a individuos, entidades o procesos no autorizados[28]. Veamos algunos aspectos importantes de la confidencialidad en el contexto de la seguridad de la información:

Importancia de la confidencialidad

- La confidencialidad de la información es un aspecto crucial debido a razones legales, económicas y sociales. La protección de los datos personales y corporativos es fundamental no solo para cumplir con la normativa local, sino también para fomentar la confianza en las interacciones digitales y proteger los derechos fundamentales de los individuos La violación de la confidencialidad puede llevar a consecuencias legales, pérdidas financieras y daño a la reputación de las organizaciones[29].

Métodos de Protección

- Para garantizar la confidencialidad, se implementan diversas técnicas y herramientas las cuales hacen parte de los protocolos estándares y generales que se deben utilizar en cualquier medio informático:

- Cifrado: Transforma la información en un formato ilegible sin una clave de cifrado, utilizándose tanto para datos en reposo como en tránsito[30].
- Control de acceso: Limita el acceso a la información a usuarios autorizados mediante el uso de listas de control de acceso (ACL), autenticación y políticas de seguridad[31].
- Autenticación y autorización: Procesos que verifican la identidad de los usuarios y garantizan que solo los que tienen permisos adecuados puedan acceder a los recursos[32].
- Seguridad en redes: Utiliza tecnologías como VPN (Redes Privadas Virtuales) y SSL/TLS (Capas de Sockets Seguros/Seguridad de la Capa de Transporte) para proteger los datos mientras se transmiten[33].

Legislación y Normativas

- Diversas legislaciones alrededor del mundo exigen a las organizaciones implementar medidas de seguridad para proteger la confidencialidad de la información personal y corporativa. Esto incluye cumplir con estándares específicos y realizar auditorías regulares

para asegurar que las medidas de seguridad son efectivas. Esto se realiza con el fin de cumplir con las normas y todo lo que se establece a políticas de confidencialidad de cada país.

Prácticas de Aplicación

- En el ámbito empresarial, la confidencialidad se aplica a través de políticas de seguridad que clasifican la información según su sensibilidad y definen quién puede acceder a qué datos.

c) Integridad:

Se refiere a la precisión, completitud y consistencia de los datos a lo largo de su ciclo de vida. Busca de manera concreta que la información no sea alterada de manera no autorizada durante su almacenamiento, transmisión o procesamiento. Es crucial debido que se debe mantener la confianza en los sistemas de información y para garantizar que las decisiones basadas en datos sean correctas y fiables[34]. La integridad se basa en aspectos puesto que así fundamenta su aplicabilidad y estos se presentan como:

- Toma de Decisiones: Decisiones empresariales, gubernamentales y personales a menudo dependen de información precisa. La falta de integridad puede llevar a decisiones erróneas con consecuencias potencialmente graves.
- Confianza en los Sistemas: La integridad de la información construye y mantiene la confianza de los usuarios en los sistemas informáticos. Si los usuarios creen que la información puede ser fácilmente corrompida, su confianza en esos sistemas y en las entidades que los manejan disminuirá[35].
- Cumplimiento Legal: Muchas regulaciones y normativas exigen que las organizaciones aseguren la integridad de la información para cumplir con los requisitos legales y evitar sanciones.

d) Disponibilidad

Es el último de los pilares fundamentales de la seguridad de la información, que asegura que los sistemas de información y los datos que manejan estén accesibles y utilizables según se requiera por parte de los usuarios autorizados. Sirve estrechamente para el funcionamiento eficiente de las organizaciones, permitiendo que operaciones y decisiones importantes se realicen sin demoras indebidas.

La disponibilidad fundamenta principalmente en la poca o nula interrupción de los sistemas donde la información es esencial para su funcionamiento y que de esta manera la rentabilidad y reputación no tenga afectaciones grandes, los sistemas deben generar disponibilidad ininterrumpida debido que el constante flujo de información es vital para funciones propias del mismo[36].

e) Ataques, amenazas y vulnerabilidades

Dentro de la seguridad de la información existen diversos riesgos los cuales actúan de manera diferente, algunos pueden ser por medio físico, otros por medio de conexión a internet, otros simplemente se presentan por fallas o debilidades dentro de los procesos de seguridad que debe llevar toda entidad.

En la actualidad se presentan diferentes ataques, amenazas y vulnerabilidades los cuales no solamente provienen de manera interna si no también externa, se sabe que cada dia se pueden ampliar más este tipo de afectaciones. A continuación, se explica más a detalle:

f) Ataques

Los ataques son la acción de explotar una vulnerabilidad específica en el sistema mediante técnicas y herramientas para realizar daño o robar datos. Un ataque es la materialización de una amenaza, es decir, cuando la potencialidad de una amenaza se convierte en un acto concreto. Los ataques pueden ser dirigidos, como en el caso de un ataque dirigido de phishing, o

indiscriminados, como puede ser un virus que se propaga automáticamente[37]. Se presenta ejemplos específicos de ataques a continuación:

- Explotación de software sin actualizar por parte de un ciberdelincuente: Cuando un atacante realmente utiliza la vulnerabilidad del software para infiltrarse en una red.
- Divulgación no autorizada de información por parte de un empleado: Si un empleado actúa sobre su amenaza potencial y divulga información, esto se considera un ataque.
- Phishing y ataques de ingeniería social: Cuando los atacantes engañan a los usuarios para que revelen información confidencial[38].
- Ataques de Denegación de Servicio (DDoS): Un ataque activo que sobrecarga los recursos del sistema para hacerlo inaccesible[39].

g) Amenazas

Las amenazas se refieren a cualquier circunstancia o evento potencial que podría dañar un sistema de información a través de la pérdida, daño, alteración o acceso no autorizado a los datos. Las amenazas a la seguridad de la información pueden ser intencionales o accidentales y pueden provenir de diversas fuentes, como agentes externos (hackers), empleados internos, fallos de software o hardware, desastres naturales, entre otros. Las amenazas son aquellas que causan un efecto negativo y tenemos las siguientes.

- Empleado descontento con acceso a información sensible: Es una amenaza porque existe el potencial de que pueda hacer un uso indebido de su acceso para causar daño.

- Software sin actualizar en una red corporativa: Representa una amenaza porque la falta de actualizaciones podría ser explotada por agentes maliciosos[40].

- Existencia de ciberdelincuentes: El mero hecho de que existan individuos o grupos que buscan explotar sistemas es en sí mismo una amenaza[41].

h) Vulnerabilidades

Una vulnerabilidad es una debilidad en el sistema que puede ser explotada por una amenaza para llevar a cabo un ataque[42]. La vulnerabilidad son pequeñas prácticas las cuales generan un riesgo mayor o generan brechas para que los sistemas puedan ser explotados. Algunas vulnerabilidades más frecuentes son:

- Procedimientos inadecuados de control de acceso: Si los sistemas no tienen controles de acceso robustos, esto puede permitir el acceso no autorizado.
- Falta de cifrado en la transmisión de datos: Esto puede permitir que un atacante intercepte y lea datos sensibles, explotando la vulnerabilidad de la transmisión insegura.

i) Controles y defensas

Para combatir, defender y controlar estas amenazas, se emplean diversos métodos y protocolos conocidos como controles de seguridad. Estos controles, diseñados estratégicamente para proteger la información desde distintos frentes, se clasifican en tres tipos principales: físicos, administrativos y técnicos.

Cada tipo cumple un papel específico en la creación de un entorno seguro, contribuyendo a reducir la superficie de ataque de la organización. Al implementar estos controles de manera integral y en capas, se fortalece la postura de seguridad, permitiendo que las debilidades en un área sean compensadas por las fortalezas en otra.

Esta estrategia no solo previene incidentes de seguridad, sino que también disminuye el impacto de posibles ataques que logren superar las primeras defensas. A continuación, se describirán los controles físicos, técnicos y administrativos en detalle.

j) Controles Físicos

Estos controles se ocupan de la seguridad física de los activos de información[43].

- Control de acceso físico: Utilizar cerraduras, tarjetas de acceso, biometría y seguridad de perímetro para restringir el acceso físico a las instalaciones.

- Protección contra desastres naturales: Implementar sistemas de supresión de incendios, resistencia a terremotos y protecciones contra inundaciones.

- Seguridad de los medios: Asegurar la destrucción adecuada de medios sensibles como discos duros, documentos impresos y dispositivos de almacenamiento portátiles.

k) Controles Administrativos

Incluyen políticas, procedimientos y prácticas de seguridad para gestionar las operaciones y el comportamiento del personal.

- Políticas de seguridad de la información: Desarrollar y mantener políticas que regulen cómo se debe proteger la información[44].
- Capacitación y concienciación sobre seguridad: Programas regulares para educar a los empleados sobre las mejores prácticas de seguridad y los riesgos actuales.
- Gestión de recursos humanos: Realizar verificaciones de antecedentes y asegurar que existan procedimientos claros para la contratación y terminación de empleados.

l) Controles Técnicos

Estos controles usan tecnología para proteger los sistemas y los datos.

- Firewalls y sistemas de detección de intrusos: Proteger las redes mediante el bloqueo de tráfico malicioso y la detección de intentos de intrusión[45].

- Antivirus y antimalware: Software actualizado para detectar y eliminar software malicioso[46].
- Cifrado de datos: Utilizar cifrado para proteger la confidencialidad e integridad de los datos, tanto en reposo como en tránsito.
- Control de acceso basado en roles (RBAC): Restringir el acceso a la información y los sistemas según las necesidades del rol del usuario.
- Autenticación multifactor (MFA): Requerir más de un método de verificación de identidad para aumentar la seguridad del acceso a los sistemas[47].
- Parcheo y mantenimiento de software: Implementar un programa regular para actualizar y parchear sistemas operativos y aplicaciones.
- Respuesta a incidentes y planes de recuperación ante desastres: Preparar y ensayar cómo responder a incidentes de seguridad y recuperarse de ellos.
- Controles Organizacionales
- Segregación de funciones: Asegurar que las tareas críticas requieran la colaboración de múltiples personas para prevenir el fraude y errores.
- Revisiones de seguridad y auditorías: Realizar evaluaciones regulares de la seguridad para identificar y remediar vulnerabilidades.
- Controles de Red
- Segmentación de redes: Dividir las redes en subredes para limitar el acceso no autorizado y contener posibles compromisos.
- VPN (Redes Privadas Virtuales): Proporcionar canales seguros para el acceso remoto.

2 Norma ISO/IEC 27001

La norma ISO/IEC 27001 es un activo fundamental para cualquier organización, ya que garantiza el éxito y la continuidad mediante una gestión efectiva de la seguridad de la información. Se considera un pilar básico para cualquier tipo de entidad, pues establece las bases esenciales para un modelo sólido de protección.

Para gestionar adecuadamente la seguridad de la información, es imprescindible implementar un sistema que se guíe por objetivos claros y documente prácticas, alcances y procedimientos. Este

sistema debe planificar de manera metódica la identificación y mitigación de riesgos, amenazas y vulnerabilidades a los que está expuesta la organización.

ISO/IEC 27001 fue desarrollado por la ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission) como un marco de gestión de seguridad aplicable a cualquier tipo de organización, ya sea pública o privada, grande o pequeña.

Esta norma establece directrices para la seguridad de la información en las empresas, y al obtener su certificación, una organización demuestra que adopta estándares internacionales y prácticas recomendadas. Además, es fundamental que todos los empleados conozcan la norma debido a su amplia aplicabilidad y relevancia en la protección de la información[48].

La norma ISO/IEC 27001 fue publicada en el año 2005 donde es el fruto de la constante evolución de estándares en las últimas dos décadas. El enfoque de la norma ISO 27001 tiene su origen dentro de la BS 7799-1 donde contenía la serie de mejores prácticas con el objetivo de ayudar a las empresas sin haber una certificación por su parte [49]

a) BS 7799

La norma BS 7799 de BSI (British Standards Institution) apareció en 1995 con objeto de proporcionar a cualquier empresa el conjunto de prácticas para la buena gestión en la seguridad de la información[50].

La norma se constituye en dos partes donde la primera (BS 7799-1) se creó en base a las buenas prácticas la cual no establecía un esquema de certificación para las empresas. La segunda parte (BS 7799-2) publicada por primera vez en 1998, estableció una serie de requisitos para el sistema de la seguridad de la información (SGSI) donde podría ser certificable por una entidad independiente. Las dos partes que conforman la norma BS 7799 fueron revisadas y adoptadas por ISO, sin cambio grandes dentro de su estructuración dando el nacimiento de ISO 17799 en el año 2000 la cual concebía la primera parte de la norma BS 7799-1. Posteriormente en 2002 se adecuo BS 7799-2 para la filosofía de ISO en los SGSI.

Para el año 2005 con más de 1700 empresas ya contaban la certificación en BS 7799-2, esta norma se publicó por ISO, con algunos cambios dando a conocer el estándar ISO 27001.
La actualización de la norma ISO 17799 en 2007 tuvo su propia revisión y actualización donde se dio a conocer como ISO 27002.

Actualmente ISO contempla el desarrollo constante de normas y actualizando dentro de la serie 27000 las cuales han recibido actualizaciones en los últimos años como la norma ISO 27001 del 2013 – 2022 donde estas últimas versiones presentan cambios importantes en la estructura, evaluación y tratamiento de riesgos.[51]

- ISO/IEC 27000
- Su publicación se llevó a cabo el 1 de Mayo de 2009. Proporciona la visión general de lo que quiere lograr la serie 27000, es la introducción a los SGSI
- ISO/IEC 27001
- Publicada el 15 de Octubre de 2005. Es la norma principal de la serie la cual contiene requisitos de SGSI y contempla la certificación por medio de autores externos de esta manera validando a la empresa y sus empleados
- ISO/IEC 27002
- Toma su nombre el día 1 de Julio de 2007, mantiene el año 2005 como su edición. Es la guía de las buenas prácticas la cual describe objetivos de control y cuál es la estructuración de los controles recomendados que se deben llevar a cabo en la seguridad de la información. La norma proporciona 39 objetivos de control y 133 controles los cuales se dividen en 11 dominios, esta norma es certificable.

3 Sensibilización del personal administrativo

La sensibilización se enfoca principalmente en dar valor e importancia hacia un objeto de estudio, se puede generar de diferentes maneras las cuales pueden dotar de información que por medio de campañas o diferentes tipos de expansión de información la gente pueda darle un sentido de pertenencia hacia el tema que va dirigida la sensibilización. Busca estrechamente poder

concientizar a la gente constantemente sobre un tema el cual se le quiera dar importancia donde activamente se trata de estructurar la información y que se le pueda dar relevancia mediante diferentes medios.[52]

En la actualidad el objetivo de la seguridad de la información es la protección de los datos como activos de suma importancia en las empresas, esto se hace con el fin de proteger a su empresa y la privacidad de sus clientes. Al hablar de la sensibilización en la seguridad de la información hacemos referencia directamente hacia que la protección de los datos tome conciencia en cada una de las personas de una empresa, buscando alcanzar el objetivo de la cultura de la protección digital de los datos tanto de empresas como de la sociedad en general, esto siendo guiado por la constante información que puede apreciar en los medios tecnológicos de hoy en día.

Uno de los objetivos más importantes que busca la sensibilización dentro del ámbito de la seguridad de los datos es mostrar de los riesgos que puede tener las brechas de la información y buscar el modo mitigar este tipo de situaciones estableciendo buenas prácticas, estándares y protocolos que puedan ser adoptados por la gente a la cual va dirigida para que se actúe de una manera preventiva.[53]

Algunos incidentes o eventos son causados por factores de poco conocimiento dentro de las empresas ya sean por su bajo conocimiento, por descuidos y falta de conciencia dentro de las personas que se encuentran en el población laboral, esto se puede dar por la negligencia, bajo presupuesto en auditorias o por el simple hecho de que se puede pensar que la seguridad no es tan importante a la vez que ocurra un incidente puede conllevar a grandes pérdidas económicas como por supuesto sanciones legales.

Sensibilizar una población, un sector o un ámbito especifico de una empresa consiste que activamente se muestre la importancia del tema bien sea con cursos, certificados, capacitaciones o en general desarrollar buenas prácticas al igual que promover los estándares y cumplir con las normativas de seguridad y tratamientos de los datos que se han previsto por entidades gubernamentales o internacionales. En la seguridad de la información se conoce a la perfección sobre el recurso humano es el eslabón más débil en lo que compete a protección de la información

por eso se está en constante búsqueda de fortalecer la formación de empleados, establecer políticas de seguridad en las empresas con el fin de sensibilizar y concientizar a su personal y mantener un adecuado nivel de seguridad. [54]

En la actualidad la sensibilización dentro de las empresas se ha convertido en una parte fundamental para ellas puesto que se ha enfocado en impactar sobre los temas generales y principales para el sostenimiento de las mismas. Se pretende reforzar el conocimiento y llevar una guía de máximo esfuerzo para lograr los objetivos propuestos. Para poder alcanzar las metas propuestas por los objetivos se debe llevar a cabo una explicación de manera concreta y apropiada los usos de sistemas de información y así proceder de la manera que se considere más conveniente dependiendo de su rol dentro de la empresa [55]

4 Herramienta virtual

En la actualidad el aprendizaje en línea forma una parte esencial para la humanidad, donde existen varias plataformas, herramientas y páginas de aprendizaje las cuales ayudan al método educativo y en la mejora continua del conocimiento. Se puede ver reflejado el uso de estos recursos sean para cursos en línea, plataformas educativas, pre grados, posgrados, técnicos, entre otros, la evidencia de la formación en línea ha construido un nuevo método de aprendizaje es bastante amplia debido que puede ser usada por cualquier persona dependiendo de su tema de estudio o lo que requiera para una formación en línea, donde puede ser de 2 maneras diferentes tales como la sincrónica la cual refiere a que tanto el transmisor como receptor tiene una interacción en tiempo real tal como se pudo evidenciar en pandemia en clases virtuales y asincrónica la cual el emisor sube recursos, videos o grabaciones que fueron realizadas con anticipación demostrando que la interacción no se produce en tiempo real así mismo como se puede evidenciar en la plataforma universitaria TAU[56].

Esta modalidad de aprendizaje en línea se distingue por la flexibilidad que tiene con el usuario debido que no es una manera presencial puede ayudar en los aspectos de tiempo, económicos, material educativo y solución de trabajos propuestos por quienes están a cargo de realizar el papel de docente en las aulas virtuales, el auge de estas plataformas sigue en ascenso debido a su

accesibilidad, disponibilidad y escalabilidad que ofrecen tanto para los estudiantes como para la institución o empresa que brinda los servicios. Considerando lo anterior dicho se puede encontrar diferentes plataformas que ofrecen servicios de sistemas de gestión de aprendizaje.

a) LMS MOODLE

Un LMS (Learning Management System) o sistema de gestión de aprendizaje es un software en línea que facilita la creación, desarrollo e implementación de procesos educativos o de entrenamiento, adaptándose a diferentes metodologías o ciclos de aprendizaje según se requiera.

Cada LMS tiene características propias, pero en general funcionan mediante un servidor que administra las operaciones, mientras que profesores y estudiantes interactúan a través de una interfaz gráfica. Estas plataformas permiten subir archivos relacionados con la materia, realizar ejercicios, trabajos y exámenes, así como evaluar y monitorear el progreso de los estudiantes, quienes participan activamente con la institución, empresa o plataforma que ofrece el aprendizaje[57].

Moodle es una plataforma LMS ampliamente adoptada por instituciones a nivel regional, nacional e internacional, destacándose por ser un sistema integrado, robusto y seguro. Su facilidad de personalización la convierte en una herramienta versátil para quienes la utilizan. El éxito de Moodle radica en su gran cantidad de funcionalidades y en sus extensiones, que permiten no solo adaptar la plataforma, sino también personalizar los cursos y recursos que se integran a ella[58]. Moodle es de acceso libre y gratuito el cual permite constantemente actualizar con nuevos métodos, apariencias y debido a sus funcionalidades se cataloga como una herramienta estable y de confianza., también su facilidad de uso hace que sea la preferida por instituciones de educación superior siendo así la mayor herramienta flexible, escalable y personalizable de todas las LMS.[59]

C. Variables de estudio

En el contexto del proyecto donde se enfoca la seguridad de la información como componente principal para la capacitación y sensibilización de la seguridad de la información basados en la norma ISO 27001.

1 Variables independientes

- Herramienta virtual para la capacitación en seguridad de la información al personal administrativo de la Universidad CESMAG

2 Variables dependientes

- Satisfacción del usuario
- Nivel de conocimiento y sensibilización.
- Tasa de cumplimiento en la capacitación de la norma ISO 27001

D. Definición nominal de variables

En el desarrollo del proyecto enfocado en una herramienta virtual para la capacitación del personal administrativo de la Universidad CESMAG, se identificaron variables nominales esenciales para alcanzar los objetivos propuestos, especialmente en lo relacionado con la formación y evaluación del conocimiento adquirido. Las variables identificadas son las siguientes:

- Herramienta virtual para la capacitación en seguridad de la información del personal administrativo de la Universidad CESMAG: Corresponde al principal resultado del proyecto, orientado a formar al personal administrativo y docente en buenas prácticas de seguridad de la información, conforme a los lineamientos de la norma ISO/IEC 27001. Esta plataforma interactiva ofrece acceso a contenidos formativos, evaluaciones, simulaciones

y actividades prácticas, con el fin de fortalecer el conocimiento y la implementación de medidas de protección de datos dentro del entorno institucional.

- Satisfacción del usuario: Esta variable representa la satisfacción del usuario al hacer uso de la herramienta finalizada su capacitación.

- Nivel de conocimiento y sensibilización: Esta variable hace referencia hacia el nivel de conocimiento adquirido por parte del personal al finalizar la capacitación mostrando su desempeño y siendo reflejado a la finalización de la capacitación.

- Tasa de cumplimiento en la capacitación sobre la norma ISO/IEC 27001: Esta variable permite evaluar el progreso en la implementación de los módulos formativos mediante el porcentaje de participación del personal administrativo y docente. La medición se basa en la cantidad de personas que hayan completado satisfactoriamente los módulos, con el objetivo de alcanzar gradualmente una cobertura del 100% del personal institucional. Para garantizar la fiabilidad de los datos, se requiere un proceso riguroso de depuración y validación de los registros de participación, tanto a nivel nominal (identificación de los participantes) como operativo (cumplimiento efectivo de las actividades).

E. Definición operativa de variables

- Herramienta virtual para la capacitación en seguridad de la información: El personal administrativo completará la capacitación asignada, que incluirá ejercicios prácticos, cuestionarios y un examen final diseñado para evaluar el conocimiento adquirido durante el proceso formativo.

- Satisfacción del usuario: La satisfacción se medirá mediante una encuesta al finalizar la capacitación, en la que los usuarios valorarán su experiencia con la herramienta y el contenido, utilizando una escala del 1 al 5.

- Nivel de conocimiento y sensibilización: Al concluir la capacitación, cada usuario podrá visualizar su calificación general, permitiendo evaluar el desempeño individual y el nivel de conocimiento adquirido.

- Tasa de cumplimiento en la capacitación de la norma ISO 27001: Esta variable será evaluada a partir del desempeño demostrado por el personal en la plataforma virtual, tomando en cuenta diversos indicadores de avance y consolidación del aprendizaje. Entre estos se incluyen los resultados obtenidos en las evaluaciones finales, el progreso individual registrado en los módulos de formación, así como las autoevaluaciones realizadas por los participantes. Así mismo, se aplicarán encuestas de percepción dirigidas a los jefes inmediatos, con el propósito de identificar cambios observables en las prácticas laborales cotidianas, derivados de la aplicación de los contenidos adquiridos. Esta metodología permitirá recopilar información tanto cuantitativa, facilitando así una medición integral del grado de integración y apropiación de los principios establecidos por la norma dentro del entorno institucional.

F. Formulación de hipótesis

1 Hipótesis de la investigación

La implementación de la herramienta virtual busca fortalecer y enriquecer el conocimiento, culturizar y sensibilizar al personal administrativo de la Universidad CESMAG sobre la seguridad de la información y tratamiento de datos.

2 Hipótesis nula

La implementación de una herramienta virtual de capacitación no tendrá un efecto significativo en la capacitación, sensibilización ni en la cultura de seguridad de la información del personal administrativo y docente de la Universidad CESMAG.

3 Hipótesis alterna

La implementación de una herramienta virtual de capacitación permite fortalecer la conciencia del personal administrativo de la Universidad CESMAG en torno a la gestión de estándares, protocolos, buenas prácticas y riesgos asociados a la seguridad de la información y al tratamiento adecuado de datos personales.

III. METODOLOGÍA

A. Paradigma

El proyecto se enmarca dentro del paradigma positivista, ya que se basa en la observación y análisis objetivo de la realidad en la Universidad CESMAG, con el fin de alcanzar los objetivos propuestos. Su desarrollo busca evidenciar cómo las variables involucradas se relacionan entre sí y permiten obtener resultados concretos mediante los métodos aplicados en la capacitación.

B. Enfoque

El proyecto se sustenta en un enfoque cuantitativo, el cual permite medir objetivamente la asimilación del conocimiento por parte de los participantes. Este enfoque, alineado con el paradigma positivista, se fundamenta en el uso de datos cuantificables que reflejan características observables del proceso de formación. A través de instrumentos como test y cuestionarios estructurados, se recopilará información que permitirá evaluar tanto el rendimiento individual como la evolución del desempeño a lo largo de cada etapa del programa de capacitación.

Esta metodología no solo facilita el análisis estadístico de los resultados obtenidos, sino que también permite valorar la eficiencia y eficacia del proceso formativo en función del logro de los objetivos establecidos. Asimismo, contribuye a fomentar un desarrollo progresivo y sostenido del conocimiento, garantizando su adecuada difusión, comprensión y consolidación entre todos los participantes.

C. Método

El proyecto adoptará el método científico como base para asegurar un enfoque riguroso y sistemático en el desarrollo de una plataforma de capacitación en seguridad informática [60]. Este proceso se estructurará en las siguientes etapas:

- **Definición del problema:** Se identificarán las necesidades de capacitación del personal administrativo de la Universidad CESMAG a partir de un diagnóstico inicial de vulnerabilidades.

- **Diseño de la solución:** Se desarrollarán módulos interactivos alineados con estándares internacionales, como la norma ISO/IEC 27001.

- **Implementación:** Los cursos serán aplicados mediante una plataforma virtual accesible y dinámica.

- **Evaluación:** Se medirá la efectividad de la capacitación a través de encuestas de satisfacción, pruebas de conocimiento y análisis comparativo de incidentes de seguridad antes y después de la intervención.

Para garantizar la calidad del proceso formativo, se emplearán herramientas de diseño instruccional y tecnologías de aprendizaje en línea, asegurando tanto la accesibilidad como la precisión del contenido. Este enfoque no solo permitirá responder a las preguntas de investigación, sino también evaluar la calidad del aplicativo y el nivel de sensibilización alcanzado por el personal, fortaleciendo así la seguridad digital institucional [60].

D. Tipo de investigación

El presente proyecto se enmarca dentro de una investigación de tipo descriptivo, cuyo propósito es especificar y caracterizar el nivel de conocimiento evidenciado por los participantes en el proceso de capacitación. A través del uso de herramientas virtuales y el análisis de resultados obtenidos mediante instrumentos cuantitativos, se pretende describir de manera sistemática el desempeño individual antes y después de la formación. Esta descripción permitirá ofrecer un panorama claro del impacto observable del proceso formativo, sin que ello implique establecer relaciones causales, sino más bien documentar con precisión las propiedades y cambios evidenciados en los participantes, lo cual puede servir como base para futuras investigaciones o intervenciones.

E. Diseño de investigación

El proyecto se centra en el desarrollo de una herramienta virtual alineada con los lineamientos de la norma ISO/IEC 27001. Se empleará un enfoque descriptivo, orientado a la recopilación y análisis de datos estadísticos generados a lo largo del uso de la plataforma por parte del usuario final. Estas estadísticas históricas permitirán medir la adherencia y aplicación del conocimiento adquirido, mediante el análisis de información correlacionada con los objetivos definidos dentro de la herramienta.

F. Población

La población objetivo de este proyecto es estrictamente dirigida hacia el personal administrativo de la Universidad CESMAG, abarcando a aquel que reciba información o archivos de cualquier índole o cualquier información por medio de plataformas.

G. Muestra

La muestra fue seleccionada aleatoriamente entre el personal administrativo que manifestó interés en participar en el proyecto de investigación y que tuvo acceso anticipado y formaron parte del primer grupo de estudio. Se procuró optimizar la eficacia en la recolección de datos, las capacitaciones fueron programadas estratégicamente durante periodos de baja actividad académica o en espacios previamente destinados por la administración para cursos y talleres relacionados con la seguridad de la información.

H. Técnicas de recolección de información

Las primeras actividades o fases consistirán en encuestas y entrevistas realizadas al personal administrativo de la Universidad CESMAG. Estas actividades permitirán un contacto directo con los participantes, buscando que proporcionen información sobre el tema abarcado por el proyecto. Se pretende determinar si las capacitaciones previas han sido efectivas y útiles para la adquisición de conocimiento y la implementación de prácticas dentro de la institución educativa.

I. Validez de las técnicas de recolección

Las técnicas se eligieron en base a la seguridad de la información, capacitación y la sensibilización donde tanto las encuestas como entrevistas que serían de manera estructurada y planteada con el fin de enriquecer la investigación de cuál es el conocimiento adquirido anteriormente mostrando así, los campos donde se encuentran mayormente las debilidades y fortalezas atendiendo así al llamado de recolección sobre el tema al cual va dirigido el proyecto.

J. Confiabilidad de las técnicas de recolección

En el proyecto, la confiabilidad de las técnicas depende estrictamente de la estructura de las encuestas y entrevistas, es decir, de los lineamientos y parámetros establecidos para su realización. Esto implica recalcar las precauciones necesarias y seguir un procedimiento riguroso. Tanto las entrevistas como las encuestas al personal administrativo proporcionarán información precisa sobre el conocimiento del tema, destacando la transparencia y veracidad de las respuestas. Los resultados de la información deben ser consistentes, detallados y uniformes, de modo que se pueda validar la confiabilidad de las técnicas utilizadas.

K. Instrumentos de recolección de información

Para garantizar la solidez metodológica del proyecto y asegurar una comprensión integral del contexto institucional, se emplearon diversos instrumentos de recolección de datos. Estos permitieron abordar el objeto de estudio desde diferentes enfoques, combinando fuentes documentales, técnicas cuantitativas y cualitativas. A continuación, se describen los instrumentos utilizados, su aplicación y el aporte específico de cada uno al desarrollo del proyecto[61].

- Revisión documental:

Se consultaron manuales, políticas y normativas internas de la Universidad CESMAG, junto con fuentes externas confiables relacionadas con la Ley 1581 de 2012 y la norma ISO/IEC 27001. Esta revisión permitió definir el marco teórico y normativo del proyecto.

- Encuestas diagnósticas:

Se aplicaron formularios digitales a personal administrativo, docente y de apoyo, para identificar su nivel de conocimiento sobre seguridad de la información y tratamiento de datos. Los cuestionarios fueron validados previamente para asegurar su claridad y relevancia.

- Entrevistas estructuradas:

Se realizaron entrevistas grabadas a actores clave de la universidad, guiadas por un guion formal. Esta técnica permitió obtener información cualitativa sobre el contexto institucional y evaluar la viabilidad de implementar la herramienta de capacitación.

IV. RESULTADOS

En este capítulo se hace la presentación detallada de todos procesos realizados para el cumplimiento del proyecto donde se implementó la metodología ADDIE y la metodología SCRUM donde de manera íntegra pudieron conformarse para el desarrollo de cada uno de los objetivos específicos del proyecto, realizando así el desarrollo del proyecto de una manera efectiva y organizada.

A. Caracterización del conocimiento del personal administrativo

Para este primer objetivo, se describe cómo fue definido el proyecto con el propósito de caracterizar el nivel de conocimiento y analizar los temas que se abordarán en el desarrollo del mismo. Para ello, fue necesario investigar el funcionamiento de la cadena de seguridad de la información dentro de la Universidad CESMAG. En este proceso, se llevó a cabo una reunión con el Mg. Jairo Andrés Casanova Caicedo, responsable de la Oficina de Seguridad de la Información, Seguridad de los Datos y Gobierno de Datos, quien explicó detalladamente cómo opera el sistema de control interno en materia de seguridad. Además, propuso incorporar al proyecto la Ley 1581 de 2012, normativa que la universidad aplica en las capacitaciones dirigidas al personal administrativo y docente.

Posteriormente, se realizó una reunión con el asesor del proyecto, Mg. Luis Arnoby Escobar Hernández, en la cual se acordó la metodología de enseñanza y aprendizaje más adecuada. Se eligió el modelo instruccional ADDIE (Análisis, Diseño, Desarrollo, Implementación y Evaluación), por su enfoque sistemático y flexible. A partir de esto, se establecieron los métodos de recolección de información que permitirán identificar las áreas con mayor necesidad de intervención, tanto en el personal administrativo como docente, facilitando así el diseño de una estrategia formativa pertinente y efectiva.

1 Análisis de la primera fase ADDIE

Para esta primera fase se realizó una investigación exhaustiva sobre los temas abordados en las capacitaciones ofrecidas por la Oficina de Seguridad de la Información. Como resultado, se

identificaron dos grupos diferenciados dentro de la población laboral de la Universidad CESMAG: por un lado, el personal externo o contratistas (trabajadores terceros), y por otro, el personal interno conformado por administrativos y docentes vinculados directamente a la institución. Esta división permitió redefinir el enfoque del proyecto, concluyendo que era necesario desarrollar dos modelos de formación diferenciados: uno orientado a la seguridad de la información para trabajadores externos, y otro enfocado en la protección de datos personales dirigido al personal interno.

En este contexto, el Mg. Jairo Andrés Casanova Caicedo convocó a una reunión en la que resaltó la relevancia del proyecto, especialmente porque la universidad tenía prevista la contratación de un seguro todo riesgo en seguridad informática. Se evidenció que contar con una plataforma de capacitación continua tendría un impacto positivo en la reducción de los costos de adquisición del seguro, destacando así el valor estratégico del proyecto.

Finalmente, se llevó a cabo una reunión conjunta con el asesor del proyecto, Mg. Luis Arnoby Escobar Hernández, y el Mg. Jairo Andrés Casanova, en la que se abordó un aspecto clave: la certificación del proceso de capacitación. Se acordó que la certificación no solo respaldaría formalmente la formación de los participantes, sino que también representaría una ventaja para la universidad al permitir capacitaciones asincrónicas. Esto facilitaría la participación de funcionarios internos y externos sin requerir su asistencia presencial, optimizando tiempos y recursos tanto para la institución como para los trabajadores.

2 Revisión de contenidos seguridad de la información

Para el desarrollo de esta actividad, se llevó a cabo una sesión virtual mediante Google Meet con el ingeniero Mg. Jairo Andrés Casanova, quien compartió de manera cordial los recursos previamente utilizados en cursos de capacitación institucional. A partir de este insumo, se establecieron los contenidos fundamentales que debía incluir el curso de capacitación en seguridad de la información. Entre los temas definidos se encuentran: conceptos básicos, técnicas de mitigación de riesgos, principios de la seguridad de la información, mecanismos de autenticación, buenas prácticas en el uso de contraseñas, periodicidad de actualización, métodos de contingencia

y tipos de vulnerabilidades. Estos elementos conforman la estructura temática del curso destinado al primer grupo de usuarios identificados en el proyecto.

3 Revisión de contenidos ley 1581 del 2012

De forma complementaria a la actividad anterior, el ingeniero Mg. Jairo Andrés Casanova también compartió los recursos utilizados en sesiones previas de capacitación orientadas al personal interno. A partir del análisis de este material, se identificó que los contenidos estaban enfocados en los actores involucrados en el Registro Nacional de Bases de Datos (RNBD), los roles específicos dentro de la universidad, la clasificación de los tipos de información o datos personales, y las acciones apropiadas para su manejo. Estos temas fueron definidos como base estructural para el desarrollo del curso dirigido al segundo grupo objetivo del proyecto: el personal administrativo y docente directamente vinculado a la institución.

4 Recolección de información general sobre la seguridad de la información para visualización del estado de administrativos, docentes y contratistas terceros

Se aplicó una encuesta diagnóstica sobre conceptos y contenidos relacionados con la seguridad de la información, la cual fue respondida por 118 personas, una muestra representativa para los fines del estudio. A continuación, se presentan algunas de las preguntas clave que permitieron identificar las principales debilidades en el conocimiento del personal encuestado, así como los aspectos donde se evidencian mayores dificultades en la comprensión y aplicación de la cadena de seguridad de la información. Estos resultados refuerzan la necesidad del proyecto, ya que permiten orientar con mayor precisión los contenidos formativos y respaldan el cumplimiento del objetivo general: fortalecer las competencias del personal en torno a la protección y gestión segura de la información institucional.

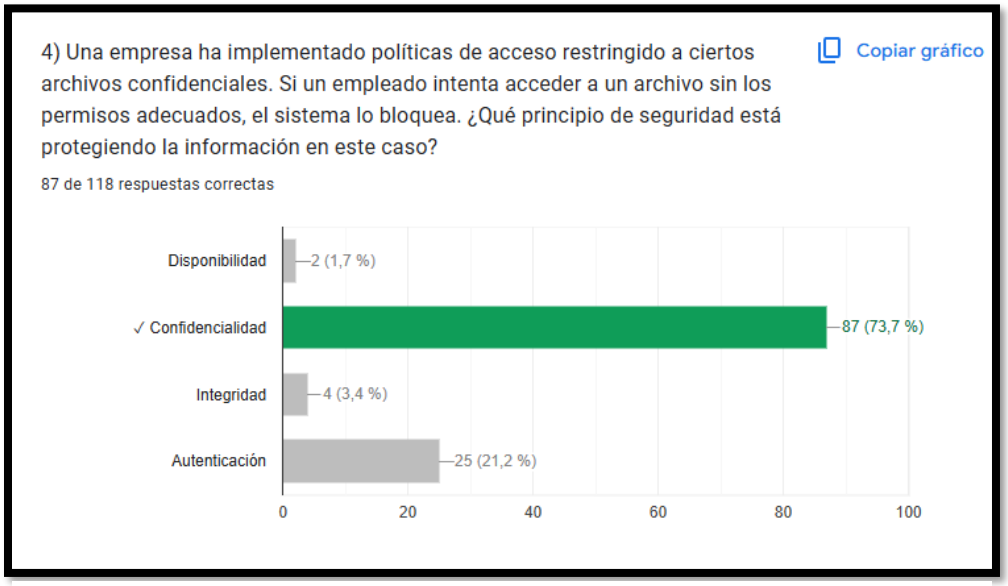


Fig.1: Pregunta 4 Formulario seguridad de la información

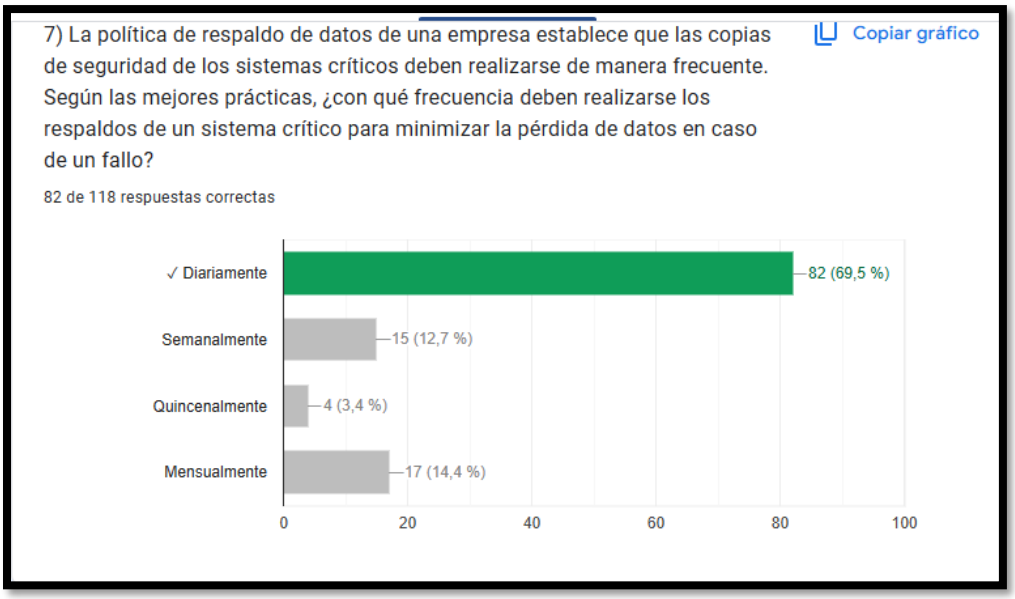


Fig. 2: Pregunta 7 formulario seguridad de la información

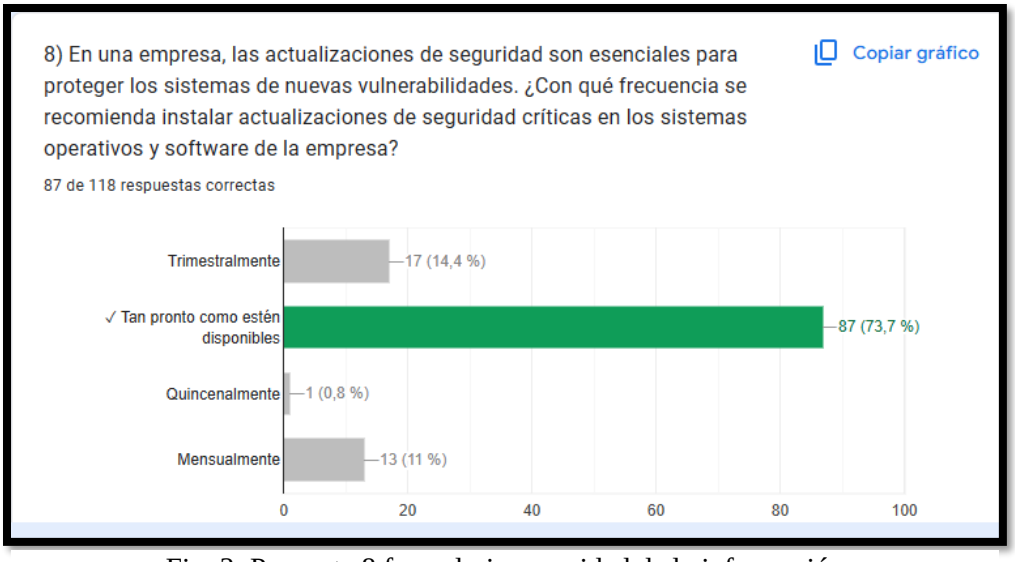


Fig. 3: Pregunta 8 formulario seguridad de la información

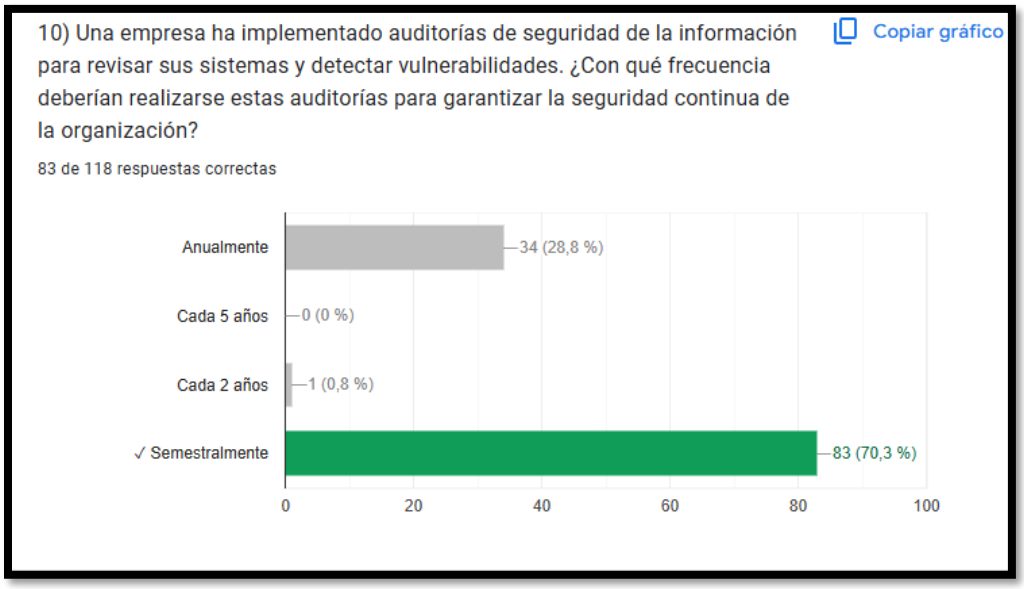


Fig.4: Pregunta 10 Formulario seguridad de la información

5 Recolección de información general sobre la ley normativa 1581 para visualización del estado de administrativos, docentes y contratistas terceros

Se aplicó una encuesta diagnóstica sobre los contenidos y conceptos fundamentales de la Ley 1581 de 2012, obteniendo respuestas de 66 personas, una muestra significativa para los fines del estudio. A continuación, se presentarán algunas de las preguntas más relevantes, que permitieron identificar las principales debilidades conceptuales en torno al tratamiento y protección de datos personales. Estos hallazgos evidencian los puntos críticos donde el conocimiento es más limitado, lo cual afecta la adecuada implementación de la cadena de seguridad de la información. Los resultados refuerzan la importancia de este proyecto, ya que permiten focalizar los contenidos formativos y contribuyen directamente al cumplimiento del objetivo general: fortalecer la cultura de protección de datos en el entorno universitario.

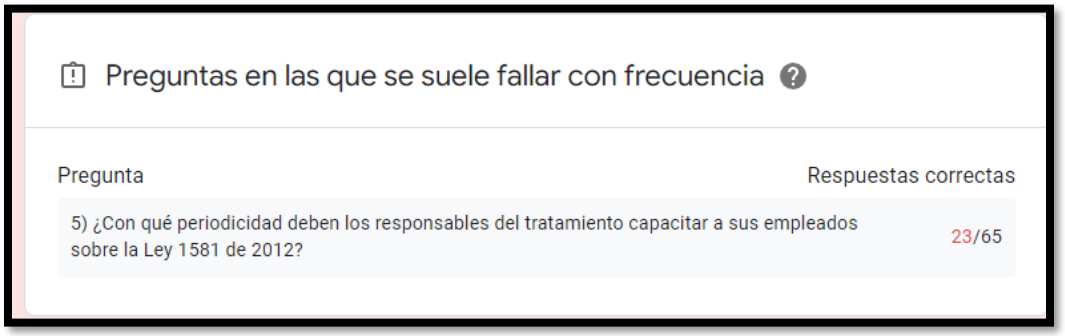


Fig. 5: Pregunta con más fallos formulario tratamiento de datos

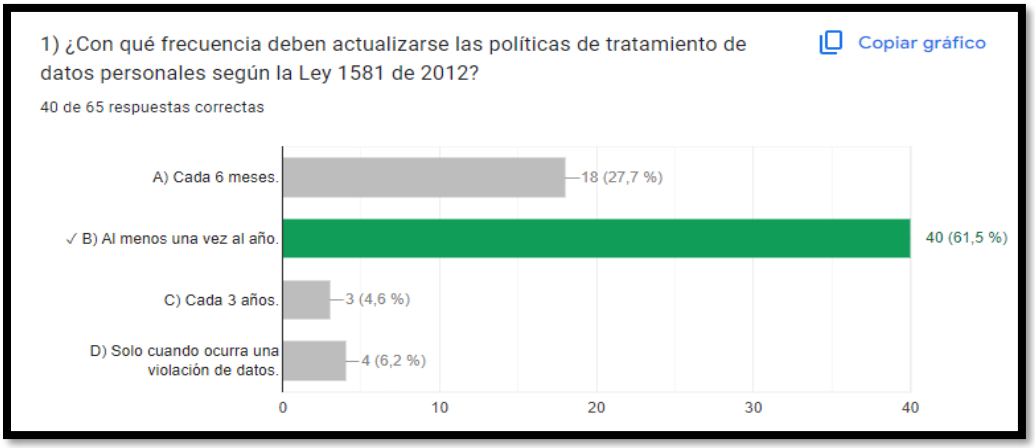


Fig. 6: Pregunta 1 formulario tratamiento de datos

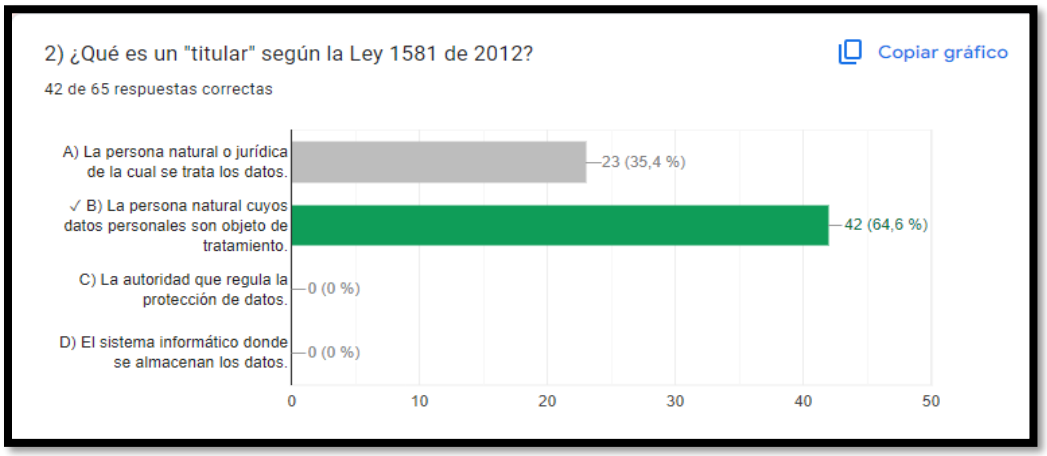


Fig. 7: Pregunta 2 formulario tratamiento de datos

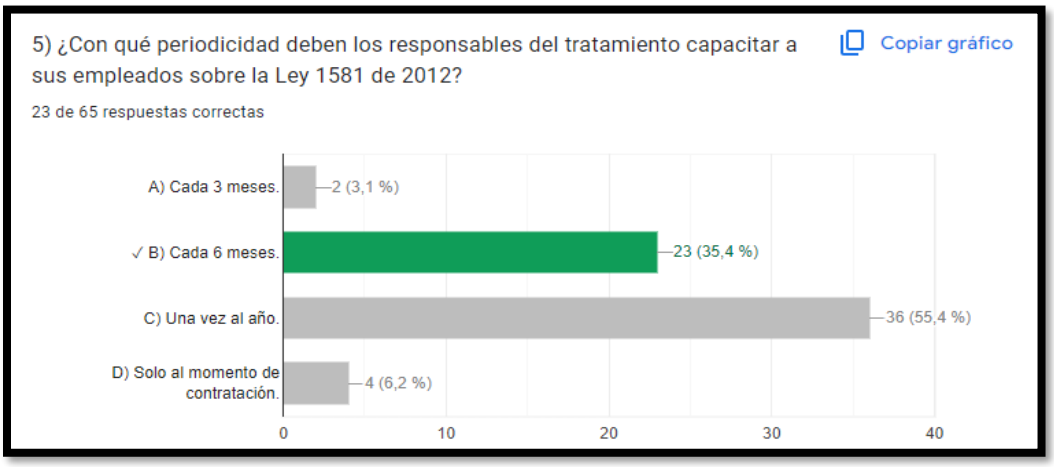


Fig. 8: Pregunta 5 formulario tratamiento de datos

6 Análisis de los resultados obtenidos por las encuestas para determinar los tópicos principales para guiar el módulo en seguridad de la información

Con base en el análisis de las encuestas aplicadas, se identificaron los temas de mayor relevancia para el desarrollo del proyecto. Estos incluyen los principios fundamentales de la seguridad de la información, la frecuencia con la que se presentan situaciones operativas relacionadas con riesgos, la periodicidad de auditorías internas y los planes de contingencia. Estos tópicos reflejan las principales áreas de interés y necesidad del personal participante, por lo que el proyecto se orientará activamente hacia ellos. Su inclusión prioritaria en el contenido formativo reafirma la pertinencia

de la iniciativa y resalta la necesidad de fortalecer estas competencias dentro de la comunidad universitaria.

7 Análisis de los resultados obtenidos por las encuestas para determinar los tópicos principales para guiar el módulo en la ley normativa 1581

El análisis de las encuestas diagnósticas permitió identificar los ejes temáticos prioritarios del proyecto, los cuales se alinean directamente con las disposiciones de la Ley 1581 de 2012 sobre protección de datos personales. Entre estos se destacan: los conceptos fundamentales sobre el tratamiento de datos, con énfasis en el respeto a los derechos de los titulares; la frecuencia de operaciones que involucran información personal, garantizando su legalidad y seguridad; la periodicidad de las auditorías internas, orientadas a verificar el cumplimiento normativo; y la gestión de contingencias, mediante protocolos eficaces ante eventuales brechas de seguridad. Aunque el proyecto aborda de forma integral la cultura de seguridad de la información, se priorizan estos componentes por su estrecha vinculación con el marco legal colombiano, contribuyendo a que la institución no solo cumpla con la normativa vigente, sino que también fortalezca la confianza de sus grupos de interés mediante prácticas transparentes y responsables en el manejo de datos.

8 Revisión de los temas y subtemas previamente abordados

Para la finalización de este primer objetivo específico se realizó una retrospección más grande sobre los tópicos anteriormente mencionados por cada uno de los módulos propuestos. Se procedio a desglosar los temas en sus subtemas para generación de especifica de contenido dando como resultado lo siguientes tópicos abarcados por cada uno.

TABLA I: TEMAS Y SUBTEMAS ABARCADOS EN EL MÓDULO DE SEGURIDAD DE LA INFORMACIÖN

Tema		Subtema	Contenido
Conceptos básicos		Confidencialidad	Proteger la información de que solo pueda ser accedida por personas autorizadas
		Integridad	Proteger la información de que no pueda ser alterada o destruida
		Disponibilidad	Proteger la información de que esté disponible cuando se necesite
		Autenticación	Proteger la información de que sea genuina
		Autorización	Proteger la información de que solo pueda ser accedida por personas autorizadas
Técnicas de mitigación		Software de seguridad	- Utilizar software de seguridad integral, como antivirus, anti espía o firewall - Utilizar filtros antispam y sistemas de encriptado de mensajes
		Copias de seguridad	Crear copias de seguridad de la información
		Almacenamiento	Almacenar información en la nube, en red y en local
		Encriptación	Codificar información para que solo puedan acceder a ella los usuarios que tienen la clave de descifrado

		Control de acceso	- Limitar el acceso a la información - Inventariar los activos y eliminar los dispositivos y aplicaciones que no se necesitan - Identificar, priorizar y remediar las vulnerabilidades
		Seguridad en línea	- Revisar los documentos y fotos que se comparten en línea - Acceder a páginas web y compras seguras Proteger el correo electrónico
Vulnerabilidades		Falta de controles de seguridad	Ausencia de medidas para proteger sistemas y datos, aumentando el riesgo de ciberataques.
		Contraseñas débiles	Uso de claves simples o repetidas, facilitando el acceso no autorizado.
		Falta de copias de seguridad	No tener respaldos de datos puede resultar en pérdida irreversible de información.
		Sistemas y aplicaciones desactualizados	Software sin parches de seguridad, exponiendo vulnerabilidades conocidas.
		Falta de formación sobre seguridad informática	Desconocimiento de buenas prácticas, aumentando el riesgo de errores humanos.
		Conexiones a redes públicas desprotegidas	Uso de redes inseguras sin cifrado, exponiendo datos a interceptación.

TABLA II: TEMAS Y SUBTEMAS ABARCADOS EN EL MÖDULO DE TRATAMIENTO DE DATOS.

Tema	Subtema	Contenido
Actores	Titular	Persona Natural Dueña del dato
	Administrador (responsable)	PJ o PN a quien el Titular le entrega los datos
	Encargado	PJ o PN a quien el encargado le sede el dato
Tipos de información	Sensible	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas.
	Privada	Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización expresa. es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización expresa.
	Semiprivada	Son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información.
	Pública	Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos,

		entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.
Incidente	Venta no autorizada	Cesión ilegal de datos personales a terceros sin consentimiento del titular, generalmente con fines comerciales.
	Fuga de datos:	Acceso, divulgación o filtración accidental o intencional de información confidencial por fallas en seguridad.
	Robo de datos	Sustracción ilícita de bases de datos por hackers, empleados malintencionados o ataques cibernéticos.
	Pérdida de datos	Extravío o destrucción accidental de información personal (ej: fallas en servidores, dispositivos sin respaldo).
	Copia no autorizada	Duplicación de datos sin permiso del titular, sea por acceso indebido interno o externo.
Seguridad	Garantizar custodia	Implementar medidas técnicas y administrativas (ej. cifrado, acceso restringido) para proteger los datos.
	Transferencia	Asegurar que los datos solo se compartan con terceros que cumplan estándares de protección y con autorización del titular.
	Finalidad	Tratar los datos únicamente para los fines específicos, legítimos e informados al titular.
	Consentimiento	Obtener autorización previa, expresa e informada del titular, salvo excepciones legales.

Sanciones	Sanciones Económicas (Multas)	-Tratamiento de datos sin autorización. -No atender derechos de los titulares (consulta, rectificación, supresión). -Transferencia ilegal de datos a terceros. -Incumplir medidas de seguridad (ej. fugas o robos de datos por negligencia).
	Sanciones Correctivas	-Suspender actividades de tratamiento de datos hasta regularizar la situación. -Ordenar la corrección, supresión o bloqueo de datos irregulares. -Implementar medidas de seguridad adicionales (ej. auditorías, cifrado).
	Sanciones de Cese o Prohibición	-Cierre temporal o definitivo de operaciones relacionadas con el tratamiento de datos (en casos graves, como venta masiva no autorizada). -Inhabilitación para manejar bases de datos por un período determinado.
	Sanciones Reputacionales	Publicación de la sanción en medios de comunicación, afectando la imagen de la empresa.

B. Construcción de una herramienta web interactiva.

Diseño y Desarrollo integrando metodología ADDIE y SCRUM

Para el desarrollo de este objetivo se incluyeron las fases de la metodología ADDIE realizando un plan detallado de enseñanza-aprendizaje creando un guion para curso de capacitación a realizar. Dentro del segundo objetivo específico, se dio inicio a la fase de diseño siguiendo como metodología principal ADDIE. Desde esta etapa, se comenzó a implementar la metodología Scrum.

Esta integración se justifica porque ambas metodologías comparten pasos cruciales tales como Product Backlog donde de manera sencilla se permite integrar la metodología SCRUM como fase dentro del proyecto donde permite plantear roles definidos, limitaciones en tiempo y recursos. El haber incluido SCRUM permitió la mejor obtención en flexibilidad y adaptabilidad del proyecto debido que el proyecto solo está siendo generado por mi persona, permitiendo así ajustes continuos en tiempos de trabajo y respuestas rápidas a cualquier cambio y necesidades que se generó durante el proceso.

1 Análisis para el comienzo de ejecución del proyecto.

Como primer paso de esta fase, se realizó una reunión con los ingenieros Mg. Jairo Andrés Casanova Caicedo y Mg. Luis Arnoby Escobar Hernández, en la que se evaluaron distintos escenarios para el desarrollo del proyecto, definiendo las siguientes propuestas. Inicialmente, se planteó crear la herramienta de capacitación mediante la plataforma LMS Moodle, alojada en un servidor propio de la universidad. Sin embargo, esta opción fue descartada debido a los elevados recursos que requeriría la duplicidad de la herramienta TAU. Para comprender mejor esta limitación, se solicitó el apoyo del ingeniero Mg. Jorge Albeiro Rivera, quien explicó el funcionamiento de TAU y la gestión de sus servidores, confirmando la inviabilidad técnica y económica de replicar dicha plataforma.

Posteriormente, el ingeniero Mg. Jorge Albeiro Rivera propuso la creación de dos módulos dentro de la plataforma TAU, que podrían ser desarrollados y administrados por el estudiante David Esteban Pantoja, con la asesoría del Mg. Luis Arnoby Escobar y la coordinación del Mg. Jairo Andrés Casanova Caicedo. Esta solución práctica optimiza recursos, resulta viable y se adapta a la infraestructura disponible en la universidad y la oficina de seguridad de la información, gobierno y protección de datos. La propuesta fue aprobada por todas las partes involucradas, consolidando al proyecto como una pieza clave dentro del sistema de seguridad de la información de la Universidad CESMAG, cubriendo necesidades fundamentales de capacitación, certificación y gestión de seguros institucionales.

2 Gestión apertura módulos de TAU

En esta etapa se gestionó formalmente con el decano de la Facultad de Ingeniería de Sistemas, ingeniero Mg. Carlos Fernando Gonzales Guzmán, la solicitud, mediante carta formal (ANEXO A), de acceso en calidad de profesor a la plataforma TAU. Dicha carta fue dirigida al ingeniero Mg. Jorge Albeiro Rivera, administrador y responsable de la plataforma, quien autorizó la apertura de dos módulos: el primero denominado Seguridad de la Información y el segundo Capacitación en Tratamiento de Datos.

De forma paralela, se realizó otra gestión formal mediante carta (ANEXO B) dirigida al ingeniero Mg. Jairo Andrés Casanova Caicedo, para solicitar el acceso a los contenidos temáticos y al registro del número de funcionarios administrativos, docentes y contratistas externos de la universidad, con el fin de iniciar el desarrollo del proyecto.

3 Diseño y desarrollo de los módulos propuestos

En esta actividad se detallan de forma secuencial los pasos seguidos para el diseño y desarrollo del proyecto dentro de los módulos TAU propuestos, integrando aspectos técnicos, herramientas y contenidos necesarios para la creación eficiente y funcional de los cursos de capacitación.

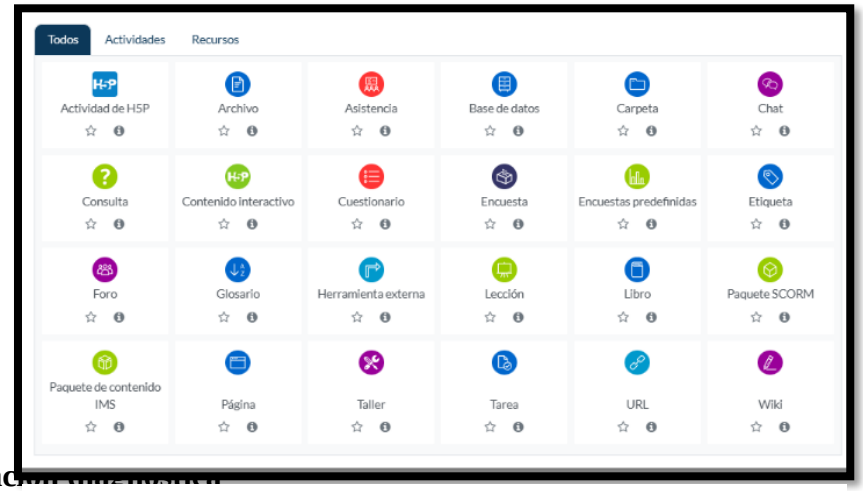
El proceso se llevó a cabo siguiendo las metodologías ADDIE y SCRUM, aplicando pasos fundamentales para el desarrollo previsto. Se consultaron temas de estudio, componentes, funcionalidades y sistemas para la generación de Objetos Virtuales de Aprendizaje (OVAs), seleccionando aquellos que mejor se ajustaron a las necesidades y recursos del proyecto.

Se definió una ruta de enseñanza y aprendizaje estructurada en unidades, concebida como un recorrido formativo. Inicialmente, se aplicó una prueba diagnóstica obligatoria para evaluar el conocimiento previo de los participantes. Luego, se presentó contenido teórico-literario, seguido de materiales y actividades interactivas, culminando con una prueba final que evaluó lo aprendido. Este proceso busca asegurar la sensibilización efectiva del personal en los temas tratados.

Como primer paso, se estudió la plataforma TAU, con especial énfasis en el contenido interactivo H5P, revisando la documentación oficial para comprender de forma óptima las funcionalidades y opciones disponibles para la creación del contenido.

Fig. 9 : Pagina principal módulos

En la imagen presente podemos observar los módulos sin contenido aun, siendo objeto de estudio para la adaptación en la agregación de contenido. Al tener un rol de profesor disponemos de la opción activar modo edición donde se pueden agregar tareas, evaluaciones, contenido interactivo entre otros



Diseño evaluación interactiva

Fig. 10: Tipos de recursos módulo

Posteriormente se procedió con la realización de la prueba diagnóstica en cada uno de los módulos, esta consta de 10 preguntas que mostrara el conocimiento previo del personal administrativo

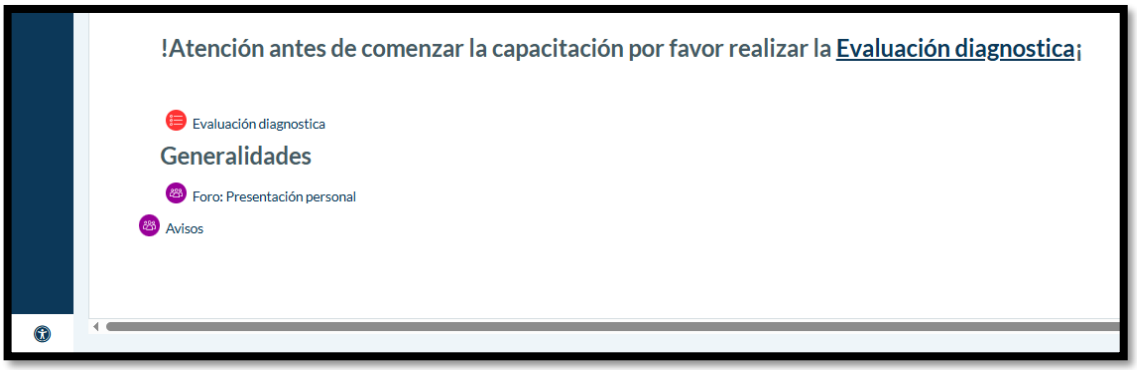


Fig. 11: Evaluación diagnostica modulo tratamiento de datos

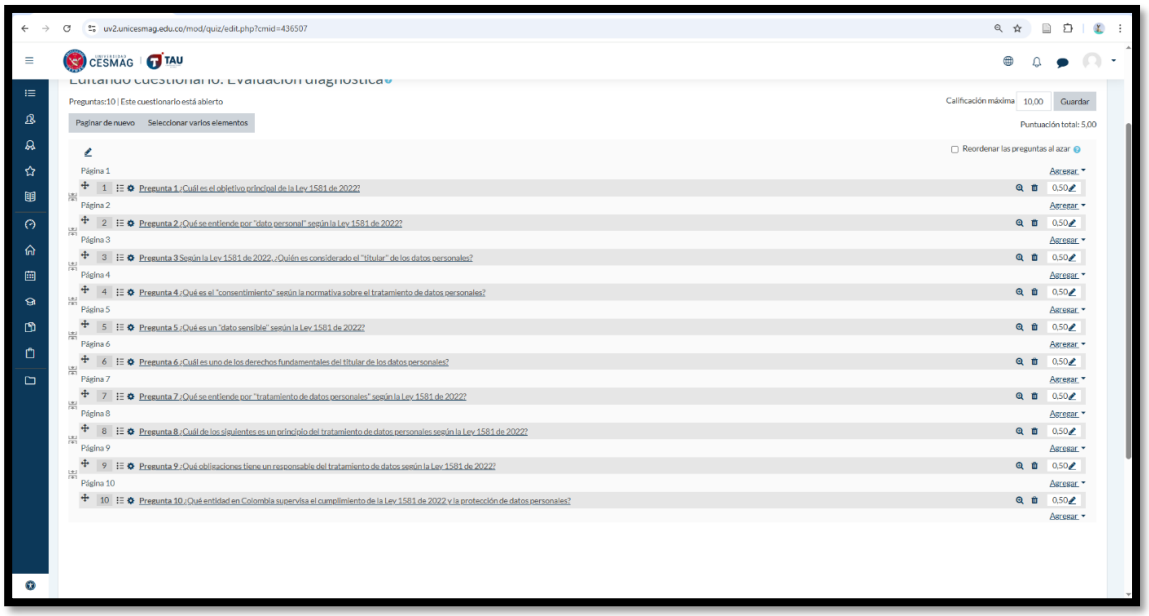


Fig. 12: Preguntas contenidas en la evaluación diagnostica

Organización de unidades

Después de realizar la prueba diagnóstica se procedió a organizar las unidades donde se hizo el análisis de la ruta de aprendizaje para que de esta manera se siga con un el conducto secuencial del aprendizaje.

Fig. 13: Unidades modulo tratamiento de datos

Integración contenido H5P

Se procedió a realizar la agregación de contenido variado tales como infografías, videos, textos, materiales completamente interactivos dentro de cada unidad

Fig. 14: Infografía tratamiento de datos

Fig. 15: Contenido interactivo infografía

Las imágenes anteriormente mostradas se refieren a infografías interactivas

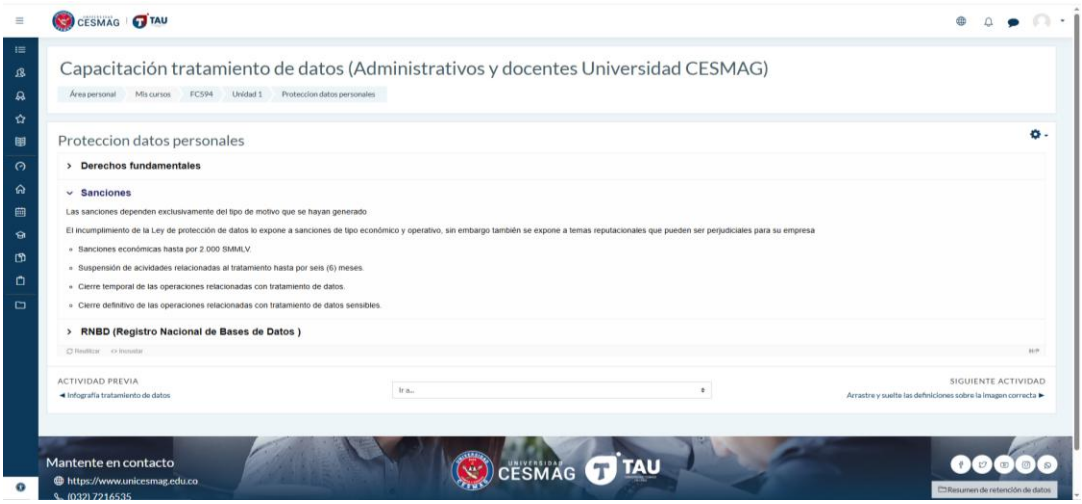


Fig. 16: Contenido por bloques de información

Esta imagen hace referencia a contenido teórico por medio de bloques

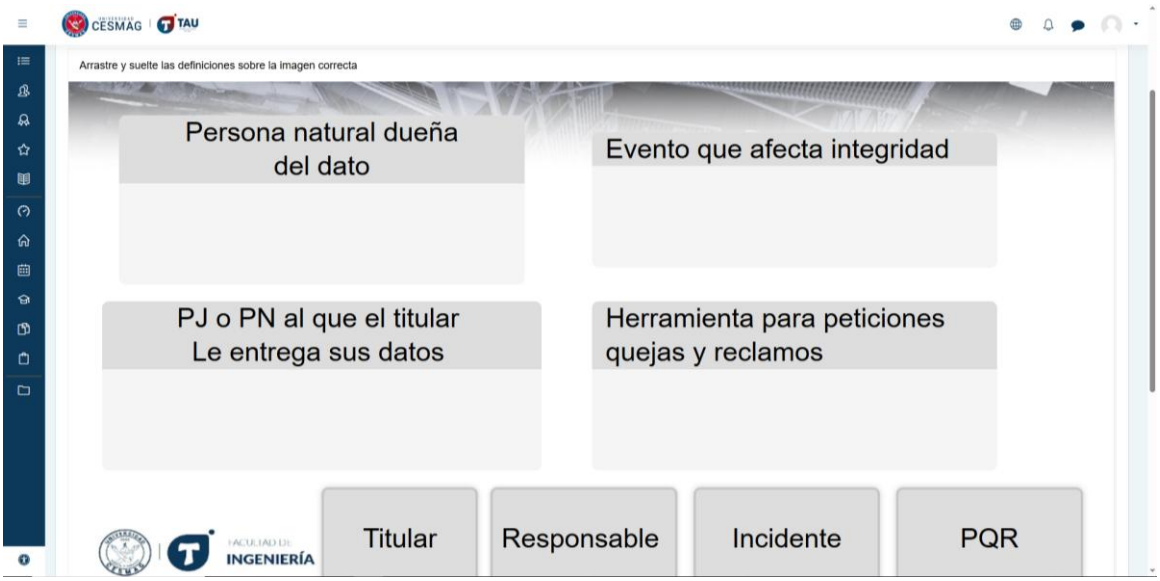


Fig. 17: Juego interactivo de relación

Fig. 18: Muestra relación de juego interactivo

Esta imagen se refiere a un pequeño OVA en el cual se arrastra y suelta las definiciones dándonos un pequeño “Score” por haber completado de manera correcta la anterior tarea

Fig. 19: Presentación interactiva el modulo

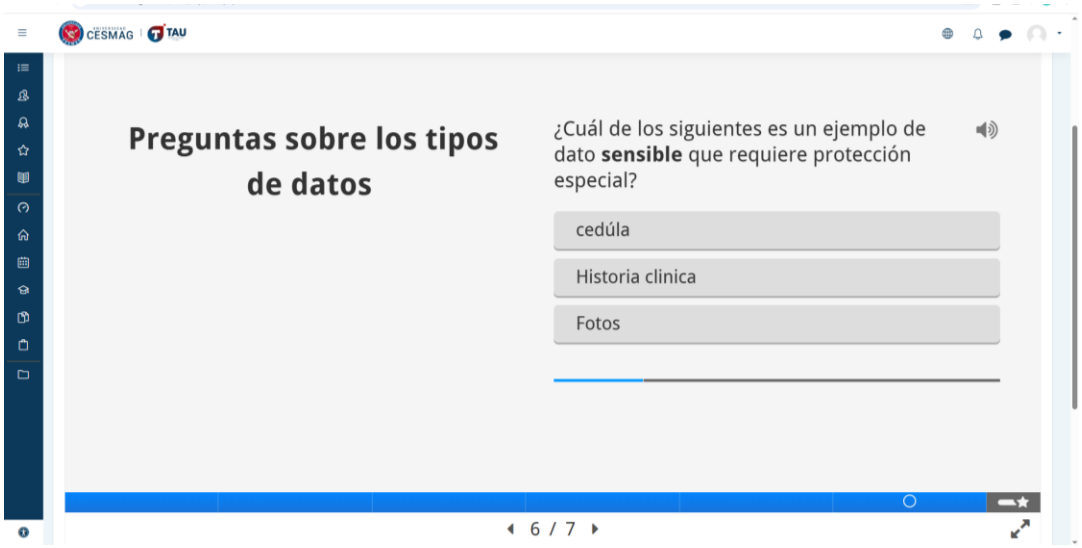


Fig. 20: Interactividad en presentación

Después se agregó una presentación interactiva que también incluye un cuestionario sobre lo anterior presentado

Fig. 21: Segunda infografía interactiva

Para la unidad 2 se incluyó otra infografía interactiva

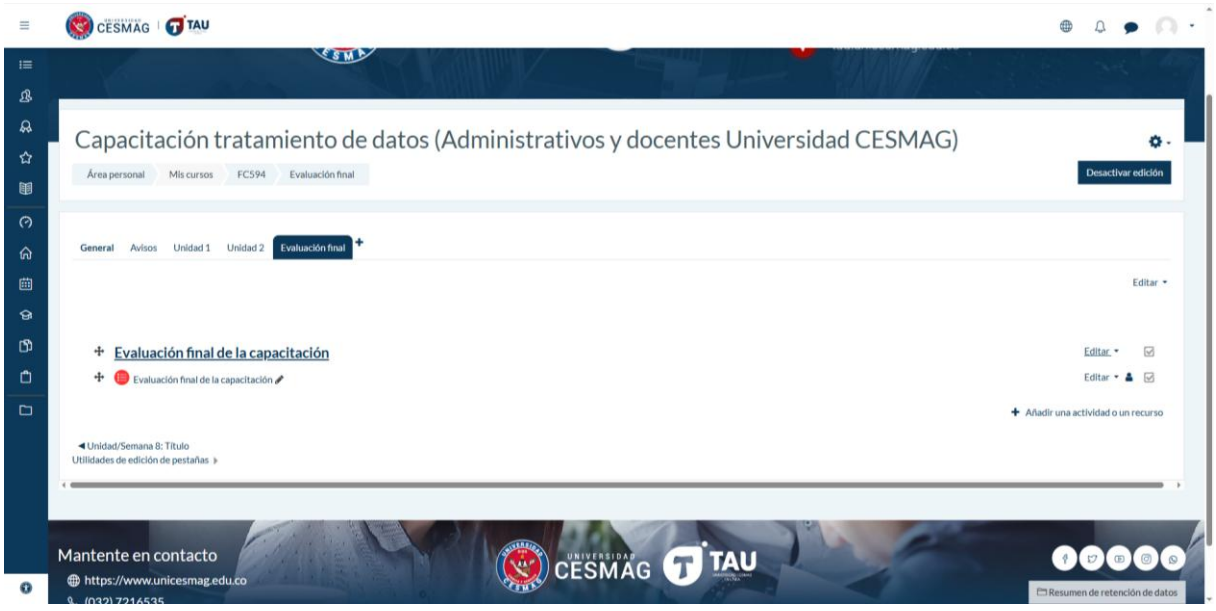


Fig. 22: Evaluación final de modulo

Como ultima unidad se tiene la evaluación final donde registrara la adquisición del conocimiento anteriormente propuesto y al final dando una certificación por la realización del mismo curso de capacitación.

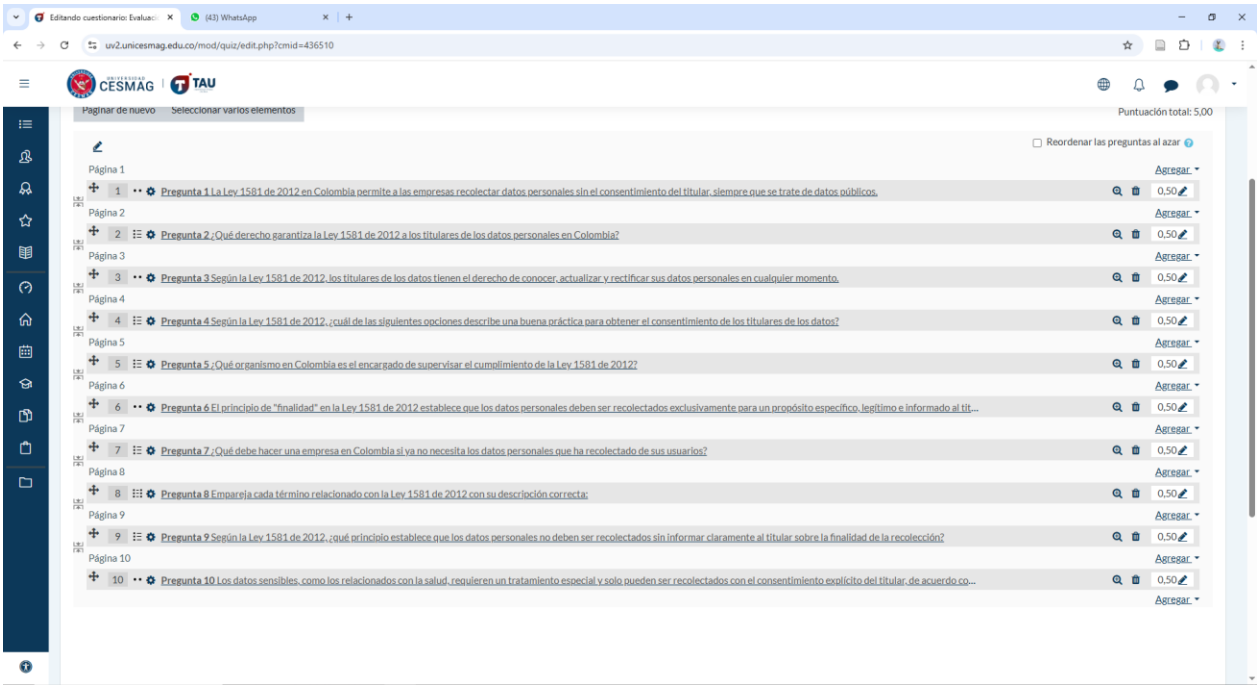


Fig. 23: Preguntas de la evaluación final

C. Evaluación el progreso y aplicación de los conocimientos.

Implementación y evaluación integrando metodología ADDIE y SCRUM

Para el desarrollo de este objetivo se incluyeron las fases de la metodología ADDIE, realizando un plan detallado para la evaluación continua del proceso de enseñanza-aprendizaje, estableciendo mecanismos de medición que permitieran valorar el entendimiento y la aplicación práctica de los conocimientos sobre seguridad de la información. Desde el segundo objetivo específico, se dio inicio a la fase de diseño siguiendo como metodología principal ADDIE, definiendo instrumentos de evaluación diagnóstica, formativa y sumativa. A partir de esta etapa, también se comenzó a implementar la metodología SCRUM para dar mayor agilidad y flexibilidad en la recolección de resultados, el análisis de la información y la implementación de mejoras continuas en las estrategias de evaluación.

La evaluación del progreso se estructuró en varias fases:

- Evaluación diagnóstica inicial, destinada a medir el conocimiento previo de los usuarios en conceptos clave de confidencialidad, integridad y disponibilidad de la información.
- Evaluaciones formativas implementadas a lo largo del desarrollo de los módulos, permitiendo identificar en tiempo real las fortalezas y debilidades en la comprensión de los contenidos y posibilitando ajustes metodológicos rápidos.
- Evaluaciones sumativas finales, orientadas a medir la adquisición y la capacidad de aplicación de los conocimientos al cierre de cada módulo.
- Seguimiento a mediano plazo, mediante encuestas de satisfacción y autoevaluaciones, para identificar cómo los conocimientos adquiridos se aplican en los entornos laborales reales.

El enfoque de trabajo ágil proporcionado por SCRUM permitió realizar evaluaciones periódicas de los resultados a través de "sprints", analizando los datos obtenidos y tomando decisiones de mejora para reforzar aquellas áreas donde los resultados evidenciaron falencias. Así mismo, se garantizó la adaptabilidad de las evaluaciones a las características particulares de los participantes y a las condiciones cambiantes del entorno organizativo.

De esta manera, la evaluación del progreso en el entendimiento y aplicación de los conocimientos sobre seguridad de la información no solo permitió verificar el cumplimiento de los objetivos formativos, sino que también sentó las bases para un proceso de capacitación dinámico, sostenible y orientado a la mejora continua dentro de la Universidad CESMAG.

1 Implementación de los módulos de capacitación en seguridad de la información

La fase de implementación del proyecto se llevó a cabo integrando las metodologías ADDIE y SCRUM, enfocándose en lograr una puesta en marcha ordenada, efectiva y adaptable de los módulos desarrollados en la plataforma TAU. Para ello, se organizaron los materiales, se configuraron las actividades de evaluación, y se preparó la infraestructura necesaria para el acceso de los participantes.

Inicialmente, se realizó la carga y estructuración de los contenidos dentro de los dos módulos habilitados: Seguridad de la Información y Capacitación en Tratamiento de Datos, asegurando que

la secuencia pedagógica planificada durante la fase de diseño fuera respetada. Cada módulo se estructuró bajo la lógica de una ruta de aprendizaje, comenzando con una prueba diagnóstica, seguida de contenidos teóricos, actividades interactivas, casos prácticos, y finalizando con una evaluación de cierre.

La integración de la metodología SCRUM en esta fase permitió que, en cada iteración o "sprint", se hiciera la revisión y mejora continua de los materiales cargados en la plataforma. De esta manera, cualquier retroalimentación proporcionada por los asesores del proyecto o por los primeros usuarios de prueba se incorporaba de forma inmediata, asegurando así un producto final más robusto y alineado a los requerimientos de la Universidad CESMAG.

Durante esta fase también se realizaron pruebas técnicas de funcionamiento, tales como:

- Verificación de enlaces y recursos multimedia.
- Pruebas de navegación y experiencia de usuario (UX) en diferentes dispositivos.
- Validación del correcto registro de notas en las evaluaciones automáticas.
- Accesibilidad para los usuarios con distintos perfiles de ingreso.

Una vez superadas estas pruebas, se procedió a habilitar formalmente el acceso a los módulos a los usuarios designados (administrativos, docentes y contratistas terceros), enviándoles las instrucciones y credenciales de acceso correspondientes. Se brindó además un acompañamiento inicial por parte del desarrollador del proyecto (David Esteban Pantoja) para resolver dudas técnicas de ingreso y navegación.

La fase de implementación culminó con la puesta en marcha oficial del programa de capacitación, lo cual representa un hito importante en la estrategia de fortalecimiento de la cultura de seguridad de la información en la Universidad CESMAG, y que queda integrado de forma sostenible dentro del ecosistema digital institucional.

2 Implementación de los módulos de capacitación en seguridad de la información

La fase de evaluación del proyecto se diseñó siguiendo los lineamientos de las metodologías ADDIE y SCRUM, buscando no solo medir el conocimiento adquirido, sino también retroalimentar continuamente el desarrollo y perfeccionamiento del curso de capacitación en seguridad de la información.

En esta fase, la evaluación se realizó de manera formativa y sumativa, permitiendo verificar el progreso individual de los participantes a lo largo del tiempo, así como la efectividad global del programa de capacitación.

Como primera medida, se aplicó una evaluación diagnóstica al inicio de cada módulo, con el objetivo de identificar el nivel de conocimiento previo de los participantes en torno a conceptos clave como confidencialidad, integridad y disponibilidad de la información. Esto permitió ajustar los enfoques didácticos dentro de cada unidad de aprendizaje en función de las necesidades detectadas.

Durante el desarrollo de los módulos, se aplicaron evaluaciones parciales mediante actividades interactivas, foros de discusión y ejercicios de aplicación práctica. Estas evaluaciones permitieron:

- Identificar de manera temprana dificultades de comprensión.
- Reforzar contenidos que presentaron un mayor grado de dificultad.
- Promover el aprendizaje activo y significativo a través de la retroalimentación inmediata.

Al finalizar cada módulo, se aplicó una evaluación final integradora que abarcó la totalidad de los temas tratados, midiendo no solo la memorización de conceptos, sino su comprensión y aplicación en situaciones reales.

Además, dentro del esquema de trabajo ágil de SCRUM, se realizaron revisiones periódicas (Sprint Reviews) en las cuales se evaluaba:

- La participación y desempeño de los usuarios.
- La efectividad de las estrategias pedagógicas aplicadas.

- La funcionalidad y usabilidad de la plataforma TAU.

Finalmente, se diseñó un sistema de seguimiento post-capacitación, en el cual se recogerán datos de desempeño a mediano plazo mediante encuestas de satisfacción, autoevaluaciones y observaciones laborales, con el objetivo de medir el impacto de la capacitación en la cultura organizacional de la universidad y en las buenas prácticas de seguridad de la información.

La evaluación de esta fase no solo sirvió como mecanismo de medición de resultados, sino que también permitió establecer mejoras continuas para futuras versiones del curso, garantizando así un ciclo permanente de actualización, optimización y crecimiento del programa de capacitación en la Universidad CESMAG.

TABLA III: HU ACTIVIDADES DE CUMPLIMIENTO

Requisito	Rol	Actividad	Estado
HU01: Registro de usuarios	INTERNO	Solicitud de usuarios a capacitar con área de RRHH y oficina de gobernanza de datos	Completado
	INTERNO	Validación de usuarios a capacitar en cruce de tablas y separación por modulo	Completado
	INTERNO	Ingresar a los usuarios de capacitación a la plataforma por medio de un archivo de bloque de datos (CSV)	Completado
HU02: Ejecución de módulos	INTERNO	Verificación de los módulos para despliegue	Completado
	INTERNO	Activación de módulos para el personal administrativo y docente	Completado
HU03: Inicialización de módulos	USUARIO	Navegar y familiarizarse con la interfaz	Completado
	USUARIO	Comprender la línea de enseñanza-aprendizaje ofrecida por el módulo	Completado
HU04: Comienzo capacitación	USUARIO	Realizar evaluación diagnostica para recolectar el conocimiento previo	Completado
	USUARIO	Completar y finalizar UNIDAD 1 donde se encuentran definiciones, conceptos e información básica del aprendizaje	Completado
	USUARIO	Completar y finalizar UNIDAD 2 donde se encuentran actividades interactivas para el fortalecimiento del aprendizaje	Completado
	USUARIO	Completar y finalizar UNIDAD 3 donde se refuerza la enseñanza-aprendizaje	Completado
HU05: Finalización capacitación	USUARIO	Completar y finalizar unidades anteriormente previstas (REQUERIDO)	Completado

	USUARIO	Realizar y completar de manera efectiva y satisfactoria la evaluación final (máximo 2 intentos)	Completado
HU06: Certificación al aprobar capacitación	INTERNO	Diseñar y desarrollar el formulario el cual certificará al usuario que realizo la capacitación	Completado
	INTERNO	Validar expedición de certificado	En progreso
	USUARIO	Expedición de certificado de capacitación terminada	En progreso
HU07: Cierre de curso	INTERNO	Validar que el 100% de los usuarios hayan terminado su modulo de capacitación respectivo	Por iniciar
	INTERNO	Cierre de curso del periodo cursado	Por iniciar
	INTERNO	Evaluar estadísticas del curso para un análisis parcial en la oficina de seguridad de la información, seguridad de los datos y gobierno de datos	Por iniciar

V. ANÁLISIS DE RESULTADOS

El proyecto evidenció mejoras sustanciales en la implementación de procesos de capacitación en seguridad de la información y protección de datos personales, enmarcados en los lineamientos de la norma ISO/IEC 27001 y la Ley 1581 de 2012. Estas normativas proporcionaron una base técnica y normativa para el diseño de contenidos y metodologías alineadas con buenas prácticas internacionales, asegurando la confidencialidad, integridad y disponibilidad de la información en el entorno institucional universitario.

Uno de los principales indicadores de impacto fue la tasa de cumplimiento en la capacitación del personal administrativo y docente participante, evidenciando un alto nivel de cobertura y adherencia a los módulos. Este dato fue validado a partir de los registros en la plataforma virtual, lo que permitió una trazabilidad completa del proceso formativo.

En cuanto al nivel de conocimiento y sensibilización reflejó una apropiación efectiva de los contenidos relacionados con gestión de riesgos, clasificación de la información, uso seguro de tecnologías y normativas aplicables. Además, se implementaron autoevaluaciones y simulaciones prácticas que reforzaron el aprendizaje contextualizado.

	F	G	H	I	J	K	L	M	N
1	Nº Cédul	Grado	Lugar de Expedici	Nombre Empleado	Cargo Especifico	Vicerrectoría y/o Rectoria	Correo Institucional	Nota apro	Grado-CRUZE
2	1085336269	Auxiliar II	Pasto (N)	Arteaga Florez Deivy Steven	Auxiliar Infraestructura Tecnologica	Direccion Administrativa	dsarteaga@unicesmag.edu.co	4.5	Auxiliar II
3	1032479967	Auxiliar II	Bogotá D.C	Bernal Muñoz German Camilo	Auxiliar de Medios Educativos	Vicerrectoria Financiera y de Desarrollo Institucional	gcbernal@unicesmag.edu.co	4.5	Auxiliar II
4	59821754	Auxiliar T	Pasto (N)	Betancourth Minganquer Maria Cristina	Auxiliar de Gestion Documental	Vicerrectoria Academica	mcbetancourth@unicesmag.edu.co	5.0	Auxiliar T
5	1085321726	Auxiliar II	Pasto (N)	Bolaños Cabeza Jennifer Andrea	Auxiliar Administrativo	Direccion Administrativa	jabolanos@unicesmag.edu.co	4.5	Auxiliar II
7	36954901	Auxiliar II	Pasto (N)	Delgado Montilla Vicki Zoraida	Auxiliar de Gestion Documental	Vicerrectoria Academica	vzdelgado@unicesmag.edu.co	4.5	Auxiliar II
8	1007254236	Auxiliar II	La Florida	Enriquez Pastas Brayan Jair	Auxiliar de Infraestructura Tecnologica	Direccion Administrativa	bjenriquez@unicesmag.edu.co	5.0	Auxiliar II
9	1085285267	Auxiliar II	Pasto (N)	Gelpud Chachinoy Jhonny Mauricio	Auxiliar de Medios Educativos	Vicerrectoria Financiera y de Desarrollo Institucional	jmgelpud@unicesmag.edu.co	4.5	Auxiliar II
10	59310452	Secretario G	Pasto (N)	Gonzalez Lopez Jully Pauliny	Secretario(a) General	Rectoria	jpgonzalez@unicesmag.edu.co	4.5	Secretario General
13	94509957	Auxiliar II	Cali (V)	Insuasti Quevedo William Alexander	Auxiliar de Medios Educativos	Vicerrectoria Financiera y de Desarrollo Institucional	wainsuasti@unicesmag.edu.co	5.0	Auxiliar II
15	1085327562	Auxiliar II	Pasto (N)	Leon Realpe Angie Tatiana	Auxiliar Administrativo	Vicerrectoria Academica	atleon@unicesmag.edu.co	4.5	Auxiliar II
16	1233191460	Auxiliar II	Pasto (N)	Mafla Delgado David Yobani	Auxiliar de Gestion Documental	Vicerrectoria Academica	dymafla@unicesmag.edu.co	4.5	Auxiliar II
18	1085307322	Auxiliar II	Pasto (N)	Muñoz Pastas Daissy Lorena	Auxiliar de Infraestructura Tecnologica	Direccion Administrativa	dlmunoz@unicesmag.edu.co	5.0	Auxiliar II
20	1061793560	Auxiliar II	Popayan	Narvaez Vargas Lucely	Auxiliar de Piscina	Vicerrectoria Financiera y de Desarrollo Institucional	lnarvaez@unicesmag.edu.co	4.5	Auxiliar II
23	1085346817	Auxiliar II	Pasto (N)	Oviedo Otaya John Erik	Auxiliar Administrativo	Direccion Administrativa	jeoviedo@unicesmag.edu.co	4.5	Auxiliar II
24	1131084770	Auxiliar II	Nariño (N)	Paz Espinoza Jesus Alberto	Auxiliar de Mantenimiento	Direccion Administrativa	japaz@unicesmag.edu.co	5.0	Auxiliar II
26	27081972	Auxiliar II	Pasto (N)	Rivera Ceballos Laura Isabel	Auxiliar de Gestion Documental	Vicerrectoria Academica	lirivera@unicesmag.edu.co	4.5	Auxiliar II

Fig. 24: Tasa de cumplimiento, nivel de conocimiento y sensibilización

Respecto a la satisfacción del usuario, se aplicaron encuestas estructuradas al finalizar cada módulo, las cuales revelaron un alto grado de aceptación en ítems relacionados con claridad de los contenidos, utilidad percibida, aplicabilidad en el contexto laboral y funcionalidad de la plataforma

e-learning. Los comentarios cualitativos destacaron la flexibilidad de los tiempos, la pertinencia del material y la calidad de los recursos audiovisuales.

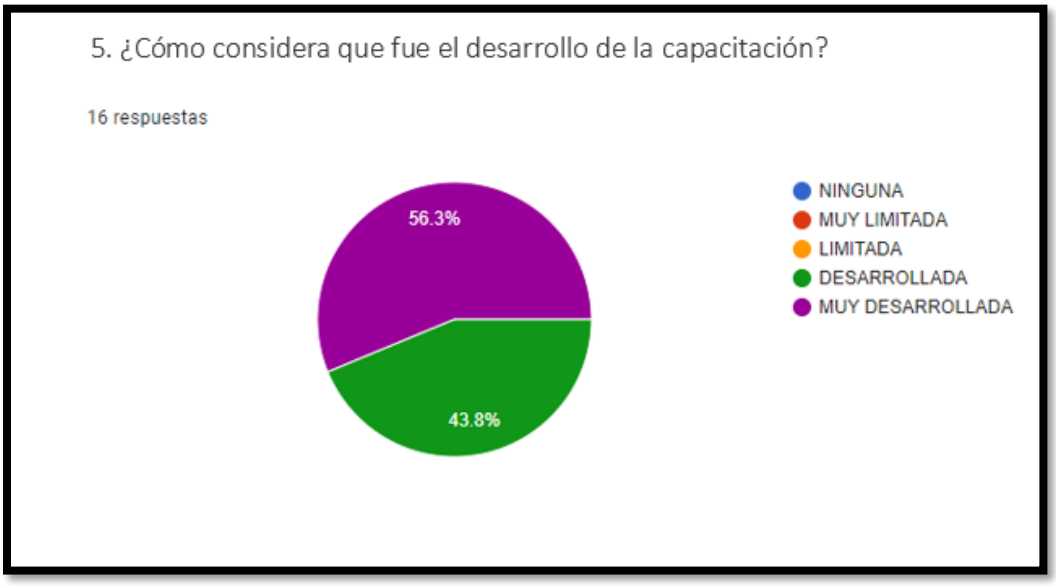


Fig. 25: Satisfacción del usuario

La estrategia metodológica fue optimizada a partir de estos datos. Se ajustó la intensidad horaria y el enfoque de cada módulo según el perfil de los participantes (docentes, administrativos, personal de apoyo), mejorando así la pertinencia y eficacia del proceso. Asimismo, la adopción de herramientas tecnológicas permitió reducir el tiempo promedio de capacitación, sin comprometer la calidad de la formación.

Finalmente, se observó un fortalecimiento tangible de la cultura organizacional en torno a la seguridad de la información. Esto se manifestó en una mayor proactividad de los usuarios frente a la protección de datos, en la identificación de riesgos cotidianos, y en la adopción voluntaria

prácticas seguras, lo que constituye un avance clave hacia la sostenibilidad del Sistema de Gestión de Seguridad de la Información (SGSI) institucional.

Fig. 26: Unidad de servicios psicológicos Leopoldo Mandic

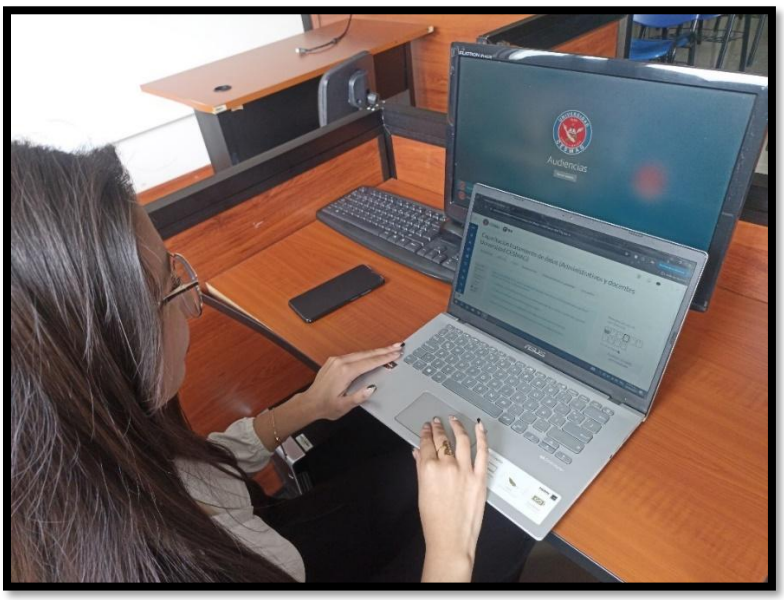


Fig. 27: Consultorios Jurídicos

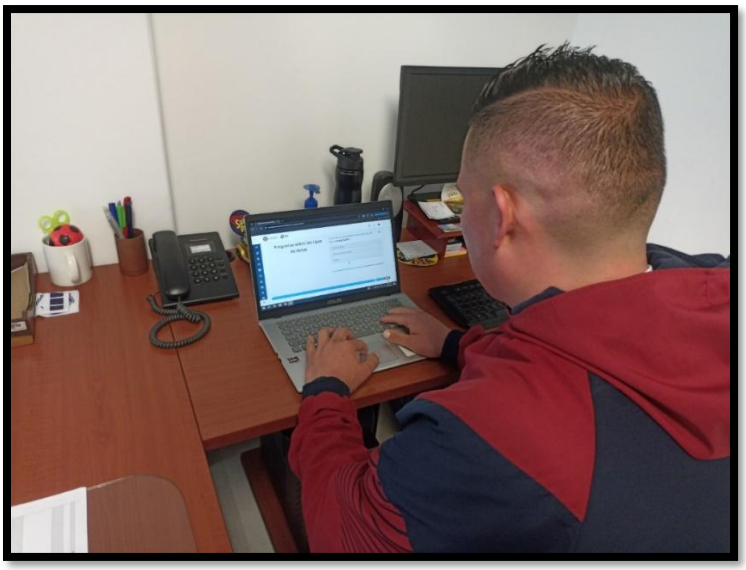


Fig. 28: Área de deporte y cultura

Además, la implementación del proyecto trajo consigo beneficios económicos tangibles. Uno de los más significativos fue la reducción de costos asociados al seguro contratado por la universidad en materia de seguridad de la información. Gracias a la disminución del riesgo humano mediante la capacitación del personal administrativo y docente, se redujo la probabilidad de errores humanos que podrían desencadenar incidentes costosos o sanciones legales. Esta reducción del riesgo fue reconocida por la aseguradora, lo cual se tradujo en primas más bajas y condiciones más favorables para la institución.

CONCLUSIONES

En este tipo de proyectos, es importante generar una caracterización y diagnóstico precisos sobre los niveles de conocimiento del personal administrativo respecto a la temática a implementar. En la Universidad CESMAG, este insumo inicial permitió establecer estrategias y recursos tecnológicos de capacitación eficientes, alineados con normativas como la ISO/IEC 27001 y la Ley 1581 de 2012.

Existen diversas metodologías para el desarrollo de procesos de enseñanza-aprendizaje, así como múltiples recursos tecnológicos, como los LMS. Sin embargo, Moodle sigue siendo una herramienta muy eficiente para la capacitación, ya que permite reducir tiempos de formación, ofrecer una amplia variedad de recursos, y gestionar la asistencia, participación y evaluación del personal capacitado. En este proyecto se integró TAU, una plataforma propia de la universidad basada en Moodle.

La implementación de herramientas digitales y los módulos de capacitación evidenciaron la viabilidad de escalar este tipo de proyectos a otras áreas, o incluso a estudiantes de las diferentes facultades, consolidando así una estrategia institucional de ciberseguridad más integral.

RECOMENDACIONES

Es fundamental que la institución mantenga un plan de formación periódico en seguridad de la información, con contenidos actualizados conforme a cambios normativos, tecnológicos y de amenazas emergentes. Esto asegurará que el personal se mantenga preparado y consciente de sus responsabilidades.

Incorporar módulos de formación sobre protección de datos y buenas prácticas digitales en los programas de inducción para nuevo personal (docente y administrativo) garantizará la alineación temprana con las políticas institucionales desde el primer día de vinculación laboral.

Se recomienda implementar o mejorar los mecanismos de comunicación para que los usuarios puedan reportar incidentes de seguridad de manera fácil, rápida y segura. Además, se deben realizar simulacros periódicos que refuercen la capacidad de respuesta institucional.

Es importante establecer indicadores de desempeño y herramientas de seguimiento que permitan medir no solo la asistencia y aprobación de los cursos, sino también la aplicación práctica del conocimiento en el entorno laboral.

BIBLIOGRAFÍA

[1] «¿Qué es la seguridad de la información (InfoSec)? | Seguridad de Microsoft». Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-information-security-infosec

[2] «NQA-ISO-27001-Guia-de-implantacion.pdf». Accedido: 31 de marzo de 2024. [En línea]. Disponible en: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

[3] «¿Qué es el aprendizaje en línea?», Metropolitan International University. Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://metrouni.us/que-es-el-aprendizaje-en-linea/

[4] S. J. H. Otalora, «CULTURA EN SEGURIDAD DE LA INFORMACIÓN».

[5] G. Solutions, «¿Qué es la norma ISO 27001 y para qué sirve?», GlobalSuite Solutions. Accedido: 31 de marzo de 2024. [En línea]. Disponible en: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

[6] A. R. A. J y J. J. C. M, «XX Encuesta Nacional de Seguridad Informática»:, *Rev. Sist.*, n.º 155, Art. n.º 155, jun. 2020, doi: 10.29236/sistemas.n155a4.

[7] «https://6327868.hs-sites.com/null». Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://6327868.hs-sites.com/null

[8] «Administración de la seguridad de la información», UNLA. Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://www.unla.mx/blogunla/administracion-de-la-seguridad-de-la-informacion

[9] «liziyoTFM0617-ANEXO E.pdf». Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://openaccess.uoc.edu/bitstream/10609/64545/7/liziyoTFM0617-ANEXO%20E.pdf

[10] «Plataformas educativas digitales: tipos y ventajas que aportan». Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://smowl.net/es/blog/plataformas-educativas-digitales/

[11] «Norma ISO 27001», Norma ISO 27001. Accedido: 31 de marzo de 2024. [En línea]. Disponible en: https://normaiso27001.es/

[12] W. I. D. A. Castrillón, «Biblioteca», Universidad CESMAG. Accedido: 6 de abril de 2024. [En línea]. Disponible en: https://www.unicesmag.edu.co/categoria/biblioteca/

[13] «queesmoodle.pdf». Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://www.uls.edu.sv/pdf/manuales_moodle/queesmoodle.pdf

[14] «¿Qué es el software de código abierto? | IBM». Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/open-source

[15] W. I. D. A. Castrillón, «Principal», Universidad CESMAG. Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://www.unicesmag.edu.co

[16] «Seguridad de la Información Estándar ISO 27001», EUD Academy. Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://eud.academy/producto/seguridad-de-la-informacion-estandar-iso-27001/

[17] «Obtener los fundamentos de la ciberseguridad correcta», ISACA. Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/getting-the-basics-of-cybersecurity-right

[18] «FTC Safeguards Rule: What Your Business Needs to Know», Federal Trade Commission. Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

[19] «About ENISA - The European Union Agency for Cybersecurity», ENISA. Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://www.enisa.europa.eu/about-enisa

[20] M. O. Díaz y P. E. S. Rangel, «Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia», *Rev. Crim.*, vol. 62, n.º 2, Art. n.º 2, jul. 2020, doi: 10.47741/17943108.168.

[21] G. A. Jiménez-Almeira y D. E. López, «Ciberseguridad y Seguridad Integral: un análisis».

[22] «866_stamped.pdf».

[23] A. Casanova, «Modelo de Evaluación Cuantitativa de Riesgos en Seguridad Informática», *INGEUAN - Tend. EN Ing.*, vol. 6, n.º 11, Art. n.º 11, 2015, Accedido: 29 de abril de 2024. [En línea]. Disponible en: https://revistas.uan.edu.co/index.php/ingeuan/article/view/414

[24] J. J. V. Romero, R. A. J. Toledo, y Á. R. T. Burbano, «Evaluación de la seguridad de la información en la Clí-nica Hispanoamérica de Pasto, basada en la norma ISO/IEC 27001», *Boletí-n Inf. CEI*, vol. 3, n.º 2, Art. n.º 2, oct. 2016.

[25] M. Gualda, «La Seguridad de la Información», Tecon. Accedido: 19 de mayo de 2024. [En línea]. Disponible en: https://www.tecon.es/la-seguridad-de-la-informacion/

[26] «¿Qué es la seguridad de datos? Definición y descripción general de la seguridad de datos | IBM». Accedido: 19 de mayo de 2024. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/data-security

[27] «¿Qué es la tríada CIA y por qué es importante? | Fortinet». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

[28] O. B. Morales, «Comité de ética en investigación», Sitio Web del Comité de ética en investigación. Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.incmnsz.mx/opencms/contenido/investigacion/

[29] «Confidencialidad en seguridad informática, ¿en qué consiste?», UNIR. Accedido: 19 de mayo de 2024. [En línea]. Disponible en: https://www.unir.net/ingenieria/revista/confidencialidad-seguridad-informatica/

[30] «Cifrado de datos y cómo hacerlo». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/encryption

[31] «¿Qué es Access Control? | Seguridad de Microsoft». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-access-control

[32] «¿Qué es el control de acceso? | Autorización vs. autenticación». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.cloudflare.com/es-es/learning/access-management/what-is-access-control/

[33] «IBM Documentation». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.ibm.com/docs/es/i/7.3?topic=security-virtual-private-networking

[34] «Integridad de la información en seguridad informática | Blog HostDime Latinoamérica, servidores dedicados». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.hostdime.la/blog/integridad-de-la-informacion-en-seguridad-informatica/

[35] «Sistema de confianza _ AcademiaLab». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://academia-lab.com/enciclopedia/sistema-de-confianza/

[36] «Disponibilidad en seguridad informática, ¿qué quiere decir?», UNIR. Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/

[37] «¿Qué es un ataque cibernético? | IBM». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/cyber-attack

[38] «¿Qué es la Ingeniería Social? | IBM». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/social-engineering

[39] «Ataque de denegación de servicio | Fundamentos | Cloudflare». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

[40] Eneko, «¿Cuáles son los riesgos al usar un software sin licencia o software pirata?», Vadillo Asesores. Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.grupovadillo.com/cuales-son-los-riesgos-al-usar-un-software-sin-licencia-o-software-pirata/

[41] «Ciberdelincuencia». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia

[42] «¿Qué es una vulnerabilidad informática y cómo protegerse?» Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.deltaprotect.com/blog/vulnerabilidad-informatica

[43] «¿Qué son los controles de seguridad? | IBM». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/security-controls

[44] «articles-5482_G2_Politica_General.pdf». Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

[45] «¿Qué es un firewall?», Cisco. Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

[46] «¿Es lo mismo antimalware y protección antivirus?», Malwarebytes. Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://es.malwarebytes.com/antivirus/

[47] «¿Qué es la autenticación multifactor? - Explicación de la autenticación multifactor - AWS», Amazon Web Services, Inc. Accedido: 14 de abril de 2024. [En línea]. Disponible en: https://aws.amazon.com/es/what-is/mfa/

[48] «2021AnaPrieto.pdf». Accedido: 27 de abril de 2024. [En línea]. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/37852/2021AnaPrieto.pdf?sequence=1&isAllowed=y

[49] «NTP ISO 27001. Origen y evolución. - ISOTools Perú». Accedido: 27 de abril de 2024. [En línea]. Disponible en: https://pe.isotools.us/iso-27001/

[50] «SGSI». Accedido: 27 de abril de 2024. [En línea]. Disponible en: https://www.iso27000.es/sgsi.html

[51] «ISO 27001 : Origen y evolución». Accedido: 27 de abril de 2024. [En línea]. Disponible en: https://pe.isotools.us/iso-27001-origen-y-evolucion/

[52] «¿Qué significado le damos a “Sensibilizar”? – Acope». Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://acope.es/que-hace-nuestro-equipo-de-sensibilizacion/

[53] «PlanDeSensibilizaciónen_Seguridad_de_la_Informacion.pdf». Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://archivo.minambiente.gov.co/images/tecnologias-de-la-informacion-y-comunicacion/pdf/PlanDeSensibilizaci%C3%B3nen_Seguridad_de_la_Informacion.pdf

[54] «Desarrollar Cultura en Seguridad».

[55] «articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf». Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

[56] «Herramientas de comunicación (sincrónica y asincrónica) | Herramientas para el tutor virtual». Accedido: 1 de mayo de 2024. [En línea]. Disponible en: http://tutoriales.grial.eu/herramientastutor2013/herramientas_de_comunicacin_sincrnica_y_asincrnica.html

[57] «¿En qué consiste un LMS y cómo funciona?» Accedido: 1 de mayo de 2024. [En línea]. Disponible en: https://www.anahuac.mx/mexico/noticias/En-que-consiste-un-LMS-y-como-funciona

[58] «Acerca de Moodle - MoodleDocs». Accedido: 1 de mayo de 2024. [En línea]. Disponible en: https://docs.moodle.org/all/es/Acerca_de_Moodle

[59] «¿Qué es la plataforma Moodle y para qué sirve?», Máxima Formación. Accedido: 1 de mayo de 2024. [En línea]. Disponible en: https://www.maximaformacion.es/blog-teleformacion/que-es-la-plataforma-moodle-y-para-que-sirve-2/

[60] «Método Científico - Concepto, pasos, características y ejemplos». Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://concepto.de/metodo-cientifico/

[61] «Formularios de Google: Generador de formularios en línea | Google Workspace». Accedido: 4 de mayo de 2024. [En línea]. Disponible en: https://www.facebook.com/GoogleDocs/

[62] «Salario para Ingeniero En Sistemas en Colombia - Salario Medio», Talent.com. Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://co.talent.com/salary

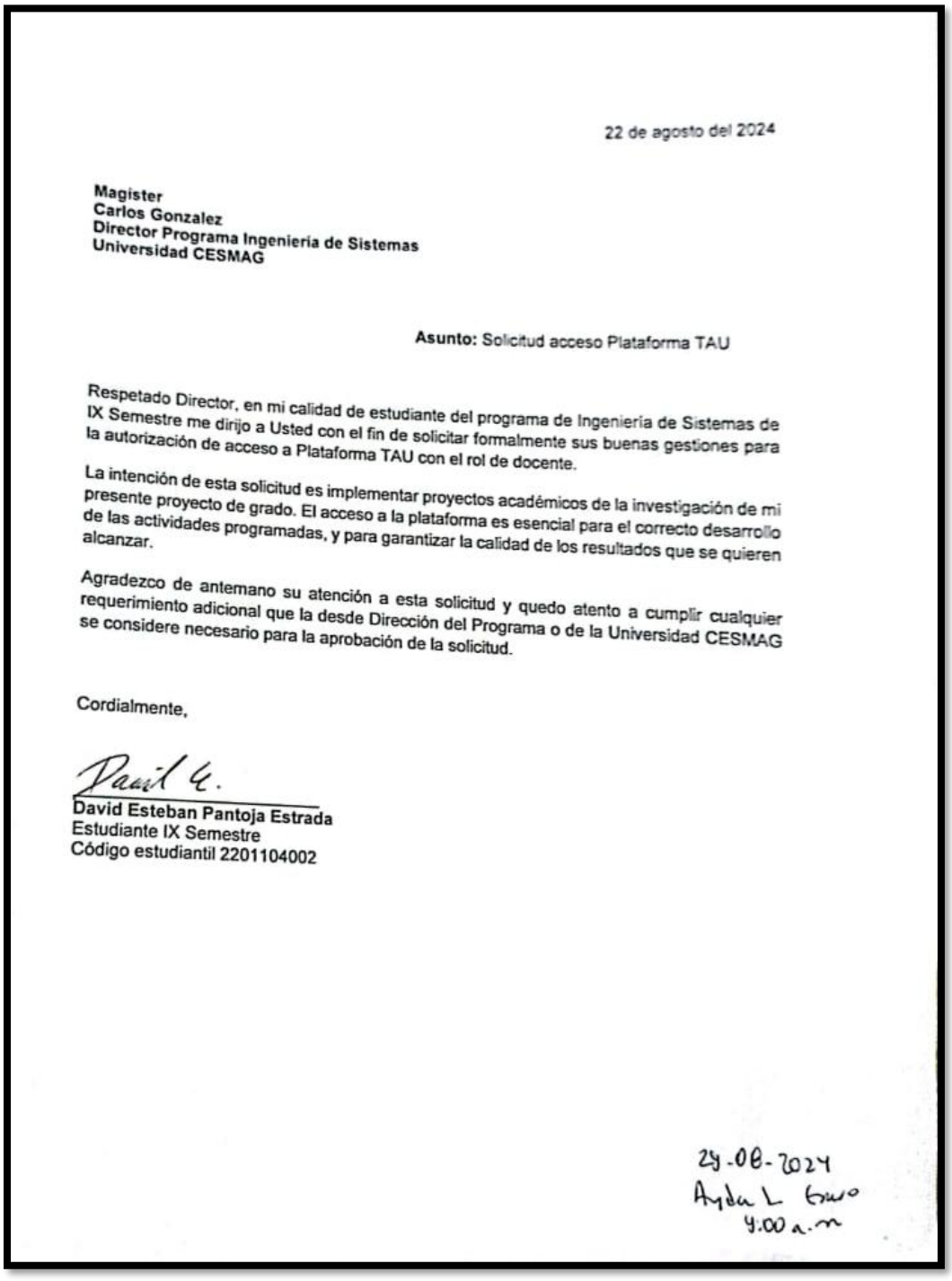
[63] «Catedráticos, les contamos por qué podría aumentar su salario dos veces este 2024 | Más Colombia». Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://mascolombia.com/catedraticos-tendran-un-doble-aumento-del-salario-en-2024/

[64] C. H. SAS, «ColombiaHosting: Hosting y Dominios», https://www.colombiahosting.com.co. Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://www.colombiahosting.com.co

[65] «Registro de Dominios Colombia», Latinoamérica Hosting Colombia. Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://www.latinoamericahosting.com.co/dominios/

[66] «Hogar | Internet Para Todos». Accedido: 13 de abril de 2024. [En línea]. Disponible en: https://www.sistemaspalacios.com/hogar/

ANEXOS



22 de agosto del 2024

Magister
Carlos Gonzalez
Director Programa Ingeniería de Sistemas
Universidad CESMAG

Asunto: Solicitud acceso Plataforma TAU

Respetado Director, en mi calidad de estudiante del programa de Ingeniería de Sistemas de IX Semestre me dirijo a Usted con el fin de solicitar formalmente sus buenas gestiones para la autorización de acceso a Plataforma TAU con el rol de docente.

La intención de esta solicitud es implementar proyectos académicos de la investigación de mi presente proyecto de grado. El acceso a la plataforma es esencial para el correcto desarrollo de las actividades programadas, y para garantizar la calidad de los resultados que se quieren alcanzar.

Agradezco de antemano su atención a esta solicitud y quedo atento a cumplir cualquier requerimiento adicional que la desde Dirección del Programa o de la Universidad CESMAG se considere necesario para la aprobación de la solicitud.

Cordialmente,

David E.

David Esteban Pantoja Estrada
Estudiante IX Semestre
Código estudiantil 2201104002

29-08-2024
Ayda L Erazo
4.00 a.m

ANEXOS 1: SOLICITUD ACCESO PLATAFORMA TAU

22 de agosto del 2024

Ingeniero
Jairo Andrés Casanova
Seguridad de la Información y gobierno de datos
Universidad CESMAG

Asunto: Proyecto de Grado - Solicitud de información

Respetado Ingeniero, en mi calidad de estudiante del programa de Ingeniería de Sistemas de IX Semestre me dirijo a Usted con el fin de solicitar formalmente acompañamiento sobre la información referente a los contenidos que se presentaran en plataforma, así como acceso a los datos sobre el número de funcionarios y docentes de la Universidad.

La intención de esta solicitud es implementar el módulo en TAU del proyecto académico de la investigación. El acceso a esta información es esencial para el correcto desarrollo de las actividades programadas y para garantizar la calidad de los resultados que se pretenden alcanzar.

Agradezco toda la colaboración hasta ahora brindada y quedo atento a cumplir con cualquier requerimiento adicional que Usted o la Universidad CESMAG consideren necesarios para la aprobación de la solicitud.

Atento a su pronta y positiva respuesta.

Cordialmente,

David E.

David Esteban Pantoja Estrada
Estudiante IX Semestre
Código estudiantil 2201104002

Recibí
Andrés Casanova
8/27/2024

ANEXOS 2: SOLICITUD DATOS PERSONAL A CAPACITAR

ANEXOS 3: POSTER PARTICIPACIÓN CONGRESO INTERNACIONAL DE INNOVACIÓN SOCIAL

ANEXOS 4: CERTIFICADO ASISTENCIA CONGRESO INTERNACIONAL DE INNOVACIÓN SOCIAL

ANEXOS 5: CERTIFICADO PONENTE CONGRESO INTERNACIONAL DE INNOVACIÓN SOCIAL

Formulario sobre conocimientos en Seguridad de la Información

Objetivo: El siguiente formulario busca recopilar información pertinente sobre su conocimiento en temas básicos de Seguridad de la información.

Las respuestas que aquí registre serán manejadas conforme a nuestras políticas de tratamiento de datos personales, y serán custodiados de manera segura con propósitos netamente académicos de proyecto de grado y de sensibilización en la seguridad de la información. Nuestra política se encuentra publicada en el sitio WEB, el cual puede visitar en el link adjunto (Véase la política aquí). Si está de acuerdo por favor agradezco confirmar con un SI.

Gracias por su colaboración en el diligenciamiento del formulario

depantoja.5964@unicesmag.edu.co Cambiar de cuenta

No compartido

* Indica que la pregunta es obligatoria

Nombres y apellidos *

Tu respuesta

¿Desea continuar? *

- ◯ Sí
- ◯ No

Siguiente

Borrar formulario

Nunca envíes contraseñas a través de Formularios de Google.

Este formulario se creó en Universidad Cesmag.
¿Parece sospechoso este formulario? Informe

Sección de preguntas

1) Ana recibe un correo de su "banco" solicitándole que actualice sus datos personales a través de un enlace. Al hacer clic, la página parece idéntica al sitio oficial. ¿Qué tipo de ataque está enfrentando Ana? * 1 punto

- ◯ Phishing
- ◯ Ransomware
- ◯ Denegación de Servicio (DoS)
- ◯ Ingeniería Social

2) Luis nota que su computadora está más lenta de lo normal y sus archivos empiezan a desaparecer. Después de un análisis, se da cuenta de que un programa malicioso está atacando su sistema. ¿Qué tipo de amenaza podría estar afectando a su equipo? * 1 punto

- ◯ Malware
- ◯ Phishing
- ◯ Spam
- ◯ Denegación de Servicio (DoS

3) En una empresa, se recomienda a los empleados cambiar sus contraseñas periódicamente para mejorar la seguridad. Si las políticas de seguridad exigen que las contraseñas se cambien cada cierto tiempo, ¿Cuál es el intervalo de tiempo más seguro recomendado por la mayoría de los expertos en ciberseguridad? * 1 punto

- ◯ Cada 3 meses
- ◯ Cada 2 años
- ◯ Cada 6 meses

4) Una empresa ha implementado políticas de acceso restringido a ciertos archivos confidenciales. Si un empleado intenta acceder a un archivo sin los permisos adecuados, el sistema lo bloquea. ¿Qué principio de seguridad está protegiendo la información en este caso? * 1 punto

- ◯ Disponibilidad
- ◯ Confidencialidad
- ◯ Integridad
- ◯ Autenticación

5) Marta está a punto de enviar un archivo confidencial a un cliente, pero su jefe le pide que antes lo codifique para protegerlo en caso de que sea interceptado. ¿Qué método debería utilizar Marta? * 1 punto

- ◯ Compresión de archivos
- ◯ Filtro de contenido
- ◯ Encriptación
- ◯ Eliminación segura

6) Julia trabaja en recursos humanos y debe acceder a datos confidenciales de los empleados. La empresa le pide que cambie su contraseña cada 90 días y que use una combinación de letras, números y símbolos. ¿Qué está implementando la empresa? * 1 punto

- ◯ Autenticación Multifactor
- ◯ Política de contraseñas seguras
- ◯ Backup de datos
- ◯ Cifrado de archivos

7) La política de respaldo de datos de una empresa establece que las copias de seguridad de los sistemas críticos deben realizarse de manera frecuente. Según las mejores prácticas, ¿con qué frecuencia deben realizarse los respaldos de un sistema crítico para minimizar la pérdida de datos en caso de un fallo? * 1 punto

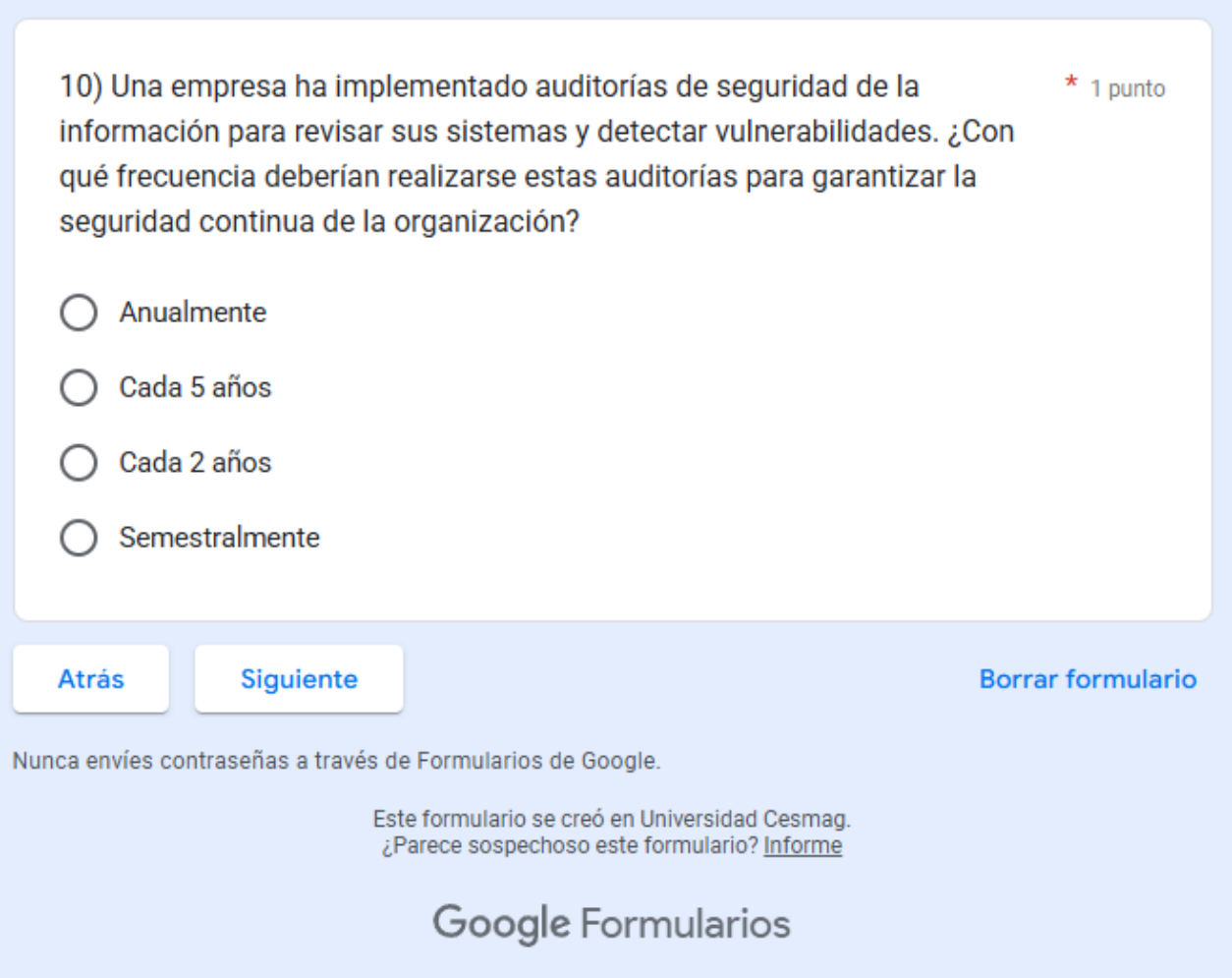
- ◯ Diariamente
- ◯ Semanalmente
- ◯ Quincenalmente
- ◯ Mensualmente

8) En una empresa, las actualizaciones de seguridad son esenciales para proteger los sistemas de nuevas vulnerabilidades. ¿Con qué frecuencia se recomienda instalar actualizaciones de seguridad críticas en los sistemas operativos y software de la empresa? * 1 punto

- ◯ Trimestralmente
- ◯ Tan pronto como estén disponibles
- ◯ Quincenalmente
- ◯ Mensualmente

9) Pablo intenta ingresar al sistema de gestión de la empresa, pero se le solicita que además de su contraseña, ingrese un código que le llega a su teléfono. ¿Qué método de seguridad está utilizando su empresa? * 1 punto

- ◯ Cifrado
- ◯ Autenticación multifactor (MFA)
- ◯ Política de contraseñas
- ◯ Certificado digital



ANEXOS 6: FORMULARIO SEGURIDAD DE LA INFORMACIÓN

Formulario sobre conocimientos en Seguridad de la Información

Objetivo: El siguiente formulario busca recopilar información pertinente sobre su conocimiento en temas básicos de Seguridad de la información.

Las respuestas que aquí registre serán manejadas conforme a nuestras políticas de tratamiento de datos personales, y serán custodiados de manera segura con propósitos netamente académicos de proyecto de grado y de sensibilización en la seguridad de la información. Nuestra política se encuentra publicada en el sitio WEB, el cual puede visitar en el link adjunto (Véase la política aquí). Si está de acuerdo por favor agradezco confirmar con un SI.

Gracias por su colaboración en el diligenciamiento del formulario

* Indica que la pregunta es obligatoria

Correo electrónico *

☐ Registrar **depantoja.5964@unicesmag.edu.co** como el correo que se incluirá al enviar mi respuesta

Nombres y apellidos *

Tu respuesta

¿Desea continuar? *

◯ Sí

◯ No

Siguiente

Borrar formulario

Sección de preguntas

1) ¿Con qué frecuencia deben actualizarse las políticas de tratamiento de datos personales según la Ley 1581 de 2012? * 1 punto

- ◯ A) Cada 6 meses.
- ◯ B) Al menos una vez al año.
- ◯ C) Cada 3 años.
- ◯ D) Solo cuando ocurra una violación de datos.

2) ¿Qué es un "titular" según la Ley 1581 de 2012? * 1 punto

- ◯ A) La persona natural o jurídica de la cual se trata los datos.
- ◯ B) La persona natural cuyos datos personales son objeto de tratamiento.
- ◯ C) La autoridad que regula la protección de datos.
- ◯ D) El sistema informático donde se almacenan los datos.

3) ¿Cada cuánto tiempo se recomienda realizar auditorías internas para verificar el cumplimiento de la Ley 1581 de 2012? * 1 punto

- ◯ A) Cada 2 años.
- ◯ B) Cada 6 meses.
- ◯ C) Al menos una vez al año.
- ◯ D) Solo cuando lo solicite la autoridad competente.

4) ¿Qué se entiende por "tratamiento de datos personales" en la Ley 1581 de 2012? * 1 punto

- A) Solo la recolección de datos.
- B) Cualquier operación sobre datos personales
- C) La eliminación de datos personales.
- D) La venta de datos personales a terceros.

5) ¿Con qué periodicidad deben los responsables del tratamiento capacitar a sus empleados sobre la Ley 1581 de 2012? * 1 punto

- A) Cada 3 meses.
- B) Cada 6 meses.
- C) Una vez al año.
- D) Solo al momento de contratación.

6) ¿Qué es la "autorización" en el contexto de la Ley 1581 de 2012? * 1 punto

- A) Un permiso otorgado por la autoridad competente.
- B) El consentimiento previo, expreso e informado del titular
- C) Un documento que acredita la propiedad de los datos.
- D) Un informe de auditoría sobre el tratamiento de datos.

7) ¿Qué tan frecuentemente deben los responsables del tratamiento revisar los procedimientos de seguridad de los datos personales? * 1 punto

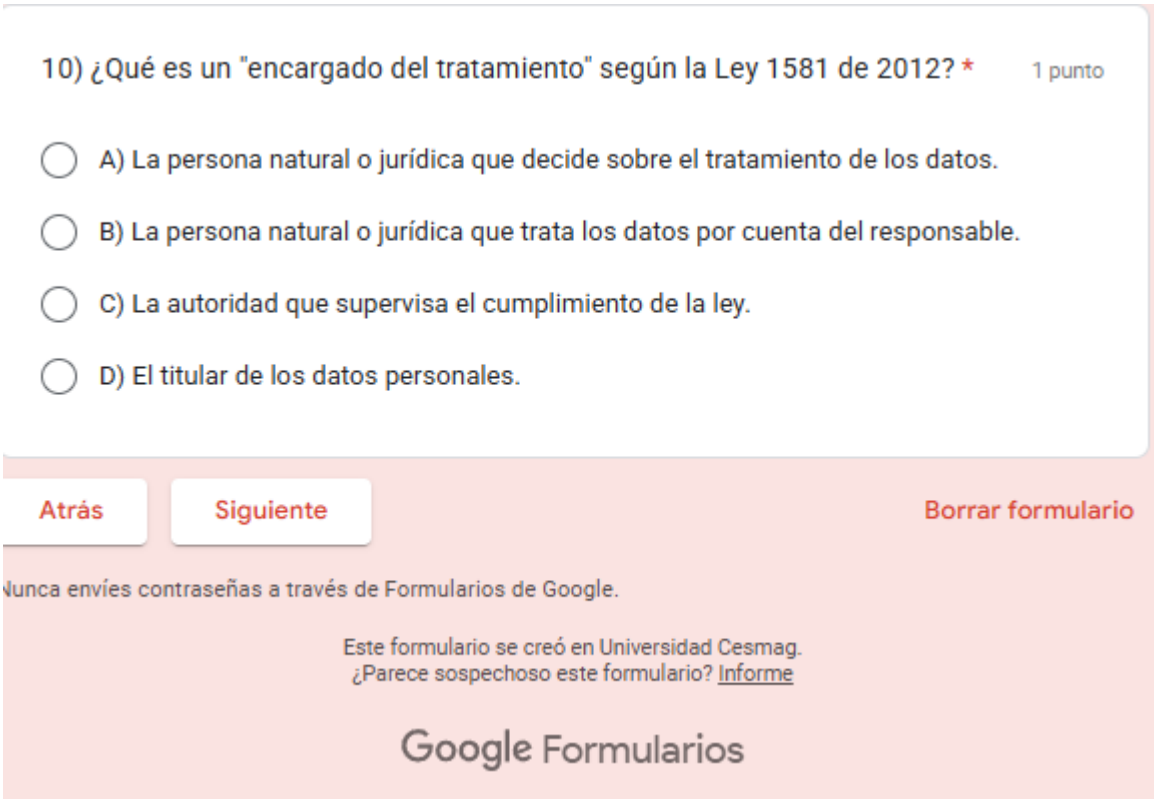
- A) Cada 2 años.
- B) Al menos una vez al año.
- C) Cada 6 meses.
- D) Solo cuando ocurra una violación de datos.

8) ¿Qué son los "datos sensibles" según la Ley 1581 de 2012? * 1 punto

- A) Datos que solo pueden ser tratados por entidades públicas.
- B) Datos que requieren un nivel de protección adicional
- C) Datos que no requieren autorización para su tratamiento.
- D) Datos que pueden ser compartidos libremente con terceros.

9) ¿Qué periodicidad debe tener la eliminación de datos personales que ya no son necesarios para los fines para los que fueron recolectados? * 1 punto

- A) Cada 6 meses.
- B) De manera inmediata al cumplirse el propósito.
- C) Cada año.
- D) Nunca, los datos deben conservarse indefinidamente.



ANEXOS 7: FORMULARIO TRATAMIENTO DE DATOS LEY 1581

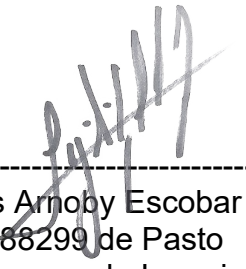
San Juan de Pasto, 03 de Septiembre de 2025

Biblioteca
REMIGIO FIORE FORTEZZA OFM. CAP.
Universidad CESMAG
Pasto

Saludo de paz y bien.

Por medio de la presente se hace entrega del Trabajo de Grado / Trabajo de Aplicación denominado Herramienta web para capacitación y sensibilización de seguridad de la información en el ámbito administrativo de la Universidad CESMAG con alineación a la norma ISO/IEC 27001 presentado por el (los) autor(es) David Esteban Pantoja Estrada, del Programa Académico Ingeniería de Sistemas al correo electrónico biblioteca.trabajosdegrado@unicesmag.edu.co. Manifiesto como asesor(a), que su contenido, resumen, anexos y formato PDF cumple con las especificaciones de calidad, guía de presentación de Trabajos de Grado o de Aplicación, establecidos por la Universidad CESMAG, por lo tanto, se solicita el paz y salvo respectivo.

Atentamente,



Luis Arnoby Escobar H.
98388299 de Pasto
Programa de Ingeniería de Sistemas
3154671444
laescobar@unicesmag.edu.co

INFORMACIÓN DEL (LOS) AUTOR(ES)	
Nombres y apellidos del autor: David Esteban Pantoja Estrada	**Documento de identidad:** 1004215964
Correo electrónico: pantojaestradad51@gmail.com	**Número de contacto:** 3176155715
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico:	**Número de contacto:**
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico:	**Número de contacto:**
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico:	**Número de contacto:**
Nombres y apellidos del asesor: Luis Arnoby Escobar Hernández	**Documento de identidad:** 98388299
Correo electrónico: laescobar@unicesmag.edu.co	**Número de contacto:** 3154671444
Título del trabajo de grado: Herramienta web para capacitación y sensibilización de seguridad de la información en el ámbito administrativo de la Universidad CESMAG con alineación a la norma ISO/IEC 27001	
Facultad y Programa Académico: Ingeniería, Ingeniería de Sistemas	

En mi (nuestra) calidad de autor(es) y/o titular (es) del derecho de autor del Trabajo de Grado o de Aplicación señalado en el encabezado, confiero (conferimos) a la Universidad CESMAG una licencia no exclusiva, limitada y gratuita, para la inclusión del trabajo de grado en el repositorio institucional. Por consiguiente, el alcance de la licencia que se otorga a través del presente documento, abarca las siguientes características:

a) La autorización se otorga desde la fecha de suscripción del presente documento y durante todo el término en el que el (los) firmante(s) del presente documento conserve (mos) la titularidad de los derechos patrimoniales de autor. En el evento en el que deje (mos) de tener la titularidad de los derechos patrimoniales sobre el Trabajo de Grado o de Aplicación, me (nos) comprometo (comprometemos) a informar de manera inmediata sobre dicha situación a la Universidad CESMAG. Por consiguiente, hasta que no exista comunicación escrita de mi(nuestra) parte informando sobre dicha situación, la Universidad CESMAG se encontrará debidamente habilitada para continuar con la publicación del Trabajo de Grado o de Aplicación dentro del repositorio institucional. Conozco(conocemos) que esta autorización podrá revocarse en cualquier momento, siempre y cuando se eleve la solicitud por escrito para dicho fin ante la Universidad CESMAG. En

estos eventos, la Universidad CESMAG cuenta con el plazo de un mes después de recibida la petición, para desmarcar la visualización del Trabajo de Grado o de Aplicación del repositorio institucional.

b) Se autoriza a la Universidad CESMAG para publicar el Trabajo de Grado o de Aplicación en formato digital y teniendo en cuenta que uno de los medios de publicación del repositorio institucional es el internet, acepto(amos) que el Trabajo de Grado o de Aplicación circulará con un alcance mundial.

c) Acepto (aceptamos) que la autorización que se otorga a través del presente documento se realiza a título gratuito, por lo tanto, renuncio(amos) a recibir emolumento alguno por la publicación, distribución, comunicación pública y/o cualquier otro uso que se haga en los términos de la presente autorización y de la licencia o programa a través del cual sea publicado el Trabajo de grado o de Aplicación.

d) Manifiesto (manifestamos) que el Trabajo de Grado o de Aplicación es original realizado sin violar o usurpar derechos de autor de terceros y que ostento(amos) los derechos patrimoniales de autor sobre la misma. Por consiguiente, asumo(asumimos) toda la responsabilidad sobre su contenido ante la Universidad CESMAG y frente a terceros, manteniéndose indemne de cualquier reclamación que surja en virtud de la misma. En todo caso, la Universidad CESMAG se compromete a indicar siempre la autoría del escrito incluyendo nombre de(los) autor(es) y la fecha de publicación.

e) Autorizo(autorizamos) a la Universidad CESMAG para incluir el Trabajo de Grado o de Aplicación en los índices y buscadores que se estimen necesarios para promover su difusión. Así mismo autorizo (autorizamos) a la Universidad CESMAG para que pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

NOTA: En los eventos en los que el trabajo de grado o de aplicación haya sido trabajado con el apoyo o patrocinio de una agencia, organización o cualquier otra entidad diferente a la Universidad CESMAG. Como autor(es) garantizo(amos) que he(hemos) cumplido con los derechos y obligaciones asumidos con dicha entidad y como consecuencia de ello dejo(dejamos) constancia que la autorización que se concede a través del presente escrito no interfiere ni transgrede derechos de terceros.

Como consecuencia de lo anterior, autorizo(autorizamos) la publicación, difusión, consulta y uso del Trabajo de Grado o de Aplicación por parte de la Universidad CESMAG y sus usuarios así:

- Permito(permitimos) que mi(nuestro) Trabajo de Grado o de Aplicación haga parte del catálogo de colección del repositorio digital de la Universidad CESMAG por lo tanto, su contenido será de acceso abierto donde podrá ser consultado, descargado y compartido con otras personas, siempre que se reconozca su autoría o reconocimiento con fines no comerciales.

En señal de conformidad, se suscribe este documento en San Juan de Pasto a los 03 días del mes de septiembre del año 2025

Firma del autor 	Firma del autor
Nombre del autor: David Esteban Pantoja Estrada	Nombre del autor:

Firma del autor	Firma del autor
Nombre del autor:	Nombre del autor:
Luis Arnoby Escobar Hernández Nombre del asesor:	