Diseño de un Plan de Concientización en Seguridad de la Información para una mediana empresa de tecnología, Aplicando las Recomendaciones de la Guía NIST SP800.50r1

Yan A. Sastoque Moreno y Jaahser J. Mendez Rodriguez

Facultad de Ingeniería, Universidad Piloto de Colombia

Investigación II

Coordinación de Postgrados TIC

Alvaro Escobar Escobar

Helen Nahir Barbosa Hurtado

02 de diciembre de 2025

Resumen

La investigación se desarrolla en una mediana empresa de tecnología. que, al avanzar en la implementación de su Sistema de Gestión de Seguridad de la Información, identifica al factor humano como uno de los principales vectores de riesgo, a partir de campañas de phishing, auditorías y análisis de riesgos que evidencian comportamientos que incrementan la exposición a amenazas. En un entorno donde los incidentes derivados de errores humanos o ingeniería social representan una proporción significativa de las brechas de seguridad, se hace necesario un programa estructurado de concientización alineado con estándares internacionales (Verizon, 2024). La investigación se apoya en la guía NIST SP 800-50r1, que plantea un Programa de Aprendizaje en Ciberseguridad y Privacidad como un sistema continuo, medible y orientado al cambio de comportamiento, articulado con los requisitos de competencia, concientización y capacitación de ISO/IEC 27001:2022 y con el control 6.3 de ISO/IEC 27002:2022, que exigen que el personal comprenda sus responsabilidades y actúe conforme a las políticas y controles definidos. Sobre esta base, se concluye que el aprendizaje en seguridad debe integrarse con la cultura organizacional y la gobernanza del SGSI. El estudio, de tipo aplicado y enfoque cualitativo, tiene como propósito planear, analizar y diseñar un Plan de Concientización en Seguridad de la Información (PCSI) ajustado a la realidad organizacional, mediante un análisis interpretativo de documentos internos que permite identificar brechas de comportamiento y necesidades formativas, y definir propósito, alcance, audiencias, roles, contenidos, lineamientos y métricas del plan. La hipótesis plantea que un PCSI alineado con la NIST SP 800-50r1 permite delimitar de forma clara el alcance, los objetivos, requisitos y brechas que se busca mitigar, habilitando, en etapas posteriores al alcance de esta investigación, una mejora en la capacidad de las personas para identificar amenazas (NIST, 2024, secc. 4.1–4.3).

Palabras Clave. NIST SP 800-50r1, información, seguridad, La “mediana empresa de tecnología”, política, concientización, PCSI

Índice general

Índice de Tablas

Índice de Figuras

Introducción

Planteamiento del Problema

La mediana empresa de tecnología utilizada para la aplicación del proyecto de investigación aplicada es una empresa colombiana del sector tecnológico, fundada en Bogotá en el año 2000, y está dedicada a soluciones de movilidad que integran hardware y software para industria, retail, grandes superficies y logística. En el marco de la implementación de un Sistema de Gestión de Seguridad de la Información conforme a ISO/IEC 27001, una consultoría externa realizada por una Empresa Consultora en seguridad identificó una brecha frente al control A.6.3 del Anexo A, relacionada con la ausencia de un Plan de concientización en seguridad de la información.

Dado que el año 2025 ha sido un año retador financieramente para la “mediana empresa de tecnología”, la compañía se ha visto en la obligación de no priorizar dentro de su presupuesto algunas de las iniciativas que la “Empresa Consultora en seguridad”, en su papel de empresa consultora, formulo dentro de la hoja de ruta para la implementación del sistema de gestión de seguridad de la información (SGSI), una de estas iniciativas con poco presupuesto pero de gran relevancia por su impacto, consiste en la creación de un plan de concientización en seguridad de la información para los empleados y contratistas de la “mediana empresa de tecnología”.

Reconociendo que la concientización en seguridad de la información de los colaboradores es importante para el cumplimiento de los objetivos del SGSI, la “mediana empresa de tecnología” ha optado por diseñar un plan no automatizado que posteriormente podrá ejecutar al interior de la organización, el cual debe cumplir con las necesidades de concientización sobre seguridad de la información que identificó la “Empresa Consultora en seguridad” durante la consultoría alineada con ISO/IEC 27001:2022 (Anexo A, 6.3) e ISO/IEC

27002:2022 (control 6.3); En respuesta a esta necesidad, los autores plantean el diseño de un plan de concientización en seguridad de la información, alineado con la guía NIST SP 800-50r1, para que la “mediana empresa de tecnología” en una posterior implementación logre despertar y fomentar la conciencia sobre amenazas y conductas seguras en sus colaboradores.

Formulación del Problema

¿Cómo el diseño de un plan de concientización en seguridad de la información fundamentado en las recomendaciones de la guía NIST SP 800-50r1, establece el marco estructural para que la “mediana empresa de tecnología” defina los elementos formativos necesarios para robustecer las competencias de sus colaboradores en seguridad de la información?

Justificación

A medida que se expande la adopción de tecnologías se eleva la superficie de ataque y la complejidad del riesgo (WEF, 2022), con ello la frecuencia de amenazas que se materializan por prácticas riesgosas de las personas (p. ej., caer en phishing, errores operativos). en este contexto, Verizon Business publicó las conclusiones de su 17º Informe anual de investigaciones sobre filtraciones de datos (DBIR 2024) donde analizó más de 30.000 incidentes y más de 10.000 brechas en 94 países y concluyó que el “elemento humano” participa en la mayoría de las brechas (68%), ya sea por error o por caer en ingeniería social (Verizon, 2024).

En el contexto de la “mediana empresa de tecnología”, la relevancia de abordar el riesgo humano es evidente. Una campaña de phishing simulada en enero de 2024 reveló que el 20% de los empleados abrió el correo y el 4% hizo clic en el enlace señuelo, confirmando la vulnerabilidad a la ingeniería social y la necesidad de reforzar las campañas de sensibilización y los protocolos de reporte de correos sospechosos (la “mediana empresa de tecnología”, 2024a). Adicionalmente, auditorías internas de 2024 identificaron áreas de mejora en el control de accesos, la estandarización de prácticas y la continuidad del negocio, aspectos que se beneficiarían enormemente de una mayor concientización y una clara definición de

responsabilidades para el personal y los custodios de activos (“mediana empresa de tecnología”, 2024b). Por lo tanto, este proyecto se enfoca en la planeación, análisis y diseño de un plan de concientización en seguridad de la información, alineado con la guía NIST SP 800-50r1, para establecer un marco estructural y componentes formativos que permitan una futura ejecución medible y coherente con las mejores prácticas, fortaleciendo así la postura de seguridad de la “mediana empresa de tecnología”.

Objetivos de la Investigación

Objetivo General

Planear, analizar y diseñar un plan de concientización en seguridad de la información que establezca las bases para fortalecer la cultura de seguridad y mejorar la capacidad de los colaboradores para identificar amenazas dentro de la “mediana empresa de tecnología”

Objetivos Específicos

Analizar el estado actual de la concientización en seguridad de la información en la “mediana empresa de tecnología” S.A.S, utilizando las brechas evidenciadas en incidentes, campañas de phishing y auditorías, para orientar la planeación del PCSI.

Definir los lineamientos, el alcance, las responsabilidades y las audiencias del PCSI en la “mediana empresa de tecnología”, como base para su diseño y futura implementación.

Diseñar la estructura anual del PCSI en la “mediana empresa de tecnología”, definiendo campañas de concientización, acciones de refuerzo y microcontenidos, orientados a fortalecer la cultura de seguridad de la información.

Establecer la metodología de evaluación del PCSI en la “mediana empresa de tecnología”, para contar con una base que permita valorar su desempeño en el tiempo.

Elaborar una propuesta de plan de implementación del PCSI en la “mediana empresa de tecnología”, que organice su puesta en marcha de forma estructurada y coherente con el diseño.

Hipótesis

Hipótesis de investigación (H1): El diseño de un plan de concientización en seguridad de la información, fundamentado en la guía NIST SP 800-50r1 y en evidencias internas sobre brechas de comportamiento de los colaboradores de la “mediana empresa de tecnología”, permite que, al ejecutar las fases de planeación, análisis y diseño, se definan claramente los objetivos, las audiencias, los contenidos y las métricas iniciales necesarias para que estructuren la implementación y evaluación a futuro del plan de concientización en seguridad de la información de la “mediana empresa de tecnología”.

Hipótesis nula (H0): El diseño de un plan de concientización en seguridad de la información, fundamentado en la guía NIST SP 800-50r1 y en evidencias internas sobre brechas de comportamiento de los colaboradores de la “mediana empresa de tecnología”, no permite que, al ejecutar las fases de planeación, análisis y diseño, se definan claramente los objetivos, las audiencias, los contenidos y las métricas iniciales necesarias para que estructuren la implementación y evaluación a futuro del plan de concientización en seguridad de la información de la “mediana empresa de tecnología”.

Alcance y Limitaciones

Alcance

El proyecto corresponde a una investigación aplicada orientada a planear, analizar y diseñar un Plan de Concientización en Seguridad de la Información (PCSI) para la “mediana empresa de tecnología”, alineado con la guía NIST SP 800-50r1 en sus fases de planificación y análisis/diseño del Programa de Aprendizaje en Ciberseguridad y Privacidad (CPLP), y con los requisitos de competencia, concienciación y formación establecidos en ISO/IEC 27001:2022 y el control 6.3 de ISO/IEC 27002:2022 (NIST, 2024, NIST SP 800-50r1, secc. 2.1–2.3 y 4.1–4.2; ISO, 2022, ISO/IEC 27001:2022, cl. 7.2–7.3; ISO, 2022, ISO/IEC 27002:2022, 6.3). En este marco, el alcance de la investigación se limita a demostrar que es posible, mediante el diseño

del PCSI, definir de manera estructurada el alcance, los objetivos, los requisitos, el cubrimiento y las brechas que el plan busca mitigar, en coherencia con la hipótesis de investigación formulada (H1).

En el plano temático, el estudio abarca el diagnóstico del estado actual de la concientización en seguridad de la información, la identificación de brechas asociadas al factor humano, la definición de objetivos generales y específicos del PCSI, la delimitación de audiencias, la propuesta de contenidos y modalidades formativas, la formulación de políticas internas que rigen el programa, la determinación de indicadores (KPIs) y el diseño de un cronograma anual de actividades no automatizadas y de bajo costo (NIST, 2024, NIST SP 800-50r1, secc. 2.2–2.3, 3.2–3.3 y 4.1; ISO, 2022, ISO/IEC 27002:2022, 6.3). El alcance cubre únicamente las fases de planificación, análisis y diseño del PCSI, incluyendo el diseño de prototipos de materiales de concientización, pero sin abarcar el desarrollo final de dichos materiales, su implementación operativa ni la medición empírica de su impacto.

En cuanto al alcance organizacional, la investigación se circunscribe a una “mediana empresa de tecnología” y a sus procesos clave (Administrativo & Financiero, Transformación & Desarrollo, Operaciones & Servicios, Comercial & Mercadeo), considerando como población objetivo conceptual a todos los colaboradores y contratistas con acceso a activos de información, pero trabajando analíticamente a partir de evidencias ya existentes: consultoría de seguridad de la información, matriz de riesgos, consolidado de controles operativos, inventario de activos, informes de riesgos de seguridad, campaña de phishing de enero de 2024 y hallazgos de auditoría que evidencian comportamientos riesgosos como uso de herramientas no autorizadas y fallas de escritorio limpio (la “Empresa Consultora en seguridad”, 2024; la “empresa auditora”, 2024; la “mediana empresa de tecnología”, 2024a; la “mediana empresa de tecnología”, 2024b). Temporalmente, el trabajo utiliza información principalmente de los años 2023 - 2025 y proyecta un horizonte teórico de doce meses para la ejecución del PCSI diseñado.

Limitaciones

Una primera limitación radica en la fase del ciclo de vida que aborda la investigación: el trabajo se concentra en las etapas de planeación, análisis y diseño del programa, sin abarcar el desarrollo completo de todos los recursos didácticos, la implementación práctica ni la evaluación sistemática posterior de resultados, niveles de aprendizaje o cambios de comportamiento en la organización (NIST, 2024, NIST SP 800-50r1, secc. 4.1–4.3). En consecuencia, la hipótesis H1 se contrasta únicamente en términos de la capacidad del diseño para estructurar alcance, objetivos, requisitos, cubrimiento y brechas, pero no se verifica empíricamente el efecto del PCSI sobre la capacidad real de los colaboradores para identificar amenazas.

Asimismo, la investigación se apoya de manera predominante en técnicas cualitativas de revisión y análisis documental de evidencias internas (informes de consultoría, campañas de phishing, auditorías, políticas y procedimientos), sin incorporar levantamiento de información primaria adicional mediante encuestas, entrevistas o grupos focales con los colaboradores (NIST, 2024, NIST SP 800-50r1, secc. 2.1–2.2). Esto implica que las conclusiones sobre brechas de concientización y necesidades de aprendizaje reflejan lo que dichas fuentes documentan para momentos y muestras concretas (por ejemplo, una campaña de phishing y una auditoría sobre una muestra limitada de equipos), por lo que pueden existir otros patrones de comportamiento no capturados por estas evidencias (la “Empresa Consultora en seguridad”, 2024; la “empresa auditora”, 2024; la “mediana empresa de tecnología”, 2024a).

Otra limitación importante es de naturaleza tecnológica y de recursos: el PCSI se concibe explícitamente como un programa “no automatizado” y de bajo costo, que se apalanca en herramientas ya disponibles (LMS proporcionado por la ARL, Microsoft 365, carteleras digitales) y excluye, en esta fase, la incorporación de plataformas avanzadas de orquestación de campañas, simuladores comerciales de phishing o rutas extensivas de formación técnica especializada (NIST, 2024, NIST SP 800-50r1, secc. 3.1–3.3; ISO, 2022, ISO/IEC 27002:2022,

6.3). Esto puede limitar el nivel de personalización y automatización del programa frente a las mejores prácticas internacionales y obliga a que futuras fases de implementación revisen el diseño a la luz de los recursos que efectivamente se asignen.

El alcance también se encuentra condicionado por el contexto normativo y documental vigente en la “mediana empresa de tecnología”: el diseño del PCSI se alinea con el SGSI en implementación, con la certificación ISO 9001:2015 y con el conjunto actual de políticas y procedimientos en seguridad de la información, TI y protección de datos personales; por tanto, cambios significativos en el marco regulatorio, contractual o en el propio sistema de gestión podrían requerir ajustes sustanciales al plan (ISO, 2022, ISO/IEC 27001:2022, cl. 4.1–4.2 y 6.1; ISO, 2022, ISO/IEC 27002:2022, 5.1 y 6.3). Además, el diseño está fuertemente contextualizado a la realidad organizacional de la “mediana empresa de tecnología”, por lo que su extrapolación a otras empresas debe hacerse con cautela, adaptando audiencias, riesgos y contenidos a cada entorno.

Finalmente, aunque el proyecto define indicadores clave de desempeño y propone un marco de medición alineado con NIST SP 800-50r1, la investigación no desarrolla un ejercicio cuantitativo completo de establecimiento de todas las líneas base, ni aborda análisis de costo-beneficio o retorno de la inversión del PCSI (NIST, 2024, NIST SP 800-50r1, secc. 5.1–5.3). Las métricas propuestas se configuran como un insumo para fases posteriores de implementación y evaluación, más que como resultados empíricamente contrastados dentro del alcance de este trabajo.

Marco Teórico

Marco Referencial

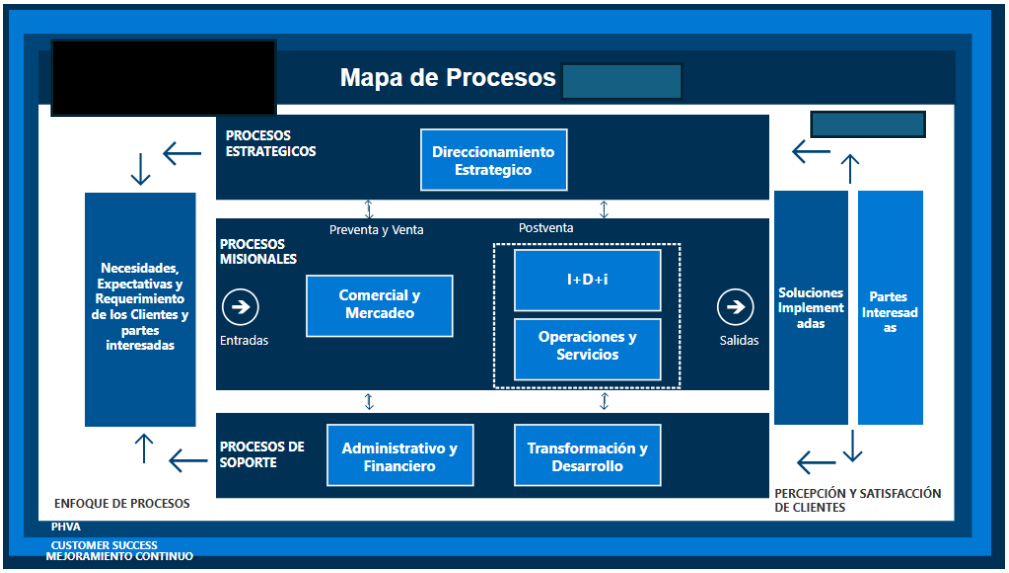
La “mediana empresa de tecnología” nació en el año 2000 como un proyecto interno de una desaparecida “empresa incubadora”., al identificar la oportunidad de introducir en Colombia equipos móviles para la gestión de información. Con el tiempo, se convirtió en una empresa

independiente, enfocada en soluciones de integración móvil. Empezó con hardware y, como parte de su estrategia, evolucionó hacia el desarrollo de software.

En 2023, para responder a las nuevas exigencias del mercado, la “mediana empresa de tecnología” realizó una consultoría en seguridad de la información con el apoyo de una “Empresa Consultora en seguridad”, empresa colombiana experta en auditoría y consultoría en este campo. Gracias a este trabajo, se identificaron brechas frente a la norma ISO/IEC 27001, se levantó el inventario de activos de información, se hizo el análisis de riesgos y se definió un plan de trabajo a dos años con 16 iniciativas. Entre ellas, destaca la creación de un Plan de Concienciación en Seguridad de la Información, que es el eje central de esta investigación aplicada.

Figura 1

Mapa de procesos de la “mediana empresa de tecnología”



Nota. Mapa de procesos de la “mediana empresa de tecnología”, Lineamientos generales, (2024)

Hoy, la “mediana empresa de tecnología” opera con una base tecnológica sólida que combina software propio y hardware para operaciones en campo. Tiene presencia en varias ciudades del país y cuenta con 84 colaboradores distribuidos en cuatro procesos clave que

pueden verse en la figura 1, Mapa de procesos: Administrativo & Financiero, Transformación & Desarrollo, Operaciones & Servicios, y Comercial & Mercadeo. La compañía dispone de un sistema formal de gobierno documental, con políticas y procedimientos vigentes en seguridad y TI, además de herramientas para la gestión del riesgo, inventarios de activos e informes técnicos y operativos. Todo esto refleja una organización que entiende la seguridad de la información como un pilar fundamental del servicio y que ha institucionalizado reglas claras, estándares técnicos mínimos y prácticas de soporte.

El entorno operativo incluye trabajo remoto y movilidad, acceso a recursos mediante VPN cuando corresponde, segmentación y control de comunicaciones a través de reglas de firewall, y normativas de escritorio y pantalla limpia, entre otros. La administración de cuentas de usuario, la gestión de activos tecnológicos y el servicio de atención de casos se encuentran normalizados con procedimientos específicos. La existencia de un inventario consolidado de activos y de una caracterización de la infraestructura tecnológica aporta visibilidad de los componentes de soporte, sus interacciones y responsables, y permite trazar dependencias relevantes para el uso de información y el manejo de configuraciones (crear conexión VPN a la “mediana empresa de tecnología”; Administración de activos tecnológicos; Inventario de activos consolidado; Caracterización Infraestructura Tecnológica).

Desde la visión de un plan de formación, este contexto supone que los comportamientos seguros deben sostener prácticas diarias en autenticación, gestión de contraseñas, resguardo de información según su clasificación, manejo ordenado de accesos y reporte oportuno de eventos. La estandarización de procesos y documentos constituye una base favorable para orientar mensajes y contenidos coherentes en el programa de capacitación (Política de contraseñas seguras; Política de clasificación de información).

La documentación vigente integra un manual de seguridad de la información y políticas específicas sobre uso aceptable de activos informáticos, contraseñas, escritorio y pantalla limpia, firewall, clasificación de la información, respaldo de información y tratamiento de datos

personales. Estas piezas establecen expectativas concretas de comportamiento para todo el personal y terceros con acceso a recursos de la compañía, definen responsabilidades y describen prácticas mínimas aceptables (“mediana empresa de tecnología”, Manual de seguridad de la información de la “mediana empresa de tecnología” S.A.S; Política de contraseñas seguras; Política de tratamiento de datos personales).

En los procesos de relación con terceros se formalizan acuerdos de confidencialidad, lo que configura un control básico en la cadena de suministro. En protección de datos personales, se disponen lineamientos sobre finalidades, deberes y procedimientos de atención a titulares. En conjunto, estos documentos constituyen la “gramática de conducta” vigente que el personal debe conocer y aplicar. Para el plan de concientización y capacitación, la presencia de este marco representa una oportunidad de reforzar la comprensión operativa de estas reglas y verificar su adopción con métricas sobre comportamientos observables (“mediana empresa de tecnología”, Acuerdo de confidencialidad Proveedores; Política de tratamiento de datos personales).

En la operación diaria existen procedimientos explícitos para la creación e inhabilitación de usuarios, la administración de activos tecnológicos, el registro y atención de casos de TI, el seguimiento a actualizaciones en equipos, y la guía básica en respuesta a incidentes. También se instruye sobre el uso de VPN para acceso remoto seguro, así como sobre parámetros y gestión del firewall. En estos procesos hay momentos clave en los que las acciones de las personas influyen directamente en la seguridad de la organización, por ejemplo, cuando se crean o inhabilitan cuentas de usuario, se devuelven equipos, se aplican actualizaciones y parches, se configuran accesos o se gestionan solicitudes e incidentes a través de los canales oficiales definidos (“mediana empresa de tecnología”, Creación e Inhabilitación de usuarios de IT; Administración de activos tecnológicos; Registro y atención casos de IT; Seguimiento a actualizaciones de equipos individuales; Guía básica de respuesta a incidentes de SI; Gestión de Incidentes de SI).

Que estas actividades estén descritas en normas y documentos ayuda a mantener el control y a hacer seguimiento de lo que ocurre. Sin embargo, también pone en evidencia que las personas deben conocer bien cada paso, entender qué riesgos se generan cuando no se cumplen y actuar de forma coherente en el día a día. Para el plan de capacitación, esto se convierte en una oportunidad para enseñar a partir de situaciones reales de trabajo y evaluar el aprendizaje con indicadores operativos concretos, como los tiempos de reporte, la calidad de los registros o el cumplimiento de los flujos de creación e inactivación de usuarios, entre otros. La organización dispone de un inventario consolidado de activos que relaciona software, hardware y servicios con procesos y responsables. Asimismo, existe una política formal de clasificación de la información que define niveles y criterios para el manejo diferenciado de datos, y una política de respaldo con definiciones de periodicidad y custodia. En la práctica, esto permite identificar qué activos y repositorios requieren mayor protección, dónde se ubica la información sensible y qué hábitos se esperan en almacenamiento, intercambio y destrucción (Inventario de activos consolidado; Política de clasificación de información; Política de respaldo de información).

La existencia de estos documentos muestra que la organización reconoce la importancia de gestionar adecuadamente el ciclo de vida de la información. Sin embargo, como su cumplimiento depende en gran medida de lo que las personas hacen en su rutina diaria, la formación y el refuerzo permanente se vuelven clave para que las reglas no se queden solo en el papel y se apliquen de manera coherente. Esto abre una buena oportunidad para que el plan de formación se centre en temas muy prácticos, como dónde guardar los archivos, qué repositorios usar, cómo marcar y compartir la información según su clasificación y cómo reportar oportunamente cualquier situación inusual.

La compañía cuenta con matrices de riesgos consolidadas, una matriz de riesgos y oportunidades del sistema de gestión, escalas de impacto y un consolidado de controles operativos con frecuencias y responsables. Además, se han elaborado informes sobre riesgos

de seguridad de la información y resultados de campañas de phishing. Esta evidencia sugiere que la organización no solo identifica y evalúa riesgos, sino que también monitorea conductas frente a vectores comunes de amenaza, especialmente ingeniería social (“mediana empresa de tecnología”, Matriz de Riesgos y Oportunidades; Escala de Impactos; Consolidado de Controles Operativos; Informe de resultados Riesgos de Seguridad Inf; 01. Informe_Phishing_de la “mediana empresa de tecnología”_Enero_2024;).

Los resultados de ejercicios de phishing muestran patrones aprovechables para orientar el contenido formativo y para segmentar audiencias en función del desempeño observado. De igual forma, los hallazgos de riesgo y la ejecución de controles operativos permiten reconocer procesos con mayor exposición humana. Para el plan, esto representa una oportunidad de convertir datos en decisiones pedagógicas: qué temas reforzar, con quién, y con qué profundidad, manteniendo la mirada en cambios de comportamiento verificables (“Empresa Consultora en seguridad”, 01. Informe_Phishing_ “mediana empresa de tecnología”_Enero_2024, 2024; La “mediana empresa de tecnología”, Consolidado de Controles Operativos).

En la organización ya existen herramientas que describen qué competencias se esperan en cada rol y cuáles son los conocimientos clave que deben tener las personas, además de procedimientos transversales para procesos como ventas, proyectos o planeación estratégica. Este soporte permite identificar mejor el nivel de riesgo asociado a cada función y muestra que los contenidos de concientización pueden ajustarse a las necesidades específicas de cada grupo. Contar con un manual de seguridad y con instructivos operativos facilita, además, llevar las políticas a la práctica, porque ofrecen guías y pasos concretos que pueden aprovecharse como base para diseñar materiales de formación claros y aplicados al trabajo diario (“mediana empresa de tecnología”, Profesiograma; Conocimientos Organizacionales).

La cultura organizacional, reflejada en la formalización de procesos y en la existencia de informes periódicos, indica disposición a medir y mejorar. La consolidación de esta cultura de

medición representa una oportunidad para que el programa de capacitación integre indicadores de adopción, cumplimiento y desempeño, alineados con los instrumentos ya existentes (La “mediana empresa de tecnología”, Lineamientos Generales; INFORME SISTEMAS DE INFORMACIÓN - “MEDIANA EMPRESA DE TECNOLOGÍA” S.A - 2024;).

Se dispone de un procedimiento de gestión de incidentes de seguridad de la información y de una guía básica de respuesta, además de una política de respaldo aplicada al resguardo de datos. Esta infraestructura documental establece roles, canales y actividades iniciales ante eventos adversos, así como los criterios base de recuperación. En la práctica, la efectividad de estos mecanismos depende de que las personas reconozcan señales tempranas, notifiquen por los canales definidos y ejecuten acciones iniciales. Esta dependencia del factor humano es una zona clara de oportunidad para el futuro plan: reforzar criterios de detección, comunicación y escalamiento, y validar comprensión mediante ejercicios prácticos sencillos (“mediana empresa de tecnología”, Gestión de Incidentes de SI; Guía básica de respuesta a incidentes de SI; Política de respaldo de información).

Síntesis del Estado Actual y Oportunidades Formativas

Los autores en la tabla 1 han resumido las principales características y oportunidades que servirán de insumo a la investigación.

Tabla 1

Síntesis estado actual de la "mediana empresa de tecnología"

Estado actual	Oportunidad
Existe un marco de políticas y procedimientos completo en materias críticas para el comportamiento seguro, con gobierno documental y trazabilidad.	Transformar estas reglas en hábitos observables y medibles, asegurando entendimiento práctico por parte de cada audiencia.
Los procesos de TI que tocan el ciclo de vida de accesos, activos, parches y casos están estandarizados.	Utilizar estos procesos como escenarios de aprendizaje, reforzando ejecución correcta y tiempos de respuesta.
Hay inventarios de activos, políticas de clasificación y respaldo, que otorgan visibilidad de lo que se protege y cómo.	Reforzar prácticas de almacenamiento, compartición y resguardo según clasificación, desde el usuario final hasta los custodios.
Se cuenta con matrices de riesgo, controles operativos e informes de phishing y de riesgos de seguridad.	Priorizar contenidos con base en evidencia, segmentar por desempeño e integrar métricas de cambio conductual.
Se han formalizado acuerdos de confidencialidad y lineamientos de datos personales para la relación con terceros.	Enfatizar responsabilidades y límites en el intercambio de información con proveedores y aliados.
La continuidad y la respuesta a incidentes están documentadas en sus elementos esenciales.	Fortalecer la preparación del personal en detección y reporte temprano, y en comprensión de acciones iniciales.

Nota. Fuente: Los autores.

Fundamentos Teóricos

ISO/IEC 27001:2022, Clausula 7.2, Competencias

Como fundamento para el desarrollo de las fases de Planificación y Estrategia del PCSI, este apartado establece la alineación organizacional con ISO/IEC 27001:2022 que justifica la necesidad de gestionar competencias y sensibilización en la "mediana empresa de tecnología", respondiendo directamente a las brechas identificadas por la "Empresa Consultora en seguridad" en su ejercicio de consultoría.

La "mediana empresa de tecnología" decidió alinearse con la norma ISO/IEC 27001:2022, como parte del proceso de implementación del SGSI, siguiendo las recomendaciones de la consultoría realizada por la "Empresa Consultora en seguridad"

Este enfoque resalta la importancia de que empleados y contratistas cuenten con las competencias necesarias para proteger la información, cumplir con la norma y generar evidencia para auditorías.

Además, busca mitigar el riesgo humano mediante formación y sensibilización, asegurando que todos sepan cómo aplicar las políticas del PCSI (Plan de Concientización en Seguridad de la Información).

En pocas palabras, sin competencias, los controles no funcionan; por eso la sensibilización se convierte en un requisito obligatorio y medible.

ISO/IEC 27001:2022, Control A.6.3

Como fundamento normativo para las fases de Análisis y Diseño del PCSI, el Control A.6.3 establece los requisitos de formación y concientización que deben cumplirse en La “mediana empresa de tecnología”, permitiendo estructurar la segmentación de audiencias, la personalización de contenidos según roles y la alineación del programa con el SGSI existente.

El control A.6.3 del Anexo A de la ISO/IEC 27001:2022 es clave porque exige que las personas reciban formación y concientización en seguridad de la información, alineada con sus responsabilidades y con los riesgos de la organización (ISO/IEC 27001, 2022, Anexo A.6.3). Este requisito respalda directamente el objetivo de la investigación, que es planear y diseñar un plan de capacitación y sensibilización estructurado para La “mediana empresa de tecnología”. Además, sirve como criterio de referencia para asegurar que el PCSI propuesto contribuya al cumplimiento de la norma y fortalezca el SGSI.

En este sentido, el control A.6.3 de la norma ISO/IEC 27001 (2022) define que:

> “El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral” (p. 14).

ISO/IEC 27002:2022, Control 6.3, Concientización, Educación y Capacitación en Seguridad de la Información

Como fundamento para el desarrollo del PCSI, este control proporciona los parámetros técnicos y operativos que orientan la definición de objetivos, la selección de canales de comunicación y la estructuración de contenidos temáticos durante las fases de Planificación y Estrategia y Análisis y Diseño.

El control 6.3 de la ISO/IEC 27002:2022 es clave porque define qué se espera de un programa formal de concientización, educación y capacitación en seguridad de la información dentro de un SGSI, incluyendo alcance, contenidos y responsabilidades (ISO/IEC, 27002:2022, control 6.3). Esto ofrece un marco de referencia reconocido internacionalmente para alinear el PCSI de la “mediana empresa de tecnología” con buenas prácticas, garantizar coherencia con la ISO/IEC 27001 y facilitar su trazabilidad frente a auditorías. Además, permite que la investigación justifique sus decisiones de diseño (objetivos, temas, segmentación de audiencias e indicadores) con base en un estándar aceptado y no solo en criterios internos (ISO/IEC, 27002:2022, control 6.3).

Este control convierte la seguridad de la información en parte fundamental e indivisible de la organización reduciendo el riesgo humano, fortalece la cultura organizacional de la información permitiendo que todos los colaboradores comprendan sus responsabilidades alineadas con estándares internacionales.

El control 6.3 establece la orientación para concientización, educación y capacitación en seguridad de la información, con el propósito de apoyar que las personas actúen en conformidad con la seguridad de la información de la organización. Su alcance incluye directrices para definir, implementar y mantener estas prácticas de forma acorde con las necesidades organizacionales (ISO, 2022b).

Un programa de concientización sobre la seguridad de la información tiene como objetivo que el personal sea consciente de sus responsabilidades respecto a la seguridad de la información y de los medios para cumplirlas (ISO,2022b).

La concientización debe planificarse considerando las funciones del personal interno y externo. Las actividades deben programarse a lo largo del tiempo, preferiblemente de forma regular, basadas en lecciones aprendidas de incidentes y en cambios relevantes (ISO,2022b).

La norma ISO/EIC27002 (2022) define que:

> "El programa debe incluir una serie de actividades a través de canales físicos o virtuales adecuados, como campañas, folletos, carteles, boletines, sitios web, sesiones informativas y correos electrónicos, entre otros.
>
> La concientización sobre la seguridad de la información debe cubrir aspectos generales tales como:
>
> a) el compromiso de la dirección con la seguridad de la información en toda la organización;
>
> b) la familiarización y el cumplimiento respecto a reglas y obligaciones de seguridad de la información, teniendo en cuenta políticas, normas, leyes, estatutos, reglamentos, contratos y acuerdos específicos del tema;
>
> c) la responsabilidad personal por acciones e inacciones, y responsabilidades generales para asegurar o proteger la información que pertenece a la organización y a las partes interesadas;
>
> d) procedimientos básicos de seguridad de la información e indicadores relevantes; y controles básicos;
>
> e) puntos de contacto y recursos para obtener información adicional y asesoramiento sobre asuntos de seguridad de la información". (ISO,2022b).

“La organización debe contar con un plan de capacitación para equipos técnicos que asegure las habilidades necesarias para mantener el nivel de seguridad requerido; si existen brechas, estas deben mitigarse”. (ISO,2022b).

“La capacitación puede combinar múltiples formas y medios (p. ej., conferencias, autoaprendizaje, mentorías/consultores, rotación, reclutamiento y formación en aula, remota o autoaprendizaje), y el personal técnico debe actualizarse de manera continua mediante fuentes profesionales y eventos especializados.” (ISO,2022b).

NIST SP 800-50r1

Como soporte central para el desarrollo del PCSI, este documento aporta la estructura conceptual y metodológica que guía la planeación, el análisis de necesidades, la segmentación de audiencias, la definición de contenidos y la formulación de criterios de medición a lo largo de las fases de Planificación y Estrategia y Análisis y Diseño.

El documento NIST SP 800-50r1 es clave para esta investigación porque ofrece una guía estructurada y actualizada para planear, analizar y diseñar programas de capacitación y concientización en seguridad de la información, exactamente el alcance definido para el PCSI de la “mediana empresa de tecnología” (NIST, 2024, cap. 2–3). Además, se alinea con los requisitos de formación y concienciación de normas como ISO/IEC 27001:2022 e ISO/IEC 27002:2022, lo que permite integrar buenas prácticas internacionales en un solo marco coherente (ISO, 2022ª; 2022b). Finalmente, proporciona criterios para segmentar audiencias, definir contenidos, seleccionar métodos y medir resultados, aspectos centrales del diseño metodológico de este proyecto (NIST, 2024, cap. 3).

La NIST SP 800□50r1 convierte la concientización en un proceso estratégico, medible y adaptable, clave para reducir el riesgo humano y fortalecer el SGSI.

El NIST SP 800-50r1 proporciona un marco integral para concebir, planificar, ejecutar y mejorar un Programa de Aprendizaje en Ciberseguridad y Privacidad (CPLP, por sus siglas en inglés) dentro de las organizaciones (National Institute of Standards and Technology [NIST],

2024, secciones 1.1–1.3). Su propósito es guiar a los líderes, responsables de seguridad, cumplimiento y Transformación & Desarrollo en el diseño de iniciativas de sensibilización, formación y desarrollo de competencias que fortalezcan la postura de seguridad y reduzcan el riesgo asociado al factor humano (NIST SP 800-50r1, 2024, secciones 1.2 y 2.1). El documento enfatiza la creación de una cultura organizacional consciente de los riesgos y el cumplimiento, donde el comportamiento seguro se convierta en la norma cotidiana y el aprendizaje sea continuo y basado en el contexto del negocio (NIST SP 800-50r1, 2024, secciones 1.3 y 3.1).

El CPLP trasciende la capacitación puntual: es un sistema vivo que integra gestión del cambio, comunicación estratégica y medición orientada a resultados; alinea mensajes, contenidos y modalidades con amenazas, requisitos y prioridades estratégicas del negocio, actuando como habilitador de la gestión de riesgos y de la resiliencia (NIST SP 800-50r1, 2024, secciones 2.1–2.3, 3.1–3.3).

El enfoque del NIST resalta asegurar patrocinio ejecutivo, clarificar roles y responsabilidades y atender la diversidad de audiencias (usuarios finales, técnicos, líderes, terceros). El aprendizaje debe enfocarse en comportamientos observables —por ejemplo, reportar incidentes, proteger datos y usar autenticación robusta— y evolucionar con cambios en amenazas, tecnología y regulación (NIST SP 800-50r1, 2024, secciones 2.2, 3.2 y 4.1).

Alineación con Marcos y Políticas. Como soporte para el desarrollo del PCSI, las siguientes directrices orientan la alineación del programa con marcos de ciberseguridad y privacidad, facilitando que, en las fases de Planificación y Estrategia y Análisis y Diseño, se definan contenidos, prioridades y controles plenamente coherentes con el ecosistema NIST.

El CPLP debe alinearse con marcos y políticas vigentes del propio NIST para garantizar coherencia, trazabilidad y desempeño; en particular, con el NIST Cybersecurity Framework (función Protect, categoría PR.AT) y con lineamientos relacionados del ecosistema NIST (p. ej., referencias sobre concienciación y capacitación que el 800-50r1 utiliza como insumos), así

como con el NIST Privacy Framework para riesgos de datos personales y prácticas responsables de tratamiento (NIST SP 800-50r1, 2024, secciones 1.1, 2.1 y 3.1).

La coherencia normativa evita duplicidades y mensajes contradictorios. Para ello, el NIST recomienda trazar contenidos del CPLP contra requisitos internos y externos pertinentes y mantener una matriz que relacione contenidos con objetivos y controles del programa de seguridad y privacidad para priorizar riesgos, definir metas y demostrar conformidad (NIST, 2024, secciones 2.3 y 3.3).

Gobernanza, Roles y Responsabilidades del CPLP. Como insumo directo para el desarrollo del PCSI, las siguientes orientaciones de gobernanza sirven para definir, durante las fases de Planificación y Estrategia y Análisis y Diseño, la estructura de roles, los mecanismos de decisión y los indicadores que regirán la gestión y el seguimiento del programa. Una buena gobernanza requiere patrocinio visible de la alta dirección, definición clara de roles (quién diseña, aprueba, imparte, mide y mejora) y políticas para gestionar el catálogo formativo, actualizar materiales, segmentar audiencias y validar la efectividad. Resulta útil un comité que revise riesgos emergentes, incidentes y lecciones aprendidas para ajustar prioridades (NIST SP 800-50r1, 2024, secciones 2.2 y 3.2).

La rendición de cuentas se fortalece con OKR/KPI por función vinculados al CPLP y revisiones periódicas, conectando aprendizaje con resultados de seguridad esperados y la mejora continua del programa (NIST SP 800-50r1, 2024, secciones 3.2–3.3).

Planificación Estratégica y Gestión del Programa. Como guía práctica para el desarrollo del PCSI, estas orientaciones del NIST se utilizan en las fases de Planificación y Estrategia y Análisis y Diseño para definir objetivos de aprendizaje, caracterizar audiencias, seleccionar modalidades, estructurar el portafolio de actividades y establecer los criterios de seguimiento y evaluación del programa. El NIST propone planificar desde el contexto organizacional y el panorama de amenazas, definiendo objetivos de aprendizaje medibles que traduzcan riesgos en conductas; incluir el mapa de audiencias, catálogo priorizado por riesgo, calendario de campañas y asignación de recursos (presupuesto, plataformas, instructores, métricas) (NIST SP 800-50r1, 2024, secciones 2.1–2.3).

La gestión del programa orquesta modalidades como microlearning, cursos virtuales y simulaciones de phishing, y se coordina con iniciativas de seguridad (vulnerabilidades, incidentes, protección de datos, continuidad). Debe ser ágil ante cambios tecnológicos, incidentes y auditorías (NIST SP 800-50r1, 2024, secciones 3.1–3.3).

La comunicación estratégica es central: mensajes breves y accionables, refuerzos periódicos y narrativas con casos reales para hacer tangible el riesgo. Las métricas se planifican desde el inicio para cada actividad (participación, aprendizaje y comportamiento) (NIST SP 800-50r1, 2024, secciones 3.1 y 3.3).

Segmentación de Audiencias y Análisis de Necesidades. Como insumo específico para el desarrollo del PCSI, las directrices de segmentación se aplican en la fase de Análisis y Diseño para caracterizar audiencias, definir contenidos diferenciados y establecer criterios de medición alineados con el nivel de riesgo y las responsabilidades de cada grupo. El CPLP segmenta por rol, acceso, exposición a datos, criticidad y madurez. Para cada segmento se analiza necesidades, brechas y preferencias, con contenidos diferenciados para usuarios finales (higiene digital, credenciales, reporte, uso aceptable, privacidad), personal técnico (endurecimiento, redes, vulnerabilidades, desarrollo seguro, nube, respuesta a incidentes) y líderes (riesgo estratégico, gobernanza, cumplimiento, crisis) (NIST SP 800-50r1, 2024, secciones 2.2, 4.1 y apéndices orientativos).

Esta segmentación eleva la relevancia e impacto, reduce fatiga y mejora la trazabilidad hacia objetivos del programa, permitiendo medir mejor la contribución de cada intervención a la reducción de riesgo (NIST SP 800-50r1, 2024, secciones 3.3 y 4.1).

Ciclo de Vida del Aprendizaje: Enfoque ADDIE Adaptado. Como marco estructural para el desarrollo del PCSI, el modelo ADDIE orienta la organización de las fases de Planificación y Estrategia y Análisis y Diseño, estableciendo la secuencia lógica de actividades, entregables y criterios de validación que guían la construcción del programa. El documento adopta el modelo ADDIE (Análisis, Diseño, Desarrollo, Implementación y Evaluación) como ciclo de vida del CPLP. Análisis identifica necesidades, riesgos, objetivos y audiencias; Diseño define resultados de aprendizaje, contenidos, modalidades, duración y evaluación; Desarrollo crea materiales y valida con expertos; Implementación despliega en plataformas, gestiona convocatorias, accesibilidad e inclusión; Evaluación es continua y multinivel sobre reacción, aprendizaje, comportamiento y resultados, realimentando el ciclo (NIST SP 800-50r1, 2024, secciones 4.1–4.3).

Este ciclo impulsa iteración basada en datos y evidencia, asegurando que contenidos y métodos evolucionen con las amenazas y mantengan pertinencia y eficiencia (NIST SP 800-50r1, 2024, secciones 3.3 y 4.3)

Contenidos, Modalidades y Frecuencia Recomendada. Como referencia práctica para el desarrollo del PCSI, las orientaciones del NIST se utilizan en la fase de Análisis y Diseño para seleccionar temas prioritarios por tipo de audiencia, definir la combinación de modalidades y frecuencia de las intervenciones, e incorporar principios de aprendizaje continuo y en el flujo de trabajo. El NIST promueve un enfoque multimodal y continuo: para audiencias generales, contraseñas y MFA, phishing e ingeniería social, manejo y clasificación de datos, seguridad de dispositivos y trabajo remoto, uso aceptable, privacidad y reporte de incidentes; para perfiles técnicos, vulnerabilidades, parches y configuración segura, nube, desarrollo seguro, redes, respuesta a incidentes, forense básico y criptografía aplicada (NIST SP 800-50r1, 2024, sección 4.1).

La frecuencia combina formación anual obligatoria con microcontenidos y campañas periódicas, simulaciones de phishing con retroalimentación y actualizaciones ad hoc ante

incidentes o nuevas amenazas. Repetición espaciada, recordatorios contextuales y nudges ayudan a consolidar hábitos; accesibilidad y localización aseguran cobertura de toda la fuerza laboral y terceros (NIST SP 800-50r1, 2024, secciones 3.1 y 4.2).

Se incentiva el aprendizaje en el flujo de trabajo (avisos contextuales, checklists, ayudas de trabajo) y comunidades de práctica técnicas; la curaduría de contenidos externos confiables mantiene vigencia y actualidad del programa (NIST SP 800-50r1, 2024, secciones 3.1 y 4.2).

Integración con Gestión de Riesgos, Controles y Cumplimiento. Como fundamento para el desarrollo del PCSI, las directrices de integración se aplican en las fases de Planificación y Estrategia y Análisis y Diseño para vincular el programa con la gestión de riesgos de La “mediana empresa de tecnología”, definir activadores de contenido basados en eventos y establecer mecanismos de coordinación con terceros. El CPLP se integra con la gestión de riesgos y los controles del programa de seguridad y privacidad, trazando contenidos y campañas a escenarios prioritarios y a prácticas/políticas internas; esto facilita auditorías, evidencia y comunicación ejecutiva (NIST SP 800-50r1, 2024, secciones 2.3 y 3.3).

La integración incluye activadores por eventos: hallazgos de auditoría, resultados de phishing, incidentes, vulnerabilidades críticas, cambios normativos o adopción tecnológica. El aprendizaje funge como tratamiento de riesgo con acciones correctivas y preventivas reflejadas en planes de mejora y registros de riesgo (NIST SP 800-50r1, 2024, sección 3.3).

La coordinación con terceros (cláusulas de capacitación, verificación de cumplimiento y métricas compartidas) es esencial para extender la cultura de seguridad a la cadena de valor (NIST SP 800-50r1, 2024, secciones 2.2 y 3.2).

Métricas, Evidencia y Mejora Continua Basada en Datos. Como base para el desarrollo del PCSI, estas directrices de medición y mejora continua se utilizan en las fases de Planificación y Estrategia y Análisis y Diseño para definir el sistema de indicadores, establecer los niveles de evaluación, identificar fuentes de datos y diseñar los mecanismos de retroalimentación del programa. La medición es un pilar del enfoque NIST: Se distinguen cuatro niveles de evaluaciones cuantitativas: participación/alcance (quiénes completan y con qué frecuencia), aprendizaje (resultados de evaluaciones y certificaciones), comportamiento (cambios observables en el puesto, reducción de errores, reporte proactivo) y resultados (impacto en indicadores de riesgo: tasa de clic en phishing, incidentes por causa humana, hallazgos repetitivos, cumplimiento de prácticas clave). dichas métricas deben ligarse a hipótesis de cambio conductual y umbrales de riesgo aceptables; la analítica combina datos del LMS, SIEM/SOAR, GRC, vulnerabilidades, mesa de ayuda y auditorías; los tableros ejecutivos deben mostrar las tendencias y las brechas; Las evaluaciones cualitativas (entrevistas, grupos focales) complementan las evaluaciones cuantitativas para comprender barreras y oportunidades. (NIST SP 800-50r1, 2024, secciones 3.3 y 4.3).

La mejora continua aplica A/B testing de mensajes, iteración instruccional, ajustes de frecuencia y modalidades y actualizaciones ágiles frente a nuevas amenazas o regulación, cerrando el ciclo de retroalimentación (NIST SP 800-50r1, 2024, sección 4.3).

Cultura Organizacional, Liderazgo y Gestión del Cambio. Como orientación para definir en la fase de Planificación y Estrategia los mecanismos de patrocinio ejecutivo, los mensajes clave del PCSI y las estrategias de comunicación que harán tangible la conexión entre seguridad y continuidad del negocio en la “mediana empresa de tecnología”, y en Análisis y Diseño los enfoques de gestión del cambio, accesibilidad e inclusión que reduzcan fricciones cognitivas y garanticen cobertura equitativa de la fuerza laboral. El éxito del CPLP depende en gran medida de la cultura y del liderazgo visible. Los líderes deben modelar comportamientos seguros, comunicar prioridades y reconocer públicamente prácticas deseadas. La narrativa organizacional debe conectar la ciberseguridad y la privacidad con la misión, la confianza del cliente y la continuidad del negocio (NIST SP 800-50r1, 2024, secciones 1.3 y 3.1).

La gestión del cambio aborda incentivos, fricciones y la carga cognitiva de los usuarios. Se promueven mensajes simples y accionables, reforzados de manera repetida y coherente, con apoyos como asistentes, plantillas y checklists. La inclusión y la accesibilidad garantizan que todas las personas tengan oportunidad real de aprender y aplicar lo aprendido, reduciendo brechas y riesgos sistémicos (NIST SP 800-50r1, 2024, secciones 3.1–3.2).

En resumen, el NIST SP 800-50r1 posiciona el aprendizaje como un habilitador estratégico de la seguridad y la privacidad: un programa intencional, medible y alineado con los riesgos del negocio, que evoluciona de manera continua y se integra con la gobernanza, los controles y la cultura para producir comportamientos sostenibles y resultados verificables (NIST SP 800-50r1, 2024, secciones 1.1–1.3 y 4.3).

Documentos de Origen de la “mediana empresa de tecnología” Alineados al Plan de Concientización en Seguridad de la Información (PCSI)

Este capítulo integra los lineamientos y prácticas internas de la “mediana empresa de tecnología” relevantes para alinear el Plan de Concientización en Seguridad de la Información (PCSI), estos documentos corporativos vigentes pueden y deben traducirse en competencias, contenidos y métricas de aprendizaje para toda la organización.

Las políticas y lineamientos de la “mediana empresa de tecnología” son fundamentales porque permiten alinear la investigación con la realidad normativa, operativa y cultural específica de la organización, evitando un diseño genérico del PCSI. Gracias a estos documentos, es posible identificar procesos, responsabilidades, riesgos y controles ya definidos, que sirven como base para perfilar públicos, priorizar temas y contextualizar los contenidos de capacitación. Al incluirlos, se obtiene un plan de concientización más pertinente, aplicable y medible, con conexiones claras entre la teoría (NIST, ISO 27001/27002) y las prácticas internas existentes (“mediana empresa de tecnología”, 2021; ISO,2022a; ISO,2022b; NIST, 2024).

Procedimiento de Capacitación y entrenamiento. Como fundamento operativo para las fases de Planificación y Estrategia y Análisis y Diseño del PCSI, este procedimiento institucional de la “mediana empresa de tecnología” proporciona la estructura, los ciclos de planificación, los indicadores y los mecanismos de evaluación que permiten alinear el diseño del programa de concientización con los procesos formales de gestión de competencias ya establecidos en la organización. Este procedimiento consolida un conjunto de prácticas que fortalecen la alineación del diseño del PCSI con la gestión de competencias y el desarrollo organizacional en la “mediana empresa de tecnología”. A través de una estructura de planificación anual, un seguimiento periódico semestral y el uso de indicadores definidos, la compañía asegura que la formación sea un proceso controlado y orientado a resultados. Los niveles mínimos de evaluación y los requisitos de documentación garantizan trazabilidad y mejora continua, ofreciendo una base sólida y confiable para el diseño del Plan de Concientización en Seguridad de la Información, de modo que se integre de manera natural y armónica con el sistema institucional de capacitación y crecimiento del talento humano (“mediana empresa de tecnología” S.A.S., 2024).

El procedimiento Capacitación y entrenamiento de la “mediana empresa de tecnología” establece los parámetros que regulan la planeación, ejecución y evaluación de todas las

actividades de formación en la organización, definiendo un marco formal que puede servir como base directa para estructurar el PCSI (Plan de Concientización en Seguridad de la Información). El objetivo de este procedimiento es fortalecer los conocimientos, competencias y habilidades del personal, tanto desde la perspectiva del desarrollo profesional como de la prevención de riesgos laborales, garantizando que la capacitación contribuya al bienestar de los colaboradores y al cumplimiento de los objetivos institucionales (“mediana empresa de tecnología”, 2024).

El proceso inicia con la identificación de las necesidades de aprendizaje, actividad que se nutre de insumos como los planes de mejora, evaluaciones de desempeño, requerimientos derivados de nuevos ingresos y análisis de riesgos prioritarios. A partir de esta información, el área de Transformación y Desarrollo consolida las necesidades, diseña o ajusta el plan de formación, lo somete a aprobación de la dirección y, una vez validado, procede con la implementación y organización de los eventos de capacitación. En su flujo operativo, el procedimiento define de manera explícita la secuencia de responsabilidades que abarca desde la solicitud inicial hasta la generación de informes para los directores de proceso, incluyendo la búsqueda de proveedores, la validación de materiales, la evaluación de la efectividad y el seguimiento documentado de resultados (“mediana empresa de tecnología”, 2024, Diagrama del proceso).

El plan de formación debe elaborarse anualmente, preferiblemente en el último trimestre del año anterior al de ejecución, para garantizar una programación anticipada y coherente con los objetivos estratégicos. Además, el procedimiento contempla la inducción para personal nuevo durante los dos primeros días de ingreso y la reinducción anual para quienes cuentan con una antigüedad superior a seis meses. El seguimiento al plan es trimestral, lo que permite evaluar de forma periódica el avance de la formación y la cobertura alcanzada. Estas directrices aseguran una planificación estable y un monitoreo continuo sobre la eficacia del programa (“mediana empresa de tecnología”, 2024, Políticas 1-2).

El procedimiento enfatiza la autorización previa del director de Transformación y Desarrollo cuando las capacitaciones impliquen viáticos o gastos logísticos y dispone que las citaciones a los participantes se envíen con mínimo ocho días de anticipación, garantizando así la disponibilidad y adecuada asistencia. También establece indicadores que orientan la gestión del aprendizaje: el indicador de cobertura, con meta de 60 %, mide la participación en capacitaciones técnicas obligatorias y organizacionales; el de calificación, con meta de 80 %, evalúa los resultados de las pruebas aplicadas a contenidos; y el de cumplimiento del plan, con meta de 90 %, establece la proporción entre actividades ejecutadas y planificadas. Estos indicadores institucionalizan los criterios de desempeño del proceso formativo y constituyen parámetros directos de medición que pueden integrarse en el PCSI como métricas de eficacia (“mediana empresa de tecnología”, 2024, Capacitación y entrenamiento, Políticas 3-4).

En cuanto a la evaluación, el documento distingue dos tipos: la evaluación del capacitador y la evaluación del contenido. Si los resultados de la evaluación al capacitador o al contenido son inferiores al 60 %, se deberán adoptar medidas correctivas, como el cambio de proveedor o la repetición del tema con material reforzado. Los procesos de inducción y reinducción aplican estos mismos criterios, repitiendo las actividades cuando las calificaciones son menores a 60 %. De manera complementaria, las evaluaciones de desempeño anuales incluyen un componente que considera las capacitaciones técnicas recibidas por cada colaborador, verificando su contribución al desempeño del cargo (“mediana empresa de tecnología” S.A.S., 2024, Capacitación y entrenamiento, Políticas 5-6; Notas aclaratorias, Actividad 8).

El contenido mínimo del plan de formación es otro parámetro formal: debe incluir el tema, objetivo, población dirigida, proceso, horas, formador, cronograma, fecha, cobertura esperada, resultado de evaluación y presupuesto asignado. En paralelo, se exige a los proveedores garantizar la disponibilidad del material o el registro grabado de la capacitación,

reforzando la trazabilidad del proceso (“mediana empresa de tecnología”, 2024, Capacitación y entrenamiento, Notas aclaratorias, Actividades 3 y 6). Finalmente, el procedimiento establece el mantenimiento de registros: el formato de Plan de formación y capacitación, las evidencias de asistencia y las evaluaciones de cada actividad deben almacenarse en los repositorios institucionales de SharePoint. Los resultados consolidados y las métricas de cobertura, calificación y ejecución se reportan anualmente a los directores de los procesos, completando el ciclo de mejora del sistema de formación (“mediana empresa de tecnología”, 2024, Capacitación y entrenamiento, Registros y Actividades 9-13).

Este procedimiento define un conjunto de prácticas verificables que soportan la coherencia del PCSI con la gestión de competencias y el desarrollo organizacional de la “mediana empresa de tecnología”. Su estructura de planificación anual, seguimiento trimestral, indicadores normados, niveles mínimos de evaluación y requerimientos de documentación proporcionan una base sólida para el diseño del Plan de Concientización en Seguridad de la Información, garantizando que este se integre sinérgicamente al sistema de formación institucional. (“mediana empresa de tecnología”, 2024, Capacitación y entrenamiento).

Política de uso de Activos y Recursos de Teleinformática. El siguiente contenido se aplica, principalmente en la fase de Planificación y Estrategia y se prolonga en Análisis y Diseño, como criterio para derivar objetivos del PCSI, perfilar conductas esperadas y priorizar temas y reglas que deben transformarse en contenidos, casos y métricas de cumplimiento. El documento Política de uso de activos y recursos de teleinformática es clave porque define las reglas de comportamiento esperado de los usuarios frente a los recursos tecnológicos de la "mediana empresa de tecnología", que son precisamente el foco del PCSI. Esta investigación busca diseñar un plan de capacitación y sensibilización que ayude a que esas reglas se entiendan, se interioricen y se cumplan de forma consistente en el trabajo diario. De este modo, el PCSI se alinea directamente con la política, traduciéndola en contenidos formativos, ejemplos prácticos y conductas observables dentro de la organización ("mediana empresa de tecnología", Política de uso de activos y recursos de teleinformática, 2021).

La política establece un marco corporativo para el uso, protección y administración de los activos tecnológicos de la "mediana empresa de tecnología", delimitando que todo uso de hardware, software, redes y servicios es exclusivamente laboral y orientado a salvaguardar la confidencialidad, integridad y disponibilidad de la información. Aplica a colaboradores y terceros que accedan a los activos, y legitima el monitoreo corporativo de los medios cuando sea necesario para control o verificación, preservando las obligaciones de custodia del usuario sobre su cuenta y equipo asignado ("mediana empresa de tecnología", Política de uso de activos y recursos de teleinformática, 2021, pp. 1–4, 8–10).

Define un modelo de administración centralizada a cargo de Infraestructura: asignación y retiro de equipos, creación de usuarios para Windows, Office 365, correo Hostmonster y SAP, estandarización de nombres de máquina, gestión de "casos especiales" y recolección de activos al finalizar la relación. Se prohíbe instalar software sin licencia y se exige la trazabilidad documental de licenciamiento; los equipos corporativos no pueden conectarse a la red de

invitados (“mediana empresa de tecnología”, Política de uso de activos y recursos de teleinformática, 2021, pp. 4–7).

En ciberhigiene técnica, el antivirus corporativo ESET Endpoint debe permanecer activo y actualizado; deshabilitarlo más de una hora es una violación grave. Las actualizaciones automáticas de sistema y aplicaciones son obligatorias en equipos y servidores; las excepciones solo pueden ser aprobadas y registradas por Infraestructura. El uso de medios extraíbles está prohibido salvo excepciones puntuales bajo condiciones de escaneo y resguardo (“mediana empresa de tecnología”, Política de uso de activos y recursos de teleinformática, 2021, pp. 5–6, 7–8).

El correo corporativo es el canal aprobado para comunicaciones internas y externas; su uso es personal e intransferible y puede ser inspeccionado por la compañía. Se prohíben suplantación, spam/hoax, compartir credenciales y vulnerar datos personales; el líder de proceso gestiona redirecciones y capacidades conforme necesidades, y toda novedad de vinculación o retiro debe escalarse oportunamente a Infraestructura (“mediana empresa de tecnología”, Política de uso de activos y recursos de teleinformática, 2021, pp. 8–10).

La navegación en Internet se limita a fines del negocio: se vetan P2P, streaming no laboral, contenidos ilícitos o que violen propiedad intelectual, evasión de controles y cualquier actividad que degrade el servicio o implique fraude o ataques. Se exige prudencia ante enlaces, descargas y ventanas emergentes, consultando a Infraestructura cuando existan dudas (“mediana empresa de tecnología”, Política de uso de activos y recursos de teleinformática, 2021, pp. 11–12).

Son inaceptables actos que comprometan la seguridad: monitoreo o captura de tráfico sin autorización, uso de herramientas de hacking o firewalls no autorizados, pruebas de vulnerabilidades, divulgación de factores de autenticación, almacenamiento de credenciales y dejar sesiones abiertas o escritorios desbloqueados. El uso de herramientas de acceso remoto

está restringido a autorizaciones formales y registradas (“mediana empresa de tecnología”, Política de uso de activos y recursos de teleinformática, 2021, pp. 12–13).

Para BYOD y VPN, el acceso personal se limita a la red de invitados y el uso de recursos internos debe hacerse exclusivamente por VPN sin almacenar credenciales. La “mediana empresa de tecnología” puede auditar, limitar o suspender el servicio de invitados; el usuario es responsable del estado de su dispositivo, su antivirus y de reportar la MAC cuando se solicite. Aplican restricciones de alto consumo de ancho de banda y se desaconseja el almacenamiento de credenciales (“mediana empresa de tecnología”, Política de uso de activos y recursos de teleinformática, 2021, pp. 13–14).

La compartición de información debe canalizarse por O365 (SharePoint/OneDrive/Delve), con gobernanza a cargo del líder de proceso, control de accesos y no uso como repositorio de copias de respaldo personales; la información es de uso interno y su divulgación externa requiere autorización (“mediana empresa de tecnología”, Política de uso de activos y recursos de teleinformática, 2021, pp. 15–16).

En computación en la nube y movilidad, se requiere cerrar sesiones, no guardar contraseñas, usar antivirus actualizado y evitar equipos inseguros o redes públicas para acceso a recursos críticos. Para portátiles y móviles, se exigen controles físicos, autenticación por inactividad y custodia diligente; el colaborador responde por pérdida o daño conforme condiciones de reposición y debe reportar incidentes de inmediato (“mediana empresa de tecnología”, Política de uso de activos y recursos de teleinformática, 2021, pp. 16–18).

Política de Firewall. Esta política se traduce, en Planificación y Estrategia y en Análisis y Diseño, en criterios concretos para priorizar riesgos técnicos, definir conductas esperadas en el uso de red y estructurar contenidos del PCSI sobre navegación segura y gestión de excepciones. La política define la arquitectura y las reglas de control perimetral y de host para proteger el tránsito de información entre la red de la “mediana empresa de tecnología” y redes externas, asegurando que todo tráfico sea gestionado por firewalls y proxy con perfiles de navegación diferenciados. Aplica a todos los equipos que ingresan a la red corporativa. Establece dos capas: el firewall del sistema operativo Windows, obligatorio y siempre activo en estaciones y servidores, cuya modificación solo procede por solicitud y registro formal; y el firewall perimetral Fortinet, administrado con soporte externo, que clasifica y filtra tráfico por categorías de URL, puertos y servicios desde y hacia Internet (“mediana empresa de tecnología”, Política de Firewall, 2021, pp. 2–3).

La política operacionaliza el control de navegación mediante perfiles de grupo (liderazgo, comercial, tecnológico, genérico). Dado que no hay Directorio Activo, la asignación se realiza por dirección MAC del equipo, lo que permite aplicar permisos según necesidades del rol. Cualquier excepción de acceso o cambio de configuración debe ser validada por Infraestructura y quedar documentada en SharePoint, garantizando trazabilidad de autorizaciones y cambios sobre reglas y listas (“mediana empresa de tecnología”, Política de Firewall, 2021, p. 3).

Complementariamente, incorpora el proxy de ESET como extensión del control cuando los equipos están fuera de las instalaciones, heredando las mismas políticas de filtrado que el firewall perimetral. Este proxy también puede regular el uso de dispositivos de almacenamiento portátiles. Excepciones para navegación o dispositivos removibles requieren autorización del director de proceso y archivarse en la carpeta de “Autorizaciones excepciones” del sitio de Infraestructura. La interacción con el canal público contempla exposición de servicios corporativos (VPN, SAP, MDM) bajo control del firewall perimetral y políticas consistentes con la

política de uso de recursos TI (“mediana empresa de tecnología”, Política de Firewall, 2021, pp. 2, 5).

Política de Respaldo de Información. La política establece el marco integral de copias de seguridad para proteger la información individual, grupal y de servidores, asignando responsabilidades compartidas entre los propietarios de la información y el proceso de Infraestructura Tecnológica. Aplica a todo equipo y servidor que almacene datos de la “mediana empresa de tecnología”, clientes y socios. Define que Infraestructura administra las herramientas y verifica confiabilidad; los dueños de información deben usar los repositorios autorizados y reportar anomalías. El acceso a respaldos puede concederse a propietarios, Infraestructura y directivos según necesidad operativa, con solicitudes registradas (“mediana empresa de tecnología”, Política de respaldo de información, 2021, pp. 1–3).

Para equipos individuales, se prioriza OneDrive de Microsoft, que sincroniza automáticamente la carpeta corporativa designada, configurada por Infraestructura y operada por el usuario; ante fallas debe generarse ticket para evitar pérdida de datos. En intervenciones de riesgo, se usan discos externos USB gestionados por Infraestructura para copias temporales y eventuales restauraciones verificadas. Para información grupal, cada proceso dispone de un sitio SharePoint con sincronización local para continuidad sin Internet, administrado por el líder de proceso y soportado por Infraestructura (“mediana empresa de tecnología”, Política de respaldo de información, 2021, pp. 3–4).

Establece parámetros de operación para OneDrive/SharePoint (límites de elementos, tamaños, nombres y profundidad de carpetas) para asegurar sincronización fiable y evitar errores. Para servidores físicos, define un esquema de NAS con tres horizontes de retención: diario, semanal y mensual, con verificación semanal de logs por el Coordinador de Infraestructura y limpieza periódica para gestionar capacidad. Se complementa con sincronización externa de OneDrive para resiliencia ante desastres en sitio (“mediana empresa de tecnología”, Política de respaldo de información, 2021, pp. 4–5).

En AWS, contempla tres mecanismos: snapshots diarios con retención de 4 días; AWS Backup con planes y caducidad de 4 días; y una herramienta propia de la “mediana empresa de tecnología” llamada Backup para la “mediana empresa de tecnología” que realiza respaldos de bases de datos y sitios en S3. La combinación de estos controles busca disponibilidad y restauración ante fallas o incidentes, cubriendo cargas on-premises y en la nube con redundancias y ciclos de vida definidos (“mediana empresa de tecnología”, Política de respaldo de información, 2021, p. 5).

Política de Escritorio y Pantalla Limpia. Este marco normativo fundamenta en Análisis y Diseño la creación de piezas gráficas y mensajes de refuerzo sobre ciberhigiene física, estableciendo los parámetros técnicos obligatorios para el bloqueo de sesiones y manejo de impresiones. La política busca prevenir accesos no autorizados y pérdidas de información mediante prácticas de orden físico y seguridad lógica en puestos de trabajo, aplicable a todos los colaboradores y terceros que gestionen información de la “mediana empresa de tecnología” en oficinas o de forma remota. Establece dos ejes: escritorio limpio, que exige retirar y resguardar documentos y medios removibles al ausentarse o al finalizar la jornada, evitando notas visibles y fomentando apagado o hibernación nocturna; y pantalla limpia, que obliga a bloquear sesión al ausentarse, mantener escritorios sin accesos directos sensibles y respaldar al cierre del día en OneDrive o SharePoint, reportando alertas de sincronización de inmediato a Infraestructura (“mediana empresa de tecnología”, Política de escritorio y pantalla limpia, 2023, pp. 1–3).

Regula la impresión bajo necesidad estricta, con retención segura en puntos de impresión, orden en áreas de impresoras y fomento de canales digitales. Permite papel reciclado solo si el reverso impreso no contiene datos personales o sensibles; detalla ejemplos de datos prohibidos. En seguridad de sesión, impone protector de pantalla automático a los 10 minutos de inactividad, gestionado por Infraestructura y no modificable por usuarios; requiere apagado al final de la jornada, permitiendo hibernación por máximo un día en casos

excepcionales. Autoriza a Infraestructura a forzar apagado o reinicio después de las 22:00 ante amenazas o vulnerabilidades críticas. Prohíbe almacenar contraseñas en navegadores, escritorios remotos o herramientas de BD (“mediana empresa de tecnología”, Política de escritorio y pantalla limpia, 2023, pp. 3–4).

En cumplimiento, advierte consecuencias disciplinarias por infracciones y faculta a Infraestructura para eliminar información que vulnere la política según el riesgo, con retención temporal de información física por áreas responsables hasta resolver la conducta y medidas correctivas correspondientes (“mediana empresa de tecnología”, Política de escritorio y pantalla limpia, 2023, p. 5).

Política de Contraseñas Seguras. Este estándar técnico suministra en Análisis y Diseño los requisitos de robustez y periodicidad que deben comunicarse a los colaboradores, justificando además el uso obligatorio del gestor de contraseñas corporativo. La política define responsabilidades y requisitos para la creación, uso, almacenamiento y renovación de contraseñas en todos los sistemas de La “mediana empresa de tecnología”, aplicable a todo colaborador. Establece que cada administrador de sistema debe exigir autenticación, forzar cambio tras restablecimientos manuales, proteger contraseñas en tránsito y almacenar hashes cifrados; mientras, el usuario es responsable de la custodia y del uso de la herramienta corporativa de gestión de contraseñas, de uso obligatorio y con base en OneDrive cifrada. Las credenciales son personales e intransferibles, y su transmisión inicial debe hacerse de forma confidencial; se restringe guardar contraseñas en navegadores, escritorios o dispositivos locales (“mediana empresa de tecnología”, Política de contraseñas seguras, 2025, pp. 1–3).

Define criterios mínimos de robustez: longitud mínima de 8 caracteres (o la máxima que permita el sistema si es inferior), combinación de mayúsculas, minúsculas, números y símbolos; evitar secuencias de teclado, repeticiones, palabras de diccionario y datos asociados al usuario o a la entidad. La periodicidad de cambio es de 90 días como mínimo; se exige cambio inmediato ante sospecha de compromiso y se bloquea la reutilización de contraseñas anteriores

cuando el sistema lo permita. Los administradores deben usar contraseñas distintas para cuentas personales y privilegiadas; cambiar credenciales predeterminadas de equipos/aplicaciones al entrar en operación; rotar contraseñas privilegiadas al retiro de personal; e inactivar credenciales de usuarios durante vacaciones. Ante sustracción de elementos que puedan contener contraseñas, el usuario debe reportar a Infraestructura en menos de 24 horas las herramientas comprometidas. Se recomienda contar con usuarios alternos de administración con privilegios mínimos para contingencias (“mediana empresa de tecnología”, Política de contraseñas seguras, 2025, pp. 3–5).

Instructivo Para Uso de VPN en La “mediana empresa de tecnología”. Este instructivo aporta, sobre todo en Análisis y Diseño, los criterios para delimitar los escenarios de trabajo remoto que el PCSI debe cubrir, así como las conductas esperadas al usar VPN desde equipos corporativos o personales. El instructivo regula el uso de la VPN corporativa para acceso remoto a recursos de la “mediana empresa de tecnología”, estableciendo políticas de auditoría, custodia de credenciales y restricciones de uso que aplican incluso cuando se conecta desde equipos personales. Las conexiones pueden ser monitoreadas por Infraestructura; los accesos son personales e intransferibles y deben eliminarse al retiro del usuario. Se prohíbe configurar la VPN en equipos públicos o no controlados, y no se permite guardar contraseñas en los dispositivos. El Coordinador de Infraestructura autoriza y revoca accesos según necesidades del cargo; los directores pueden solicitar accesos y resolver discrepancias con Dirección General. El usuario debe reportar pérdidas o exposición de credenciales o equipos donde configuró VPN para que se roten las claves de inmediato (“mediana empresa de tecnología”, Instructivo VPN, 2019, pp. 1–3).

Operativamente, se utiliza FortiClient con dos perfiles de conexión (VPN_ “MEDIANA EMPRESA DE TECNOLOGÍA” y SSL_VPN) para redundancia por gateways y proveedores distintos; ambos deben configurarse siguiendo parámetros específicos de gateway y puertos descritos. (“mediana empresa de tecnología”, Instructivo VPN, 2019, pp. 4–10).

Procedimiento de Gestión de Incidentes de Seguridad de la Información. Este procedimiento aporta, en Planificación y Estrategia y en Análisis y Diseño, los flujos, roles y tiempos de respuesta que el PCSI debe enseñar y practicar para que el reporte y manejo de incidentes se ejecute sin ambigüedades. El procedimiento estandariza la gestión integral de incidentes de SI desde el reporte hasta el cierre, cubriendo preparación, contención, respuesta, recuperación y cierre. Establece canales de notificación (CRM de servicio y correo reporteseguridad@medianaempresadetecnología.com.co), obligación de reporte inmediato por parte de colaboradores y terceros, y la intervención del Oficial de Seguridad para analizar, clasificar, priorizar y escalar. Define un Equipo de Respuesta a Incidentes multidisciplinario, revisiones anuales de planeación y resguardo de evidencia para base de conocimientos. Incidentes que afecten bases de datos personales deben reportarse a la SIC en 15 días hábiles; cuando involucren datos personales, se notifica al Oficial de Protección de Datos. Transformación & Desarrollo y Jurídica intervienen según corresponda. La trazabilidad se concentra en el CRM de servicio (“mediana empresa de tecnología”, Gestión de Incidentes de SI, 2024, pp. 1–3).

Las actividades clave incluyen: validar el evento y recolectar información; analizar impacto en confidencialidad, integridad y disponibilidad; clasificar y priorizar; y ejecutar contención, erradicación y recuperación. Medidas de contención contemplan aislar instancias mediante grupos de seguridad o ACL, etiquetar cuarentena, bloquear IP/puertos/unidades, aplicar parches y, si es necesario, activar el plan de recuperación ante desastres. La erradicación implica eliminar programas maliciosos, limpiar sistemas afectados y fortalecer accesos; la recuperación prioriza restablecer servicios críticos, restaurar desde backups y reactivar cuentas. Se especifica la preservación y, si procede, adquisición forense por terceros con credenciales, incluyendo imágenes bit a bit y cálculo de hash. Finalmente, se documentan impactos y causa raíz, se prepara y ejecuta un plan de tratamiento, y se registran lecciones

aprendidas antes de la revisión y cierre formal por el Oficial de Seguridad (“mediana empresa de tecnología”, Gestión de Incidentes de SI, 2024, pp. 3–6).

Procedimiento Gestión de Vulnerabilidades Técnicas. El procedimiento define cómo identificar, evaluar, priorizar, tratar y hacer seguimiento a vulnerabilidades técnicas en la infraestructura y aplicaciones de la “mediana empresa de tecnología”, asegurando trazabilidad y reducción del riesgo tecnológico. Establece responsabilidades para el Equipo de Infraestructura y áreas técnicas, desde la detección (escaneos programados, alertas de fabricantes, reportes de terceros) hasta el cierre, con registro en la herramienta correspondiente y evidencias de mitigación. Incluye criterios de clasificación de criticidad para priorizar remediaciones y establece ventanas de atención diferenciadas según severidad, además de escalamiento cuando se afecten activos críticos o existan riesgos de explotación activa (“mediana empresa de tecnología”, Procedimiento Gestión de vulnerabilidades técnicas, s. f., visión general).

El flujo típico contempla: inventario de activos y alcance de escaneo; ejecución de herramientas de análisis; consolidación de hallazgos con CVE/CVSS; validación técnica para descartar falsos positivos; clasificación por severidad e impacto; definición del plan de tratamiento (parcheo, configuración, compensación temporal); pruebas controladas; despliegue en producción en ventanas aprobadas; y verificación post-parcheo. Se contempla gestión especial para vulnerabilidades de día cero y aquellas sin parche disponible, con controles compensatorios y monitoreo reforzado. El procedimiento requiere comunicación a responsables de activos, documentación de excepciones justificadas con fecha de expiración y revisión periódica de efectividad. Finalmente, se reportan métricas como tiempo medio de remediación por severidad, porcentaje de cobertura de escaneo y excepciones vigentes para la mejora continua (“mediana empresa de tecnología”, Procedimiento Gestión de vulnerabilidades técnicas, s. f., buenas prácticas y flujo operativo).

Diseño Metodológico

Tipo de Investigación

El estudio se enmarca en una investigación aplicada, orientada al diseño de un Plan de Concientización en Seguridad de la Información (PCSI) para la “mediana empresa de tecnología”, alineado con el SGSI y las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, así como con la guía NIST SP 800-50r1.

Enfoque

El enfoque es cualitativo con apoyo de datos cuantitativos descriptivos. Los datos numéricos provenientes de auditorías, pruebas de phishing y evaluaciones internas se emplean como evidencia para describir el estado actual y dimensionar brechas de comportamiento, pero no se plantea un diseño experimental ni pruebas de hipótesis estadísticas. Este enfoque busca identificar cómo los colaboradores se relacionan con las políticas y controles del SGSI, contrastando el comportamiento observado con el esperado según ISO/IEC 27001:2022, para diseñar un Plan de Concientización en Seguridad de la Información (PCSI) contextualizado y basado en el análisis de brechas que se realizó en la consultoría y auditoría.

Técnicas e Instrumentos de Recolección de Datos

Para el diseño del Plan de Concientización en Seguridad de la Información (PCSI) en la “mediana empresa de tecnología”, se utilizaron técnicas e instrumentos de recolección de datos centrados en la información ya existente en la organización. Este enfoque se alinea con la guía NIST SP 800-50r1, que sugiere usar datos disponibles para la fase de planeación de programas de concientización (NIST, 2024).

La técnica principal fue la revisión documental y análisis de evidencias internas. Se recopilaron informes de auditoría, reportes de campañas de phishing, resultados de evaluaciones de capacitación y documentos normativos internos (políticas y procedimientos de seguridad de la información y protección de datos personales). Estos documentos sirvieron

como fuentes primarias para obtener evidencias sobre comportamientos y niveles de cumplimiento (“mediana empresa de tecnología”, 2024).

Como instrumentos específicos, se consultó el informe de auditoría de la “empresa auditora” de 2024, del cual se extrajeron datos sobre prácticas como el escritorio limpio y el uso de servicios no autorizados (“empresa auditora”, 2024). También se utilizó el informe de campaña de phishing de la “Empresa Consultora en seguridad”, que proporcionó registros de tasas de apertura, clic y reporte de correos simulados, directamente de la plataforma del proveedor (“Empresa Consultora en seguridad” S.A., 2024).

Adicionalmente, se emplearon los resultados de la evaluación posterior a la capacitación sobre datos personales, aplicada a gran parte del personal. Estos resultados, obtenidos del sistema de evaluación interno, incluyeron calificaciones y desempeño por pregunta (“mediana empresa de tecnología”, 2024).

Finalmente, se revisaron las políticas y procedimientos internos de seguridad de la información. Estos documentos formales establecieron los requisitos y expectativas de comportamiento que luego se contrastarían con la información recopilada (ISO, 2022).

Población

La población está conformada por todos los colaboradores de la “mediana empresa de tecnología” que tienen relación directa o indirecta con la seguridad de la información, incluyendo personal de Infraestructura Tecnológica (TI), Recursos Humanos (T&D), Administrativo y Financiero (A&F), y otras áreas que manejan o acceden a información sensible o crítica para la organización. Esto incluye desde el director general hasta los empleados operativos, ya que todos forman parte del sistema de gestión de seguridad de la información y pueden ser sujetos de sensibilización.

Técnicas de Análisis de Datos

Las técnicas de análisis de datos usadas en el proyecto se apoyan en un enfoque cualitativo con soporte cuantitativo sencillo, orientado a identificar brechas de comportamiento y

convertirlas en necesidades formativas claras. En primer lugar, se realizó un análisis documental de diferentes fuentes internas: auditoría de seguridad (“empresa auditora”), informe de phishing (“Empresa Consultora en seguridad”), evaluación interna de protección de datos personales y políticas y procedimientos del SGSI. A partir de estos documentos se extrajeron indicadores clave, como porcentajes de equipos con hallazgos, tasas de apertura y clic en correos de prueba, ausencia de reportes y distribución de puntajes en la evaluación de datos personales. (“empresa auditora”, 2024; “Empresa Consultora en seguridad” S.A., 2024; “mediana empresa de tecnología”, 2024; Autores del PCSI, 2025).

Estos datos se trataron con estadística descriptiva básica (proporciones y porcentajes) para dimensionar el problema: por ejemplo, 10 % de incumplimiento en escritorio limpio, 10 % de uso de repositorios no oficiales, 4 % de clics en un correo malicioso y 0 % de reportes, o cerca de 25 % de bajo desempeño en temas críticos de datos personales. Estas cifras se usaron como línea base para fijar metas de mejora del plan, como reducir el CTR por debajo del 4 %, disminuir los hallazgos en auditoría y aumentar los reportes de phishing. (Autores del PCSI, 2025).

La técnica central fue un análisis de brechas: se comparó el comportamiento observado con el comportamiento esperado según políticas internas y controles ISO/IEC 27002:2022 (por ejemplo, escritorio limpio, uso aceptable de activos, transferencia de información, reporte de incidentes). Cuando la diferencia era consistente, se concluía que la política no se había consolidado como hábito y se definía una brecha de concientización. Así se agruparon los hallazgos en cuatro brechas principales: escritorio y pantalla limpia, uso de repositorios no oficiales, comportamiento ante correos maliciosos y comprensión insuficiente de aspectos críticos de protección de datos personales. (Autores del PCSI, 2025).

A partir de estas brechas se elaboró un catálogo de necesidades formativas. Cada brecha se vinculó con objetivos de aprendizaje, temas específicos y documentos de referencia. De allí se identificaron las necesidades de concientización del PCSI (concientización básica,

buenas prácticas y controles, manejo de incidentes, tratamiento de datos personales) y los contenidos concretos del curso a publicar en el LMS, las campañas y los microcontenidos.

Esta cadena "datos → brechas → contenidos → indicadores" asegura que el esfuerzo formativo responda a problemas reales y medibles, y no a temarios genéricos. (Autores del PCSI, 2025).

Todo este enfoque de análisis está alineado directamente con la NIST SP 800-50r1, que indica que un programa de aprendizaje en ciberseguridad y privacidad debe iniciar con la revisión de evidencias internas, definir brechas como diferencia entre estado actual y deseado, y traducirlas en necesidades de aprendizaje segmentadas por audiencia, con indicadores que permitan evaluar cambios en el tiempo. El proyecto aplicó precisamente estas recomendaciones en las fases de planeación y análisis del PCSI. (NIST, 2024).

Desarrollo

A continuación, se desarrolla el Plan de Concientización en Seguridad de la Información (PCSI) para la "mediana empresa de tecnología", estructurado bajo el rigor metodológico de las fases de Planificación y Estrategia, y Análisis y Diseño propuestas por la guía NIST SP 800-50r1 (NIST, 2024, Sec. 1.3). El contenido se organiza de manera lógica para establecer primero los cimientos del programa, definiendo su propósito, visión y la gobernanza necesaria para su éxito. Posteriormente, se avanza hacia la estructuración técnica donde se identifican las necesidades específicas de la organización y se diseña la arquitectura pedagógica y operativa que dará forma al plan.

A través de este desarrollo, se documenta la creación de un marco de trabajo alineado con los requisitos de competencia y concientización de la norma ISO/IEC 27001:2022 (ISO/IEC, 2022, Cláusulas 7.2 y 7.3). El lector encontrará el detalle de la segmentación de audiencias, la definición de temas clave de seguridad adaptados al contexto de la "mediana empresa de tecnología" y la construcción de un sistema de métricas diseñado para monitorear el progreso

del programa. Estas etapas consolidan el diseño integral del PCSI, proporcionando una hoja de ruta clara y técnica que responde a los objetivos de investigación planteados en este proyecto

Ciclo de Vida del PCSI

El PCSI de la “mediana empresa de tecnología” se estructura tomando como referencia la guía NIST SP 800-50r1, que recomienda el uso del modelo ADDIE (Analizar, Diseñar, Desarrollar, Implementar y Evaluar) como marco para crear programas de capacitación y sensibilización en seguridad de la información (NIST, 2024).

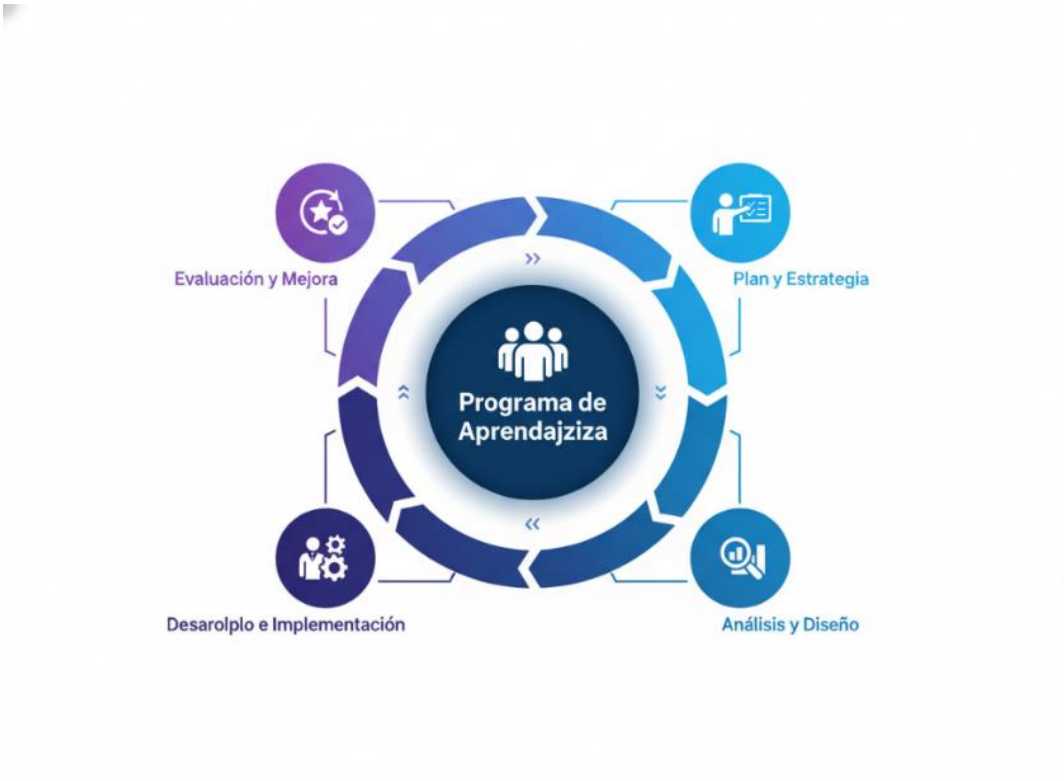
En este proyecto se adopta una variación del modelo ADDIE sugerida por la NIST, incorporando una fase preliminar denominada planificar. En esta fase se definen elementos de gobernanza, estrategia y estructura del PCSI, que no impactan directamente la operación de las etapas de análisis, diseño, desarrollo, implementación y evaluación, pero constituyen su soporte no operativo. Gracias a esta fase es posible establecer la estructura documental del plan, delimitar responsabilidades, alinear el PCSI con los objetivos estratégicos de la organización y definir cómo se medirá su impacto y cumplimiento (NIST, 2024).

La fase analizar se orienta a identificar brechas, necesidades y audiencias del PCSI, a partir de la información recopilada. Estos resultados son el insumo principal para definir qué contenidos, formatos y estrategias se requieren en la etapa de diseño, de modo que el plan responda a problemas concretos y no a temarios genéricos (NIST, 2024).

En el contexto de este proyecto de investigación aplicada, el alcance se extiende hasta la etapa de diseño. Los investigadores elaboran los documentos de diseño de los artefactos que estructuran una futura implementación, desarrollo y evaluación del PCSI. Así, se dejan establecidas las bases para que la “mediana empresa de tecnología” continúe con las siguientes fases del ciclo de vida ADDIE, ejecute el plan y avance en su mejora continua en concientización de seguridad de la información (NIST, 2024, NIST SP 800-50r1, secc. 5.1–5.3).

Figura 2

Modelo ADDIE.



Nota. Adaptada de la guía NIST SP:800.50r1(p.6), por NIST,2024, https://doi.org/10.6028/NIST.SP.800-50r1

Planificar

Establecer objetivos, audiencias, contenidos y métricas del PCSI basados en riesgos del SGSI y en políticas y procedimientos internos (p. ej., uso aceptable, clasificación, contraseñas, respaldo, escritorio limpio, VPN, incidentes, vulnerabilidades, activos, datos personales). (NIST, 2024, NIST SP 800-50r1, secc. 2.2 y 4.1; ISO, 2022, ISO/IEC 27001:2022, cl. 6.1 y 7.2–7.3; ISO, 2022, ISO/IEC 27002:2022, 6.3).

Entradas: Reporte de incidentes, hallazgos de auditoría, políticas internas vigentes. (ISO, 2022, ISO/IEC 27001:2022, cl. 4.2 y 9.2; NIST, 2024, NIST SP 800-50r1, secc. 2.1–2.2).

Entregables: Plan anual por audiencia, mapa de contenidos, cronograma, indicadores (KPI/KRI), presupuesto, gobernanza. (NIST, 2024; ISO, 2022, ISO,2022a).

Diseñar

Traducir riesgos y políticas a itinerarios y lecciones de aprendizaje por audiencia con microlearning y práctica guiada que cambie conductas. (NIST, 2024, NIST SP 800-50r1, secc. 3.2–3.4; ISO, 2022, ISO/IEC 27002:2022, 6.3).

Componentes:

Concienciación: Concientización continua, campañas mensuales, mensajes breves y repetidos, cartelería digital. (NIST, 2024, NIST SP 800-50r1, secc. 3.3).

Entregables: Prototipos de curso para el LMS, material de refuerzo y microcontenidos. (NIST, 2024, NIST SP 800-50r1, secc. 3.2–3.4).

Métricas ejemplo: Contenidos mapeados con políticas, tasa de revisión y aprobación por T&D. (ISO, 2022, ISO/IEC 27001:2022, cl. 7.5 y 8.1).

Implementar

Objetivo: Ejecutar el plan en el LMS y canales corporativos, asegurar participación y soporte. (NIST, 2024, NIST SP 800-50r1, secc. 4.2–4.3).

Actividades:

Onboarding: inducción obligatoria en 15 días por rol, aceptación de políticas, evaluación diagnóstica. (ISO, 2022, ISO/IEC 27002:2022, 6.7).

Formación continua: rutas anuales, cápsulas periódicas, campañas de refuerzo y microcontenidos. (NIST, 2024, NIST SP 800-50r1, secc. 3.3).

Prácticas: phishing simulado (NIST, 2024, NIST SP 800-50r1, secc. 3.3–3.4).

Soporte y accesibilidad: helpdesk, FAQs, reenvíos, alternativas asincrónicas. (NIST, 2024, NIST SP 800-50r1, secc. 3.4).

Entregables: registros en LMS, evidencias de campañas, bitácoras de simulaciones y reportes de participación. (ISO, 2022, ISO/IEC 27001:2022, cl. 7.5).

Métricas ejemplo: participación, tasa de finalización, tasa de reporte de phishing simulado vs. clic. (NIST, 2024, NIST SP 800-50r1, secc. 5.1–5.3).

Evaluar

Objetivo: Medir eficacia en tres niveles: aprendizaje, comportamiento y resultados del negocio/SGSI. (NIST, 2024, NIST SP 800-50r1, secc. 4.4 y 5.1–5.3).

Niveles:

Aprendizaje: pre/post tests, rúbricas, microevaluaciones. (NIST, 2024, NIST SP 800-50r1, secc. 5.1).

Comportamiento: reducción de clic en phishing, aumento de reportes correctos, cumplimiento de políticas (p. ej., contraseñas, escritorio limpio), tiempos de reporte de incidentes. (NIST, 2024, NIST SP 800-50r1, secc. 5.2).

Resultados: disminución de incidentes por error humano, reducción de riesgos priorizados, menos hallazgos de auditoría, cumplimiento de requisitos de partes interesadas. (ISO, 2022, ISO/IEC 27001:2022, cl. 9.1; NIST, 2024, NIST SP 800-50r1, secc. 5.3).

Entregables: tablero de KPIs/KRIs, informe periodico, lecciones aprendidas y acciones de mejora. (ISO, 2022, ISO/IEC 27001:2022, cl. 9.1 y 9.3).

Métricas ejemplo: delta de conocimientos, CTR de phishing simulado, ratio reporte/clic, incidentes por canal humano, cumplimiento de rutas por rol. (NIST, 2024, NIST SP 800-50r1, secc. 5.1–5.3).

Planificar

Propósito

Establecer un Plan de Concientización en Seguridad de la Información (PCSI) para la “mediana empresa de tecnología” que cambie comportamientos, reduzca exposición a riesgos atribuibles a comportamiento humano y soporte los objetivos del negocio y del SGSI.

Además, servir como marco de coordinación entre Infraestructura Tecnológica, Transformación & Desarrollo, Mercadeo y el director general para asegurar que todo el personal y terceros comprendan y apliquen las políticas corporativas y los controles del SGSI.

Alcance

Cobertura Organizacional. Todo el personal de la “mediana empresa de tecnología” y terceros con acceso a activos de información, segmentados por: a) roles generales; b) roles críticos encargados de la seguridad de la información e Infraestructura Tecnológica. La segmentación por audiencias se establece desde la planificación para asegurar pertinencia de contenidos por riesgo y función.

Temáticas Núcleo. Protección de datos; phishing e ingeniería social; gestión de contraseñas y MFA; uso aceptable de activos; clasificación y manejo de la información; respaldo y recuperación; seguridad de endpoint; respuesta y reporte de incidentes; concienciación en privacidad de datos personales. La priorización de contenidos y campañas se ajusta a hallazgos previos en consultorías y auditorias, y a las políticas internas vigentes.

Condiciones *de* Trabajo y Ubicaciones. Cobertura de sedes físicas y trabajo híbrido. El diseño instruccional considerará condiciones de aprendizaje según contexto (on-site o remoto) y dispositivos corporativos o autorizados, para asegurar accesibilidad, disponibilidad de contenidos y refuerzos contextuales

Modalidades y Accesibilidad. Onboarding para nuevos ingresos; e-learning en el Proporcionado por la ARL (LMS), simulaciones de phishing, cartelería digital (Bogotá) y microcontenidos de refuerzo. Idioma principal: español; se cumplirán criterios de accesibilidad y buenas prácticas de experiencia para maximizar la adopción.

Obligaciones y Estándares. Alineado al SGSI ISO/IEC 27001:2022 (cláusulas de competencia, concienciación, control de comunicación y mejora) y a ISO/IEC 27002:2022 (control 6.3 concienciación, educación y formación en seguridad de la información). Se integran métricas y evidencias para auditoría.

Trazabilidad a Políticas y Procesos Internos. Los contenidos, campañas y evaluaciones se derivarán de las políticas y procedimientos vigentes (uso aceptable, clasificación de la información, contraseñas, respaldos, respuesta a incidentes, escritorio limpio,

firewall, tratamiento de datos personales entre otros), garantizando que cada audiencia reciba la formación del PCSI.

Plataforma y Analítica. Proporcionado por la ARL (herramienta de gestión de aprendizaje o LMS por sus siglas en ingles, *Learning Management System*), Herramientas de Microsoft como Authenticator (MFA), Forms (Encuestas), Power Automate (Automatizar tabulación de resultados) y SharePoint para gestionar las capacidades de muestreo y métricas, Herramientas de marketing digital para operar como el simulador de phishing y SharePoint como repositorio de evidencias.

Métricas y Evidencias. Se consolidarán métricas operativas (finalización, evaluación, clics de phishing, reportes) y cualitativas (encuestas) con trazabilidad a objetivos, con almacenamiento en repositorios institucionales (SharePoint) y control documental para auditoría.

Privacidad y Tratamiento de Datos de Formación. Se aplicarán principios de minimización, base legal y retención definidos por A&F y políticas de datos personales.

Visión del PCSI de la "mediana empresa de tecnología"

A partir de los resultados del ejercicio de phishing realizado por la "Empresa Consultora en seguridad", en el que el 20 % de los usuarios abrió un correo señuelo y el 4 % accedió al enlace malicioso, y de los hallazgos de auditoría ejecutada por la "empresa auditora", que evidenciaron que cerca del 10 % de las personas incumple la política de escritorio limpio y otro 10 % utiliza medios distintos de OneDrive para transferir información, la visión del PCSI es que, en los próximos doce meses, estos porcentajes de comportamiento de riesgo disminuyan de manera sostenida, reflejando una evolución cultural en la que los colaboradores reconozcan mejor las señales de amenaza y asimilen de forma consistente las políticas que la "mediana empresa de tecnología" ha implementado en su SGSI ("empresa auditora", 2024; "Empresa Consultora en seguridad", 2024).

Objetivos del Plan de Concientización en Seguridad de la Información (PCSI)

Objetivo General. Establecer el marco integral del Plan de Concientización en Seguridad de la Información (PCSI) que desarrolle comportamientos seguros, competencias medibles y una cultura organizacional orientada al riesgo, para reducir incidentes, cumplir los requisitos normativos y sostener la mejora continua del SGSI de la “mediana empresa de tecnología”.

Objetivos Específicos. En los próximos doce meses:

Reducir la exposición de la “mediana empresa de tecnología” al phishing y la ingeniería social, disminuyendo la interacción con contenidos maliciosos frente a la línea base inicial, mediante la ejecución de campañas y microcontenidos del PCSI, alineados con sus lineamientos y alcance (“Empresa Consultora en seguridad”, 2024).

Incrementar el cumplimiento de las prácticas de seguridad de la información por parte de los colaboradores, reduciendo comportamientos inadecuados (ej. gestión de información) frente a la auditoría la “Empresa auditora”, aprovechando el análisis de brechas y las acciones de sensibilización del PCSI, según su alcance y audiencias (“Empresa auditora”, 2024).

Diseñar, implementar y mantener un marco de medición y reporte del PCSI, que permita el seguimiento sistemático de la participación, cambio de comportamiento y evolución del riesgo humano, con indicadores, responsables y periodicidad definidos, alineados a la metodología de evaluación del plan. (NIST, 2024, cap. 2).

Diseñar y documentar la estructura de los materiales de concientización del PCSI (campaña anual, refuerzos, microcontenidos), asegurando su coherencia y adaptación a las audiencias, formatos y medios definidos en los lineamientos del plan, para optimizar su efectividad.

Objetivos de Aprendizaje

El Plan de Concientización en Seguridad de la Información (PCSI) para la “mediana empresa de tecnología” se concibe como un programa organizacional integral, diseñado para

transformar las políticas y normativas en hábitos seguros y medibles, alineado con el SGSI basado en ISO/IEC 27001:2022 e ISO/IEC 27002:2022. Su objetivo principal es fomentar un cambio de comportamiento observable en los colaboradores, reduciendo la vulnerabilidad ante amenazas como el phishing, el uso inadecuado de recursos y el incumplimiento de prácticas esenciales de seguridad (“Empresa Consultora en seguridad” S.A., 2024; “empresa auditora”, 2024)

Requisitos del PCSI

El PCSI debe partir de una base normativa clara: alinearse con los requisitos de competencia, toma de conciencia y comunicación establecidos por ISO/IEC 27001:2022, que exige un programa sistemático de concientización, educación y capacitación en seguridad de la información para todo el personal y partes interesadas relevantes.

Desde la perspectiva del aprendizaje, el PCSI requiere que los objetivos estén formulados de manera observable y medible, vinculando cada resultado de aprendizaje con riesgos específicos, políticas internas y comportamientos esperados. Esto implica definir qué debe ser capaz de reconocer, decidir o hacer cada audiencia frente a amenazas como phishing, manejo inadecuado de información, uso de credenciales y reporte de incidentes, integrando el análisis de brechas evidenciado en auditorías y campañas de phishing.

Adicionalmente, el PCSI debe contar con requisitos mínimos de gobernanza, segmentación y medición: patrocinio visible de la alta dirección, roles y responsabilidades definidos, criterios para segmentar audiencias según exposición al riesgo y un conjunto de indicadores que permitan evaluar participación, aprendizaje, cambio de comportamiento y resultados sobre el riesgo humano, en coherencia con las recomendaciones de NIST para programas de concientización y capacitación.

Políticas que Rigen el PCSI de la "mediana empresa de tecnología"

Mandato y Alcance. Se establece el mandato y el alcance del PCSI a través de las siguientes políticas.

El Plan de Concientización en Seguridad de la Información (PCSI) es de cumplimiento obligatorio para todo el personal de la "mediana empresa de tecnología" (empleados, contratistas, personal en misión) con acceso a activos de información. Su propósito es fomentar comportamientos seguros y reducir riesgos asociados al factor humano.

El PCSI se enfoca en la concientización sobre riesgos de seguridad de la información y en la adopción de las políticas del SGSI relacionadas con el comportamiento humano, no en capacitación técnica profunda. Busca generar comprensión básica y actitud proactiva.

Periodicidad de la Concientización. Se establece la periodicidad del PCSI a través de las siguientes políticas.

Se realizará anualmente una campaña de concientización en seguridad de la información de carácter obligatorio para todo el personal.

Se implementarán acciones de refuerzo de concientización semestrales, adicionales a la campaña anual, para mantener la relevancia y actualidad de los mensajes de seguridad.

Se implementarán microcontenidos mensuales para reforzar mensajes clave, comunicar alertas rápidas y mantener la concientización de forma continua.

Todo nuevo colaborador de la "mediana empresa de tecnología" (incluyendo contratistas y personal en misión) deberá completar un paquete mínimo de concientización en seguridad de la información como parte de su proceso de inducción u onboarding, el primer día calendario de vinculación. Este paquete deberá abordar al menos los riesgos clave de la organización, las políticas básicas de seguridad de la información, las responsabilidades individuales del colaborador y la información en manejo de datos personales.

La planificación de campañas y refuerzos se coordinará con Transformación & Desarrollo, Infraestructura Tecnológica (TI) y otras áreas, evitando picos operativos y alineándose con la planificación de comunicados de la compañía.

Roles y Responsabilidades del PCSI. Se establece los roles y responsabilidades dentro del PCSI a través de las siguientes políticas.

La dirección general (A&F) se encarga de aprobar la política del PCSI, asignar recursos y comunicar el compromiso de la alta dirección con la seguridad de la información.

El proceso de Transformación y Desarrollo (T&D) debe integrar el PCSI con los procesos de gestión del talento, coordinar la ejecución y administrar los registros de participación.

Infraestructura Tecnológica (TI) / CISO debe liderar el diseño temático del PCSI, priorizar contenidos según riesgos e incidentes, asegurar coherencia con el SGSI y monitorear indicadores de comportamiento.

Los responsables por cada proceso deben reforzar mensajes del PCSI en sus áreas, facilitar la participación del personal y retroalimentar sobre la efectividad de las actividades.

Los colaboradores en generar deben participar activamente en las actividades del PCSI, aplicar prácticas seguras obtenidas en la concientización y reportar incidentes o situaciones de riesgo identificadas a través de la información recibida.

Cumplimiento y Consecuencias. Se establece los parámetros de cumplimiento y las consecuencias para los colaboradores que no cumplan con dichos parámetros dentro del PCSI a través de las siguientes políticas.

El cumplimiento del PCSI se evaluará mediante indicadores de participación, finalización de actividades y resultados de simulaciones o pruebas.

La no participación, participación parcial o fuera de plazo en las actividades obligatorias del PCSI podrá registrarse como incumplimiento en materia de seguridad de la información y podrá ser considerada en las revisiones de desempeño, auditorías internas y revisiones del SGSI/SGC.

Ante el primer incumplimiento injustificado de actividades obligatorias del PCSI, se podrá aplicar una medida correctiva inicial que incluya recordatorios formales, reprogramación de la actividad y/o sesiones adicionales de concientización enfocadas en el riesgo identificado.

El incumplimiento reiterado e injustificado de las actividades obligatorias del PCSI podrá ser escalado conforme a los procedimientos disciplinarios internos de la “mediana empresa de tecnología”, pudiendo incluir llamados de atención formales, anotaciones en la hoja de vida interna y otras medidas establecidas por la organización.

Cuando el incumplimiento de las obligaciones del PCSI se traduzca en comportamientos que violen políticas de seguridad de la información o de protección de datos (por ejemplo, compartir credenciales, divulgar información confidencial, ignorar procedimientos de reporte de incidentes), se aplicarán las medidas disciplinarias y contractuales definidas en las políticas internas y en la legislación laboral y de protección de datos aplicable.

En el caso de terceros y proveedores, el incumplimiento de las obligaciones de concientización definidas contractualmente podrá dar lugar a la aplicación de cláusulas de penalización, revisión de condiciones contractuales o terminación del contrato, según lo establecido en los acuerdos de confidencialidad y de servicio.

Los casos de incumplimiento y sus consecuencias serán analizados de forma detallada para identificar causas recurrentes y mejorar el diseño del PCSI (contenidos, formatos, tiempos, comunicaciones), siguiendo el enfoque de mejora continua recomendado por NIST para la gestión de programas de concientización.

Medios de Difusión del PCSI. Se establece los medios de difusión autorizados para el despliegue del PCSI a través de las siguientes políticas.

El LMS Proporcionado por la ARL es el medio corporativo principal para realizar la campaña de concientización anual del PCSI (módulos estructurados de concientización y evaluaciones asociadas). Todas las campañas anuales de concientización y las actividades

obligatorias deberán estar disponibles y registradas en esta plataforma para asegurar trazabilidad y medición.

La cartelera digital corporativa se utilizará como medio complementario para el lanzamiento y refuerzo de campañas del PCSI, priorizando mensajes visuales de alto impacto sobre riesgos clave, comportamientos esperados y llamados a la acción (por ejemplo, “buenas prácticas”, “protege tu contraseña”), reforzando la presencia del PCSI en los espacios físicos o digitales visibles para todo el personal.

Los microcontenidos se publicarán por medios digitales de acceso individual directamente sobre las herramientas Microsoft de comunicación individual como Teams, o comunicación general como Viva Engage, priorizando mensajes visuales de alto impacto sobre riesgos clave, comportamientos esperados y llamados a la acción (por ejemplo, “reporta phishing”, “protege tu contraseña”).

Los contenidos publicados en Proporcionado por la ARL, Microsoft Viva Engage, Teams y cartelera digital deben ser coherentes entre sí en cuanto a mensajes, terminología y lineamientos de seguridad de la información, de forma que cada canal refuerce los mismos comportamientos y políticas sin generar contradicciones.

Aunque Engage, Teams y la cartelera digital se utilizan principalmente para difusión y refuerzo, el registro oficial de cumplimiento de actividades obligatorias del PCSI se gestionará en el LMS Proporcionado por la ARL garantizando evidencias para auditoría y métricas del programa.

Contenidos y Formas de Presentación del PCSI. Se establece contenidos y formas de presentación para el despliegue del PCSI a través de las siguientes políticas.

Los contenidos del PCSI deben enfocarse en comportamientos concretos a reforzar y en los riesgos de seguridad de la información priorizados para la “mediana empresa de tecnología” (por ejemplo, phishing, manejo de información confidencial, uso de correo corporativo, gestión

de contraseñas), evitando temas genéricos que no se relacionen con el contexto y los riesgos reales de la organización.

Los contenidos del PCSI deben estar diseñados para concientización con mensajes claros, ejemplos cotidianos y recordatorios prácticos. No deben sustituir ni duplicar programas de capacitación técnica o formación por rol, que se gestionan por otros procedimientos.

Los contenidos del PCSI deben adaptarse a las audiencias internas utilizando ejemplos, lenguaje y nivel de detalle acordes con su rol y exposición al riesgo, conforme al análisis de audiencias y tareas.

Los contenidos del PCSI deben revisarse y actualizarse periódicamente para incorporar lecciones aprendidas de incidentes, cambios tecnológicos, nuevos riesgos y cambios en políticas internas, evitando el uso prolongado de materiales desactualizados.

Los contenidos y ejemplos utilizados en el PCSI no deben exponer datos personales ni información sensible real de colaboradores, clientes o terceros. Cuando se usen casos reales, deben anonimizarse o generalizarse, en coherencia con las políticas de tratamiento de datos personales y confidencialidad de la “mediana empresa de tecnología”.

Los contenidos del PCSI deben utilizar un lenguaje respetuoso, constructivo y orientado a aprendizaje, evitando mensajes culpabilizantes o que generen miedo, para fomentar la participación y el reporte proactivo de incidentes.

Todo contenido del PCSI debe contar con versión, fecha y responsable, y debe ser aprobado por los roles definidos en la gobernanza del PCSI antes de su publicación, garantizando consistencia, precisión técnica y alineación con las políticas vigentes.

Cobertura de Audiencias

Todo el personal de la “mediana empresa de tecnología” (empleados permanentes, temporales), contratistas que acceden a información, y proveedores críticos con acceso lógico o físico a activos de información.

Roles en el PCSI

Director General. Establecer la dirección y prioridades del PCSI; aprobar el plan anual, presupuesto y métricas; remover impedimentos; exigir el cumplimiento por parte de líderes; revisar trimestralmente resultados e impulsar mejora continua. Estas funciones emanan del liderazgo y compromiso exigidos por ISO/IEC 27001 y del principio de alineación estratégica del programa de concienciación del NIST. (ISO, 2022, ISO/IEC 27001:2022, cl. 5.1–5.3 y 9.3; NIST, 2024, NIST SP 800-50r1, secc. 2.1–2.2).

Responsable de Seguridad de la Información / CISO. Asegurar alineación del PCSI con el SGSI, el análisis de riesgos y los incidentes; validar exactitud técnica y de control de los contenidos; definir requisitos mínimos por rol; integrar métricas del PCSI a indicadores de seguridad; patrocinar campañas de alto riesgo (p. ej., phishing, contraseñas, clasificación). ISO 27002 demanda concienciación estructurada y el NIST enfatiza la orientación por riesgo. (ISO, 2022, ISO/IEC 27002:2022, control 6.3; ISO, 2022, ISO/IEC 27001:2022, cl. 6.1; NIST, 2024, NIST SP 800-50r1, secc. 2.2 y 3.2).

Transformación & Desarrollo. Integrar PCSI en onboarding, cambios de rol y offboarding; administrar el LMS, inscripciones, trazabilidad de asistencia y evaluaciones; coordinar comunicaciones internas y recordatorios; apoyar la accesibilidad e inclusión de contenidos. ISO 27002 requiere seguridad en la gestión de RR. HH. y NIST recomienda facilitar recursos y accesibilidad a la audiencia. (ISO, 2022, ISO/IEC 27002:2022, 6.7; ISO, 2022, ISO/IEC 27001:2022, cl. 7.2–7.3; NIST, 2024, NIST SP 800-50r1, secc. 3.2–3.4).

Mercadeo. Liderar la producción, adaptación y publicación de piezas comunicacionales del PCSI (newsletters, infografías, videos, piezas para cartelería física/digital, mensajes para intranet/canales internos), garantizando consistencia visual y claridad del mensaje; coordinar el calendario editorial de campañas de concienciación y promoción; colaborar con Talento Humano para la correcta distribución por canales y con Seguridad (CISO) para validar exactitud técnica y sensibilidad de la información; asegurar accesibilidad, lenguaje inclusivo y pertinencia para las audiencias segmentadas; medir el alcance de las campañas (aperturas, clics, visualizaciones) y retroalimentar al programa para mejoras continuas. La función de comunicación y promoción refuerza la transferencia del contenido y el cambio de comportamiento, tal como sugiere NIST al estructurar campañas y materiales accesibles por audiencia, y como recoge ISO 27002 en el control de concienciación (NIST, 2024, NIST SP 800-50r1, secc. 3.3–3.4; ISO, 2022, ISO/IEC 27002:2022, control 6.3).

***Usuario General*.** Completar las rutas de formación asignadas según su rol dentro de los plazos; leer y aceptar las políticas aplicables (p. ej., uso aceptable, clasificación de información, contraseñas, respaldo, escritorio/pantalla limpia, VPN, incidentes, vulnerabilidades, datos personales); aplicar en el día a día las prácticas seguras (creación y resguardo de contraseñas, manejo de información clasificada, reporte oportuno de incidentes y correos sospechosos, respeto a las directrices de escritorio limpio y uso de activos); participar en simulaciones (phishing, ejercicios de reporte) y cumplir con las evaluaciones y refuerzos. Estas responsabilidades responden a los requisitos de competencia y toma de conciencia de ISO 27001 y a la finalidad conductual del programa de NIST (ISO, 2022, ISO/IEC 27001:2022, cl. 7.2–7.3; NIST, 2024, NIST SP 800-50r1, secc. 3.1–3.3).

Tabla 2

Roles y responsabilidades del PCSI

Rol	Responsabilidad
Director General	Aprobar el plan, asignar recursos y comunicar compromiso.
Transformación & Desarrollo	Administrar LMS, inscripciones y trazabilidad.
CISO / Infraestructura	Validar contenidos técnicos y monitorear indicadores.
Mercadeo	Diseñar piezas comunicacionales y coordinar campañas.
Usuarios	Completar rutas, aplicar prácticas seguras y participar en simulaciones.

Nota. Fuente: Los autores

Matriz RACCI

Tabla 3

Matriz RACCI PCSI

Actividad	Director General	CISO / Seguridad	Transformación & Desarrollo	Mercadeo	Usuario General	Nota
Definir objetivos anuales del PCSI alineados al SGSI y al negocio	A	R	C	I	I	Objetivos basados en riesgos y prioridades
Aprobar plan anual, presupuesto y KPIs/KRIs	A	C	C	I	I	Gobernanza y patrocinio ejecutivo
Mapear riesgos/políticas a contenidos por rol	I	A/R	C	I	I	Trazabilidad a políticas internas y matriz de riesgos
Diseñar currículos y microcontenidos del PCSI	I	A/R	C	C	I	Estructura pedagógica y accesibilidad
Validar exactitud técnica de contenidos	I	A/R	C	I	I	Controles y prácticas seguras
Gestionar LMS, inscripciones, trazabilidad y recordatorios	I	I	A/R	C	I	Operación formativa y evidencias
Onboarding/inducción por rol (aceptación de políticas y evaluación)	I	C	A/R	I	I	Inducción en primeros 15 días
Ejecutar campañas de concienciación/promoción	I	R	R/C	A	I	Mensajería, branding, canales internos
Producción y publicación de piezas comunicacionales (arte, videos, etc.)	I	C	C	A/R	I	Diseño, redacción y calendario editorial
Ejecutar prácticas: phishing simulado, laboratorios MFA/contraseñas	A	R	C	I	I	Simulaciones y ejercicios prácticos
Gestionar señalización y campañas visuales (cartelería digital/física)	I	C/R	R	A	I	Diseño consistente y despliegue multicanal
Consolidar métricas (participación, evaluaciones, CTR phishing, reportes)	I	A/R	C	I	I	Tableros y análisis

Actividad	Director General	CISO / Seguridad	Transformación & Desarrollo	Mercadeo	Usuario General	Nota
Analizar eficacia y proponer mejoras	I	A/R	C	C	I	Aprendizaje, conducta y resultados
Presentar informe trimestral y revisión por la dirección	A	R	C	I	I	Gobernanza y decisiones
Aprobar acciones de mejora y remover impedimentos	A	C	I	I	I	Patrocinio y recursos
Evidencia documental (registros, actas, versiones de contenido)	I	C/R	A/R	C	I	Control documental y trazabilidad
Cumplir rutas de formación, aceptar políticas y reportar incidentes/phishing	I	I	I	I	A/R	Responsabilidades del usuario final

Nota. Fuente: Los autores

Tabla 4

Alineación de objetivos

Objetivos investigación	Objetivos del PCSI	Explicación alineación
1	2	Usan directamente los hallazgos de auditoría y el análisis de brechas como punto de partida para definir y medir la mejora de comportamiento
2	1	Asumen y hacen explícito que las acciones de reducción de phishing se ejecutan dentro del alcance y lineamientos del PCSI
	2	Conecta los cambios de comportamiento con el alcance del PCSI y las audiencias priorizadas
	3	Concreta la dimensión de responsabilidades al asignar quién mide, qué y con qué frecuencia se reporta, dentro del marco del PCSI.
	4	Trabajan explícitamente con audiencias, formatos y medios previstos por los lineamientos del PCSI.
3	1	Se apoya directamente en la estructura de campañas y microcontenidos diseñada, usando esos componentes como mecanismo para lograr la reducción del riesgo de phishing.
	2	Convierte la estructura diseñada en acciones de sensibilización orientadas a cerrar brechas de comportamiento detectadas.
	4	Desarrolla en detalle los materiales que concretan esa estructura anual (campaña, refuerzos, microcontenidos).
4	3	Diseñar, implementar y mantener un marco de medición y reporte del PCSI, con indicadores, responsables y periodicidad alineados a la metodología del plan.
	4	Traduce operativamente la metodología de evaluación en un marco concreto de indicadores, roles y frecuencia de reporte para monitorear el desempeño del PCSI y su impacto en el factor humano.
	De forma indirecta 1 y 2	Hablar de reducción frente a una línea base (phishing y comportamientos inadecuados), dependen de los criterios de medición y evaluación definidos, aunque no lo detalla.

Nota. Fuente: Los autores

Determinación de KPIS para el PCSI

En este apartado se definen las métricas y los indicadores clave de desempeño (KPIs) que permitirán medir la efectividad del Plan de Concientización en Seguridad de la Información (PCSI) en la “mediana empresa de tecnología”. Estas métricas están alineadas con las brechas identificadas en el diagnóstico inicial, utilizando como insumo los hallazgos en auditoria de la “Empresa auditora” y en las pruebas de Phishing realizadas por la “Empresa Consultora en seguridad” y constituyen la base para establecer metas de mejora continua. La selección de estos KPIs se fundamenta en las mejores prácticas establecidas por la NIST SP 800-50r1 y las normas ISO 27001:2022 e ISO 27002:2022, que enfatizan la importancia de medir y evaluar el impacto de los programas de concientización para fortalecer la cultura de seguridad (NIST, 2014; ISO/IEC, 2022a; ISO/IEC, 2022b).

A continuación, se describa cada KPIs seleccionados y su relación con brechas identificadas.

CTR (Tasa de Clics) en Simulaciones Phishing. Este KPI mide la proporción de usuarios que hacen clic en enlaces maliciosos durante simulaciones controladas de phishing. Es un indicador directo de la vulnerabilidad de los colaboradores frente a ataques de ingeniería social.

Identificación. Nombre. CTR (tasa de clics) en simulaciones de phishing.

Propósito. medir vulnerabilidad conductual ante ingeniería social (qué tanto el usuario "muerde el anzuelo"). (NIST, 2024, secc. 3.3 y 4.3).

Nivel de evaluación. principalmente Nivel 3 (Comportamiento) y se puede leer también como Nivel 4 (Resultados) cuando se relaciona con reducción de incidentes/costos. (NIST, 2024, secc. 4.3)

Definición operacional. Clic. Interacción del usuario con el enlace señuelo (o botón) contenido en el correo simulado.

Población de prueba. Total de destinatarios válidos (excluyendo rebotes) dentro del alcance de la campaña. (NIST, 2024, secc. 3.3).

Fórmula y unidad. Fórmula. número de clics / población de prueba

Unidad. porcentaje (%).

Fuente de datos y recolección. Fuente primaria. reporte de la herramienta/campaña de phishing simulado (o el informe del proveedor si aplica).

Recolección. Exportación de resultados por campaña y archivo como evidencia del PCSI en repositorio institucional. (ISO, 2022, ISO/IEC 27001:2022, cl. 7.5; NIST, 2024, secc. 4.3).

Periodicidad. Medición. Por cada simulación (recomendado: al menos 1 anual, y ojalá 2 si la operación lo permite). (NIST, 2024, secc. 3.3).

Reporte. Trimestral (si hay simulaciones) y mínimo anual en revisión de cierre del PCSI. (ISO, 2022, ISO/IEC 27001:2022, cl. 9.1 y 9.3).

Línea base, meta y umbrales. Línea base. 4% según el documento, tomado del ejercicio inicial.

Meta. reducir por debajo de 4%.

Umbrales sugeridos (para decisión). Verde, < 4% (en mejora vs línea base).

Amarillo, 4% a 6% (sin mejora; requiere refuerzo). (NIST, 2024, secc. 4.3).

Rojo, > 6% (deterioro; intervención prioritaria). (NIST, 2024, secc. 4.3).

Interpretación y acciones. Si el CTR baja sostenidamente, es una señal de adopción de hábitos de verificación (pausa, revisión de remitente/enlace, etc.). (NIST, 2024, secc. 4.3).

Si el CTR sube o se estanca, el plan debe ajustar contenido + frecuencia + refuerzos (microcontenidos cercanos a la simulación, retroalimentación inmediata post-clic, mini refuerzo por audiencia). (NIST, 2024, secc. 3.3 y 4.3).

Dueño del KPI (RACI sugerido). Responsable de cálculo y consolidación. CISO/TI.

Co-responsable de intervención formativa (acciones). T&D y Mercadeo (mensajería/refuerzos).

Relación con requisitos/controles. Soporta la evidencia de efectividad del programa de concientización/capacitación. (ISO, 2022, ISO/IEC 27001:2022, Anexo A, control 6.3; NIST, 2024, secc. 4.3).

Relación con la Brecha. En el diagnóstico inicial se identificó una alta tasa de clics en simulaciones phishing (La “Empresa Consultora en seguridad” S.A.S, 2024), lo que evidencia una brecha significativa en la capacidad de los colaboradores para identificar y evitar ataques de este tipo. La medición inicial dio como resultado un 4% de clic en enlaces maliciosos y sirvió como línea base para establecer la meta de reducción y mejorar la resistencia ante amenazas reales.

Reportes de Incidentes por Pruebas de Phishing. Este KPI refleja la proporción de usuarios que reportan incidentes o sospechas de phishing durante las pruebas realizadas por La “Empresa Consultora en seguridad” S.A.S en el año 2024, lo que indica la efectividad de la cultura de reporte y la sensibilización sobre la importancia de comunicar posibles amenazas.

Identificación. Nombre. Reportes de incidentes por pruebas de phishing.

Propósito. medir cultura de “detectar y reportar” (convertir al usuario en sensor, no solo en receptor). (NIST, 2024, secc. 3.3 y 4.3).

Nivel de evaluación. principalmente Nivel 3 (Comportamiento). (NIST, 2024, secc. 4.3).

Definición operacional. Reporte válido. reporte realizado por canal definido por La “mediana empresa de tecnología” (ej. mesa de ayuda/correo oficial) indicando sospecha razonable del mensaje.

Fórmula y unidad. Fórmula. Tasa de reporte = número de reportes / población de prueba.

Unidad. porcentaje (%).

Fuente de datos y recolección. Fuente primaria. Conteo de reportes en el canal oficial (mesa de ayuda / buzón de reportes) cruzado con la campaña.

Recolección. Registro del ticket/correo y consolidado por campaña en el tablero de KPIs del PCSI. (NIST, 2024, secc. 4.3).

Periodicidad. Medición. Por cada simulación. (NIST, 2024, secc. 3.3).

Reporte. Trimestral (si aplica) y anual para revisión de dirección del SGSI/PCSI. (ISO, 2022, ISO/IEC 27001:2022, cl. 9.3).

Línea base, meta y umbrales. Línea base. 0% reportes (según ejercicio inicial).

Meta. > 0% (tal como está en el documento).

Umbrales sugeridos (para decisión). Rojo, 0% (cultura de reporte ausente).

Amarillo, >0% y <5% (arranque, pero bajo). (NIST, 2024, secc. 4.3).

Verde, ≥5% (ya hay hábito inicial; se puede escalar meta luego). (NIST, 2024, secc. 4.3).

Interpretación y acciones. Si el reporte se mantiene en 0%, el PCSI debe intervenir en dos frentes: (1) claridad del canal (qué, dónde y cómo reportar) y (2) refuerzo conductual (microcontenido + recordatorio justo antes/durante simulación + retroalimentación posterior). (NIST, 2024, secc. 3.3 y 4.3).

Si el reporte sube, pero el CTR no baja, el mensaje se está entendiendo “a medias” (reportan algunos, pero aún caen); aquí conviene reforzar habilidades de verificación y “pausa antes del clic”. (NIST, 2024, secc. 4.3)

Dueño del KPI (RACI sugerido). Responsable de cálculo y consolidación. CISO/TI.

Co-responsable de intervención formativa (acciones). T&D y Mercadeo (mensajería/refuerzos).

Relación con requisitos/controles. Evidencia directa de “toma de conciencia” y de comportamiento esperado ante amenazas, como parte del programa de concientización. (ISO, 2022, ISO/IEC 27001:2022, cl. 7.3; NIST, 2024, secc. 4.3).

Relación con la Brecha. Se detectó que los colaboradores no reportaron adecuadamente los incidentes de phishing, lo que limita la capacidad de respuesta temprana. La medición inicial mostró un nivel de cero reportes (0%) en simulaciones phishing (“Empresa Consultora en seguridad”, 2024), La medición inicial dio como resultado un 0% de reportes por lo que la meta busca fomentar una cultura activa de reporte y vigilancia que sobrepase el resultado del primer ejercicio de phishing.

Uso de Herramientas no Autorizadas para Gestión de Información en Auditoría. Este KPI mide la proporción de hallazgos en auditorías donde se detecta el uso de herramientas no autorizadas para la gestión de información, lo que representa un riesgo para la seguridad y confidencialidad de los datos.

Identificación. Nombre. Uso de herramientas no autorizadas para gestión de información en auditoría.

Propósito. reducir exposición por fuga o pérdida de control de la información por canales no aprobados (ej. transferencia por servicios externos) (NIST, 2024, secc. 4.3).

Nivel de evaluación. Nivel 3 (Comportamiento) y puede reflejar Nivel 4 (Resultados) cuando baja el riesgo operativo. (NIST, 2024, secc. 4.3)

Definición operacional. Hallazgo. evidencia en auditoría/validación de uso de herramienta no autorizada para compartir/gestionar información (p. ej., WeTransfer), sobre una muestra definida.

En el documento se vincula este comportamiento con la política interna de uso de activos/recursos TI.

Fórmula y unidad. Fórmula. Tasa de hallazgos = número de hallazgos / población muestra.

Unidad. porcentaje (%) y también se recomienda guardar el N absoluto (hallazgos) por transparencia.

Fuente de datos y recolección. Fuente primaria. informe de auditoría / planilla de validación aplicada sobre muestra de equipos o usuarios.

Recolección. consolidado anual de hallazgos por tipo (p. ej., “herramientas no autorizadas”) y por proceso/área cuando sea posible. (NIST, 2024, secc. 4.3; ISO, 2022, ISO/IEC 27001:2022, cl. 9.1)

Periodicidad. Medición. cada vez que se haga auditoría/validación (ideal: semestral o anual). (ISO, 2022, ISO/IEC 27001:2022, cl. 9.2 y 9.1).

Reporte. trimestral si se hace seguimiento interno, y anual en el cierre del PCSI. (ISO, 2022, ISO/IEC 27001:2022, cl. 9.3).

Línea base, meta y umbrales. Línea base. 10% en muestra reportada en el documento.

Meta. reducir hallazgos por debajo de 10%.

Umbrales sugeridos (para decisión). Verde, < 10%.

Amarillo, 10% a 15% (no mejora / ligera desviación).

Rojo, > 15% (deterioro). (NIST, 2024, secc. 4.3).

Interpretación y acciones. Si hay hallazgos, normalmente no basta con “recordar la política”: toca revisar fricciones (por qué usan la herramienta externa) y responder con alternativa fácil (guía rápida de OneDrive/SharePoint, plantilla de compartir con terceros, límites de tamaño, etc.). (NIST, 2024, secc. 3.1 y 4.3)

Acciones correctivas típicas, microcontenido “Dónde sí/dónde no”, refuerzo a líderes, y verificación por muestreo en el siguiente trimestre. (NIST, 2024, secc. 4.3)

Dueño del KPI (RACI sugerido). Responsable de cálculo y consolidación. CISO/TI.

Co-responsable de intervención formativa (acciones). T&D + CISO (contenido y seguimiento), líderes de proceso (refuerzo local).

Relación con requisitos/controles. Evidencia de cumplimiento conductual esperada por el programa de concientización y por el SGSI, y útil para auditorías internas y revisión por la dirección. (ISO, 2022, ISO/IEC 27001:2022, cl. 7.3, 9.1 y 9.3).

Relación con la Brecha. El diagnóstico realizado por la “empresa auditora” en la auditoria de 2024 evidenció la presencia de herramientas no autorizadas en uso por parte de los colaboradores, lo que vulnera la Política de uso de activos y recursos de informática. La medición inicial estableció el nivel actual de incumplimiento en un valor de 10% de hallazgos de uso de Wetransfer sobre la muestra realizada (10 equipos), y la meta toma este valor como referencia y busca reducirlo para fortalecer el control y cumplimiento normativo.

Reducción de Hallazgos de Escritorio en Auditoría. Este KPI evalúa la proporción de hallazgos relacionados con el incumplimiento de la política de escritorio y pantalla limpios, que es fundamental para proteger la información visualmente y evitar accesos no autorizados.

Identificación. Nombre. Reducción de hallazgos de escritorio/pantalla limpia en auditoría.

Propósito. bajar el riesgo de exposición visual/física y mejorar disciplina operativa. (NIST, 2024, secc. 4.3).

Nivel de evaluación. principalmente Nivel 3 (Comportamiento). (NIST, 2024, secc. 4.3).

Definición operacional. Hallazgo. no conformidad observada (escritorio digital con información expuesta, no bloqueo, etc.) contra la política interna aplicable.

Fórmula y unidad. Fórmula. Tasa de hallazgos = número de hallazgos / población muestra.

Unidad. porcentaje (%).

Fuente de datos y recolección. Fuente primaria. informe de auditoría/validación con evidencia (fotografías o registros).

Recolección. consolidado por periodo (y si se puede, por proceso/ubicación) con evidencia almacenada como registro del PCSI/SGSI. (ISO, 2022, ISO/IEC 27001:2022, cl. 7.5; NIST, 2024, secc. 4.3).

Periodicidad. Medición. cada auditoría/validación (ideal: semestral). (ISO, 2022, ISO/IEC 27001:2022, cl. 9.2).

Reporte. trimestral si hay controles internos; mínimo anual. (ISO, 2022, ISO/IEC 27001:2022, cl. 9.1 y 9.3).

Línea base, meta y umbrales. Línea base. 10% (según el documento).

Meta. reducir hallazgos por debajo de 10%.

Umbrales sugeridos (para decisión). Verde, < 10%.

Amarillo, 10% a 12% (no mejora / ligera desviación).

Rojo, > 12% (deterioro). (NIST, 2024, secc. 4.3).

Interpretación y acciones. Este KPI suele mejorar más cuando se combina: recordatorio mensual + “checklist” simple + ejemplo visual de “cómo se ve un escritorio limpio” + refuerzo de líderes. (NIST, 2024, secc. 3.3 y 4.3).

Si no mejora, normalmente el problema es de hábito (no de conocimiento), así que la intervención debe ser práctica (nudges, mini retos, revisión por pares) y no solo “más teoría”. (NIST, 2024, secc. 4.3).

Dueño del KPI (RACI sugerido). Responsable de cálculo y consolidación. CISO/TI.

Co-responsable de intervención formativa (acciones). T&D + líderes de proceso (hábitos del día a día).

Relación con requisitos/controles. Aporta evidencia de desempeño de controles y de efectividad del componente de concientización, integrable a medición del SGSI y a revisión por la dirección. (ISO, 2022, ISO/IEC 27001:2022, cl. 9.1 y 9.3; NIST, 2024, secc. 4.3).

Relación con la Brecha. Se identificaron incumplimientos en RTD-IT-005 Política de escritorio y pantalla limpia, lo que representa un riesgo físico y operativo para la información de La "mediana empresa de tecnología". La medición inicial de 10% de hallazgos sobre los equipos revisados, permitió cuantificar esta brecha, y la meta apunta a mejorar la disciplina y cumplimiento en este aspecto reduciendo los hallazgos por debajo del 10%.

Porcentaje Finalización Capacitación en LMS Este KPI mide el porcentaje de colaboradores inscritos en el curso de concientización en seguridad de la información que completan el 100% de la capacitación en el LMS Escuela Sura. Es un indicador clave de la cobertura y compromiso con el programa.

Identificación. Nombre. Porcentaje de finalización de capacitación en LMS.

Propósito. medir cobertura/alcance real del PCSI (sin finalización no hay base mínima de aprendizaje). (NIST, 2024, secc. 3.3 y 4.3).

Nivel de evaluación. principalmente participación/alcance (equivalente a "nivel de actividad"), y complementa evaluación de aprendizaje cuando se cruza con notas/resultado. (NIST, 2024, secc. 4.3).

Definición operacional. Finalización. completar el 100% del curso (y, si aplica, cumplir criterio de aprobación).

Fórmula y unidad. Fórmula. Finalización LMS = número de finalizaciones / número de inscritos.

Unidad. porcentaje (%).

Fuente de datos y recolección. Fuente primaria. reportes del LMS Proporcionado por la ARL (matriculados, completado, aprobado, intentos, tiempo).

Recolección. export mensual (o por cohorte) y almacenamiento como evidencia del programa (trazabilidad). (ISO, 2022, ISO/IEC 27001:2022, cl. 7.5; NIST, 2024, secc. 4.3).

Periodicidad. Medición. mensual durante el despliegue, y acumulado anual. (NIST, 2024, secc. 4.3).

Reporte. mensual a T&D/CISO y trimestral a dirección (si así lo definen). (ISO, 2022, ISO/IEC 27001:2022, cl. 9.3).

Línea base, meta y umbrales. Línea base. no queda cuantificada en el texto del KPI; lo más práctico es fijarla con el primer corte de ejecución (Mes 1 o Mes 2) como “% completado acumulado”.

Meta. 100% tasa de finalización.

Umbrales sugeridos (para decisión). Verde, ≥90% acumulado a la fecha esperada de cierre (por ejemplo, al mes 12). (NIST, 2024, secc. 4.3).

Amarillo, 70%–89% (requiere empuje de comunicaciones/recordatorios). (NIST, 2024, secc. 4.3).

Rojo, <70% (intervención con líderes y reprogramación). (NIST, 2024, secc. 4.3).

Interpretación y acciones. Este KPI no prueba por sí solo cambio de comportamiento; prueba cobertura. Por eso conviene gestionarlo como condición habilitante y cruzarlo con CTR/Reportes/Auditorías para el “impacto real”. (NIST, 2024, secc. 4.3)

Acciones típicas cuando hay desviación: campaña de recordatorios, apoyo de líderes, y ventanas de tiempo claras; si hay barreras de acceso, se corrige operación del LMS antes de culpar a la gente. (NIST, 2024, secc. 3.2 y 4.3).

Dueño del KPI (RACI sugerido). Responsable de cálculo y consolidación. T&D (por gestión del LMS y trazabilidad).

Co-responsable de intervención formativa (acciones). CISO/TI (para alinear cohortes y priorización por riesgo).

Relación con requisitos/controles. Aporta evidencia de competencia/conciencia y de que se ejecutan actividades de concientización, útil para auditoría y mejora. (ISO, 2022, ISO/IEC 27001:2022, cl. 7.2–7.3 y Anexo A control 6.3; NIST, 2024, secc. 4.3)

Relación con la Brecha. El diagnóstico mostró una baja tasa de finalización en las capacitaciones, lo que limita el impacto del PCSI. La medición inicial estableció esta línea base, y la meta busca incrementar la participación y el compromiso para asegurar que el conocimiento llegue a toda la organización.

Importancia de la Mejora Continua. El CPLP se basa en un ciclo de mejora continua, donde los resultados de estas métricas serán revisados periódicamente para identificar áreas de oportunidad, actualizar contenidos y estrategias, y fortalecer la cultura de seguridad en toda la organización. Este enfoque garantiza que el programa evolucione conforme a las necesidades y riesgos emergentes, contribuyendo a la resiliencia organizacional y al cumplimiento normativo (ISO/IEC, 2022a; ISO/IEC, 2022b; NIST, 2014).

Temática del Pcsi Alineada a Políticas Internas y Riesgos

El PCSI cubrirá, como mínimo, los temas requeridos por las políticas y procedimientos internos vigentes: uso aceptable de activos, clasificación y manejo de la información, contraseñas seguras, respaldo, escritorio/pantalla limpia, firewall y navegación segura, gestión de activos, VPN, respuesta y gestión de incidentes, gestión de vulnerabilidades y tratamiento de datos personales, entre otros actuales y por crearse. (NIST, 2024, NIST SP 800-50r1, secc. 2.2 y 3.3; ISO, 2022, ISO/IEC 27002:2022, controles 5.1, 6.3 y 8.x según aplique).

Referencias internas (para derivar contenidos y casos): Uso de activos; Clasificación de información; Contraseñas; Respaldo; Escritorio y pantalla limpia; Firewall; VPN; Usuarios;

Incidentes; Vulnerabilidades; Activos; Datos personales. Integrar políticas al programa refuerza cumplimiento de ISO 27001/27002 sobre conciencia (ISO, 2022, ISO/IEC 27001:2022, cl. 7.2–7.3; ISO, 2022, ISO/IEC 27002:2022, 6.3).

Cronograma Anual del PCSI

El Plan de Concientización en Seguridad de la Información (PCSI) de La “mediana empresa de tecnología” se despliega a lo largo de 12 meses, combinando formación en el LMS Proporcionado por la ARL, campañas visuales en cartelera digital y microcontenidos mensuales distribuidos por Microsoft Teams y Viva Engage. El programa busca cerrar brechas identificadas en la cultura de seguridad, fortalecer buenas prácticas y fomentar el reporte oportuno de incidentes, todo alineado con el Sistema de Gestión de Seguridad de la Información (SGSI) y las normativas ISO 27001:2022 e ISO 27002:2022 (ISO, 2022).

Arranque y Preparación (Meses 1 y 2). El PCSI arranca en el Mes 1 con dos actividades fundamentales que sientan las bases del programa. ***Primero***, se dicta la Formación PCSI a líderes, una capacitación dirigida a la Audiencia 4 (líderes de procesos y alta dirección) donde se explican los objetivos del PCSI, los roles y responsabilidades de cada área, y cómo se hará el seguimiento a través de indicadores y métricas a lo largo del año (NIST, 2024). Esta sesión es clave para asegurar el compromiso de la dirección y la alineación estratégica del programa con los objetivos organizacionales. En paralelo, el equipo de T&D y TI/CISO trabaja en la preparación de contenidos para el LMS, diseñando y ajustando los materiales del Capítulo 1 (Concientización básica) y Capítulo 2 (Buenas prácticas y controles básicos). Se definen objetivos de aprendizaje, se redactan guiones, se diseñan preguntas de evaluación y se configura la estructura base de los cursos en el LMS Proporcionado por la ARL. Durante este mes aún no se envían microcontenidos a los colaboradores, ya que el foco está en la preparación interna y la gobernanza del programa.

En el Mes 2 continúa la fase de preparación, ahora concentrada en el montaje de los Capítulos 3 (Manejo de incidentes y reporte) y 4 (Principios del tratamiento de datos

personales). Se cierran guiones, se ajustan evaluaciones y se configura todo en el LMS (duración, intentos, criterios de aprobación). Además, se planifica el calendario de refuerzos: se definen los meses en que se activarán las campañas de cartelera digital y se preparan los primeros insumos gráficos y mensajes clave para microcontenidos. Un hito importante de este mes es el inicio de la primera campaña de cartelera digital, que se extenderá durante los Meses 2, 3 y 4, mostrando mensajes introductorios sobre qué es el PCSI, la importancia de la seguridad de la información y mensajes culturales generales que preparan el terreno para los contenidos específicos que vendrán.

Despliegue de Concientización Básica (Meses 3 a 5). A partir del Mes 3 comienza formalmente el despliegue a los colaboradores. Se lanza el primer subcapítulo del Capítulo 1: Conceptos básicos de seguridad de la información, con el tema "Contextualización en seguridad". Este módulo busca cerrar las brechas 1, 2 y 4 (falta de conocimiento básico, desconocimiento de políticas y falta de cultura de seguridad), introduciendo a los colaboradores en los fundamentos de la seguridad de la información y su relevancia en la “mediana empresa de tecnología” (ISO, 2022). Se comunica que, idealmente, al cierre del Mes 3 todos deberían haber completado este módulo, aunque el curso permanece disponible los 12 meses. Este mes también marca el inicio de los microcontenidos mensuales: se publica el primer microcontenido en Teams y Viva Engage con el tema "la seguridad es trabajo en equipo", reforzando de manera visual y sintética lo que se ve en el LMS. La primera campaña de cartelera digital sigue en curso, alineando los mensajes visuales con el lanzamiento del primer subcapítulo.

En el Mes 4 la audiencia 1 debe avanzar como mínimo al segundo subcapítulo, con el tema "Reconocimiento de impacto organizacional". Aquí se busca que los colaboradores comprendan qué pasa si falla la seguridad: impactos operacionales, reputacionales y económicos para la “mediana empresa de tecnología”, atacando las brechas 1 y 4 (ISO, 2022). El microcontenido del mes refuerza este mensaje con ejemplos concretos: "Cada clic es una

decisión heroica. Protege tus acciones". La primera campaña de cartelera cierra en este mes, completando 3 meses de exposición visual con mensajes sobre la importancia de la seguridad.

El Mes 5 cierra el Capítulo 1 con el subcapítulo Principales tipos de ataque, enfocado en la "Conceptualización de exposición" (malware, phishing, ingeniería social, etc.), atacando la brecha 3 (desconocimiento de amenazas). El microcontenido del mes presenta "Tu compromiso de hoy construye la fortaleza del mañana", fijando en la memoria los conceptos clave que se ven en el LMS.

Buenas Prácticas y Controles Básicos (Meses 6 a 8). El Mes 6 marca el inicio del Capítulo 2 con el subcapítulo Gestión de contraseñas y autenticación, tema "Gestión de credenciales y MFA". Este módulo ataca la brecha 3 (malas prácticas con contraseñas) y busca que los colaboradores mejoren la calidad de sus credenciales, conozcan la autenticación multifactor (MFA) y usen herramientas de gestión como KeePass (ISO, 2022). El microcontenido del mes presenta " Una contraseña robusta es como el anillo de linterna verde", reforzando de manera práctica y accionable lo aprendido en el LMS.

En el Mes 7 se aborda el subcapítulo Manejo seguro del correo electrónico y navegación, con el tema "Reconocimiento y reporte de phishing", atacando la brecha 3 (vulnerabilidad ante ataques de ingeniería social). Este mes es especialmente importante porque, además del curso en LMS, se ejecuta una simulación de phishing sobre la población definida, midiendo indicadores clave como la tasa de clics (CTR) y la tasa de reporte (NIST, 2024). El microcontenido del mes refuerza justo en este momento: " Los verdaderos héroes protegen datos", apoyando la simulación y sensibilizando sobre las señales de alerta en correos sospechosos.

El Mes 8 avanza con el subcapítulo Protección de la información en dispositivos y red, tema "Proteger la información de la empresa en dispositivos móviles y redes", atacando las brechas 1, 2 y 3 (desconocimiento de políticas de uso de dispositivos y riesgos en redes no confiables) (ISO, 2022, cap. 6.7, 8.1). El microcontenido del mes puede enfocarse en "Tu

imaginación es el límite para crear contraseñas indecifrables. Un hito clave de este mes es el inicio de la segunda campaña de cartelera digital, que se extenderá durante los Meses 8 al 12, concentrándose en temas de protección de dispositivos, manejo de incidentes y repositorios autorizados. Con esta segunda campaña se completan los 6 meses totales de exposición en cartelera durante el año.

Manejo de Incidentes y Políticas Internas (Meses 9 a 11). El Mes 9 introduce el Capítulo 3 con el subcapítulo Reconocer un incidente y pasos iniciales, tema "Respuesta inicial a incidentes y reportes", atacando las brechas 3 y 4 (desconocimiento de qué es un incidente y cómo reportarlo, falta de cultura de reporte). Este módulo es fundamental para que los colaboradores sepan identificar situaciones anómalas y conozcan el canal de reporte en La “mediana empresa de tecnología” (ISO, 2022, cap. 5.24, 5.25, 5.26). El microcontenido del mes pregunta directamente: "¿Qué es un incidente y cómo lo reportas?", incluyendo ejemplos y el canal claro de reporte. La segunda campaña de cartelera sigue en curso.

En el Mes 10 se aborda el Capítulo 4 con el subcapítulo Políticas y normativas internas, tema "Uso correcto de repositorios autorizados (OneDrive/SharePoint)", atacando las brechas 1 y 2 (desconocimiento de políticas de clasificación y uso de herramientas no autorizadas). El objetivo es dirigir a las personas hacia los repositorios oficiales y evitar el uso de herramientas externas que pongan en riesgo la información (ISO, 2022). El microcontenido del mes muestra visualmente "Dónde sí y dónde no guardar información de La “mediana empresa de tecnología”".

El Mes 11 continúa con el Capítulo 4, ahora con el subcapítulo Escritorio y pantalla limpia, atacando la brecha 1 (desconocimiento de políticas de escritorio limpio y riesgos de exposición física de información). Este módulo refuerza prácticas como no dejar información sensible visible en el escritorio físico o en la pantalla, y bloquear equipos al ausentarse (ISO, 2022). El microcontenido del mes presenta "Lo que nunca deberías dejar a la vista en tu puesto de trabajo", aplicable tanto a papel como a pantallas y pizarras.

Cierre y Evaluación (Mes 12). El Mes 12 cierra el ciclo anual del PCSI con dos componentes fundamentales. Primero, se lanza el último subcapítulo del Capítulo 4: Tratamiento de datos personales, tema "Protección de datos personales (principios y obligaciones)", atacando la brecha 4 (desconocimiento de obligaciones legales y principios de protección de datos personales). Este módulo refuerza la responsabilidad sobre los datos personales acorde a la política interna de La “mediana empresa de tecnología” y la normativa vigente (Ley 1581 de 2012 y Decreto 1377 de 2013). El microcontenido del mes sintetiza "Datos personales: las 5 cosas que no puedes olvidar", reforzando de manera muy concreta los principios y deberes.

Segundo, en este mes se realiza la revisión y evaluación anual del PCSI. Se convoca a los líderes para presentar los resultados del año: tasas de finalización de cursos, resultados de la simulación de phishing, hallazgos de auditorías, incidentes reportados, y el cumplimiento de los KPIs definidos en la matriz (NIST, 2024). Se identifican brechas persistentes o nuevas necesidades, y se definen ajustes al programa para el siguiente ciclo.

Revisiones Extraordinarias del PCSI. También existen revisiones extraordinarias del PCSI, que pueden ocurrir durante el año si hay eventos de seguridad relevantes, nuevas políticas o cambios regulatorios que lo ameriten (ISO, 2022), para estas debe convocarse al equipo de encargados del PCSI para definir acciones a seguir o nuevos temas que deben incluirse en el LMS, campañas o microcontenidos.

On Boarding. El On Boarding es un proceso de inducción corporativo que puede ocurrir en cualquier mes del año, según los ingresos de nuevos colaboradores. Incluye contenidos de seguridad de la información y datos personales, pero no se expresa como actividad fija en el cronograma mensual del PCSI. Se mantiene como una actividad adicional y variable, gestionada por T&D, que complementa el despliegue anual del programa (Véase en el Anexo B un resume el cronograma detallado para la implementación del PCSI).

Presupuesto Anual del PCSI

El año es financieramente retador para la “mediana empresa de tecnología”, motivo por el cual el proyecto está orientado a un PCSI “no automatizado” y de bajo costo, donde se privilegian recursos existentes y se excluyen las capacitaciones técnicas formales por su costo elevado (“mediana empresa de tecnología”, 2024).

Enfoque General sin Costos en Dinero. Para la planeación del PCSI nos vamos a centrar únicamente en horas-hombre, es decir, en el tiempo que dedican los diferentes roles de la “mediana empresa de tecnología” (CISO/Responsable de Seguridad, TI, T&D, Dirección A&F, líderes de proceso, etc.) a las actividades de concientización y capacitación, sin traducirlo a pesos. Esto es coherente con el enfoque de planificación del programa de sensibilización que propone NIST para identificar recursos, responsables y frecuencia de las actividades, sin obligar a monetizarlas desde el inicio (NIST, 2024).

Se estimas los costos de fases posteriores más allá del alcance del proyecto, para que sean tenidas en cuenta en el desarrollo de las mismas.

Herramientas ya Disponibles (Costo Cero en el Presupuesto del PCSI). Microsoft 365: Teams, Viva Engage, Forms, SharePoint, Authenticator, etc., ya incluidos en las licencias pagadas anualmente.

LMS entregado por la ARL sin costo por uso específico.

Pantalla de video cartelera ya en operación y depreciada contablemente.

OpenShot para edición de video y GoPhish para phishing son software de libre distribución.

Por lo tanto, no se cargan licencias ni suscripciones al presupuesto del PCSI; solo se consideran horas de trabajo interno.

Costos Hora Hombre por Fase. ***Fase de Planeación y Estrategia.*** Esta fase agrupa el trabajo de gobierno del programa, alineación con riesgos organizacionales y seguimiento estratégico. Se incluyen actividades como la definición anual del plan de concientización y las revisiones periódicas de avance, donde participan el CISO, la Dirección A&F y T&D (NIST, 2024, sec. 2.1–2.4).

Horas-hombre estimadas: 8 horas anuales.

La estimación considera reuniones de trabajo estratégicas de duración acotada (entre 2 y 4 horas por evento), realizadas al inicio del ciclo y en momentos clave de revisión. Este nivel de esfuerzo es coherente con un programa en fase inicial que requiere alineación directiva sin generar sobrecarga administrativa. Se asumió que la planificación no demanda procesos complejos de análisis cuantitativo, sino sesiones de consenso y priorización basadas en riesgos conocidos y en lecciones del período anterior.

Fase de Análisis y Diseño. En esta fase se realiza el análisis de audiencias, la segmentación por roles y la definición del currículo de concientización, así como la actualización periódica de contenidos digitales (presentaciones, guiones, cuestionarios). El liderazgo recae en T&D con validación técnica del CISO y apoyo de Mercadeo (NIST, 2024).

Horas-Hombre Estimadas: 14 Horas Anuales.

Se consideró que el diseño requiere una inversión inicial de tiempo mayor (6 horas) para estructurar la segmentación y los objetivos de aprendizaje por rol, mientras que las actualizaciones semestrales de contenidos son más ágiles (4 horas cada una) porque parten de materiales ya existentes. Esta lógica responde a la recomendación de NIST de mantener los contenidos vivos sin rediseñar todo el programa cada ciclo, aprovechando la base documental y ajustando según incidentes reales o cambios normativos internos.

Fase de Desarrollo e Implementación. Esta es la fase con mayor carga de trabajo, pues concentra todas las actividades de entrega del programa: sesiones de creación de contenido, campañas digitales de comunicación, simulación de phishing, soporte operativo y

gestión de evidencias. Participan todos los roles del PCSI de forma recurrente a lo largo del año (NIST, 2024).

Horas-Hombre Estimadas: 103 Horas Anuales.

La estimación se construyó sumando:

Sesiones de Formación. se asumió una frecuencia mensual para inducciones de personal nuevo (1,5 horas por sesión, 12 eventos), sesiones de refuerzo anual para toda la organización divididas en grupos (2 horas por sesión, 4 eventos), un taller anual con líderes de proceso (3 horas) y sesiones trimestrales con el equipo de TI (1,5 horas por sesión, 4 eventos). Estas duraciones son estándar en programas de concientización para no saturar a los participantes y permitir interacción.

Campañas Digitales. se planificaron 2 campañas temáticas al año (3 horas de planificación por campaña) con difusión continua de mensajes breves (0,5 horas por acción, 24 acciones en el año). Este volumen busca mantener presencia constante sin generar fatiga comunicacional.

Simulación de Phishing. se incluyó una sola campaña anual (6 horas para diseño, ejecución y análisis) con 2 sesiones breves de retroalimentación (1 hora cada una). Esta decisión responde al alcance inicial del programa y a la madurez actual de La “mediana empresa de tecnología”.

Soporte operativo. se estimaron 2 horas mensuales para gestión de convocatorias y recordatorios (24 horas anuales) y 1 hora mensual para archivo digital de evidencias (12 horas anuales), reconociendo que estas tareas son recurrentes, pero de baja complejidad individual.

El peso de esta fase refleja que la efectividad del PCSI depende de la ejecución sostenida de actividades de concientización y del acompañamiento operativo que garantice trazabilidad y participación.

Fase de Evaluación y mejora. Esta fase agrupa las actividades de medición de resultados, definición de indicadores y reporte a la dirección. Incluye el diseño y aplicación de

evaluaciones de conocimientos, la revisión de indicadores del programa y la elaboración de informes ejecutivos. Participan principalmente el CISO, T&D y la Dirección A&F (NIST, 2024; ISO/IEC 27001, 2022).

Horas-hombre estimadas: 21 horas anuales.

Se consideró que el diseño de cuestionarios requiere un esfuerzo moderado (4 horas) para alinear preguntas con riesgos y políticas, mientras que la aplicación y consolidación de resultados demanda más tiempo (8 horas) por la coordinación con participantes y el análisis inicial de datos. La definición de indicadores se estimó en 3 horas, asumiendo una sesión de trabajo focalizada, y el informe ejecutivo anual en 6 horas, reconociendo que debe integrar múltiples fuentes de información y presentarse en lenguaje directivo. Esta fase es esencial para demostrar el valor del programa y fundamentar decisiones de mejora continua.

Resumen Global. El presupuesto total del PCSI es de 146 horas-hombre al año, con la siguiente distribución:

Planeación y estrategia: 8 horas (5%)

Análisis y diseño: 14 horas (10%)

Desarrollo e implementación: 103 horas (71%)

Evaluación y mejora: 21 horas (14%)

(Véase en el Anexo C un resume del presupuesto detallado para la implementación del PCSI).

Analizar

Método de Análisis

Para determinar las brechas de comportamiento, se adoptó el enfoque de la fase de análisis del ciclo de vida de un plan de concientización y entrenamiento en seguridad de la información descrito en la NIST SP 800-50r1, el cual propone identificar el estado actual a partir de fuentes de evidencia, compararlo con el estado deseado definido por políticas y requisitos y, a partir de ese contraste, derivar las brechas de conocimiento, habilidad o hábito (National Institute of Standards and Technology [NIST], 2024, NIST SP 800-50r1, secc. 3.1).

En coherencia con dicha guía, las brechas se entendieron como la diferencia entre los comportamientos observados en la organización y los comportamientos esperados según metas y políticas, para lo cual se utilizaron datos provenientes de auditorías, ejercicios de phishing y revisiones de políticas como insumos principales para su identificación sistemática.

En primer lugar, se realizó una lectura y síntesis de los datos cuantitativos y cualitativos obtenidos de los documentos disponibles, considerando indicadores como el porcentaje de equipos con hallazgos, el porcentaje de usuarios que abren o hacen clic en correos y la cantidad de reportes recibidos de la población objetivo de las pruebas.

A continuación, se identificó el comportamiento observable asociado a cada hallazgo, por ejemplo, escritorios desordenados, uso de herramientas no autorizadas como WeTransfer o ausencia de reporte de intentos de phishing.

Posteriormente, para cada hallazgo se efectuó un contraste sistemático con los comportamientos esperados definidos en las políticas internas y en los lineamientos de las normas ISO, tales como mantener el escritorio y la pantalla limpios, utilizar canales autorizados para la transferencia de información y reportar incidentes o correos sospechosos.

Cuando un hallazgo evidenciaba, de forma consistente, un comportamiento diferente al esperado (por ejemplo, 10 % de equipos con hallazgos o 4 % de usuarios que hicieron clic en enlaces maliciosos), se interpretó como indicio de que la política no se había consolidado como hábito, constituyéndose así en una brecha de aprendizaje.

Finalmente, para cada brecha identificada se localizaron las políticas internas de La “mediana empresa de tecnología” que abordan de manera directa el tema correspondiente y, con base en dichos documentos, se describió el estado de comportamiento esperado, precisando cómo actuaría o qué dejaría de hacer un usuario en su trabajo diario en caso de haber adoptado efectivamente la política y los controles asociados.

Determinar las Brechas de Concientización

Brecha 1. Incumplimiento de Política de Escritorio Limpio. *Insumos y Hallazgo.* Insumos y hallazgo. A partir del informe de la “Empresa auditora” se identificó que, en el 10 % (1 de 10) de los equipos de cómputo auditados, no se cumple la política de escritorio limpio, la cual forma parte del esquema de seguridad de la información de la “mediana empresa de tecnología” (“empresa auditora”, 2024). La evidencia fotográfica asociada al hallazgo muestra un escritorio de Windows con múltiples íconos y elementos visibles, lo que fue interpretado por el auditor como un indicio de la no aplicación de las prácticas de escritorio y pantalla limpia, así como de una posible exposición innecesaria de información en el entorno digital de trabajo (“empresa auditora”, 2024).

Este hallazgo se contrastó con la Política de escritorio y pantalla limpia, en la cual se establece que la pantalla debe mantenerse libre de información o accesos directos visibles que puedan exponer datos sensibles o confidenciales (“mediana empresa de tecnología” S.A., 2023). De igual forma, se relacionó con el control 7.7 de la ISO/IEC 27002:2022, que exige definir y aplicar reglas para mantener escritorios y pantallas libres de información sensible, como parte de las medidas de protección de la información en los puestos de trabajo

(International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC], 2022, ISO/IEC 27002:2022, secc. 7.7).

Brecha. Al analizar este caso desde el enfoque de la NIST SP 800-50r1, se identificó una brecha clara entre el comportamiento esperado y el comportamiento observado: aunque la política de escritorio y pantalla limpia se encuentra formalmente definida y ha sido comunicada a los colaboradores, una parte de los usuarios aún no la ha interiorizado ni la aplica de manera consistente en su trabajo diario (National Institute of Standards and Technology [NIST], 2024, NIST SP 800-50r1, secc. 3.1, 3.1.2.1). En términos de esta guía, la brecha se interpreta como la diferencia entre el estado actual (escritorios “sucios” o con información visible y accesos directos no controlados) y el estado deseado (escritorios y pantallas limpios, en cumplimiento permanente de la política), lo que requiere ser abordado mediante acciones específicas de concientización, capacitación y refuerzo de comportamientos seguros (NIST, 2024, NIST SP 800-50r1, secc. 3.1).

Cierre. Desde la perspectiva de la NIST SP 800-50r1, la diferencia entre el estado actual (90 % de cumplimiento en la muestra analizada) y el estado deseado (idealmente 100 % de cumplimiento o, al menos, un umbral objetivo superior al nivel observado) se configura como una brecha de aprendizaje y comportamiento. Esta brecha debe ser atendida por el PCSI mediante acciones de sensibilización dirigidas a todos los usuarios y actividades prácticas de refuerzo orientadas al cumplimiento de la Política de escritorio y pantalla limpia, de forma que se logre consolidar el hábito de mantener escritorios y pantallas limpios como parte de la cultura de seguridad de la información de la “mediana empresa de tecnología” (NIST, 2024, NIST SP 800-50r1, secc. 2.4, 3.1).

Brecha 2. Uso de Repositorios no Oficiales para Información Corporativa. *Insumos y Hallazgo.* A partir del informe de la “Empresa auditora” se identificó que, en el 10 % (1 de 10) de los equipos de cómputo de la muestra auditada, el colaborador utilizó canales externos para mover información corporativa fuera de los repositorios institucionales (“empresa auditora”, 2024). La evidencia asociada muestra que algunos colaboradores, en la práctica, no utilizan OneDrive ni SharePoint como repositorios oficiales de información y recurren a servicios externos como WeTransfer para compartir archivos, lo que refuerza la existencia de un patrón de uso de repositorios no autorizados en lugar de los repositorios oficiales provistos por la organización (“empresa auditora”, 2024). Este comportamiento se contrasta directamente con la Política de uso de activos y recursos de teleinformática, que establece, entre otros aspectos, que la utilización de los recursos tecnológicos de la compañía debe estar alineada con los fines del negocio, que los recursos compartidos deben gestionarse a través de herramientas corporativas como SharePoint y OneDrive y que los repositorios institucionales son el lugar donde debe almacenarse la información relevante, evitando el uso de medios alternos no controlados para copias o transferencias de información (“mediana empresa de tecnología” S.A., 2021). De forma complementaria, este análisis se alinea con el control 7.7 y otros controles de la ISO/IEC 27002:2022 sobre uso aceptable de activos, transferencia de información y uso seguro de servicios en la nube, que subrayan la necesidad de utilizar canales autorizados y controlados para la gestión de la información (International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC], 2022, ISO/IEC 27002:2022, controles 5.10, 5.14, 5.23).

Brecha. Al analizar este caso desde el enfoque de la NIST SP 800-50r1, se identifica una brecha de cumplimiento por parte del usuario frente al uso de los repositorios oficiales definidos en la Política de uso de activos y recursos de teleinformática, aunque los colaboradores deben utilizar OneDrive y SharePoint para almacenar y compartir información, en algunos casos optan por recurrir a repositorios externos como WeTransfer, que no forman parte de los canales autorizados por la política (“mediana empresa de tecnología” S.A., 2021, “Política de uso de activos y recursos de teleinformática”, secc. 2.6, 2.6.1, 2.7). En términos de la NIST SP 800-50r1, esta situación se ajusta a la definición de brecha como la diferencia entre el estado actual, donde el 10 % de usuarios utiliza servicios externos no oficiales, y el estado deseado, en el que el 100% de la información corporativa se gestiona exclusivamente a través de repositorios institucionales y servicios en la nube aprobados por la organización (National Institute of Standards and Technology [NIST], 2024, NIST SP 800-50r1, secc. 3.1, 3.1.2.1).

La conducta observada sugiere que el usuario aún no ha interiorizado que OneDrive y SharePoint son los canales obligatorios para la gestión y el intercambio de documentos y que el uso de servicios de terceros lo coloca en una situación de incumplimiento de la RTD-IT-001 Política de uso de activos y recursos de teleinformática, además de aumentar el riesgo de pérdida de control sobre la información corporativa (“mediana empresa de tecnología” S.A., 2021; NIST, 2024, NIST SP 800-50r1, secc. 2.7.1, 4.1.1). Desde esta perspectiva, la brecha no se limita al conocimiento abstracto de la existencia de la política, sino que involucra también el hábito y la competencia práctica: el colaborador no solo debe saber que WeTransfer no es un repositorio oficial, sino también sentirse capaz de cumplir sus objetivos cotidianos (por ejemplo, compartir archivos con clientes o proveedores) utilizando de forma natural OneDrive y SharePoint como medios aprobados por la organización (NIST, 2024, NIST SP 800-50r1, secc. 4.1.1, 4.1.2).

Cierre. Desde la lógica de la NIST SP 800-50r1, la diferencia entre el estado actual, en el que al menos un 10 % de los equipos muestreados ha permitido y potencialmente utilizado servicios de reposición de información no oficiales, y el estado deseado, en el que el uso de repositorios externos como WeTransfer para información corporativa debería ser nulo, mientras que toda la información (100%) se canaliza a través de OneDrive y SharePoint como repositorios oficiales, se interpreta como una brecha de aprendizaje y comportamiento que el PCSI debe abordar de manera explícita (NIST, 2024, NIST SP 800-50r1, secc. 2.4, 3.1). Cuantitativamente, la muestra de la “Empresa auditora” refleja que un 10 % de los de los usuarios incumple la Política de uso de activos y recursos de teleinformática respecto al uso de repositorios oficiales, cuando el objetivo debería ser que el 100 % de los usuarios utilice exclusivamente los repositorios institucionales para almacenar y compartir información o, al menos, que el porcentaje de uso de servicios externos se reduzca a menos del 10 % identificado en el hallazgo (“mediana empresa de tecnología” S.A., 2024, “Planilla de validación, “Mediana Empresa de Tecnología” – Auditoría de aspectos de SI 2023”, hallazgo 4; “mediana empresa de tecnología” S.A., 2021, “Política de uso de activos y recursos de teleinformática”).

En consecuencia, la brecha puede formularse de manera sintética así: actualmente, una fracción de los colaboradores continúa utilizando repositorios externos no oficiales para gestionar información, en lugar de los repositorios institucionales definidos en la Política de uso de activos y recursos de teleinformática; mediante acciones de sensibilización y entrenamiento específico en el uso de OneDrive y SharePoint, el PCSI debe fortalecer su conocimiento y apropiación de esta política, de modo que el uso de repositorios no oficiales descienda a menos del 10 % evidenciado en la muestra, asegurando que la gran mayoría de la información se gestione exclusivamente en los repositorios corporativos autorizados (NIST, 2024, NIST SP 800-50r1, secc. 2.4, 3.1)..

Brecha 3. Comportamiento Ante Correos Maliciosos. ***Insumos y Hallazgo.*** Del Informe de Phishing de la “Empresa Consultora en seguridad” para la “mediana empresa de tecnología”, correspondiente a enero de 2024, se tomaron como referencia los resultados de la campaña “¡Súper oferta de 24 horas!”, enviada a 100 usuarios de la organización (“Empresa Consultora en seguridad”, 2024), En esta campaña se registró que el 20 % de los correos fue abierto, el 4 % de los usuarios hizo clic en el enlace incluido en el mensaje, y el 0 % reportó el correo como malicioso o sospechoso a través de los canales establecidos (“Empresa Consultora en seguridad”, 2024, pp. 10–13). El informe señala que el mensaje contenía varios elementos que podían considerarse indicadores de posible phishing y recomienda establecer métricas de preparación frente a este tipo de ataques, reforzar las campañas de concientización y promover el reporte activo de correos sospechosos (“Empresa Consultora en seguridad”, 2024).

Estos resultados se relacionan directamente con el procedimiento de gestión de incidentes de seguridad de la información y con la guía básica de respuesta a incidentes de la “mediana empresa de tecnología”, así como con los controles de la ISO/IEC 27002:2022 sobre concientización, reporte de eventos de seguridad y gestión de incidentes, y con la NIST SP 800-50r1, que propone el uso de campañas de phishing simuladas para medir comportamientos reales y ajustar el contenido del plan de concientización (“mediana empresa de tecnología” S.A., 2024; International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC], 2022; National Institute of Standards and Technology [NIST], 2024, NIST SP 800-50r1).

Brecha. Desde el enfoque de la NIST SP 800-50r1, estos datos evidencian dos brechas claras de comportamiento. La primera se observa en el 4 % de usuarios que hizo clic en el enlace del correo de prueba, lo que indica que existe un grupo de personas que aún no identifica adecuadamente indicadores básicos de un mensaje potencialmente malicioso o que, ante la duda, no ha incorporado el hábito de detenerse y analizar el contenido antes de interactuar con él (“Empresa Consultora en seguridad”, 2024). La segunda brecha, más evidente, corresponde al 0 % de reportes: ni quienes hicieron clic ni quienes solo abrieron o sospecharon del mensaje utilizaron el canal formal de reporte definido por el procedimiento de gestión de incidentes, lo que sugiere que el comportamiento ante mensajes sospechosos no está instalado como reacción natural en los usuarios (″Empresa Consultora en seguridad″, 2024).

El comportamiento esperado, en línea con los controles de concientización (6.3), reporte de eventos (6.8) y gestión de incidentes (5.24–5.27) de la ISO/IEC 27002:2022, es que cualquier colaborador con formación básica en seguridad reconozca señales de posible phishing y, ante la duda, se abstenga de hacer clic y reporte el correo mediante los canales formales (International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC], 2022, ISO/IEC 27002:2022, controles 6.3, 6.8, 5.24–5.27). La distancia entre ese comportamiento esperado y el comportamiento observado configura, según la NIST SP 800-50r1, una brecha de aprendizaje y de hábito, en la que no basta con conocer el concepto de phishing; se requiere que el usuario adopte patrones de respuesta concretos ante casos reales y actúe como un “sensor activo” de posibles amenazas (NIST, 2024, NIST SP 800-50r1, secc. 2.4, 2.5, 3.1.2.1).

Cierre. Desde la perspectiva cuantitativa que sugiere la NIST SP 800-50r1, el estado actual muestra que un 4 % de los usuarios hace clic en un correo de phishing simulado y un 0 % lo reporta, frente a un estado deseado en el que la tasa de clics ante campañas de dificultad similar se reduzca de forma medible (a un valor objetivo < 4 %, valor actual) y la tasa de reportes aumente significativamente (alcanzar un valor al > 0 % actual, de reportes en futuras campañas simuladas, utilizando el canal formal de incidentes) (“Empresa Consultora en seguridad” S.A., 2024, pp. 14–15; “mediana empresa de tecnología” S.A., s.f., “Gestión de Incidentes de SI”; NIST, 2024, NIST SP 800-50r1, secc. 2.4.2, 2.5.1).

En términos de formulación para el PCSI, la brecha puede expresarse así: en el estado actual, una parte de los usuarios continúa haciendo clic en correos de phishing y prácticamente ninguno los reporta; mediante acciones de concientización y entrenamiento práctico en reconocimiento y reporte de correos maliciosos, se requiere reducir la tasa de clics desde el 4 % actual y aumentar la tasa de reportes desde el 0 %, valor actual, de manera que los colaboradores pasen de ser un punto vulnerable a convertirse en un mecanismo activo de detección temprana de intentos de phishing (“Empresa Consultora en seguridad”, 2024; NIST, 2024, NIST SP 800-50r1, secc. 2.4, 2.5).

Brecha 4. Datos Personales. ***Insumos y Hallazgo.*** El informe ejecutivo sobre la evaluación interna de protección de datos personales en la “mediana empresa de tecnología”, realizado en entre 2024 y 2025, evidencia una alta participación de los empleados, con más del 90 % de los colaboradores activos que completaron la evaluación, y un porcentaje significativo que repitió el examen para mejorar su conocimiento (“mediana empresa de tecnología”, 2024). Los resultados reflejan un buen nivel general de conocimiento en temas básicos, como el habeas data y la definición de datos personales, con la mayoría de los empleados obteniendo puntajes satisfactorios entre 4 y 6 sobre 6 puntos posibles. Sin embargo, se identificaron áreas de oportunidad en temas críticos, tales como las sanciones legales por incumplimiento, el principio de responsabilidad demostrada y la identificación clara de los responsables internos de la protección de datos, donde la tasa de respuestas correctas fue considerablemente menor (“mediana empresa de tecnología”, 2024). Este hallazgo indica que, aunque existe un conocimiento general aceptable, persisten brechas específicas en aspectos fundamentales para el cumplimiento normativo y la cultura organizacional en materia de protección de datos personales.

Brecha. Desde la perspectiva de la NIST SP 800-50r1, esta situación representa una brecha de aprendizaje focalizada en temas clave de protección de datos personales. El estado observado muestra que, si bien la mayoría de los empleados posee un conocimiento básico adecuado, un porcentaje significativo (aproximadamente 25 %) presenta puntajes bajos en áreas críticas que comprometen la correcta aplicación de la política de protección de datos. Esto indica que el conocimiento teórico no se ha traducido completamente en comprensión y aplicación práctica en todos los colaboradores (National Institute of Standards and Technology [NIST], 2024, NIST SP 800-50r1, secc. 3.1). La brecha se manifiesta en la insuficiente internalización de conceptos esenciales como las sanciones legales, la responsabilidad demostrada y la identificación de los responsables internos, lo que puede afectar la efectividad del Plan de Concientización en Seguridad de la Información (PCSI) y el cumplimiento de las normativas legales vigentes.

Cierre. Cuantitativamente, el informe revela que el 25 % de los empleados evaluados obtuvieron puntajes bajos en temas críticos de protección de datos personales, evidenciando una brecha significativa en el conocimiento y la aplicación de estos aspectos (“mediana empresa de tecnología”, 2024). El objetivo del PCSI debe ser reducir esta proporción mediante acciones de capacitación y sensibilización específicas, con el fin de alcanzar un nivel de conocimiento homogéneo y satisfactorio en toda la organización, idealmente logrando que menos del 25 % de los colaboradores obtenga puntajes aprobatorios en futuras evaluaciones. En términos prácticos, la brecha puede formularse así: “Aunque existe un buen nivel general de conocimiento sobre protección de datos personales, es necesario fortalecer la capacitación en temas críticos como sanciones legales, responsabilidad demostrada y roles internos, para reducir la proporción de empleados con bajo desempeño a un nivel objetivo inferior al 25 %, asegurando así un cumplimiento efectivo y una cultura organizacional robusta en materia de protección de datos” (“mediana empresa de tecnología”, 2024; National Institute of Standards and Technology [NIST], 2024, NIST SP 800-50r1, secc. 2.4 y 3.1).

Identificar las Necesidades de Concientización

Propósito. Generar un catálogo estructurado de temáticas para el PCSI que funcione como guía para el desarrollo de materiales de concientización y capacitación. El catálogo priorizará temas en función de las brechas identificadas en auditorías y ejercicios de phishing y estará estrictamente alineado con las políticas y procedimientos vigentes de la “mediana empresa de tecnología” Cada entrada se formulará como un macro-módulo (esquema instruccional) que especificará: la(s) brecha(s) que aborda, los objetivos de aprendizaje, y los documentos internos de referencia que deben emplearse para la construcción del contenido.

Capítulo 1 — Concientización Básica en Seguridad Informática. ***Unidad 1 - Conceptos Básicos de Seguridad de la Información. Objetivo.*** Asegurar que todos compartan un lenguaje mínimo para interpretar riesgos y políticas; evitar que actividades operativas se realicen sin contextualizar el impacto sobre la información.

Brechas que Reduce*. Refuerza comprensión de Brecha 1 (escritorio limpio), Brecha 2 (uso de repositorios) y Brecha 4 (tratamiento de datos).*

Insumos: Política de clasificación de información (“mediana empresa de tecnología”, 2021).

Unidad 2 - Importancia de la Seguridad en el Entorno Laboral. Objetivo. Generar responsabilidad demostrable; favorece adopción de comportamientos esperados por SGSI.

Brechas que Reduce. Especialmente Brecha 1 (prácticas de escritorio) y Brecha 4 (responsabilidad en datos personales).

Insumos. Procedimiento de Capacitación y entrenamiento (“mediana empresa de tecnología”, 2024).

Unidad 3 - Principales Tipos de Ataque. Objetivo. Genera capacidad de identificación temprana y reduce la probabilidad de interacción imprudente con contenidos maliciosos.

Brechas que Reduce. Brecha 3 (phishing) principalmente; además apoya reducción de Brecha 4 (evitar fuga de datos por ingeniería social).

Insumos. Informe de campaña de phishing (“Empresa Consultora en seguridad” S.A., 2024); Procedimiento de gestión de incidentes (“mediana empresa de tecnología”, 2024).

Capítulo 2 — Aplicar Buenas Prácticas y Controles Básicos. ***Unidad 1 - Gestión de Contraseñas Y Autenticación. Objetivo.*** Pasar del conocimiento a la habilidad práctica (crear, almacenar y usar contraseñas seguras, activar 2FA), reduciendo compromiso de credenciales.

Brechas que Reduce. contribuye a mitigar Brecha 3 (phishing/exposición de credenciales) y Brecha 2 (uso indebido de cuentas para mover información).

Insumos. Política de contraseñas seguras (“mediana empresa de tecnología”, 2025).

Unidad 2 - Manejo Seguro del Correo Electrónico y Navegación. Objetivo. Reducir clics e impulsar uso del canal de reporte; entrenar con ejemplos reales y ejercicios reduce la tasa de interacción con phishing.

Brechas que Reduce. Brecha 3 (phishing) — objetivo directo de reducción de CTR (Por sus siglas en ingles Click-Through Rate o tasa de clics) y aumento de reportes. (“Empresa Consultora en seguridad”, 2024).

Insumos. Procedimiento de incidentes y Guía básica de respuesta a incidentes de SI (“mediana empresa de tecnología”, 2024).

Unidad 3 - Protección de la Información en Dispositivos y Red. Objetivo. Definir comportamientos concretos (no conectarse a redes públicas sin VPN, reportar pérdida de equipo, no usar USB no autorizado) que reducen exposición.

Brechas que Reduce. Brecha 1 (escritorio/pantalla limpia), Brecha 2 (evita fuga por dispositivos) y Brecha 3 (vector técnico para phishing/malware).

Insumos. Política de uso de activos y recursos de teleinformática (“mediana empresa de tecnología”, 2021); Instructivo VPN (2019); Política de Firewall. (2019).

Unidad 4 - Uso Correcto de Repositorios Institucionales. Objetivo. Transformar el conocimiento en hábito operativo (guardar y compartir en repositorios aprobados), eliminando la dependencia de canales externos no controlados.

Brechas que Reduce. Brecha 2 (uso de repositorios no oficiales).

Insumos. Política de respaldo de información (“mediana empresa de tecnología”, 2021); Política de uso de activos (2019).

Unidad 5 - Escritorio y Pantalla Limpia. Objetivo. Realizar ejercicios prácticos y recordatorios que conviertan la política en hábito observable.

Brechas que Reduce. Brecha 1 (incumplimiento política escritorio limpio). (“empresa auditora”, 2024).

Insumos. Política de escritorio y pantalla limpia (“mediana empresa de tecnología”, 2023).

Capítulo 3 — Manejo de Incidentes y Reporte. ***Unidad 1 - Reconocer un Incidente y Pasos Iniciales. Objetivo.*** Reducir tiempo de detección/contención y mejorar la calidad de la información del reporte para el equipo de respuesta.

Brechas que Reduce. Brecha 3 (falta de reporte de phishing) y Brecha 4 (mejora respuesta ante incidentes que involucran datos personales).

Insumos. Procedimiento de gestión de incidentes y Guía básica de respuesta (“mediana empresa de tecnología”, 2024).

Capítulo 4 — Principios del Tratamiento de Datos Personales. ***Unidad 1 - Políticas y Normativas Internas. Objetivos.*** Convertir documentación en comportamientos esperados; facilita trazabilidad y cumplimiento en auditoría.

Brechas que Reduce. Brecha 1 (escritorio limpio), Brecha 2 (repositorios no oficiales) y transversalmente contribuye al cumplimiento general.

Insumos. Política de uso de activos (“mediana empresa de tecnología” S.A.S, 2021); Política de Firewall (2021); Política de escritorio y pantalla limpia (2023).

Unidad 2 - Tratamiento de Datos Personales. Objetivo. Cerrar lagunas en comprensión normativa y aplica prácticas concretas (consentimiento, finalidades, manejo de incidentes con datos personales).

Brechas que Reduce. Brecha 4 (conocimiento insuficiente en sanciones, responsabilidad demostrada, responsables internos).

Insumos. Política de tratamiento de datos personales; Tratamiento de datos personales (“mediana empresa de tecnología”, 2024).

Tabla 5

Resumen de contenidos del PCSI

Capítulos	Tema	Brecha objetivo	Insumo documental	Prioridad
Capítulo 1	Concientización Básica en Seguridad Informática	1, 2 y 4	POLÍTICA DE CLASIFICACIÓN DE INFORMACIÓN, CAPACITACIÓN Y ENTRENAMIENTO	Alta
Capítulo 1.1	Conceptos básicos de seguridad de la información	1, 2 y 4	POLÍTICA DE CLASIFICACIÓN DE INFORMACIÓN	Alta
Capítulo 1.2	Importancia de la seguridad en el entorno laboral	1 y 4	CAPACITACIÓN Y ENTRENAMIENTO	Alta
Capítulo 1.3	Principales tipos de ataque	3	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Alta
Capítulo 2	Aplicar buenas prácticas y controles básicos	1, 2 y 3	POLÍTICA DE CONTRASEÑAS SEGURAS, POLÍTICA DE USO DE ACTIVOS Y RECURSOS DE TELEINFORMÁTICA, POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA	Alta
Capítulo 2.1	Gestión de contraseñas y autenticación	3	POLÍTICA DE CONTRASEÑAS SEGURAS	Alta
Capítulo 2.2	Manejo seguro del correo electrónico y navegación	3	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Alta
Capítulo 2.3	Protección de la información en dispositivos y red	1, 2 y 3	POLÍTICA DE USO DE ACTIVOS Y RECURSOS DE TELEINFORMÁTICA, USO DE VPN EN INFOTRACK	Media
Capítulo 2.4	Uso correcto de repositorios institucionales	2	POLÍTICA DE RESPALDO DE INFORMACIÓN DE INFOTRACK, POLÍTICA DE USO DE ACTIVOS Y RECURSOS DE TELEINFORMÁTICA	Alta
Capítulo 2.5	Escritorio y pantalla limpia	1	POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA	Media
Capítulo 3	Manejo de incidentes y reporte	3 y 4	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, GUÍA BÁSICA DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Alta
Capítulo 3.1	Reconocer un incidente y pasos iniciales	3 y 4	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, GUÍA BÁSICA DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Alta
Capítulo 4	Principios del tratamiento de datos personales	1, 2 y 4	Política de tratamiento de datos personales, Tratamiento de Datos Personales	Alta
Capítulo 4.1	Políticas y normativas internas	1 y 2	POLÍTICA DE USO DE ACTIVOS Y RECURSOS DE TELEINFORMÁTICA, Política de Firewall, POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA	Alta
Capítulo 4.2	Tratamiento de datos personales	4	Política de tratamiento de datos personales, Tratamiento de Datos Personales	Alta

Nota. Fuente: Los autores

Identificar la Audiencia del Plan de Concientización

De acuerdo con la NIST SP 800-50r1, la identificación de audiencias debe basarse en la función, el nivel de exposición al riesgo y el acceso a activos de información, de modo que los mensajes y refuerzos sean relevantes y accionables para cada grupo ([NIST], 2024). Además, las evidencias internas —informes de phishing, auditorías y la evaluación de protección de datos— permiten priorizar segmentos concretos según el riesgo observado en la “mediana empresa de tecnología” (“Empresa Consultora en seguridad”, 2024; “empresa auditora”, 2024; “mediana empresa de tecnología”, 2024).

Para este PCSI se definen dos segmentos de audiencia, seleccionados según función, nivel de exposición y acceso a información, de modo que las necesidades detectadas se traduzcan en intervenciones pertinentes para cerrar las brechas identificadas durante el análisis del programa ([NIST], 2024).

Usuarios Generales. comprende al grupo de colaboradores que realiza tareas cotidianas con herramientas corporativas. Las comunicaciones para este grupo deben priorizar mensajes claros, prácticos y de alta frecuencia, microcontenidos en Teams y cartelería digital, que promuevan comportamientos verificables (NIST SP 800-50r1, 2024).

Usuarios Específicos. incluye a quienes, por sus funciones o nivel de acceso, requieren mensajes más concretos. Para este segmento se diseñan intervenciones con mayor nivel de detalle, casos prácticos, guías rápidas y refuerzos vinculados a procedimientos internos, y se documenta la evidencia de cumplimiento y comprensión para mitigar brechas detectadas en la evaluación de protección de datos y en auditorías previas ([NIST], 2024).

Usuarios Generales. ***Audiencia 1 — Usuarios Operativos y Administrativos. Quiénes.*** Colaboradores de Comercial & Mercadeo, Operaciones & Servicios y áreas administrativas que usan herramientas corporativas en tareas diarias.

Riesgos. Apertura y clic en correos phishing, uso de repositorios no oficiales y prácticas de escritorio y pantalla no conformes (“Empresa Consultora en seguridad” S.A., 2024; “empresa auditora”, 2024).

Material. mensajes breves y repetidos que promuevan comportamientos concretos — por ejemplo, identificar señales de phishing, usar repositorios autorizados y aplicar medidas básicas de higiene de puesto— entregados por canales de alta frecuencia (LMS microcontenidos, nudges por Teams, cartelería digital) (NIST, 2024; “mediana empresa de tecnología”, 2024).

Usuarios Específicos. ***Audiencia 2 — Personas con Responsabilidades Sobre Datos Sensibles. Quiénes.*** colaboradores que manejan datos personales o información confidencial (procesos identificados en políticas de tratamiento de datos y gestión documental).

Riesgos. brechas en comprensión de sanciones, rol de responsables y principio de responsabilidad demostrada según la evaluación interna de protección de datos (“mediana empresa de tecnología”, 2024).

Material. comunicaciones focalizadas que aclaren obligaciones básicas, rutas de reporte interno y ejemplos prácticos de manejo seguro, con evidencia documentada en repositorios corporativos y recordatorios periódicos (NIST, 2024; “mediana empresa de tecnología”, 2024).

Audiencia 3 — Personal técnico e Infraestructura (CISO / TI). Quiénes. equipo de Infraestructura Tecnológica, responsables de operaciones de red, administración de acceso, respaldos y respuesta a incidentes.

Riesgos. puntos de interacción humana en gestión de parches, configuración y respuesta ante incidentes que requieren coordinación con acciones formativas y operativas

(“mediana empresa de tecnología”, 2024, Gestión de vulnerabilidades técnicas; Gestión de incidentes de seguridad de la información).

Material. piezas de comunicación técnica de alto nivel (resúmenes ejecutables, listas de verificación operativas y alertas situacionales) que faciliten decisiones rápidas y coherencia con controles técnicos; seguir canales formales de coordinación entre TI y T&D para asegurar trazabilidad (NIST, 2024; “mediana empresa de tecnología”, s. f., Gestión de vulnerabilidades técnicas; Gestión de incidentes de seguridad de la información).

Audiencia 4 — Mandos Medios, Dirección y Proveedores Críticos. Quiénes. directores y jefaturas (quienes aprueban recursos y políticas) y proveedores/contratistas con acceso a activos críticos.

Riesgos. decisiones que pueden generar excepciones operativas y brechas en la cadena de suministro; necesidad de evidencia contractual sobre cumplimiento de obligaciones (“mediana empresa de tecnología”, Acuerdo de Confidencialidad proveedores).

Material. mensajes estratégicos y resúmenes de indicadores clave (KPIs/KRIs) que permitan seguimiento, priorización y firma de compromisos contractuales; comunicaciones puntuales para terceros con evidencia de cumplimiento (NIST, 2024, NIST SP 800-50r1, secc. 2.2–3.2; “mediana empresa de tecnología”, s. f., Acuerdo de Confidencialidad proveedores).

Tabla 6

Síntesis de audiencias

Audiencia	Descripción	Riesgos	Material	Prioridad
Usuarios operativos y administrativos	Colaboradores de Comercial & Mercadeo, Operaciones & Servicios y áreas administrativas que usan herramientas corporativas en tareas diarias.	Apertura y clic en correos phishing, uso de repositorios no oficiales y prácticas de escritorio y pantalla no conformes.	Mensajes breves y repetidos que promuevan comportamientos concretos —por ejemplo, identificar señales de phishing, usar repositorios autorizados y aplicar medidas básicas de higiene de puesto— entregados por canales de alta frecuencia.	Alta
Personas con responsabilidades sobre datos sensibles	Colaboradores que manejan datos personales o información confidencial (procesos identificados en políticas de tratamiento de datos y gestión documental).	Brechas en comprensión de sanciones, rol de responsables y principio de responsabilidad demostrada.	Comunicaciones focalizadas que aclaren obligaciones básicas, rutas de reporte interno y ejemplos prácticos de manejo seguro, con evidencia documentada en repositorios corporativos y recordatorios periódicos.	Alta
Personal técnico e Infraestructura (CISO / TI)	Equipo de Infraestructura Tecnológica, responsables de administración de acceso, respaldos y respuesta a incidentes.	Puntos de interacción humana en gestión de parches, configuración y respuesta ante incidentes.	Piezas de comunicación técnica de alto nivel (resúmenes ejecutables, listas de verificación operativas y alertas situacionales) que faciliten decisiones rápidas y coherencia con controles técnicos; seguir canales formales de coordinación entre TI y T&D para asegurar trazabilidad.	Media
Mandos medios, dirección y proveedores críticos	Directores y jefaturas (quienes aprueban recursos y políticas) y proveedores/contratistas con acceso a activos críticos.	Decisiones que pueden generar excepciones; necesidad de evidencia sobre cumplimiento de obligaciones.	Mensajes estratégicos y resúmenes de indicadores clave (KPIs/KRIs) que permitan seguimiento, priorización y firma de compromisos contractuales; comunicaciones puntuales para terceros con evidencia de cumplimiento.	Media

Nota. Fuente: Los autores

Diseñar

Documento de Diseño para el Curso Implementado en el LMS

Propósito del Curso. Este documento de diseño define, de manera estructurada y trazable, los lineamientos pedagógicos, técnicos y operativos para el desarrollo, implementación y evaluación del curso de Concientización Básica en Seguridad de la Información dentro del Plan de Concientización en Seguridad de la Información (PCSI) de la “mediana empresa de tecnología”, en el entorno del LMS “Proporcionado por la ARL”.

Objetivos del Curso. Fortalecer las competencias básicas de seguridad de la información y protección de datos personales de todos los colaboradores de la “mediana empresa de tecnología”, de modo que comprendan su rol en la protección de los activos de información y apliquen prácticas seguras en su trabajo diario, en coherencia con el PCSI y el SGSI basado en ISO/IEC 27001:2022 (ISO, 2022a; ISO, 2022b).

Concientización Básica en Seguridad Informática. Reconocer los conceptos fundamentales de la seguridad de la información, los tipos de amenazas más frecuentes y su impacto en los activos de la “mediana empresa de tecnología”, para fortalecer la primera capa de protección en el marco del PCSI.

Aplicar Buenas Prácticas y Controles Básicos Para Prevenir Incidentes de Seguridad de la Información en el Trabajo Diario. Implementar en las labores cotidianas prácticas seguras de contraseñas, correo electrónico, navegación, uso de dispositivos y reporte de incidentes, reduciendo la probabilidad y el impacto de eventos que afecten la confidencialidad, integridad y disponibilidad de la información.

Fomentar una Cultura de Seguridad Continua y Cumplimiento Normativo en la Organización. Interiorizar las políticas internas de seguridad de la información y las responsabilidades individuales, promoviendo comportamientos seguros y sostenidos que apoyen el cumplimiento del PCSI y del SGSI basado en ISO/IEC 27001 e ISO/IEC 27002.

Comprender y Aplicar los Principios del Tratamiento de Datos Personales Conforme a la Política Interna y la Normativa Vigente. Identificar los principios y obligaciones asociados al tratamiento de datos personales y aplicarlos correctamente en las actividades diarias, asegurando el cumplimiento de la política interna de protección de datos y de la legislación aplicable.

Antecedentes del *Curso.* La “mediana empresa de tecnología” cuenta con un conjunto de capacitaciones internas en video, grabadas desde Microsoft Teams, sobre manejo de OneDrive y SharePoint, tratamiento de datos personales y presentaciones asociadas, las cuales se han utilizado como base conceptual y contextual para estructurar los contenidos del presente curso de concientización básica en seguridad de la información, alineado con el PCSI (ISO, 2022b).

Adicionalmente, las políticas internas de seguridad de la información y uso de activos (incluyendo políticas de contraseñas, escritorio limpio y uso de recursos de TI) se emplean como insumos normativos para el diseño de los módulos y actividades del curso, garantizando la coherencia entre la formación y el SGSI de La “mediana empresa de tecnología” (ISO, 2022a; ISO, 2022b).

En la plataforma Microsoft Forms se dispone de una evaluación previa del curso de datos personales, cuyos resultados, estructura y reactivos sirven de referencia para el diseño de las evaluaciones del presente curso en el LMS Proporcionado por la ARL, buscando mejorar la medición de competencias y la trazabilidad del desempeño de los participantes (NIST, 2024, cap. 3.2.5).

Público Objetivo. El curso está dirigido a todo el personal de la “mediana empresa de tecnología” que participa en el tratamiento, uso o administración de información y datos personales en el marco del PCSI, incluyendo colaboradores de áreas administrativas, operativas, comerciales y de soporte. Se orienta especialmente a usuarios finales que utilizan de forma regular servicios como OneDrive, SharePoint, correo corporativo y aplicaciones de negocio, independientemente de su nivel de conocimiento previo en seguridad de la información.

Esquema del Curso. El curso de Concientización Básica en Seguridad de la Información se estructurará en cuatro unidades temáticas principales, diseñadas para ser implementadas en el LMS Proporcionado por la ARL ((Véase en el Anexo D un resume detallado para la implementación del PCSI).). Cada unidad integrará recursos didácticos variados, incluyendo videos explicativos, presentaciones, preguntas de autoevaluación y exámenes finales, con el fin de reforzar los objetivos de aprendizaje definidos para el PCSI.

La primera unidad abordará los conceptos fundamentales de la seguridad informática y las amenazas comunes. La segunda se centrará en la aplicación de buenas prácticas y controles básicos para la prevención de incidentes en el trabajo diario. La tercera unidad buscará fomentar una cultura de seguridad continua y el cumplimiento normativo dentro de la organización. Finalmente, la cuarta unidad se dedicará a la comprensión y aplicación de los principios del tratamiento de datos personales, conforme a la política interna y la normativa vigente.

Para el desarrollo de estos contenidos, se aprovecharán materiales existentes como grabaciones de capacitaciones internas sobre OneDrive, SharePoint y datos personales, así como las políticas de seguridad de la información de la “mediana empresa de tecnología”. Además, se integrarán videos disponibles en herramientas de video externas que ayuden a clarificar temas de los que no hay información en la “mediana empresa de tecnología”, estos recursos deben ser libres y de duración reducida para no ser monótonos al público. Los

recursos se adaptarán para su integración en el LMS, siguiendo las directrices de configuración de elementos de contenido y evaluación.

Estrategia de Instrucción*.* Cada objetivo del curso se implementará como un capítulo en el LMS Proporcionado por la ARL, compuesto por una o más unidades temáticas según la complejidad del contenido, sin número especifico de unidades, de modo que cada tema quede claramente explicado y alineado con los objetivos del PCSI (NIST, 2024).

Cada unidad iniciará con una pregunta detonante no evaluable que introduzca el tema y genere reflexión en el colaborador; posteriormente se presentará un video interno de La "mediana empresa de tecnología" o externo de una entidad especializada en seguridad de la información o ciberseguridad que explique el contenido central de la unidad, seguido de dos preguntas no evaluables que permitan al participante verificar su comprensión inmediata del material visto.

A continuación, se incluirá una presentación que sintetice y amplíe los conceptos clave de la unidad, reforzando lo expuesto en el video; finalmente, se aplicará un examen final evaluable por unidad, configurado como elemento autocalificable en el LMS, que el colaborador deberá aprobar con una calificación mínima del 80 % para poder avanzar a la siguiente unidad o capítulo, en coherencia con los criterios de competencia definidos para el SGSI (NIST, 2024; Ayuda LMS Proporcionado por la ARL; ISO, 2022a).

Medio de Entrega. El curso de Concientización Básica en Seguridad de la Información se impartirá en modalidad 100 % virtual, de forma asincrónica, a través del LMS Proporcionado por la ARL, lo que permite que los colaboradores de la "mediana empresa de tecnología" accedan a los contenidos en cualquier momento y lugar, utilizando sus credenciales corporativas y los dispositivos autorizados por la organización (NIST, 2024; ISO, 2022b).

La estructura del curso en el LMS seguirá el flujo de creación definido en la plataforma: información básica del curso, registro de objetivos, diseño por capítulos y unidades, configuración de elementos de contenido (videos, presentaciones, lecturas) y elementos

autocalificables (exámenes finales), así como los criterios de aprobación y visibilidad, de acuerdo con las pautas descritas en el Anexo A, Ayuda LMS proporcionado por la ARL.

Esta modalidad virtual facilita la estandarización del mensaje de seguridad de la información en toda la organización, permite la trazabilidad del progreso de cada colaborador y habilita el uso de indicadores de participación, avance y aprobación del curso, integrando la formación en el PCSI y en los procesos del Sistema de Gestión de Seguridad de la Información de la “mediana empresa de tecnología” (NIST, 2024; ISO, 2022a).

Evaluación. En cada unidad del curso se implementará un examen final autocalificable, compuesto por preguntas de selección múltiple u otros formatos objetivos disponibles en el LMS Proporcionado por la ARL, configurado con una calificación mínima de aprobación del 80 % como requisito para avanzar a la siguiente unidad o capítulo, asegurando un nivel homogéneo de competencia básica en seguridad de la información.

Adicionalmente, se utilizarán preguntas no evaluables de diagnóstico y reforzamiento al inicio y después de los videos, con el fin de orientar la reflexión del colaborador y monitorear, de manera cualitativa, la comprensión del contenido, aunque sin impacto directo en la nota final del curso (NIST, 2024; Anexo A, Ayuda LMS proporcionado por la ARL).

Para medir la efectividad del curso en el marco del PCSI, se registrarán y analizarán métricas tales como: porcentaje de colaboradores inscritos y que completan el curso, tasas de aprobación por unidad y por cohorte, número de intentos por evaluación y tiempo promedio de finalización, datos que se integrarán a los indicadores del PCSI para retroalimentar la mejora continua del programa de capacitación (NIST, 2024; ISO, 2022a; ISO, 2015).

Firma y Aceptación de las Partes Interesadas. Con la firma de este apartado, las partes interesadas confirman que han revisado el presente documento de diseño del curso “Concientización Básica en Seguridad de la Información” en el marco del PCSI de la “mediana empresa de tecnología”, y que aprueban su propósito, objetivos, público objetivo, estrategia de instrucción, medio de entrega, evaluaciones y métricas definidas, comprometiéndose a apoyar su implementación, seguimiento y mejora continua dentro del SGSI y del Sistema de Gestión de la Calidad.

1. Líder de Infraestructura Tecnológica (TI)

Nombre: _____

Cargo: _____

Firma: _____ Fecha: ___ / ___ / _____

2. Líder de Transformación y Desarrollo

Nombre: _____

Cargo: _____

Firma: _____ Fecha: ___ / ___ / _____

3. Jefe comercial o área de Mercadeo

Nombre: _____

Cargo: _____

Firma: _____ Fecha: ___ / ___ / _____

Instrucciones de *Configuración* en el LMS Proporcionado por la ARL. Las siguientes instrucciones describen, de manera general, cómo configurar el curso de Concientización Básica en Seguridad de la Información en el LMS Proporcionado por la ARL, siguiendo el flujo de la plataforma y el diseño definido para el PCSI (Anexo E, secciones 1–5; NIST, 2024).

Información Básica del Curso. Ingresar al LMS Proporcionado por la ARL, desplegar el menú de cursos y seleccionar “Crear curso”. En la sección de información básica, digita el título acordado del curso, una descripción breve que resuma propósito y beneficios, selecciona modalidad “Virtual”, tipo “Curso”, nivel “Básico” y la categoría relacionada con “Seguridad de la información”. Definir los pres-requisitos solo si se requieren conocimientos mínimos de informática y guarda los cambios para continuar (Anexo A, secciones 1.1 y 1.4).

Imágenes, Profesor, Colaboradores y Bibliografía. Cargar el encabezado panorámico y la imagen destacada del curso, cuidando que representen la temática de seguridad de la información. Asignar un profesor responsable y, si aplica, colaboradores que apoyarán la administración o actualización del contenido. En la sección de bibliografía registrar las principales fuentes utilizadas, incluyendo políticas internas de la “mediana empresa de tecnología”, y luego clic en guardar y avanzar (Anexo A, secciones 1.2 y 1.4; ISO, 2022a; ISO, 2022b).

Registro de Objetivos del Curso. En el paso de objetivos, copiar el objetivo general y los objetivos específicos definidos en el documento de diseño, registrándolos en los campos correspondientes del LMS. Asegurar que cada objetivo específico quede claramente formulado y asociado a los resultados de aprendizaje esperados. Utilizar la vista de relación entre objetivos y unidades para confirmar que luego sea posible vincular las unidades de cada capítulo a su objetivo correspondiente (Anexo A, secciones 2.1–2.3; NIST, 2024,).

Creación de Capítulos y Unidades. En la sección de diseño del curso, crear un capítulo por cada objetivo del curso y, dentro de cada capítulo, añadir las unidades temáticas necesarias para cubrir el contenido. Para cada unidad, registrar un título claro y una breve descripción, y luego utiliza la opción “Añadir elemento” para incorporar, en este orden genérico, una pregunta inicial no evaluable, un video explicativo, dos preguntas no evaluables de verificación, una presentación de refuerzo y un examen final autocalificable. Repitir esta estructura de manera consistente para todos los capítulos y unidades del curso, ajustando únicamente los contenidos específicos de cada tema (Anexo A, secciones 3.1–3.3 y 3.6; NIST, 2024).

Configuración de Exámenes y Criterios de Aprobación. Al crear los exámenes de cada unidad, seleccionar los tipos de preguntas autocalificables disponibles (por ejemplo, selección múltiple, verdadero/falso o numéricas) y configura el porcentaje mínimo de aprobación del 80 % para considerar superada la unidad. Verificar que el LMS impida avanzar a la unidad siguiente si no se cumple este umbral y, en el paso de publicación, definir también el porcentaje mínimo global de aprobación del curso, el certificado de finalización y la visualización del curso como “privado” y “gratuito” para el personal de La “mediana empresa de tecnología” (Anexo A, secciones 3.6, 3.7 y 5.1–5.5; NIST, 2024; ISO, 2022a).

Para ver el instructivo creado por los autores a partir de la ayuda que ofrece el LMS Proporcionado por la ARL, puede acceder al anexo A, Ayuda LMS Proporcionado por la ARL; en el cual podrá acceder a la información paso a paso para la creación de cualquier curso dentro de la herramienta.

Prototipo del curso en el LMS. ***Introducción al Prototipo.*** La implementación del prototipo del curso de Concientización Básica en Seguridad de la Información se realizó en el LMS “Proporcionado por la ARL”, una plataforma web a la que la “mediana empresa de tecnología” accede como valor agregado de su contrato de aseguramiento de riesgos laborales con la ARL. Esta plataforma permite crear cursos virtuales, gestionar contenidos, registrar objetivos, estructurar capítulos y unidades, así como configurar evaluaciones autocalificables y criterios de aprobación, en línea con el diseño definido previamente para el PCSI (Autores del PCSI, 2025; NIST, 2024).

Tal como se describió en el “Documento de Diseño para el Curso Implementado en el LMS”, el Proporcionado por la ARL ofrece las funcionalidades necesarias para organizar, distribuir y evaluar el material del curso, así como para medir el avance y desempeño de cada colaborador mediante indicadores de participación, aprobación y tiempos de finalización (Autores del PCSI, 2025). De esta manera, la plataforma se convierte en el medio operativo para materializar los lineamientos pedagógicos, técnicos y de evaluación definidos en el diseño, en coherencia con las recomendaciones de la NIST SP 800-50r1 sobre el uso de herramientas que faciliten la trazabilidad y la medición del aprendizaje en programas de concientización (NIST, 2024).

Para la elaboración del prototipo que se presenta en este capítulo, se realizó el montaje completo del curso en el LMS, incluyendo la creación de los capítulos y unidades definidos en el diseño, la carga de videos de demostración, la configuración de preguntas inductivas no evaluables, la incorporación de presentaciones de contenido y la parametrización de las evaluaciones autocalificables con umbral mínimo de aprobación del 80 %. Cada uno de estos elementos responde directamente a las necesidades de concientización identificadas en la etapa de análisis del PCSI, donde se establecieron brechas en temas como escritorio y pantalla limpia, uso de repositorios oficiales, comportamiento ante correos maliciosos y tratamiento de datos personales (Autores del PCSI, 2025; NIST, 2024).

En consecuencia, el propósito de esta sección es mostrar cómo el prototipo implementado en el LMS Proporcionado por la ARL evidencia la coherencia entre el diseño instruccional documentado y su ejecución práctica, y ofrecer al lector una guía para interpretar las imágenes y configuraciones que se presentan como prueba de concepto del curso dentro del PCSI de la “mediana empresa de tecnología” (Autores del PCSI, 2025).

Guía de Lectura de las Capturas de Pantalla del Prototipo. Para facilitar la comprensión y el análisis de las capturas de pantalla que ilustran la implementación del prototipo del Plan de Concientización en Seguridad de la Información (PCSI) en el LMS proporcionado por la ARL, es importante tener en cuenta los siguientes aspectos. Estas directrices buscan orientar la interpretación de los elementos visuales, asegurando que se comprenda la correspondencia entre el diseño conceptual y su materialización en la plataforma (Autores del PCSI, 2025; NIST, 2024).

Contexto General de la Interfaz del LMS. Las imágenes presentadas corresponden a la interfaz de administración y visualización del curso dentro del LMS Proporcionado por la ARL. Aunque algunas capturas muestran la configuración interna (como la definición de objetivos o el diseño de unidades), otras reflejan la experiencia del usuario final. Es fundamental observar los menús laterales, las barras de progreso y los encabezados, ya que proporcionan información sobre la sección específica del curso que se está visualizando (Autores del PCSI, 2025).

Identificación de Elementos Clave. Cada captura de pantalla ha sido seleccionada para destacar un componente específico del diseño del PCSI. Se recomienda prestar atención a:

- **Títulos y Subtítulos:** Indican el nombre del curso, capítulos, unidades o elementos didácticos.
- **Iconografía:** El LMS utiliza íconos distintivos para representar diferentes tipos de contenido, como videos (icono de cámara de video), documentos (icono de documento),

preguntas (icono de casilla de verificación o signo de interrogación) y evaluaciones (icono de examen o balanza).

- **Barras de Progreso y Calificación:** En algunas imágenes, se observan indicadores de progreso o porcentajes de calificación, que reflejan el avance del usuario o el peso de una actividad dentro del curso.
- **Botones y Enlaces:** Elementos interactivos como "Continuar", "Comenzar examen" o "Descargar Archivo" señalan las acciones disponibles para el usuario.

Relación entre Diseño y Prototipo. El objetivo principal de estas imágenes es demostrar cómo los requisitos y la estructura definidos en el "Documento de Diseño para el Curso Implementado en el LMS" se han traducido fielmente en el prototipo funcional. Por ejemplo, la configuración de los objetivos específicos del curso (como se ve en la imagen "2 LMS Objetivos.jpg") se refleja en la estructura de los capítulos y unidades (como en la imagen "4 LMS Diseno curso.png" y "7 LMS Objetivo1.jpg"), donde cada objetivo se desglosa en contenidos y actividades específicas (Autores del PCSI, 2025).

Elementos Didácticos y de Evaluación. Las capturas de pantalla que muestran las unidades didácticas (imágenes "11 LMS Pregunta de inicio.JPG", "12 LMS Video capitulo.JPG", "13 LMS Pregunta refuerzo.JPG", "14 LMS Documento unidad.JPG" y "15 LMS Evaluación unidad.JPG") ilustran la variedad de recursos y actividades interactivas. Es importante notar cómo las preguntas de inicio y refuerzo, los videos explicativos, los documentos de apoyo y las evaluaciones finales de unidad se integran para reforzar el aprendizaje y medir la comprensión de los participantes, siguiendo las mejores prácticas en capacitación y sensibilización (NIST, 2024).

Al considerar estos puntos, se podrá apreciar con mayor claridad la funcionalidad y la alineación del prototipo con los objetivos del PCSI, así como la efectividad de la plataforma Proporcionado por la ARL como herramienta para la concientización en seguridad de la información en la “mediana empresa de tecnología”.

Correspondencia entre Elementos de Diseño y Ejecución en el Prototipo.

La tabla a continuación muestra la alineación de los elementos del prototipo con las necesidades de concientización identificadas en la etapa de análisis, y con los elementos definidos en el documento de diseño del curso implementado en el LMS.

Tabla 7

Alineación del prototipo con las necesidades de concientización y con los elementos del diseño del curso.

Elemento de Diseño	Descripción del Diseño	Implementación en el Prototipo	Evidencia Visual (Figura)
Información Básica del Curso	Definición de modalidad, título, descripción, nivel, profesor, colaboradores, área de conocimiento y palabras clave del curso.	Configuración completa de los metadatos del curso en la sección 'Información básica' del LMS, incluyendo encabezado, imagen destacada y descripción general.	figura 3 (Información básica del curso en la etapa de implementación)
Objetivos del Curso	Registro de un objetivo general y cuatro objetivos específicos alineados con las necesidades de concientización identificadas en la etapa de análisis del PCSI.	Creación de objetivos en la sección 'Objetivos' del LMS: un objetivo general y cuatro específicos que estructuran los capítulos del curso.	La figura 4 (Objetivos del curso en la etapa de implementación)
Diseño del Curso (Estructura Modular)	Organización del curso en capítulos y unidades didácticas, cada una con elementos específicos (preguntas, videos, documentos, evaluaciones) según el objetivo de aprendizaje.	Configuración de la estructura modular en la sección 'Diseño del curso', mostrando unidades, elementos autocalificables, videos, documentos y exámenes organizados por objetivo.	figura 5 (Diseño del curso en la etapa de implementación)
Marketing del Curso	Definición de imagen promocional y elementos visuales para atraer la atención de los colaboradores hacia el curso.	Carga de imagen promocional del curso (Ciberseguridad) en la sección 'Marketing del curso' del LMS.	figuras 6 (Marketing del curso en la etapa de implementación)
Publicación del Curso	Configuración de requisitos de certificación, puntaje de aprobación, visualización y comunidad de formación antes de habilitar el curso para los colaboradores.	Verificación de parámetros de publicación en la sección 'Publicar curso', incluyendo resumen general con número de unidades, secciones y duración estimada (7h 52m).	figuras 7 (Publicación del curso en la etapa de implementación)

Elemento de Diseño	Descripción del Diseño	Implementación en el Prototipo	Evidencia Visual (Figura)
Objetivo Específico 1: Conceptos Básicos de Seguridad de la Información	Reconocer los conceptos fundamentales de la seguridad de la información y su importancia en el entorno laboral.	Implementación del primer capítulo con unidades que incluyen preguntas inductivas, video conceptual, preguntas de refuerzo, documento de apoyo y examen final.	figura 8 (Implementación del Objetivo 1)
Objetivo Específico 2: Buenas Prácticas y Controles Básicos	Aplicar buenas prácticas y controles básicos para prevenir incidentes de seguridad de la información en el trabajo diario.	Implementación del segundo capítulo con múltiples unidades sobre gestión de contraseñas, autenticación, phishing, navegación segura, protección de dispositivos y manejo de incidentes.	figura 9 (Implementación del Objetivo 2)
Objetivo Específico 3: Cultura de Seguridad Continua	Fomentar una cultura de seguridad continua y cumplimiento normativo en la organización.	Implementación del tercer capítulo con unidades sobre políticas internas de seguridad, normatividad (ISO 27001, RTDP-IT-003, políticas de contraseñas, escritorio limpio) y campaña de concientización sobre ciberseguridad.	figura 10 (Implementación del Objetivo 3)
Objetivo Específico 4: Tratamiento de Datos Personales	Comprender y aplicar los principios de tratamiento de datos personales conforme a la política interna y la normativa vigente.	Implementación del cuarto capítulo con unidades sobre caracterización de datos personales, gestión de datos, evaluación de datos personales y examen final.	figura 11 (Implementación del Objetivo 4)
Preguntas Inductivas (No Evaluables)	Preguntas de inicio en cada unidad para activar conocimientos previos y contextualizar el tema, sin calificación.	Implementación de preguntas de selección múltiple con retroalimentación inmediata, marcadas como 'Autocalificable' pero sin peso en la nota final.	figura 12 (Pregunta de inicio por unidad)
Videos Explicativos	Inclusión de videos cortos (3-5 minutos) que expliquen conceptos clave de forma clara y accesible.	Integración de videos de YouTube embebidos en las unidades, con descripción contextual y controles de reproducción.	figura 13 (Video por unidad)
Preguntas de Refuerzo	Preguntas autocalificables intercaladas en las unidades para reforzar conceptos y verificar comprensión progresiva.	Implementación de preguntas de selección múltiple con retroalimentación correctiva inmediata y registro de intentos.	figura 14 (Pregunta refuerzo por unidad)

Elemento de Diseño	Descripción del Diseño	Implementación en el Prototipo	Evidencia Visual (Figura)
Documentos de Apoyo	Presentaciones en PowerPoint o documentos PDF descargables que complementan el contenido de cada unidad.	Carga de archivos descargables (presentaciones PowerPoint) con botón 'Descargar Archivo' visible en la interfaz del usuario.	figura 15 (Material de apoyo por unidad)
Evaluaciones Finales de Unidad/Capítulo	Exámenes finales por unidad o capítulo con calificación mínima de aprobación del 80%, intentos múltiples (máximo 3) y tiempo estimado de 10 minutos.	Configuración de exámenes finales con instrucciones claras, tiempo límite, número de preguntas, criterio de aprobación (80%) y botón 'Comenzar examen'.	figura 16 (Evaluación por unidad)

Nota. Fuente: Los autores

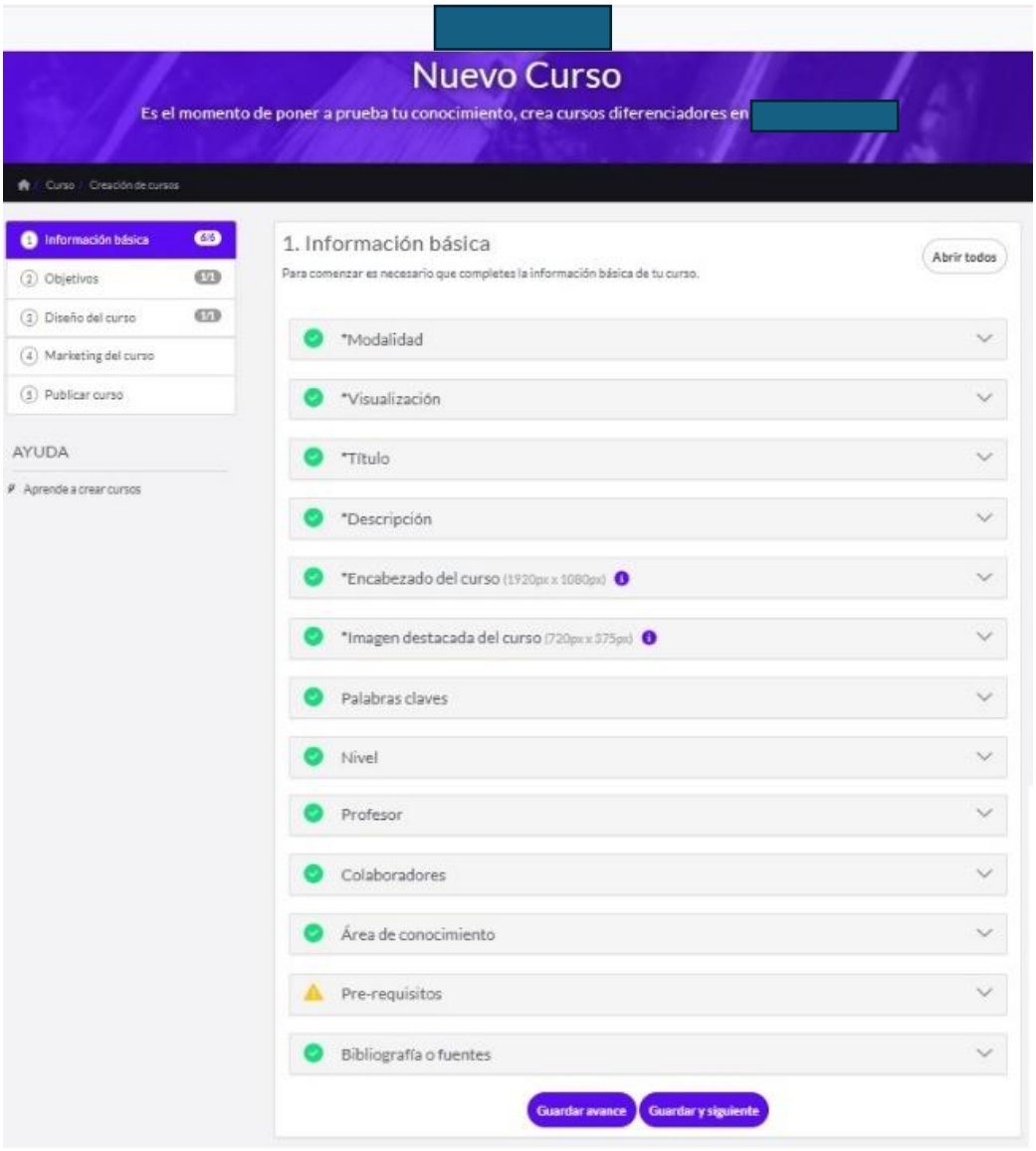
Presentación visual del prototipo implementado. En esta sección se presenta la evidencia gráfica del prototipo del curso “Concientización Básica en Seguridad Informática” implementado en el LMS proporcionado por la ARL, con el fin de mostrar cómo se materializan en la plataforma los elementos definidos en el diseño instruccional del PCSI para La “mediana empresa de tecnología” (Autores del PCSI).

En primer lugar, las figuras 3 a 7 corresponden al proceso de creación y configuración global del curso.

La figura 3 (*Información básica del curso en la etapa de implementación)* muestra la pantalla de Información básica, donde se parametrizan modalidad, título, descripción, nivel, profesor, prerequisitos y recursos bibliográficos, alineados con el documento de diseño del curso.

Figura 3

Información básica del curso en la etapa de implementación.

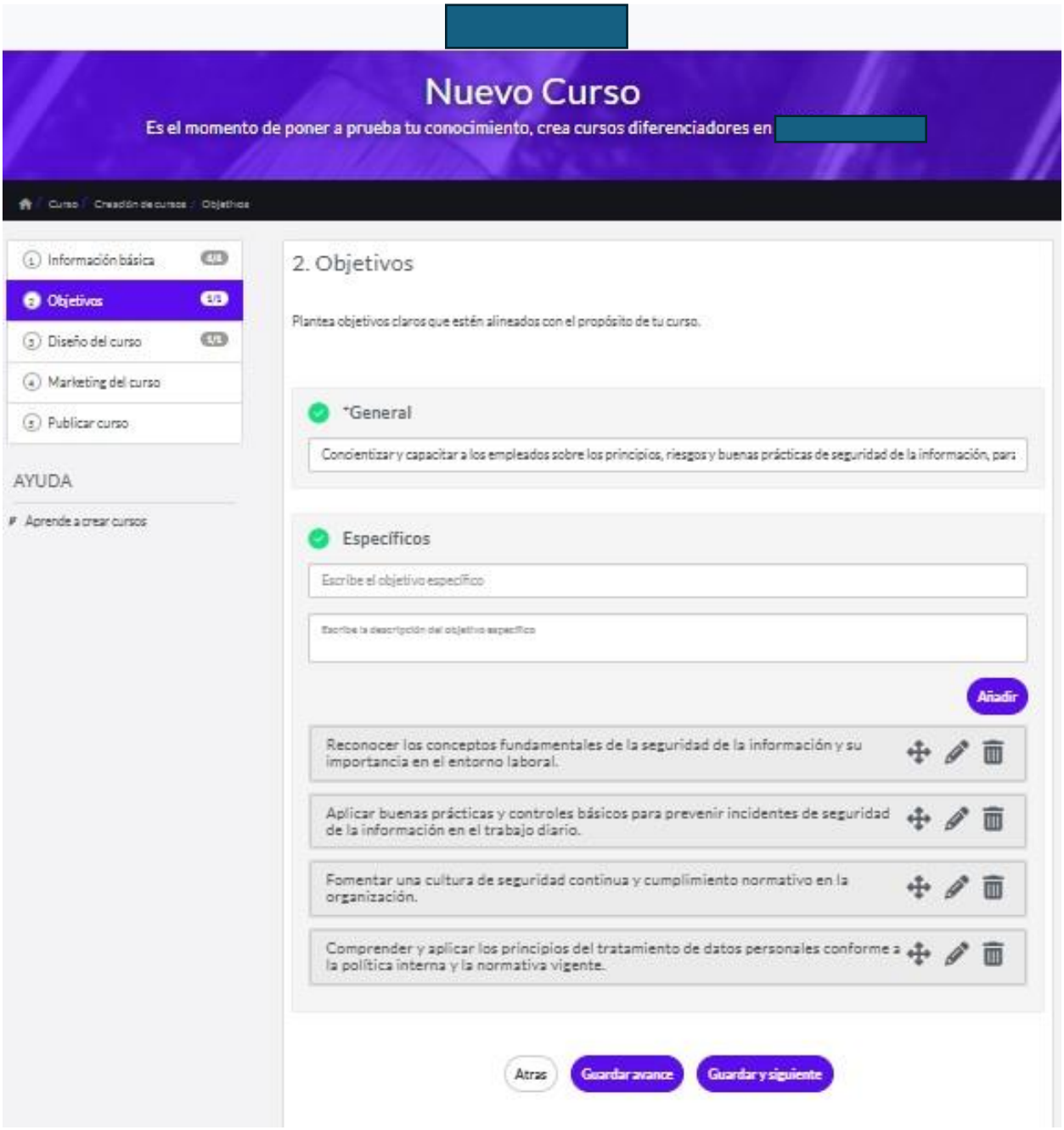


Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

La figura 4 (Objetivos del curso en la etapa de implementación) evidencia el registro del objetivo general y de los cuatro objetivos específicos que estructuran el PCSI, mientras que la figura 5 (Diseño del curso en la etapa de implementación*)* presenta la vista de Diseño del curso, en la que se organizan unidades y elementos didácticos por objetivo.

Figura 4

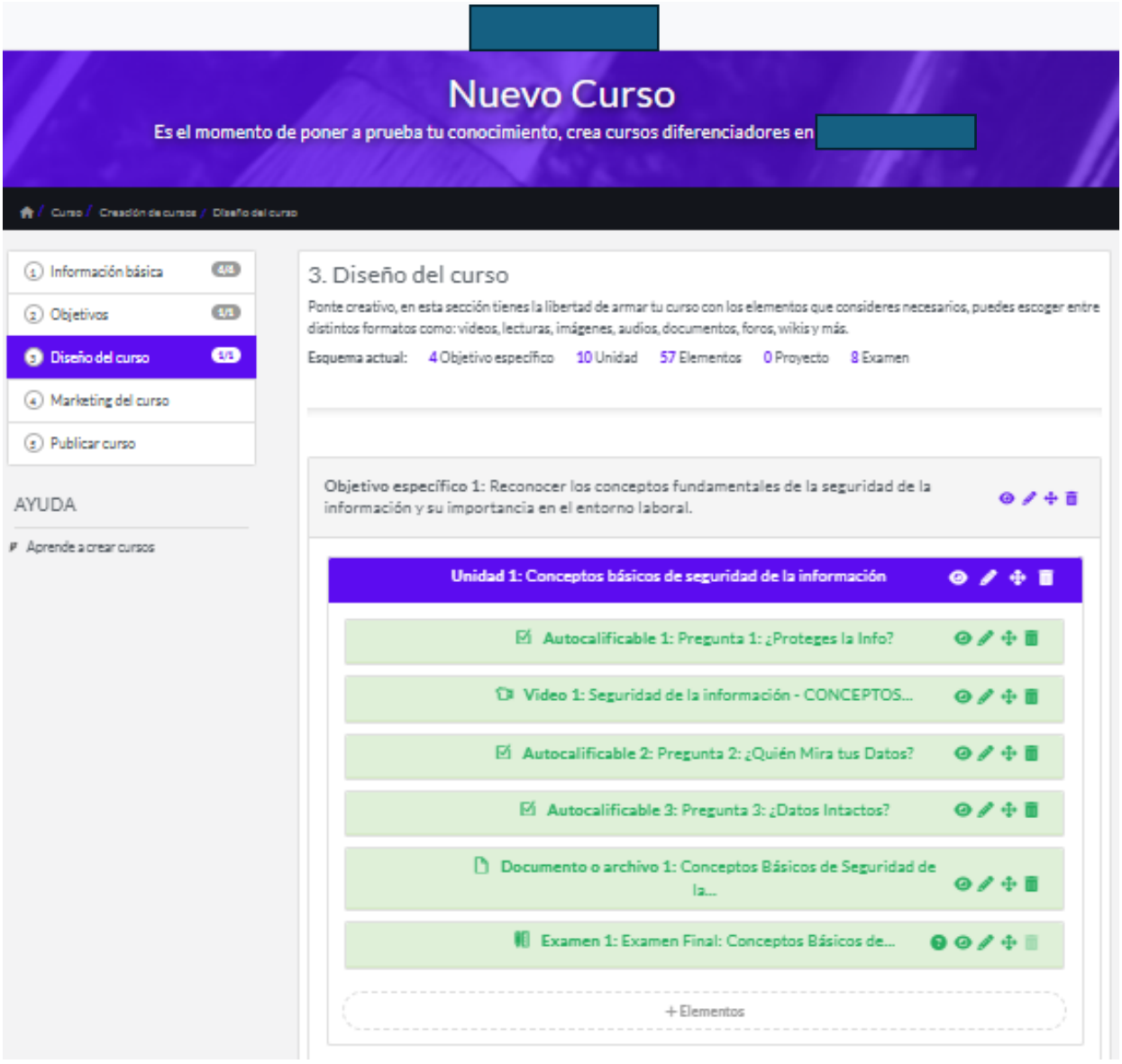
Objetivos del curso en la etapa de implementación



Nota: Adaptado de la web [captura de pantalla], LMS Proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

Figura 5

Diseño del curso en la etapa de implementación

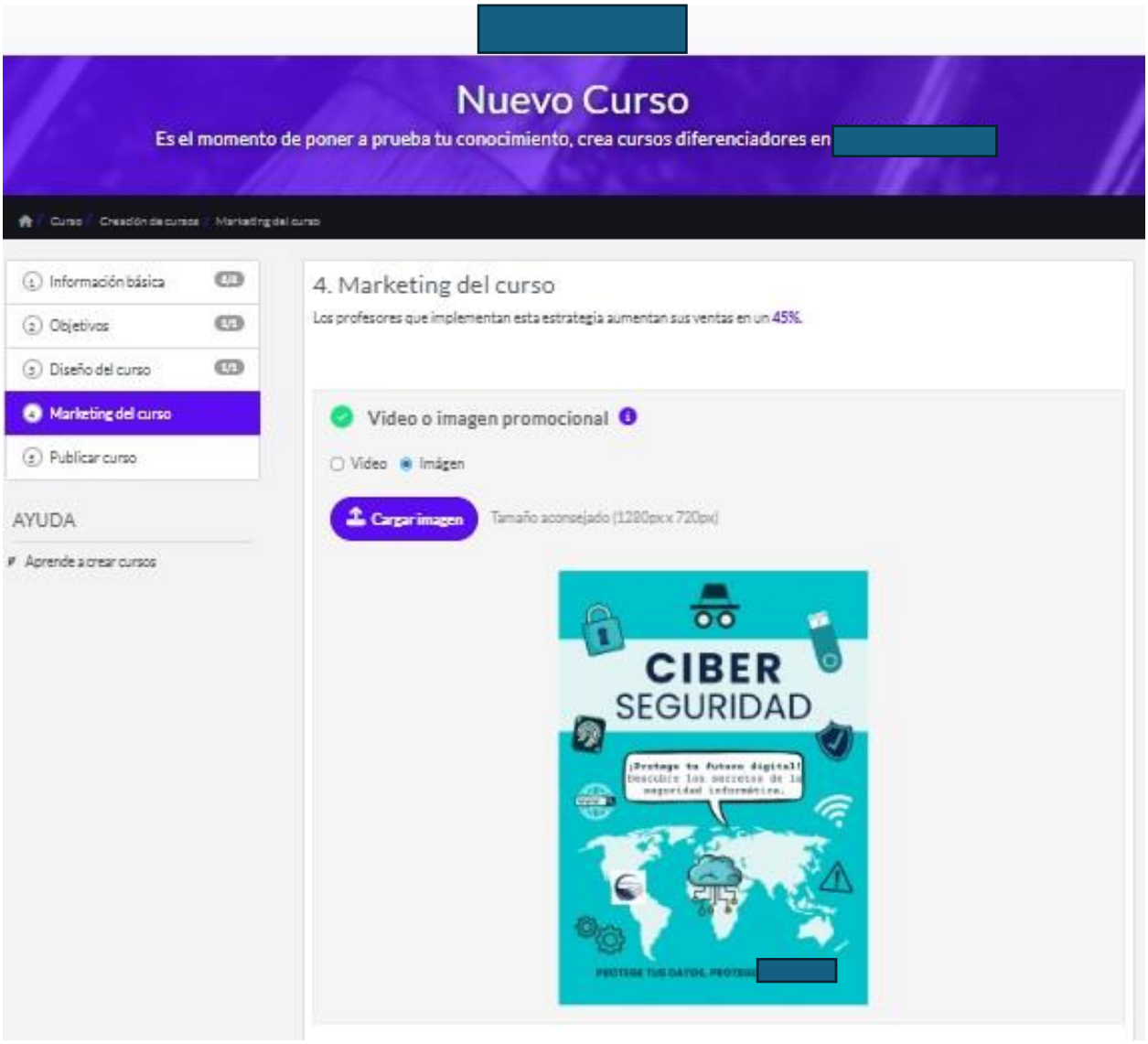


Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

Las figuras 6 y 7 (Marketing y Publicación del curso en la etapa de implementación) ilustran la configuración de la imagen promocional y los criterios de certificación y aprobación del curso, respectivamente.

Figura 6

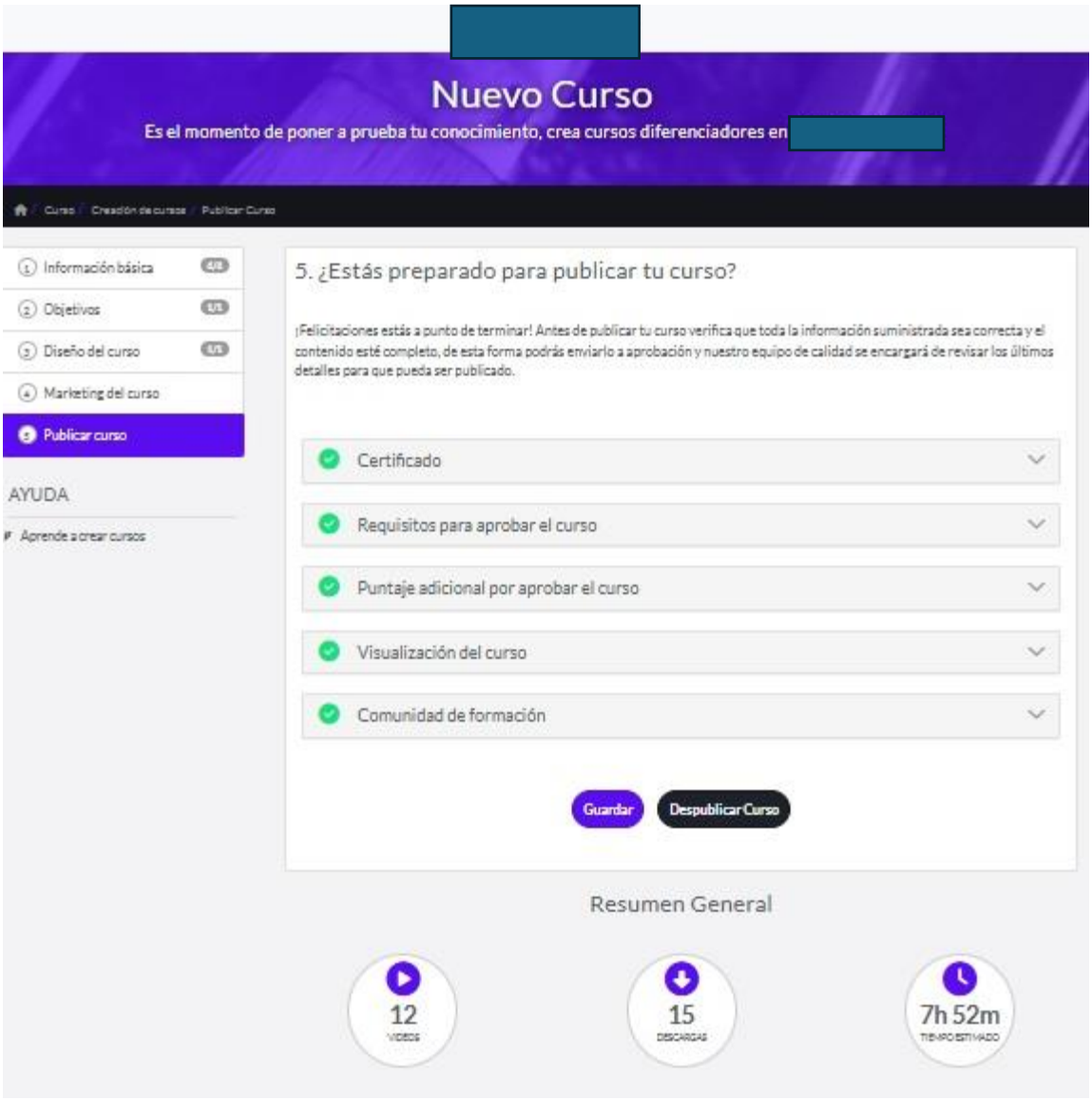
Marketing del curso en la etapa de implementación



Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

Figura 7

Publicación del curso en la etapa de implementación

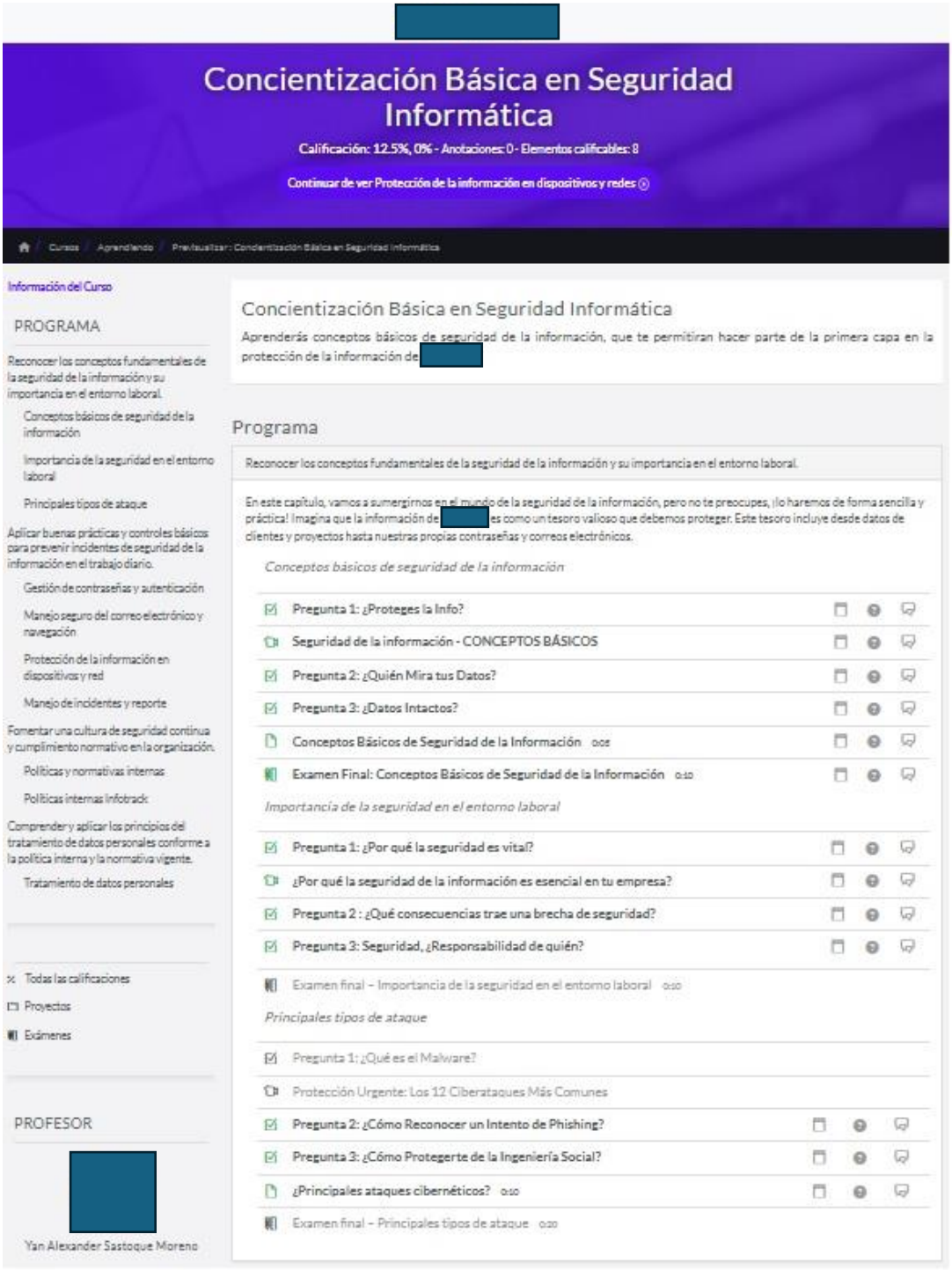


Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

Por último, la figura 8 (Implementación del Objetivo 1) muestra la vista del curso desde la perspectiva del participante, con el programa y el avance por elementos.

Figura 8

Implementación del Objetivo 1



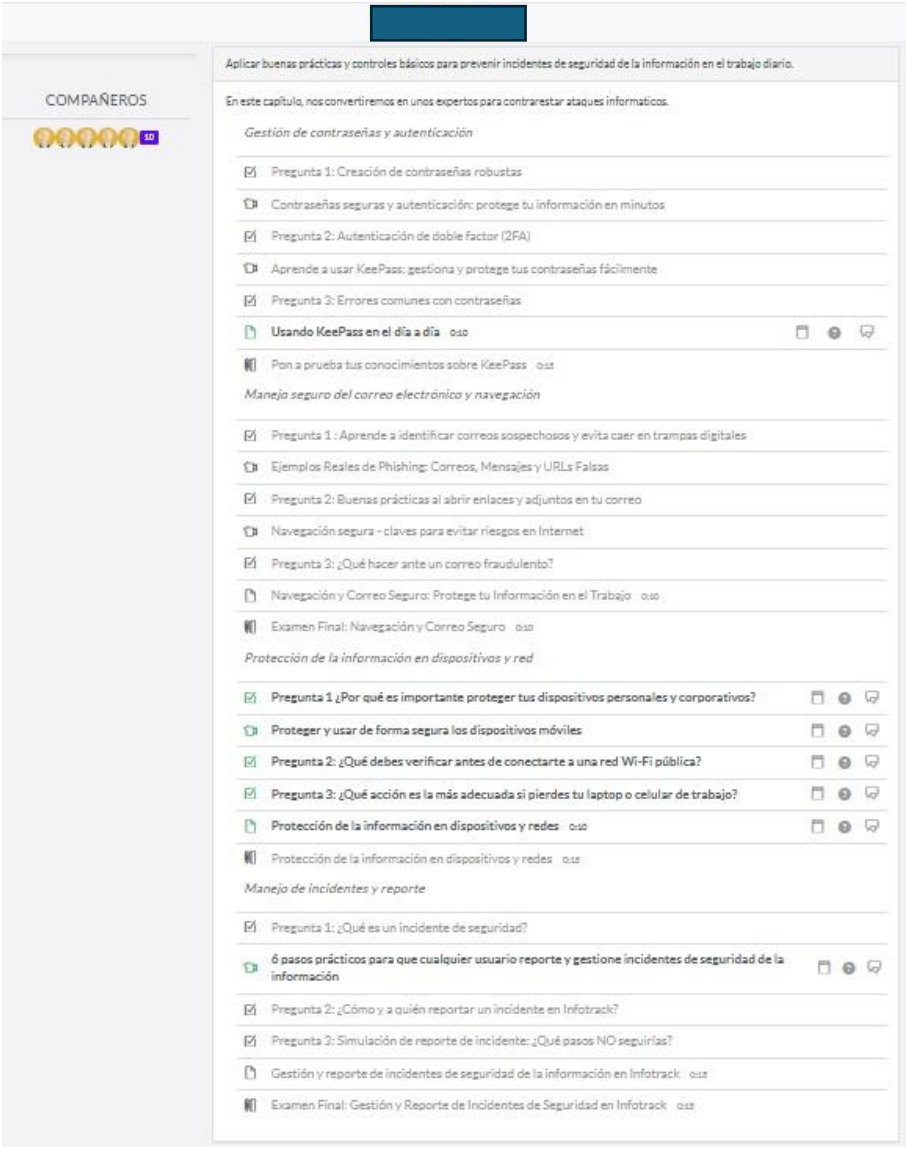
Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

En segundo lugar, las figuras 9 a 12 documentan cómo cada objetivo específico se implementa como capítulo dentro del LMS.

La figura 9 (Implementación del Objetivo 2) corresponde al capítulo de buenas prácticas y controles básicos,

Figura 9

Implementación del Objetivo 2

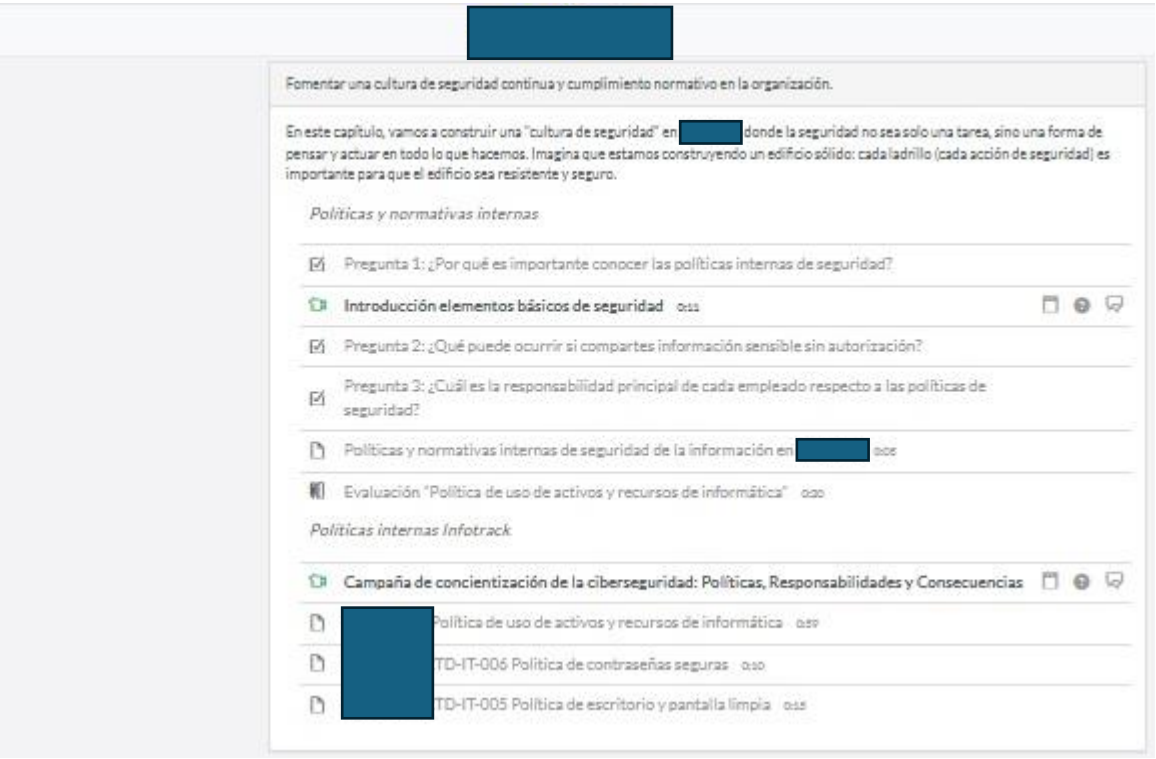


Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://lamediana empresa de tecnología".colegiosura.com/).

La figura 10 (Implementación del Objetivo 3) al capítulo de cultura de seguridad y normatividad interna,

Figura 10

Implementación del Objetivo 3

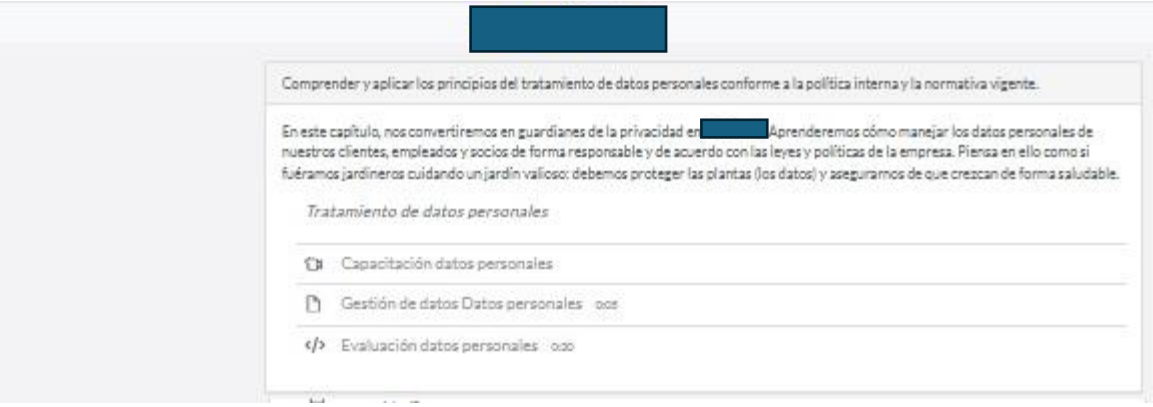


Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

y la figura 11 (Implementación del Objetivo 4) al capítulo de tratamiento de datos personales.

Figura 11

Implementación del Objetivo 4



Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

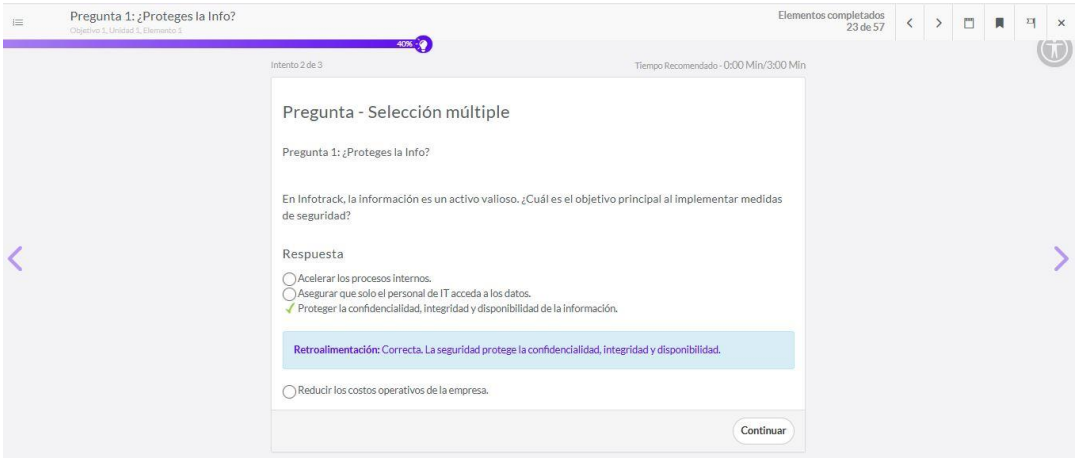
En todas se observa el desglose en unidades temáticas y actividades, lo que permite verificar la coherencia entre los objetivos definidos y la estructura del curso (Autores del PCSI, 2025).

Finalmente, las figuras 12 a 16 ilustran los elementos didácticos previstos para cada unidad.

La figura 12 (Pregunta de inicio por unidad) muestra una pregunta inductiva de selección múltiple con retroalimentación inmediata;

Figura 12

Pregunta de inicio por unidad

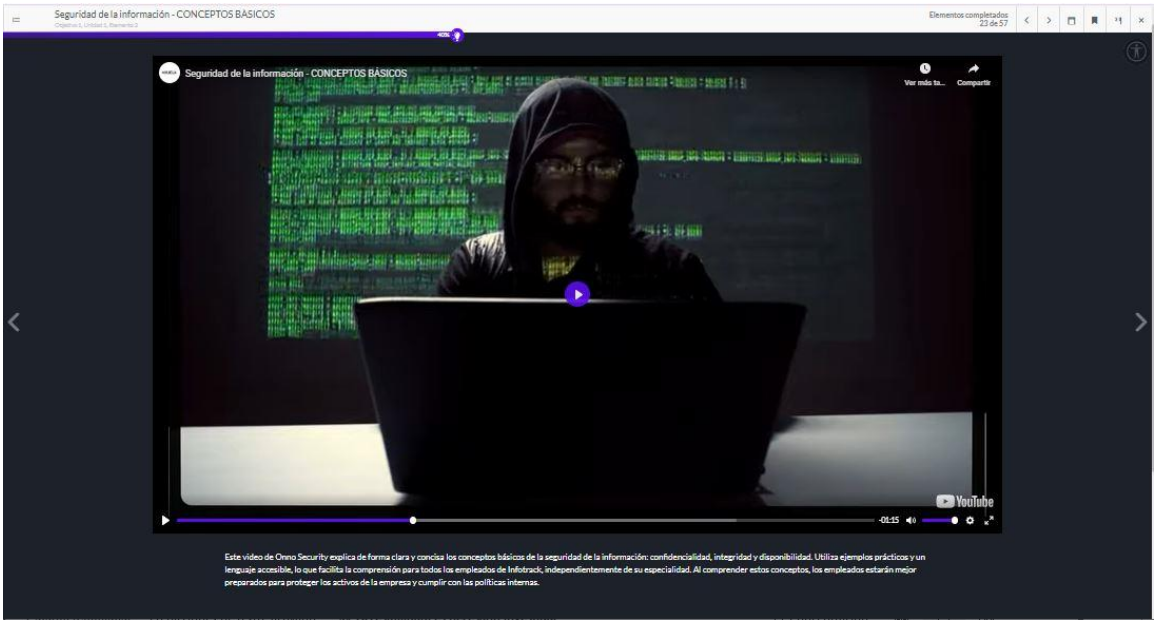


Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

la figura 13 (Video por unidad) presenta un video explicativo embebido desde YouTube;

Figura 13

Video por unidad

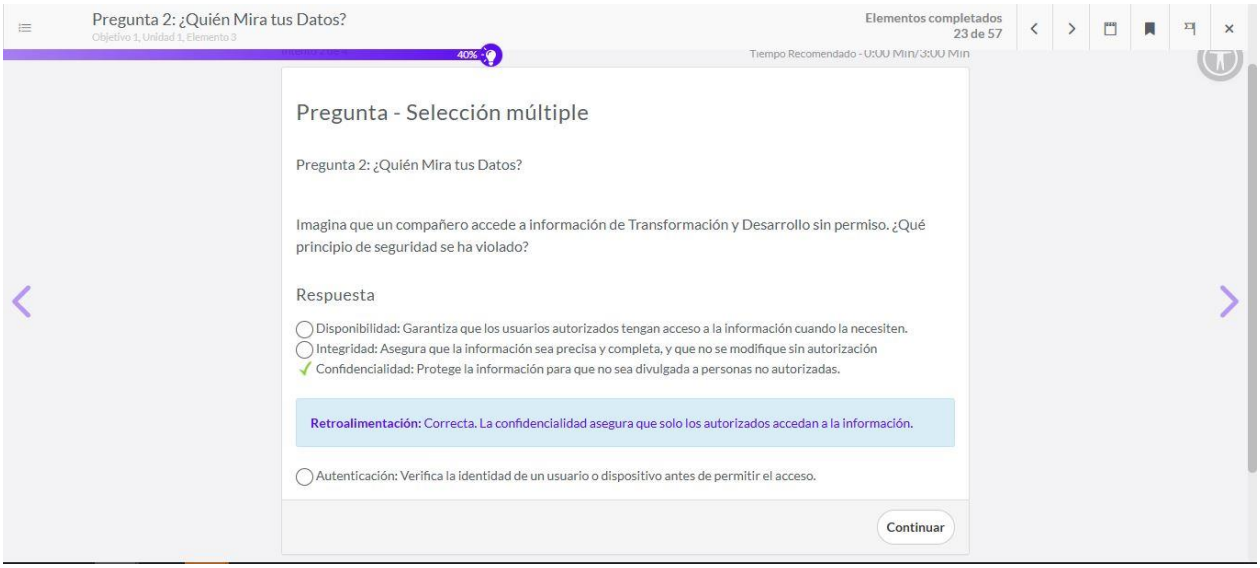


Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

la figura 14 (Pregunta refuerzo por unidad) evidencia una pregunta de refuerzo;

Figura 14

Pregunta refuerzo por unidad



Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

la figura 15 (Material de apoyo por unidad) muestra un documento de apoyo descargable en formato de presentación, el cual es descargable para el participante del curso;

Figura 15

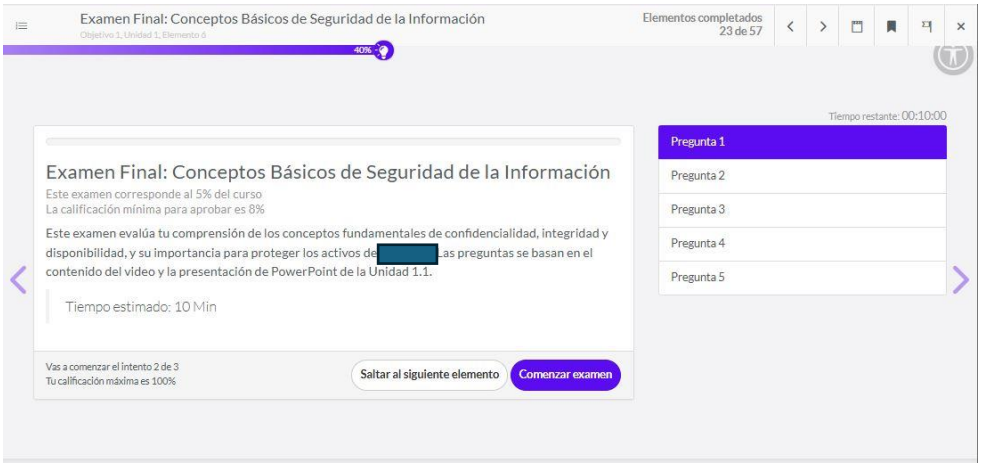
Material de apoyo por unidad

Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

y la figura 16 (Evaluación por unidad) exhibe la evaluación final de la unidad, con criterio de aprobación y tiempo estimado.

Figura 16

Evaluación por unidad



Nota: Adaptado de la web [captura de pantalla], LMS proporcionado por la ARL, 2025, (https://“mediana empresa de tecnología”.colegiosura.com/).

En conjunto, estas capturas permiten constatar que el prototipo cumple con los lineamientos de uso de contenidos múltiples, evaluación formativa y sumativa recomendados para plan de concientización en seguridad de la información (NIST, 2024).

Documento de Diseño para el Material de Refuerzo

Propósito del material. El material de la cartelera digital en formato de video breve tiene como propósito reforzar, de manera continua y visual, los mensajes clave del PCSI de la “mediana empresa de tecnología”, complementando el curso virtual principal de concientización básica en seguridad de la información y contribuyendo al logro de los objetivos del SGSI basado en ISO/IEC 27001:2022 (ISO, 2022a; ISO, 2022b).

Estos videos buscan mantener la seguridad de la información como un tema presente en la rutina diaria de las personas colaboradoras, facilitando el recuerdo de comportamientos seguros, el cumplimiento de políticas internas y el apoyo a la cultura organizacional y de calidad de la “mediana empresa de tecnología”.

Objetivos del *material. Objetivo del Video 1.* Buenas prácticas básicas de seguridad de la información Recordar a las personas colaboradoras las buenas prácticas y controles básicos de seguridad de la información (como manejo de contraseñas, bloqueo de pantalla, cuidado del correo y dispositivos), para que las apliquen de forma consistente en su trabajo diario y contribuyan a reducir incidentes habituales, en línea con los requisitos de concienciación y comportamiento seguro definidos por el SGSI (ISO, 2022a; ISO, 2022b).

Objetivo del Video 2. Cultura de seguridad y tratamiento adecuado de datos personales. Reforzar la cultura de seguridad continua y el cumplimiento normativo en la "mediana empresa de tecnología", enfatizando que cada persona es responsable de proteger datos personales y otra información sensible, aplicando los principios de tratamiento definidos en las políticas internas y en la regulación vigente, de acuerdo con las buenas prácticas de concientización establecidas en ISO/IEC 27001(ISO, 2022a).

Antecedentes del material. El material de la cartelera digital se apoya en el curso virtual principal de Concientización Básica en Seguridad de la Información del PCSI, previamente publicado en el LMS Proporcionado por la ARL.

Asimismo, los videos se fundamentan en las políticas, procedimientos y lineamientos internos de la "mediana empresa de tecnología", que soportan el SGSI alineado con ISO/IEC 27001:2022, garantizando coherencia entre los mensajes de cartelera, los cursos del LMS y los requisitos formales de la organización (ISO, 2015).

Público objetivo. El público objetivo principal de estos videos de cartelera digital son todas las personas colaboradoras de la "mediana empresa de tecnología", incluyendo personal administrativo, operativo y directivo, quienes transitan por áreas comunes, pasillos y salas de espera donde se proyectarán los contenidos (NIST, 2024).

Adicionalmente, estos videos pueden ser vistos por visitantes, proveedores y otras partes interesadas que se encuentren en las instalaciones de la "mediana empresa de

tecnología”, contribuyendo a una percepción general de la importancia que la organización otorga a la seguridad de la información y al tratamiento de datos personales (ISO, 2022a).

Esquema del *material.* Los videos de cartelera digital del PCSI de la “mediana empresa de tecnología” serán piezas mudas, es decir, sin audio ni voz en off, diseñadas para funcionar únicamente con el impacto visual y el texto en pantalla. Cada video tendrá una duración aproximada entre 1 y 3 minutos, y un tamaño máximo de archivo de 150 MB para garantizar su correcta reproducción en el TVBox utilizado por la organización para la video cartelera, lo que implica un uso eficiente de imágenes, transiciones sencillas y ausencia de elementos multimedia pesados.

La estructura narrativa estándar se basará en una secuencia de diapositivas que combinan ilustraciones llamativas con mensajes cortos. El video inicia con una diapositiva de apertura que presenta una metáfora visual sobre el valor de la información o la importancia de los datos personales, seguida por un bloque de escenas que muestran riesgos cotidianos y un mensaje de alerta y recomendación concreta en cada una. Posteriormente se incluye un bloque de refuerzo del comportamiento deseado, centrado en la cultura de seguridad y la responsabilidad individual y colectiva, para terminar con una diapositiva de cierre que contiene una llamada a la acción alineada con el PCSI.

Dado que el contenido se verá en televisores ubicados en espacios comunes y muchas personas lo observarán de forma parcial o en movimiento, el texto en pantalla será autosuficiente, conciso y de alta legibilidad, con una idea clave por diapositiva y contrastes de color adecuados para lectura a distancia. Las imágenes e íconos (escudos, candados, héroes, dispositivos, huellas digitales, símbolos de IA, etc.) se utilizarán como soporte visual para que el mensaje se entienda incluso si la persona solo alcanza a leer una parte del texto, reforzando así las buenas prácticas de concientización sugeridas por NIST e ISO para campañas visuales breves en el lugar de trabajo (ISO, 2022b; NIST, 2024).

Estrategia de instrucción. La estrategia de instrucción para los videos de cartelera digital se centra en el refuerzo y no en la enseñanza exhaustiva: el objetivo es que las personas recuerden, en pocos segundos, comportamientos seguros ya introducidos en el curso virtual y en las políticas internas de la “mediana empresa de tecnología”, utilizando mensajes breves, directos y fáciles de aplicar en situaciones cotidianas de trabajo y vida digital (NIST, 2024).

Para ello, los contenidos se estructuran en micro-mensajes visuales donde cada diapositiva presenta una sola idea clave: un riesgo reconocible y una acción concreta recomendada (ejemplo: “WiFi público = riesgo” + “usa VPN o datos móviles”; “archivo sospechoso” + “no abras, consulta con TI”). Este enfoque por “píldoras” visuales responde a las recomendaciones de NIST para recordatorios breves y a los requisitos de concienciación continua, asegurando coherencia con el PCSI y con el SGSI de la “mediana empresa de tecnología” (ISO, 2022a; ISO, 2022b; NIST, 2024).

El tono comunicativo será cercano pero profesional, evitando tecnicismos innecesarios y utilizando metáforas o referencias culturales sencillas (héroes, videojuegos, redes sociales, IA) que faciliten la conexión emocional sin trivializar los riesgos.

Los mensajes enfatizarán la responsabilidad compartida, la colaboración entre equipos y el impacto de las acciones individuales en la protección de la información y de los datos personales, en línea con el énfasis de ISO en cultura organizacional y responsabilidad de las personas en seguridad de la información (ISO, 2022a; ISO, 2022b).

Relación con los capítulos del curso principal. Los videos de cartelera digital se diseñan como refuerzo visual de los cuatro capítulos y objetivos del curso principal de Concientización Básica en Seguridad de la Información, de manera que cada mensaje en pantalla recuerde un concepto ya trabajado en el LMS y en las políticas internas de la “mediana empresa de tecnología”, cumpliendo con la recomendación de NIST de combinar formación estructurada con recordatorios continuos en el lugar de trabajo (NIST, 2024).

En el Video 1, las diapositivas sobre valor de la información, phishing, contraseñas, uso de WiFi público, actualizaciones, dispositivos móviles, redes sociales, respaldos y trabajo en equipo retoman los contenidos básicos de buenas prácticas de seguridad, protección de credenciales, uso seguro de tecnología, prevención de incidentes frecuentes y rol de cada persona en el SGSI. Esto refuerza los capítulos del curso relacionados con principios generales de seguridad, amenazas comunes y controles básicos, alineados con los requisitos de concienciación y comportamiento seguro definidos en ISO/IEC 27001 (ISO, 2022a).

En el Video 2, las diapositivas se orientarán a cultura de seguridad continua, cumplimiento normativo y tratamiento adecuado de datos personales, vinculando visualmente los principios de protección de datos, confidencialidad, uso responsable de tecnologías y responsabilidad ética. De esta forma, se refuerzan los capítulos del curso que abordan obligaciones legales, políticas internas de la “mediana empresa de tecnología” y rol de cada colaborador en el cumplimiento, en consonancia con los lineamientos de ISO/IEC 27001, ISO/IEC 27002 y la importancia del apoyo visible de la dirección y de la cultura organizacional en la concientización (ISO, 2022a; ISO, 2022b; NIST, 2024).

Lineamientos de diseño audiovisual. Los videos utilizarán un estilo gráfico coherente con la identidad visual de la “mediana empresa de tecnología” y con el resto de materiales del PCSI, privilegiando ilustraciones claras, colores contrastados y tipografías legibles desde varios metros. Se recomienda usar fondos limpios, alto contraste entre texto y fondo, y evitar bloques extensos de texto, cada diapositiva debe comunicar una sola idea con una frase principal y, como máximo, dos líneas adicionales de apoyo, para facilitar la lectura rápida en movimiento (ISO, 2022a).

El ritmo visual se basará en transiciones suaves entre diapositivas, con tiempos de permanencia de 6 a 10 segundos por imagen, ajustados a la cantidad de texto y a la complejidad de la ilustración. No se incorporará audio ni voz en off, por lo que el impacto dependerá de la combinación entre metáfora visual (héroes, cofres, dispositivos, IA, etc.) y mensaje escrito; se evitarán animaciones complejas o pesadas para mantener el archivo final por debajo de 150 MB, de acuerdo con la capacidad del TVBox .

Al inicio o al final de cada video se incluirá una diapositiva breve que haga referencia explícita al PCSI y a la responsabilidad compartida en seguridad de la información, por ejemplo con mensajes tipo “PCSI de “mediana empresa de tecnología”: la seguridad empieza contigo” o “En la “mediana empresa de tecnología” 2025: protegemos la información entre todos”. Esto conecta visualmente el material de cartelera con el SGSI, reforzando el mensaje de cultura organizacional y compromiso con la protección de datos y activos de información (ISO, 2015).

Plan de exhibición de los videos de cartelera digital. Los videos se programarán en los TVBox de las carteleras digitales ubicadas en la cafetería de la “mediana empresa de tecnología”, de forma cíclica durante la jornada laboral. Se recomienda que cada pieza aparezca varias veces al día, alternada con otros contenidos corporativos, para aumentar las oportunidades de exposición sin generar saturación visual, en línea con las buenas prácticas de recordatorios breves y repetidos en el lugar de trabajo.

Se sugiere mantener una rotación periódica de mensajes, por ejemplo: exhibir el Video 1 de forma intensiva durante seis meses y, posteriormente, dar mayor presencia al Video 2 por otros seis meses, manteniendo siempre al menos un video del PCSI activo en las pantallas. Esta alternancia ayuda a reforzar distintos objetivos del programa a lo largo del año y se alinea con la recomendación de NIST e ISO de sostener la concienciación como un proceso continuo, integrado en la operación diaria de la organización (ISO, 2022a; NIST, 2024).

Métricas simples para los videos de cartelera digital. Dada la naturaleza pasiva y breve de los videos de cartelera digital, la medición de su impacto se enfocará en métricas indirectas y cualitativas, buscando correlaciones con otros indicadores del del PCSI. No se esperan mediciones directas de visualización o retención de mensajes específicos, sino una contribución al ambiente general de seguridad y a la cultura organizacional (NIST, 2024).

Una forma básica de estimar o asociar el impacto es la observación cualitativa por parte del equipo de TI y T&D puede realizar observaciones informales sobre el comportamiento de las personas colaboradoras en áreas comunes (ej. bloqueo de pantallas al ausentarse, menor uso de dispositivos personales para tareas laborales sensibles) y la retroalimentación espontánea sobre los mensajes de las carteleras.

Estas métricas, aunque no son concluyentes por sí solas, ofrecen una visión complementaria al seguimiento del curso principal y contribuyen a la mejora continua del PCSI, en línea con los requisitos de evaluación del desempeño y mejora de ISO/IEC 27001 (ISO, 2022a; NIST, 2024).

Firma y aceptación de las partes interesadas. Las personas firmantes declaran que han revisado el diseño instruccional y los contenidos propuestos para los videos de cartelera digital del Plan de Concientización en Seguridad de la Información (PCSI) de la “mediana empresa de tecnología”. Con su firma, autorizan su uso en las carteleras digitales de la organización y se comprometen a apoyar su difusión y actualización, en coherencia con el SGSI basado en ISO/IEC 27001:2022, ISO/IEC 27002:2022 y el Sistema de Gestión de Calidad ISO 9001:2015.” (ISO, 2015; ISO, 2022a).

1. Líder de Infraestructura Tecnológica (TI)

Nombre: _____

Cargo: _____

Firma: _____ Fecha: ___ / ___ / _____

2. Líder de Transformación y Desarrollo

Nombre: _____

Cargo: _____

Firma: _____ Fecha: ___ / ___ / _____

3. Jefe comercial o área de Mercadeo

Nombre: _____

Cargo: _____

Firma: _____ Fecha: ___ / ___ / _____

Instrucciones de *publicación.* El personal de TI es el responsable de publicar los videos de concientización del PCSI en los TVBox mediante la plataforma MDM Scalefusion, por lo que lo primero es comprobar que cada TVBox esté encendido y con conexión de red estable; sin este requisito, la gestión remota y la transferencia del archivo de video pueden fallar o quedar incompletas.

Una vez verificada la conectividad, la persona administradora accede a la consola web de Scalefusion con sus credenciales autorizadas y localiza el dispositivo o grupo de dispositivos correspondientes a las carteleras digitales, a través del menú de “Dispositivos” o de “Perfiles de dispositivo”, según la configuración que use la “mediana empresa de tecnología”.

Prototipo del material de refuerzo. *Introducción al Prototipo del Material de Refuerzo.* El Plan de Concientización en Seguridad de la Información (PCSI) de la “mediana empresa de tecnología”, diseñado bajo la guía de la publicación especial NIST SP 800-50r1 (NIST, 2024), contempla una estrategia integral para fortalecer la cultura de seguridad. Una pieza fundamental de esta estrategia es el material de refuerzo, cuyo propósito es mantener los conceptos clave del curso de concientización frescos y relevantes en la mente de los colaboradores. Este material actúa como un recordatorio continuo, esencial para la sostenibilidad del programa de concienciación (NIST, 2024).

Según el diseño establecido, el material de refuerzo se concibió para ser dinámico y adaptable a diversos canales. En esta sección, nos enfocamos en la materialización de este diseño a través de prototipos funcionales para la video-cartelera interna de la “mediana empresa de tecnología”. Este medio específico fue seleccionado por su capacidad para captar la atención visual y ofrecer mensajes concisos en puntos estratégicos de la organización.

El prototipo implementado consiste en dos videos con publicación semestral, diseñados para ser proyectados de forma continua en las pantallas de la video-cartelera. Estos videos buscan reforzar los temas de seguridad de la información de manera lúdica y atractiva, alineándose con el cronograma general del PCSI. A diferencia de otras piezas de material de

refuerzo que podrían distribuirse por correo electrónico o repositorios compartidos, estos videos están específicamente adaptados para el formato de cartelera digital, aprovechando su naturaleza visual y de difusión pasiva para impactar a la audiencia de la “mediana empresa de tecnología”. La ejecución de estos prototipos permite validar la efectividad del diseño conceptual y su adecuación al canal de comunicación elegido, asegurando que los mensajes de seguridad sean percibidos y asimilados por el personal de manera efectiva (NIST, 2024).

Desde la consola, se procede a cargar el archivo MP4 del video utilizando la opción gestión de archivos de Scalefusion, confirmando que el tamaño del archivo no supere los 150 MB definidos como límite para el TVBox. Tras la carga, se crea o actualiza un perfil de contenido asociado a la cartelera digital, incorporando el nuevo video a la lista de reproducción y definiendo su orden y, si aplica, su frecuencia de aparición, de forma alineada con el plan de exhibición establecido para el PCSI (NIST, 2024). Posteriormente, se asigna este perfil de contenido al TVBox o al grupo de TVBox deseado, lo que hace que Scalefusion envíe automáticamente la instrucción de descarga y reproducción al dispositivo.

Finalmente, el personal de TI verifica desde la propia consola el estado del dispositivo, comprobando que el contenido se haya distribuido correctamente, y valida, cuando sea posible, la reproducción directa en la pantalla del TVBox en sitio. Este flujo sencillo permite que la publicación y actualización de los videos de cartelera se realice de forma controlada, repetible y trazable, en coherencia con los principios de operación planificada y comunicación efectiva del PCSI (ISO, 2022a; NIST, 2024).

Guía de lectura de las imágenes del material de refuerzo. Las imágenes incluidas en este capítulo corresponden a fotogramas de los videos prototipo proyectados en la video cartelera interna de la “mediana empresa de tecnología”. Su función principal, en el contexto del PCSI, es servir como evidencia visual de la ejecución del diseño del material de refuerzo, más que representar contenidos temáticos específicos del curso. En coherencia con las recomendaciones de NIST SP 800-50r1, estos recursos se utilizan como recordatorios breves y frecuentes que apoyan los mensajes centrales del plan de concientización, sin sustituir los contenidos formales del curso (NIST, 2024).

Cada imagen debe interpretarse como una escena dentro de una narrativa audiovisual más amplia. De acuerdo con el diseño definido los videos emplean ilustraciones con alto contraste, personajes reconocibles y metáforas visuales sencillas para captar la atención del usuario en pocos segundos. Así, la lectura de las figuras se orienta a identificar tres elementos clave: el contexto gráfico (fondo, dispositivos, personajes), el mensaje principal (texto corto en la parte inferior o central) y el llamado a la acción implícito o explícito asociado a una buena práctica de seguridad (por ejemplo, verificar correos, proteger credenciales o mantener sistemas actualizados).

En cuanto a los elementos visuales, la iconografía se apoya en símbolos comúnmente asociados con tecnologías digitales y seguridad (dispositivos, sobres de correo, candados, escudos, signos de alerta), lo que facilita la rápida asociación con riesgos o controles sin necesidad de explicaciones extensas. Los colores vivos y contrastados se utilizan para diferenciar (usuarios, amenazas, héroes de la información) y resaltar zonas críticas de atención, en línea con las buenas prácticas de diseño instruccional para mensajes breves en entornos de trabajo (NIST, 2024). El texto complementario, ubicado normalmente en una franja inferior, refuerza en lenguaje cotidiano la conducta deseada, conectando la metáfora visual con la acción concreta esperada del colaborador.

La relación de estas imágenes con los temas del curso se realiza a nivel de macrocontenidos y momentos del cronograma, más que por coincidencia literal entre cada fotograma y cada módulo. Tal como se definió en el diseño del PCSI, los videos semestrales se sincronizan con los bloques temáticos priorizados en el cronograma (por ejemplo, protección de la información, amenazas comunes, responsabilidades del usuario), de modo que los mensajes visuales acompañan y refuerzan los aprendizajes adquiridos en el LMS, las sesiones sincrónicas u otros canales formales del programa (NIST, 2024).

Correspondencia entre Elementos de Diseño y Ejecución del Material de Refuerzo

NIST SP 800-50r1 sugiere documentar cómo los elementos de diseño (frecuencia, formato, mensajes clave, público objetivo) se concretan en la implementación, más a nivel de “mecanismo de entrega” y “tipo de mensaje” que de diapositiva individual.

Tabla 8

Característica de diseño del material de refuerzo.

Elemento de Diseño	Descripción del Diseño	Implementación en el Prototipo
Formato de video para video-cartelera	El material de refuerzo para este canal se definió en formato de video corto, con mensajes secuenciales y recursos animados, específico para reproducción continua en las pantallas internas de La “mediana empresa de tecnología”, de acuerdo con el cronograma semestral del PCSI.	Se desarrollaron dos videos, uno por semestre, con duración y ritmo visual adecuados a la atención de los colaboradores en espacios de tránsito, reforzando los temas priorizados del PCSI en cada periodo.
Uso de narrativas visuales lúdicas	El diseño conceptual estableció el uso de metáforas, personajes y escenas lúdicas para reducir la percepción de tecnicismo y acercar los mensajes de seguridad al lenguaje cotidiano del colaborador.	Los videos emplean personajes tipo caricatura y escenas inspiradas en cultura popular y entornos digitales, construyendo pequeñas historias visuales que introducen o refuerzan comportamientos seguros.
Mensajes breves y orientados a la acción	Los mensajes del material de refuerzo debían formularse en frases cortas, en tono cercano, y siempre asociadas a una conducta concreta esperada (por ejemplo, verificar, actualizar, proteger, reportar).	En los videos se integran cintillos de texto en la parte inferior de la pantalla, donde se expresan llamados a la acción en lenguaje sencillo que complementan la metáfora visual de cada escena.
Enfoque en refuerzo, no en formación primaria	El diseño del PCSI definió que las piezas para video-cartelera funcionarían como recordatorios posteriores a la formación principal, evitando introducir contenidos nuevos complejos y enfocándose en reforzar conceptos ya abordados en el curso.	Los guiones de los videos se construyeron a partir de los temas del cronograma del curso, retomando ideas clave como responsabilidades del usuario, amenazas frecuentes y protección de la información, sin pretender reemplazar los módulos formales del LMS.
Exclusividad del canal video-cartelera	Para evitar saturación por múltiples canales, el diseño estableció que estos videos serían exclusivos de las pantallas internas de La “mediana empresa de tecnología”, diferenciándose de otros materiales de refuerzo previstos para correo o repositorios digitales.	Los videos fueron cargados y configurados en el sistema de video-cartelera de la organización, con reproducción cíclica en las áreas definidas, sin distribución por correo electrónico, Teams ni Viva Engage.
Integración con el cronograma semestral del PCSI	El material de refuerzo debía sincronizarse con el cronograma del PCSI, de modo que cada video acompañara los temas trabajados en el semestre correspondiente, manteniendo la coherencia temporal del programa.	Se produjeron dos versiones de video, una para cada semestre, cuyos mensajes visuales refuerzan los bloques temáticos priorizados en ese periodo, siguiendo la recomendación de mantener continuidad y consistencia en el tiempo.

Nota. Fuente (Los autores)

Presentación visual del prototipo del material de refuerzo. Las imágenes incorporadas en este capítulo muestran fotogramas de los dos videos prototipo desarrollados para la video cartelera interna de la “mediana empresa de tecnología”. Como se definió en el diseño del PCSI, estos videos constituyen un componente específico del material de refuerzo, orientado a mantener la seguridad de la información presente en el día a día mediante estímulos visuales breves y reiterados (NIST, 2024). Aunque los fotogramas no se corresponden de forma exacta con cada tema del curso, sí reflejan las decisiones de diseño implementadas para apoyar los bloques temáticos del cronograma semestral.

En las Figuras de la 17 a la 19 se observa una pantalla de la video cartelera instalada en una zona común de la organización. El fotograma muestra una escena con dispositivos y múltiples íconos digitales en movimiento, acompañados de un cintillo de texto en la parte inferior. Esta composición ilustra el uso de gráficos de alto impacto y mensajes cortos, diseñados para captar la atención de los colaboradores en contextos de tránsito, reforzando de manera general la importancia de la tecnología y las prácticas seguras asociadas a su uso, en línea con el enfoque de “recordatorios ambientales” recomendado por NIST para programas de concienciación (NIST, 2024).

En otro fotograma de la video cartelera (Figura 18), en el que se utilizan personajes tipo caricatura ubicados frente a un equipo de cómputo, con sobres de correo y signos de alerta en el fondo. Esta escena ejemplifica la aplicación de narrativas visuales lúdicas y metáforas sencillas para representar situaciones de riesgo y la necesidad de cautela en la interacción con medios digitales. Aunque el fotograma se tomó en un momento puntual del video, la pieza completa se articula con los contenidos del PCSI relacionados con identificación de amenazas y comportamiento seguro del usuario, tal como fue previsto en la integración entre cronograma de temas y material de refuerzo.

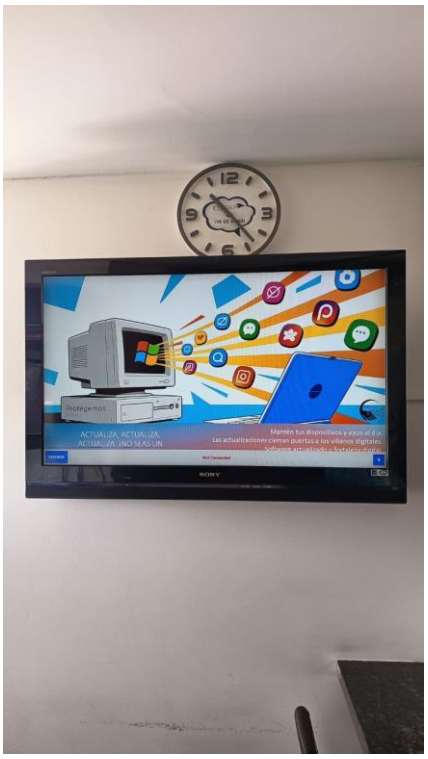
En la Figura 19 se aprecia un personaje con estética de superhéroe frente a un entorno de servidores y un escudo con candado en primer plano. Esta imagen pone de manifiesto el

mensaje transversal de corresponsabilidad en la protección de la información: cada colaborador es un “guardián” de los activos de información de la organización. El uso de iconografía de seguridad (escudo, candado, centro de datos) combinado con un héroe visual refuerza la idea de que las conductas cotidianas alineadas con el PCSI son un “superpoder” organizacional. Este enfoque responde a la recomendación de NIST de asociar la concienciación con mensajes positivos sobre el rol del personal, en lugar de centrar la comunicación solo en el miedo al riesgo (NIST, 2024).

En conjunto, las tres figuras evidencian la coherencia entre el diseño conceptual y la ejecución del prototipo, se confirma el uso de videos exclusivos para la video cartelera, el empleo de recursos visuales llamativos, mensajes concisos orientados a la acción y una integración general con los bloques temáticos del PCSI según el cronograma semestral, cumpliendo con los lineamientos de planificación y diseño establecidos para el material de refuerzo (NIST, 2024).

Figura 17

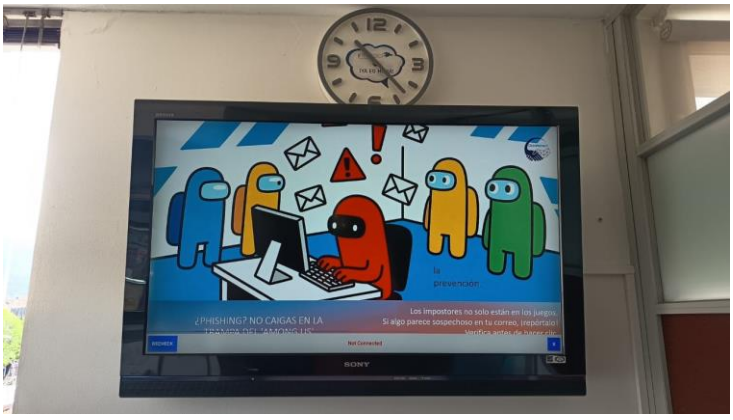
Fotografía de video cartelera con material de apoyo publicado - 1



Nota: Fotografía de los autores [fotografía], video cartelera de la “mediana empresa de tecnología”, 2025.

Figura 18

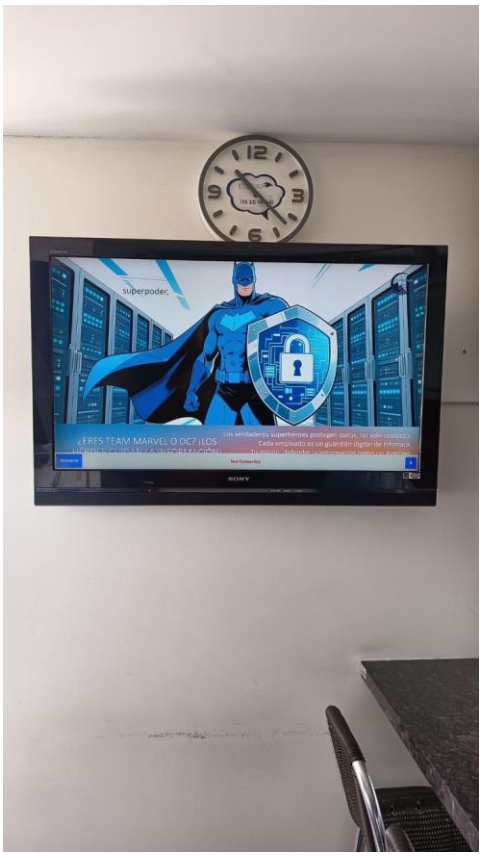
Fotografía de video cartelera con material de apoyo publicado - 2



Nota: Fotografía de los autores [fotografía], video cartelera de la “mediana empresa de tecnología”, 2025.

Figura 19

Fotografía de video cartelera con material de apoyo publicado - 3



Nota: Fotografía de los autores [fotografía], video cartelera de la “mediana empresa de tecnología”, 2025.

Documento de Diseño para los Microcontenidos

Propósito del Material. El propósito de los microcontenidos es reforzar, de forma breve y recurrente, los mensajes clave del curso de “Concientización Básica en Seguridad de la Información”, facilitando que las personas recuerden y apliquen en su trabajo diario los comportamientos esperados en materia de protección de la información y datos personales. Estos materiales actúan como recordatorios puntuales que mantienen vivo el aprendizaje entre sesiones formales de capacitación. (NIST, 2024; ISO, 2022a; ISO, 2022b).

Objetivos del Material. Los microcontenido tiene los siguientes objetivos

Recordar y Reforzar los Mensajes Clave del Curso. Reforzar, de forma breve y frecuente, los conceptos y comportamientos fundamentales tratados en el curso de “Concientización Básica en Seguridad de la Información”, de manera que las personas los tengan presentes en su trabajo cotidiano (por ejemplo, buen uso de contraseñas, protección de datos personales, manejo adecuado de incidentes). (NIST, 2024; ISO, 2022a; ISO, 2022b).

Orientar Hacia Conductas Concretas Esperadas. Traducir los contenidos del curso en mensajes accionables (“haz / no hagas”) que apoyen el cumplimiento de políticas internas, procedimientos y controles del SGSI, facilitando que el personal sepa qué se espera que haga en situaciones comunes de manejo de información. (NIST, 2024; ISO, 2022a; ISO, 2022b)

Mantener la Atención y la Cultura de Seguridad en el Tiempo. Mantener la concientización activa durante todo el año mediante impactos cortos pero regulares, reduciendo la “curva de olvido” posterior a la formación formal y fortaleciendo la cultura de seguridad de la información y protección de datos personales en la “mediana empresa de tecnología”. (NIST, 2024; ISO, 2022a; ISO, 2022b).

Apoyar el Cumplimiento Normativo y de Auditoría. Contribuir a evidenciar que la "mediana empresa de tecnología" realiza actividades continuas de sensibilización y comunicación en seguridad de la información y datos personales, como complemento a los cursos formales y a las comunicaciones del SGSI y del SGC. (ISO, 2022a; ISO, 2022b; NIST, 2024)

Antecedentes del Material. El diseño de estos microcontenidos surge como complemento al curso virtual de "Concientización Básica en Seguridad de la Información" del PCSI, el cual ya define propósito, objetivos, esquema por capítulos y estrategia de instrucción para todo el personal que trata información o datos personales en la "mediana empresa de tecnología". Este curso constituye el eje formativo principal, mientras que los microcontenidos actúan como refuerzos breves posteriores y paralelos a la capacitación formal. (NIST, 2024; ISO, 2022a; ISO, 2022b)

Adicionalmente, la "mediana empresa de tecnología" cuenta con políticas, procedimientos y lineamientos internos que requieren ser conocidos y aplicados por el personal en el día a día, más allá de los momentos puntuales de formación. Los microcontenidos se conciben como un mecanismo de comunicación y sensibilización continua que traduce estos requisitos y controles del SGSI en mensajes simples y accionables. (ISO, 2022a; ISO, 2022b; NIST, 2024)

Finalmente, los resultados de evaluaciones internas, análisis de riesgos, reportes de incidentes y diagnósticos de protección de datos personales han evidenciado la necesidad de reforzar conductas específicas relacionadas con el uso de contraseñas, manejo de correo, protección de datos personales y uso adecuado de recursos tecnológicos. Los microcontenidos se alinean con esa necesidad al proporcionar recordatorios frecuentes, breves y focalizados sobre los temas con mayor impacto para el riesgo de seguridad de la información en la organización. (NIST, 2024; ISO, 2022a; ISO, 2022b)

Público Objetivo. El público objetivo principal de los microcontenidos del PCSI está conformado por todo el personal de la “mediana empresa de tecnología” que tiene acceso a información corporativa o trata datos personales en el marco de sus funciones, incluyendo personal administrativo, operativo, comercial, de soporte, líderes de proceso y contratistas que utilizan los sistemas de información de la compañía. (ISO, 2022a; ISO, 2022b; NIST, 2024).

Estos materiales se publicarán en canales de acceso general de forma que lleguen de manera homogénea a toda la organización, independientemente del rol o nivel jerárquico, reforzando los mensajes clave del PCSI en los espacios digitales cotidianos. (ISO, 2022a; ISO, 2022b; NIST, 2024).

Estrategia de Instrucción. La estrategia de instrucción se basará en mensajes muy breves, claros y orientados a conducta, diseñados para recordar “qué hacer” y “qué evitar” en situaciones cotidianas (por ejemplo, ante un correo sospechoso, al guardar archivos o al manejar datos personales). Los microcontenidos funcionarán como refuerzos en el flujo de trabajo, conectando directamente con las políticas internas y con los temas del curso del PCSI, más que como explicaciones extensas. (NIST, 20242; ISO, 2022a; ISO, 2022b).

Cada pieza privilegiará estructuras simples: preguntas disparadoras (“¿Reconocerías un correo de phishing?”), tips rápidos (“Antes de hacer clic, revisa remitente y enlace”) y recordatorios explícitos de políticas (“La información de la “mediana empresa de tecnología” se guarda en OneDrive/SharePoint, no en herramientas externas”). Esta repetición espaciada de mensajes claves apoya el cambio de hábitos y la reducción de brechas detectadas en incidentes, auditorías y campañas de phishing. (NIST, 2024; ISO, 2022a; ISO, 2022b)

Tono, Lenguaje e Iconografía. El tono será cercano pero profesional, respetuoso y constructivo, evitando mensajes culpabilizantes o alarmistas; se enfatizará que la seguridad es responsabilidad compartida y que los errores se gestionan mejor cuando se reportan a tiempo. El lenguaje será directo, en segunda persona (“tú”), con verbos de acción (“protege”, “verifica”, “reporta”) y sin tecnicismos innecesarios, salvo cuando se requiera mencionar un control o política específica. (ISO, 2022a; ISO, 2022b; NIST, 2024).

Las piezas usarán iconografía sencilla y coherente con la identidad visual de la “mediana empresa de tecnología” y del PCSI: símbolos de candado, superhéroes, dispositivos, inteligencia artificial y personas colaborando, entre otros. Las imágenes reforzarán la idea principal sin sobrecargar la pieza, y se mantendrá consistencia en colores, tipografías y estilos para que los usuarios identifiquen rápidamente que se trata de contenidos oficiales de concientización en seguridad de la información. (NIST, 2024; ISO, 2022a; ISO, 2022b).

Canales de Publicación. Los microcontenidos del PCSI se difundirán principalmente a través de la intranet y de los canales corporativos de Microsoft, priorizando el grupo general al que tiene acceso todo el personal y las comunidades en Microsoft Viva Engage, complementados, cuando aplique, por publicaciones en Teams. Estos canales permiten una alta cobertura y se integran naturalmente al entorno digital de trabajo diario del personal. (ISO, 2022a; NIST, 2024)

Los microcontenidos se coordinarán con el resto de las comunicaciones del PCSI para evitar saturación y garantizar coherencia en los mensajes.

Frecuencia y Ritmo de Publicación. Se propone una frecuencia base de un microcontenido mensual alineado al cronograma del PCSI, garantizando al menos 12 impactos breves al año, uno por cada tema priorizado del curso de concientización básica. De forma complementaria, se podrán usar piezas adicionales en momentos clave (por ejemplo, durante la simulación de phishing o ante cambios relevantes en políticas), sin exceder en general 1 pieza por semana para evitar fatiga de mensajes. (NIST, 2024; ISO, 2022a)

La calendarización seguirá el hilo temático anual: en los primeros meses, mensajes introductorios y de cultura general de seguridad; en los meses intermedios, foco en buenas prácticas; y hacia el cierre, énfasis en incidentes, repositorios autorizados, escritorio limpio y datos personales, en consonancia con los objetivos y métricas del PCSI. (ISO, 2022a; ISO, 2022b; NIST, 2024).

Reglas de Diseño de Contenido. Cada microcontenido seguirá una estructura sencilla y repetible, que facilite el reconocimiento y el recuerdo del mensaje principal. Se sugiere mantener siempre:

un título breve (máx. 8–10 palabras),

un mensaje central conductual (“haz / no hagas”),

un apoyo visual (icono o ilustración simple) y

un llamado a la acción claro (“si dudas, reporta a… / revisa la política…”).

Esta consistencia facilita que el personal identifique rápidamente de qué trata el contenido y qué se espera que haga. (NIST, 2024; ISO, 2022a; ISO, 2022b).

Los textos priorizarán una sola idea clave por pieza. Evitaremos saturar el diseño con múltiples recomendaciones simultáneas; en su lugar, se buscará que cada microcontenido refuerce un comportamiento concreto, alineado a un riesgo priorizado (por ejemplo, phishing, protección de datos, uso de repositorios autorizados). Esta focalización apoya el principio de “pocos mensajes, muy claros, muchas veces”, recomendado en programas de concientización efectivos. (NIST, 2024; ISO, 2022a).

Los diseños respetarán la identidad gráfica corporativa de la “mediana empresa de tecnología” (colores, tipografías, uso de logotipo), manteniendo una plantilla común para todos los microcontenidos del PCSI de manera que se reconozcan como parte de una misma campaña anual. Se recomienda un uso equilibrado del color para resaltar el mensaje clave sin generar ruido visual, con suficiente contraste para garantizar legibilidad. (ISO, 2022a; NIST, 2024).

Efectividad de los Microcontenidos Dentro del PCSI. La efectividad de los microcontenidos del PCSI se evaluará combinando indicadores cuantitativos y cualitativos, siguiendo las directrices de NIST para asegurar que la concientización no solo exponga, sino que también genere comprensión y cambios de conducta. (NIST, 2024). Esta medición se integrará con los mecanismos de seguimiento del SGSI y SGC de la “mediana empresa de tecnología”, contribuyendo a la mejora continua. (ISO, 2022a).

Se establecerán indicadores de exposición y alcance para determinar a cuántas personas llegan los mensajes. Esto incluirá la cobertura de audiencia y métricas de visualización o alcance digital en plataformas corporativas. (NIST, 2024). También se verificará la frecuencia de exposición, asegurando que se cumpla la planificación de al menos un microcontenido mensual y refuerzos puntuales. (ISO, 2022a).

Para medir el involucramiento, se usarán indicadores de interacción y compromiso. Se analizarán reacciones, comentarios y compartidos en Viva Engage y Teams para identificar temas de mayor interés. (NIST, 2024).

Finalmente, los indicadores de aprendizaje y cambio de conducta evaluarán se revisarán por medio de indicadores operativos como resultados de campañas de phishing simulado, oportunidad en el reporte de incidentes y hallazgos de auditoría relacionados con las buenas prácticas promovidas. (ISO, 2022a).

Los resultados se revisarán periódicamente con CISO/TI y T&D para ajustar el PCSI, reforzar temas y priorizar nuevas piezas, garantizando una mejora continua y adaptada a las necesidades de la “mediana empresa de tecnología”. (ISO, 2022a; NIST, 2024).

Firma y aceptación de las partes interesadas. Las personas firmantes declaran que han revisado los microcontenidos (textos e imágenes) y las instrucciones de publicación definidas para el Plan de Concientización en Seguridad de la Información (PCSI) de la “mediana empresa de tecnología”, específicamente para su difusión en el canal general de la “mediana empresa de tecnología” en Microsoft Teams y en la comunidad InfoSocialTrack en Viva Engage. Con su firma, autorizan su uso en estos canales corporativos y se comprometen a apoyar su correcta publicación, difusión y actualización, en coherencia con el Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001:2022, ISO/IEC 27002:2022 y el Sistema de Gestión de la Calidad ISO 9001:2015. (ISO, 2015; ISO, 2022a; ISO, 2022b)

1. Líder de Infraestructura Tecnológica (TI)

Nombre: _____

Cargo: _____

Firma: _____ Fecha: ___ / ___ / _____

2. Líder de Transformación y Desarrollo

Nombre: _____

Cargo: _____

Firma: _____ Fecha: ___ / ___ / _____

3. Jefe comercial o área de Mercadeo

Nombre: _____

Cargo: _____

Firma: _____ Fecha: ___ / ___ / _____

Instrucciones de publicación de microcontenidos del PCSI en Teams y Viva Engage. El responsable de la publicación de los microcontenidos del PCSI será el CISO (Coordinador de IT), quien deberá seguir las siguientes instrucciones básicas para garantizar consistencia y trazabilidad en los canales definidos de la “mediana empresa de tecnología”.

Publicación en el canal general de la “mediana empresa de tecnología” en Microsoft Teams. Abrir Microsoft Teams con la cuenta corporativa y ubicar el equipo llamado Teams para la “mediana empresa de tecnología” y el canal General.

Ingresar al icono “Publicar en el canal”, donde se visualizan los mensajes del canal, para iniciar una nueva publicación en la parte inferior, según el diseño del canal.

Escribir un título breve y pegar el texto del microcontenido del PCSI, verificando ortografía y tono antes de publicar.

Adjuntar la imagen del microcontenido con el icono de Adjuntar archivo desde el equipo, asegurando que el archivo tenga el nombre estándar definido en el PCSI.

Opcionalmente, puede usar el botón de formato para resaltar ideas clave y, usar el icono de anuncio para que el mensaje llegue a todos los colaboradore.

Revisar que el mensaje incluya claramente:

Mensaje principal del microcontenido.

Llamado a la acción (por ejemplo, “Si dudas, reporta a…”, “Consulta la política en…”).

Relación con el PCSI (por ejemplo, “Microcontenido PCSI – Mes X”).

Publicar seleccionando el botón “Publicar”, y verificar visualmente que el mensaje se vea correcto en el canal.

En caso de detectar errores después de publicar, editar y corregir el mensaje, manteniendo la trazabilidad del microcontenido asociado al mes o tema correspondiente.

Publicación en la comunidad InfoSocialTrack en Viva Engage (integrado en Teams). Desde Teams, acceder a la aplicación de Viva Engage (antes Yammer) o a la sección donde se muestran las comunidades, y seleccionar la comunidad InfoSocialTrack, definida como canal oficial para temas de seguridad de la información y cultura organizacional.

Crear una nueva publicación seleccionando “Discusión”. En el caso de microcontenidos del PCSI, se debe usar anuncio cuando el mensaje tenga carácter corporativo transversal.

Ingresar un título claro y pegar el texto del microcontenido; la imagen asociada, adjuntarla mediante la opción agregar imagen, verificando que el diseño corresponda al tema del PCSI.

Evitar el uso excesivo de emojis, GIFs o elementos que distraigan del mensaje principal de seguridad; su uso debe ser puntual y coherente con el tono definido en el PCSI.

Antes de publicar, revisar:

Coherencia con la versión publicada en el canal general de Teams.

Fecha de publicación, para asegurar alineación con el cronograma mensual del PCSI.

Seleccionar Publicar y, posteriormente, monitorear semanalmente las interacciones básicas (reacciones, comentarios) para alimentar los indicadores de efectividad definidos en el PCSI.

Reglas generales para el responsable de publicación. Publicar únicamente los microcontenidos aprobados en el marco del PCSI, respetando texto, imagen y fecha definidos en el plan. (NIST, 2024)

Verificar, antes de cada publicación, que el contenido sea consistente con las políticas y procedimientos vigentes de la “mediana empresa de tecnología”, especialmente aquellos relacionados con seguridad de la información y protección de datos personales. (ISO, 2022a; ISO, 2022b)

Evitar duplicar mensajes en periodos muy cortos; cualquier reenvío o refuerzo deberá coordinarse con T&D para no saturar los canales. (NIST, 2024)

Conservar un registro interno de la fecha, canal y enlace de cada publicación realizada, para facilitar el seguimiento y la medición de efectividad. (ISO, 2022a)

Prototipo del material de microcontenidos. ***Introducción al prototipo de microcontenidos.*** El prototipo de microcontenidos desarrollado para el Plan de Concientización en Seguridad de la Información (PCSI) de la “mediana empresa de tecnología” materializa el diseño instruccional definido en el proyecto, trasladando los objetivos de aprendizaje a piezas visuales breves, concretas y accionables. Cada microcontenido parte de riesgos priorizados en el análisis de contexto, como phishing, uso de contraseñas, redes Wi-Fi públicas, dispositivos móviles, inteligencia artificial y cultura de reporte, entre otros. Estos temas se traducen en mensajes simples, memorables y alineados con el rol de cada colaborador como “guardián digital” de la organización.

Siguiendo las recomendaciones para programas de sensibilización efectivos, los microcontenidos se diseñaron como cápsulas en formato visual estático, imágenes tipo viñeta o storyboard listas para ser utilizadas como piezas gráficas autónomas. La estética incorpora elementos de cultura popular, metáforas visuales (tesoro, escudo, superhéroes, videojuegos, memes) y mensajes directos que facilitan la recordación y promueven comportamientos específicos de protección de la información.

En esta fase de prototipado, el énfasis está en validar el concepto, el tono y la estructura de los microcontenidos. Para ello, se elaboró un set de quince piezas temáticas que cubren, entre otros, el valor de la información como activo, la gestión de contraseñas, la prevención del phishing, el uso seguro de redes Wi-Fi públicas, la protección de dispositivos móviles, la verificación de archivos sospechosos, la gestión de respaldos, la seguridad como trabajo en equipo, el uso responsable de la inteligencia artificial, el impacto de las publicaciones en redes sociales y la detección de deepfakes y noticias falsas.

En este prototipo las unidades se implementan como imágenes estáticas de alta calidad que pueden ser utilizadas directamente en canales digitales internos (Microsoft Teams, Viva

Engage, correo electrónico corporativo). La selección de estos canales responde al criterio de integrar el PCSI en los flujos cotidianos de trabajo, tal como sugiere NIST para incrementar la exposición y la efectividad de los mensajes de concientización. De este modo, se demuestra la coherencia entre el diseño conceptual del PCSI y su primera ejecución visual en forma de prototipo de microcontenidos.

Guía de lectura de las imágenes de microcontenidos. Las imágenes que conforman el prototipo de microcontenidos deben leerse como cápsulas visuales de sensibilización, cada una diseñada para transmitir un solo mensaje clave de seguridad de la información en un vistazo. En línea con las recomendaciones de NIST para programas de awareness, cada pieza combina un concepto central, un gancho emocional o lúdico y una instrucción concreta de “qué hacer” o “qué evitar”, facilitando la comprensión incluso cuando la atención del colaborador es limitada (NIST,2024).

Cada imagen se estructura en dos zonas principales:

un bloque visual dominante, donde se representa la metáfora (cofre del tesoro, escudo, superhéroes, videojuegos, redes sociales, Wi-Fi público, robot de IA, etc.), y

una franja inferior de texto, donde se incluye el título llamativo y un breve conjunto de recomendaciones prácticas. Esta separación ayuda a que primero se capte la idea general y luego se refuercen las acciones esperadas, tal como se definió en el Documento de Diseño de Microcontenidos del PCSI.

Los elementos visuales clave que el lector debe observar incluyen:

Mensajes principales: el título en mayúsculas o destacado (“LA INFORMACIÓN ES EL NUEVO ORO”, “CONTRASEÑAS: TU ESCUDO DE VIBRANIUM”, “¿PHISHING? NO CAIGAS EN LA TRAMPA…”) resume el comportamiento deseado.

Llamados a la acción: en la parte derecha inferior se indican acciones específicas: actualizar dispositivos, no compartir contraseñas, verificar correos sospechosos, usar VPN,

bloquear el móvil, hacer copias de seguridad, no abrir archivos raros, reportar incidentes, usar IA con ética, etc.

Identidad visual y branding: el logotipo de On1nfotrack y el uso consistente de colores corporativos conectan el mensaje con la estrategia de seguridad de la organización y refuerzan que se trata de lineamientos oficiales, no de contenido genérico.

Estas imágenes se relacionan directamente con los temas del curso principal del PCSI: gobierno y valor de la información, protección de credenciales, amenazas comunes (phishing, malware, redes inseguras), protección de dispositivos, continuidad (respaldos), trabajo colaborativo seguro, protección de datos personales y uso responsable de nuevas tecnologías como la inteligencia artificial. NIST indica que los materiales de sensibilización deben reforzar, de manera breve y recurrente, los contenidos tratados en formaciones más extensas, utilizando canales cotidianos como Teams, intranet o correo electrónico (NIST,2024). En coherencia con ello, cada microcontenido se concibe como un recordatorio periódico alineado con el cronograma anual del PCSI y con las políticas internas de seguridad de la información de La “mediana empresa de tecnología”.

Correspondencia entre Elementos de Diseño y Ejecución del Material de Microcontenidos.

La tabla número 9, resume como los contenidos propuestos se relacionan con la estructura de diseño para el microcontenido del PCSI.

Tabla 9

Correspondencia entre elementos de diseño y prototipo del material de microcontenidos

Mes	Elemento de Diseño	Descripción del Diseño	Implementación en el Prototipo	Evidencia Visual (Figura)
1	Tema: Valor de la información como activo	Transmitir que la información es un recurso crítico que debe protegerse al nivel de un activo financiero o físico clave. Formato: imagen tipo microcontenido. Mensaje central: "la información es valiosa y todos somos responsables de cuidarla".	Se representa un cofre del tesoro lleno de monedas, documentos y componentes tecnológicos, reforzando la metáfora de la información como "nuevo oro". El texto principal indica "LA INFORMACIÓN ES EL NUEVO ORO. Protégela como si fuera tuya – La “mediana empresa de tecnología” 2025", conectando valor y responsabilidad individual.	Valor de la información como activo (Figura 20)
2	Tema: Rol del colaborador como héroe de la seguridad	Resaltar que cada persona es un "guardián digital" y que la seguridad no es solo función de TI. Duración objetivo: 30–60 segundos. Formato: imagen inspiracional con metáfora de superhéroe.	Muestra a un personaje tipo superhéroe con escudo de candado en un centro de datos. El mensaje "¿ERES TEAM MARVEL O DC? ¡LOS HÉROES CUIDAN LA INFORMACIÓN!" y el texto de apoyo refuerzan que cada empleado es responsable de proteger datos y sistemas.	Colaborador como héroe de la seguridad (Figura 21)
3	Tema: Contraseñas fuertes y gestión segura	Reforzar buenas prácticas de contraseñas: longitud, complejidad, no reutilización y uso de gestores. Duración: 30–60 segundos. Formato: pieza gráfica asociada a cultura popular.	Se utiliza el escudo del Capitán América como metáfora de contraseña fuerte. El texto "CONTRASEÑAS: TU ESCUDO DE VIBRANIUM" y las instrucciones de usar frases largas y gestores de contraseñas traducen las recomendaciones técnicas en un mensaje sencillo y memorable.	Contraseñas fuertes y gestión segura (Figura 22)
4	Tema: Prevención de phishing y correos sospechosos	Alertar sobre correos y enlaces fraudulentos, promoviendo la verificación y el reporte. Duración: 30–60 segundos. Formato: imagen alusiva a videojuegos/juegos en línea.	La escena con personajes estilo "Among Us" y múltiples alertas visuales simboliza impostores ocultos en el correo. El título "¿PHISHING? NO CAIGAS EN LA TRAMPA DEL 'AMONG US'" y el texto explican que los impostores no solo están en los juegos y animan a reportar y verificar antes de hacer clic.	Prevención de phishing y correos sospechosos (Figura 23)
5	Tema: Actualización de software y dispositivos	Promover la instalación oportuna de parches y actualizaciones como medida clave de seguridad. Duración: 30–60 segundos. Formato: pieza humorística/comparativa.	Se contrasta un computador antiguo con un portátil moderno mientras fluyen iconos de aplicaciones. El mensaje "ACTUALIZA, ACTUALIZA, ACTUALIZA: ¡NO SEAS UN WINDOWS XP!" se complementa con instrucciones sobre mantener dispositivos y apps al día como barrera frente a atacantes.	Actualización de software y dispositivos (Figura 24)

Mes	Elemento de Diseño	Descripción del Diseño	Implementación en el Prototipo	Evidencia Visual (Figura)
6	Tema: Uso seguro de redes Wi-Fi públicas	Fomentar el uso de VPN, evitar el acceso a información sensible y priorizar conexiones seguras. Duración: 30–60 segundos. Formato: escena cotidiana en lugar público.	Un usuario trabaja en un café bajo iconos de peligro y señal Wi-Fi, simbolizando el riesgo. El título "REDES WIFI PÚBLICAS: NO TODO LO GRATIS ES SEGURO" y las recomendaciones (usar VPN, preferir hotspot propio) traducen políticas técnicas a acciones concretas.	Uso seguro de redes Wi Fi públicas (Figura 25)
7	Tema: No compartir credenciales	Reforzar la regla de no compartir contraseñas y promover el uso de mecanismos seguros para acceso compartido. Duración: 30–60 segundos. Formato: comparación lúdica (memes vs contraseñas).	Un grupo de personas comparte contenido en sus celulares, contrastado con un candado y la indicación "do not share". El mensaje "¿COMPARTIR MEMES? SÍ. ¿COMPARTIR CONTRASEÑAS? ¡JAMÁS!" y el texto complementario explican que las contraseñas son como llaves de casa y deben mantenerse personales.	No compartir credenciales (Figura 26)
8	Tema: Deepfakes, desinformación y verificación de fuentes	Sensibilizar sobre deepfakes y noticias falsas, promoviendo la verificación previa a compartir información. Duración: 30–60 segundos. Formato: viñeta comparativa antes/después.	Se muestran dos rostros del mismo personaje, uno real y otro tipo deepfake, con un símbolo de alerta entre ambos. El mensaje "DEEPFAKES Y FAKE NEWS: NO TODO LO QUE VES ES REAL" y las instrucciones de usar fuentes confiables y fact-checkers orientan al escepticismo informado.	Deepfakes, desinformación y verificación de fuentes (Figura 27)
9	Tema: Huella digital y redes sociales responsables	Promover el cuidado de la información publicada en redes, la configuración de privacidad y el impacto reputacional. Duración: 30–60 segundos. Formato: composición de íconos de redes y huella digital.	Una gran huella digital se combina con iconos de redes sociales y mensajes. El texto "CUIDADO CON LO QUE PUBLICAS: ¡INTERNET NUNCA OLVIDA!" y las recomendaciones para pensar antes de publicar y configurar privacidad refuerzan la gestión responsable de la identidad digital.	Huella digital y redes sociales responsables (Figura 28)
10	Tema: Seguridad en dispositivos móviles	Destacar que el teléfono es una "oficina en el bolsillo" y requiere medidas específicas de protección. Duración: 30–60 segundos. Formato: imagen centrada en smartphone.	La ilustración de un móvil con huella biométrica y símbolos de candado y escudo resalta la protección. El mensaje "DISPOSITIVOS MÓVILES: TU OFICINA EN EL BOLSILLO" se acompaña de acciones como bloquear el celular, usar biometría y evitar apps de origen dudoso.	Seguridad en dispositivos móviles (Figura 29)

Mes	Elemento de Diseño	Descripción del Diseño	Implementación en el Prototipo	Evidencia Visual (Figura)
11	Tema: Manejo de archivos sospechosos y malware	Prevenir la apertura de archivos adjuntos o descargas sospechosas, promoviendo la consulta a TI y el uso de antivirus. Duración: 30–60 segundos. Formato: contraste archivo malicioso vs archivo protegido.	Dos "carpetas" personificadas, una maliciosa y otra protegida con escudo, simbolizan el riesgo. El título "¿TE LLEGÓ UN ARCHIVO RARO? ¡NO LO ABRAS, NI POR CURIOSIDAD!" y el texto explican que la curiosidad puede causar incidentes y recomiendan escanear con antivirus y consultar a TI.	Manejo de archivos sospechosos y malware (Figura 30)
12	Tema: Respaldos y continuidad del negocio	Enfatizar la importancia de copias de seguridad periódicas y del uso de servicios de backup confiables. Duración: 30–60 segundos. Formato: metáfora de videojuegos ("save game").	Un gran botón "Save" rodeado de iconos de candado, carpeta y nube refuerza el concepto de copia de seguridad. El texto "RESPALDOS: TU 'SAVE GAME' EN LA VIDA REAL" conecta el hábito de guardar partidas con la rutina de hacer backups y proteger el trabajo diario.	Respaldos y continuidad del negocio (Figura 31)

Nota: Los autores

Presentación visual del prototipo del material de microcontenidos.

Valor de la información como activo (Figura 20)

Este microcontenido muestra la información como un tesoro (cofre, monedas, documentos y tecnología), reforzando la idea de que es un activo crítico que debe protegerse por todos y busca que los colaboradores identifiquen como suyo este tesoro para fomentar su compromiso con la seguridad.

Figura 20

Valor de la información como activo

Nota. Los Autores

Colaborador como héroe de la seguridad (Figura 21)

La pieza usa la metáfora de un superhéroe con escudo de candado para presentar a cada colaborador como “héroe digital” responsable de cuidar la información día a día.

Figura 21

Colaborador como héroe de la seguridad

Nota. Los Autores

Contraseñas fuertes y gestión segura (Figura 22)

Se representa el escudo del Capitán América como símbolo de contraseña robusta, conectando buenas prácticas (longitud, complejidad, gestores) con una imagen fácil de recordar.

Figura 22

Contraseñas fuertes y gestión segura

Nota. Los Autores

Prevención de phishing y correos sospechosos (Figura 23)

La ilustración tipo “Among Us” sitúa al usuario frente a impostores ocultos en el correo, motivando a desconfiar de enlaces dudosos y reportar antes de hacer clic.

Figura 23

Prevención de phishing y correos sospechosos

Nota. Los Autores

Actualización de software y dispositivos (Figura 24)

Se contrasta un equipo desactualizado con uno moderno para enfatizar que aplicar parches y actualizaciones es una defensa clave frente a vulnerabilidades

Figura 24

Actualización de software y dispositivos

Nota. Los Autores

Uso seguro de redes Wi-Fi públicas (Figura 25)

La escena del colaborador en un café con iconos de riesgo destaca que las Wi-Fi abiertas no son seguras y propone usar VPN o redes confiables.

Figura 25

Uso seguro de redes Wi Fi públicas

Nota. Los Autores

No compartir credenciales (Figura 26)

Mediante un contraste lúdico entre compartir memes y no compartir contraseñas, se refuerza que las credenciales son personales e intransferibles.

Figura 26

No compartir credenciales

Nota. Los Autores

Deepfakes, desinformación y verificación de fuentes (Figura 27)

Dos rostros (real y deepfake) alertan sobre contenidos manipulados y recuerdan la necesidad de verificar fuentes antes de creer o reenviar información.

Figura 27

Deepfakes, desinformación y verificación de fuentes

Nota. Los Autores

Huella digital y redes sociales responsables (Figura 28)

La huella digital combinada con íconos de redes ilustra que “internet no olvida” e invita a pensar antes de publicar y a configurar la privacidad.

Figura 28

Huella digital y redes sociales responsables

Nota. Los Autores

Seguridad en dispositivos móviles (Figura 29)

Un smartphone con símbolos de candado y biometría comunica que el celular es una “oficina en el bolsillo” que requiere bloqueo, biometría y apps confiables.

Figura 29

Seguridad en dispositivos móviles

Nota. Los Autores

Manejo de archivos sospechosos y malware (Figura 30)

La comparación entre carpeta maliciosa y protegida recuerda no abrir adjuntos extraños por curiosidad y consultar a TI ante dudas

Figura 30

Manejo de archivos sospechosos y malware

Nota. Los Autores

Respaldos y continuidad del negocio (Figura 31)

El gran botón “Save” y la metáfora del “save game” conectan el hábito de guardar partidas con la importancia de realizar copias de seguridad periódicas.

Figura 31

Respaldos y continuidad del negocio

Nota. Los Autores

Etapas del PCSI posteriores al alcance del proyecto

El diseño del Plan de Concientización en Seguridad de la Información (PCSI) realizado por los investigadores para la “mediana empresa de tecnología” ha establecido ya un conjunto robusto de elementos estructurales que permiten pasar de la fase de análisis y diseño a la fase de desarrollo, implementación, evaluación y mejora continua del programa, en coherencia con las recomendaciones de los capítulos 4 (CPLP Development and Implementation) y 5 (CPLP Assessment and Improvement) de la NIST SP 800-50r1 (NIST, 2024). En esta sección se describe cómo la “mediana empresa de tecnología” debe ejecutar en la practica lo ya diseñado en el proyecto, operativizando los insumos definidos.

En primer lugar, el proyecto ya ha dejado establecidos los principales componentes de gobierno y diseño del PCSI. Adicionalmente, se ha definido la alineación del PCSI con el procedimiento Capacitación y entrenamiento, con el fin de integrarlo al sistema institucional de formación, y se han identificado las herramientas disponibles para su despliegue. Sobre esta base, las actividades futuras que se describen a continuación se orientan exclusivamente a ejecutar lo ya diseñado.

Desde la perspectiva del desarrollo e implementación (capítulo 4 de la NIST SP 800-50r1), el primer bloque de actividades que La “mediana empresa de tecnología” debe realizar consiste en convertir el diseño instruccional del PCSI en materiales concretos dentro de las herramientas definidas. Transformación & Desarrollo (T&D), en coordinación con el Infraestructura, debe tomar la estructura de contenidos definida en los Capítulos 1 a 4 y construir, en el LMS Proporcionado por la ARL, los módulos de formación, cuestionarios, rutas de aprendizaje por audiencia y criterios de aprobación, siguiendo la matriz de audiencias y contenidos ya establecida en el proyecto. El coordinador de IT debe validar la exactitud técnica de los contenidos y la coherencia con las políticas internas y el SGSI, mientras que la Dirección General (A&F) aprueba su publicación, de acuerdo con la gobernanza del PCSI.

En paralelo, el área de Mercadeo, apoyada por T&D y e Infraestructura, debe materializar las campañas de concientización y los microcontenidos definidos en el cronograma anual. Para ello, produce las piezas gráficas y textuales para la cartelera digital y para los microcontenidos que se publicarán en Teams y Viva Engage, alineadas a los temas, meses y brechas que el proyecto ya calendarizó. Estas piezas no implican redefinir contenidos, sino traducir los mensajes ya establecidos en el diseño a formatos comunicacionales accesibles y consistentes, en línea con la recomendación de NIST de emplear múltiples canales y formatos para reforzar el aprendizaje y facilitar la transferencia al comportamiento (NIST, 2024).

Otro componente crítico del desarrollo, previsto explícitamente en el cronograma del PCSI, es la simulación de phishing. El equipo de Infraestructura Tecnológica debe configurar la herramienta de simulación (GoPhish), definiendo las plantillas de correo, la población objetivo y el calendario, de manera coherente con el subcapítulo “Manejo seguro del correo electrónico y navegación – Reconocimiento y reporte de phishing” programado para el Mes 7. Esta configuración debe alinearse con la línea base obtenida en la campaña de phishing de La “Empresa Consultora en seguridad”, de forma que se evalúe comparativamente la evolución del CTR y de los reportes de phishing, tal como lo plantean los KPIs del PCSI, y siguiendo la guía de NIST sobre el uso de simulaciones como herramienta de práctica y medición del cambio de comportamiento (NIST, 2024).

Una vez construidos los materiales en el LMS, las piezas de campaña y la configuración de la simulación, la fase de implementación se centra en ejecutar sistemáticamente el cronograma que el proyecto definió. T&D debe incorporar formalmente el PCSI al Plan de Formación anual regulado por el procedimiento Capacitación y entrenamiento, sometiéndolo a aprobación de la Dirección y asegurando que las actividades del PCSI aparezcan como parte del plan corporativo de capacitación (“mediana empresa de tecnología”, 2024, Capacitación y entrenamiento, 2024). Con el plan aprobado, T&D debe programa la apertura de los módulos en Proporcionado por la ARL y cada mes emitir las citaciones y recordatorios dentro de los plazos

definidos en Capacitación y entrenamiento, mientras que Mercadeo publica las piezas en la cartelera digital y en Teams/Viva Engage según el calendario de campañas y microcontenidos. El equipo de Infraestructura Tecnológica ejecuta la simulación de phishing en el mes previsto y monitorea su ejecución. Los líderes de proceso, por su parte, cumplen la función que el proyecto les asignó: asegurar la participación efectiva de sus equipos, facilitar tiempos para el curso y reforzar, en el contexto de sus procesos, los mensajes clave del PCSI (NIST, 2024).

Dentro de esa implementación continua, el proceso de Onboarding y reinducción cobra especial relevancia. T&D debe integrar el “paquete mínimo de concientización” definido en las políticas del PCSI dentro del proceso de inducción institucional, de modo que todo nuevo colaborador, contratista o personal en misión complete en sus primeros días los módulos fundamentales sobre riesgos clave, políticas básicas de seguridad, responsabilidades individuales y tratamiento de datos personales (“On Boarding”). De igual forma, la reinducción anual, ya regulada por Capacitación y entrenamiento, debe utilizar contenidos del PCSI para asegurar que el personal con antigüedad superior a seis meses reciba un refuerzo sistemático alineado a los riesgos y políticas vigentes (“mediana empresa de tecnología”, 2024; NIST, 2024).

La ejecución del PCSI implica también aplicar de manera consistente el esquema de cumplimiento y consecuencias previsto en el propio programa. Transformación & Desarrollo y el Coordinador de IT deben aprovechar los reportes del LMS y las métricas definidas para identificar casos de no participación, participación tardía o resultados deficientes en las actividades obligatorias, y reportarlos a la Dirección General y a los líderes de proceso conforme a las políticas de cumplimiento. Las medidas correctivas iniciales y, en caso de reincidencia, las medidas disciplinarias o contractuales descritas en el PCSI, deben aplicarse siguiendo los procedimientos internos de la “mediana empresa de tecnología”, reforzando así la idea de que la concientización es una obligación organizacional y no una actividad opcional, en concordancia con ISO/IEC 27001:2022 (ISO, 2022).

En cuanto a la evaluación y mejora (capítulo 5 de la NIST SP 800-50r1), el proyecto ha definido ya un conjunto de KPIs que sirven como base para la medición de la eficacia del PCSI: CTR (tasa de clics) en simulaciones de phishing, porcentaje de reportes durante dichas simulaciones, porcentaje de hallazgos de uso de herramientas no autorizadas (como WeTransfer) y de incumplimiento de la política de escritorio y pantalla limpios, así como el porcentaje de finalización de la capacitación en el LMS. La tarea de la “mediana empresa de tecnología” en esta fase es configurar las fuentes de datos que alimentarán cada KPI y operar la medición según las fórmulas y metas ya fijadas.

Para el KPI de finalización en LMS, T&D debe configurar en Proporcionado por la ARL reportes estándar que permitan conocer, por curso, audiencia y periodo, el número de inscritos y el número de colaboradores que completan el 100 % de la capacitación, de manera que se pueda calcular el porcentaje de finalización y contrastarlo con la meta del 100 %, integrándolo además con el indicador de cobertura definido en el procedimiento Capacitación y entrenamiento (“mediana empresa de tecnología”, 2024). Para los KPIs relacionados con phishing (CTR y reportes), el Coordinador de TI deberán extraer de la plataforma de simulación los datos de clics y reportes obtenidos en el ejercicio anual, comparándolos con la línea base del informe de la “Empresa Consultora en seguridad” y verificando si se cumple la meta de reducción de CTR por debajo del 4 % y la aparición de reportes mayores a 0 %. En cuanto a los hallazgos de escritorio limpio y uso de herramientas no autorizadas, T&D y el coordinador de IT deben coordinar con Auditoría interna y con los proveedores de auditoría para recibir o replicar los resultados de muestreos análogos a los de 2024, y recalcular los indicadores de hallazgos sobre la muestra, comparando con la línea base del 10 % y las metas de reducción.

Con estas fuentes de datos definidas, deben construir un tablero de indicadores del PCSI, que puede apoyarse en listas de SharePoint y visualizaciones en Power BI u otra herramienta disponible, mostrando la evolución mensual o trimestral de cada KPI: porcentaje de finalización en LMS, CTR de phishing, porcentaje de reportes, porcentaje de hallazgos de

escritorio y de uso de herramientas no autorizadas, así como cualquier otro indicador que el proyecto haya vinculado a la medición del cambio de comportamiento. Este tablero cumple la función recomendada por NIST de proporcionar una vista consolidada del desempeño del programa y de servir de insumo para la toma de decisiones en la revisión ejecutiva (NIST, 2024).

Sobre la base de este tablero, T&D y el equipo de Infraestructura deben elaborar informes de avance con la periodicidad ya alineada al modelo institucional: informes trimestrales, coherentes con el seguimiento al plan de formación del procedimiento Capacitación y entrenamiento, y un informe anual específico del PCSI. Los informes trimestrales deben presentar los resultados de participación y finalización en los módulos del PCSI, el comportamiento de los KPIs disponibles en ese momento (por ejemplo, avance de finalización, progresos parciales antes o después de la simulación de phishing) y las observaciones relevantes para cada proceso; estos informes se socializan con los líderes de proceso y con la Dirección General, según lo previsto en la Matriz RACCI. El informe anual, por su parte, debe integrar todos los resultados: tasas de finalización, resultados de la simulación de phishing, hallazgos en escritorio limpio y uso de herramientas, incidencias asociadas al factor humano y grado de cumplimiento de los objetivos SMART del PCSI, tal como se planteó en el proyecto.

Con los resultados cuantitativos y cualitativos consolidados, la mejora continua se concreta a través de la revisión por la dirección y de la toma de decisiones sobre ajustes de ejecución. El Director General, en su rol definido por el PCSI y por ISO/IEC 27001:2022, debe convocar al menos una reunión anual de revisión específica del PCSI, idealmente articulada con la revisión del SGSI, en la que participen CISO, T&D, Mercadeo y líderes de proceso. En esta reunión se analizan los KPIs, se comparan con las metas y con las líneas base (phishing, hallazgos de auditoría, finalización de cursos) y se decide qué aspectos del programa deben mantenerse, reforzarse o ajustarse para el ciclo siguiente. Los ajustes que se acuerdan no buscan redefinir la estructura del PCSI, sino optimizar su ejecución dentro del mismo marco

diseñado: por ejemplo, repetir o adelantar una simulación de phishing si el CTR no disminuye suficientemente, añadir microcontenidos de refuerzo en los meses posteriores a un resultado adverso, o intensificar mensajes sobre escritorio limpio y uso de repositorios autorizados si los hallazgos de auditoría se mantienen por encima de las metas.

Finalmente, todas las actividades de evaluación y mejora deben quedar documentadas. T&D y el Coordinador de IT registran en los repositorios institucionales de SharePoint los informes trimestrales y el informe anual del PCSI, las actas de revisión, las decisiones tomadas y las acciones correctivas o preventivas definidas, utilizando la lógica de registros que ya maneja el procedimiento Capacitación y entrenamiento y el SGSI. Esta evidencia permite demostrar, ante auditorías internas y externas, que el PCSI no solo fue diseñado, sino que se desarrolla, se implementa y se mejora conforme al ciclo de vida, cerrando el ciclo entre diseño, ejecución y mejora continua del plan de concientización en seguridad de la información de la “mediana empresa de tecnología”. (NIST, 2024).

Resultados

Enfoque de los Resultados en la Investigación Aplicada

Los resultados obtenidos corresponden al diseño y estructuración de un Plan de Concientización en Seguridad de la Información (PCSI) para la “mediana empresa de tecnología”, desarrollado como investigación aplicada con énfasis en las fases de planeación, análisis y diseño de un plan de concientización en seguridad de la información , siguiendo el marco de la NIST SP 800-50r1 y su adaptación del ciclo ADDIE (análisis, diseño, desarrollo, implementación y evaluación) (National Institute of Standards and Technology [NIST], 2024).

En coherencia con este enfoque, los resultados no se expresan en términos de cambios ya observados en el comportamiento de las personas, sino en productos concretos de diseño que dejan a la organización en capacidad de implementar el PCSI, medir su desempeño y, en una fase posterior, verificar empíricamente el efecto sobre el riesgo humano y la capacidad de identificar amenazas (NIST, 2024).

Asimismo, el diseño se mantuvo alineado con los requisitos de competencia, concientización y evidencia documental establecidos por ISO/IEC 27001:2022 (cláusulas 7.2, 7.3, 7.5, 9.1 y 9.3) y con el control 6.3 de ISO/IEC 27002:2022 sobre concientización, educación y capacitación en seguridad de la información, asegurando que el PCSI pueda ser utilizado como apoyo directo al SGSI y a su esquema de auditoría y mejora continua (International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC], 2022).

Resultados Frente al Objetivo 1: Análisis del Estado Actual y Brechas de Concientización

El primer objetivo específico buscaba analizar el estado actual de la concientización en seguridad de la información en la “mediana empresa de tecnología”, utilizando como insumos incidentes, campañas de phishing y auditorías, con el fin de orientar la planeación del PCSI. Para ello se aplicó la fase de análisis propuesta por la NIST SP 800-50r1, que sugiere partir de evidencias internas, comparar el estado actual con el comportamiento esperado según políticas y requisitos, e identificar brechas de conocimiento, habilidad o hábito (NIST, 2024).

Con base en el informe de auditoría de la “empresa auditora” sobre aspectos de seguridad de la información y en la planilla de validación asociada, se identificó que el 10 % de los equipos revisados presentaba incumplimientos a la política de escritorio y pantalla limpia, así como uso de herramientas externas no autorizadas (WeTransfer) para transferir información, lo que evidenció dos brechas claras: a) incumplimiento de prácticas de escritorio/pantalla limpia y b) uso de repositorios no oficiales frente a los lineamientos de uso de activos y respaldo de información (“empresa auditora”, 2024; “mediana empresa de tecnología”, 2021, Política de uso de activos y recursos de teleinformática; “mediana empresa de tecnología”, 2023, Política de escritorio y pantalla limpia).

A partir del informe de phishing ejecutado por la “Empresa Consultora en seguridad”, se estableció una línea base conductual: 20 % de apertura del correo señuelo, 4 % de clic en el enlace malicioso y 0 % de reportes por los canales formales. Esto permitió caracterizar una tercera brecha, relacionada con el reconocimiento y manejo de correos maliciosos: existe un

grupo de colaboradores que sigue interactuando con mensajes sospechosos y, además, prácticamente nadie adopta el hábito de reportarlos como incidente, a pesar de contar con un procedimiento formal de gestión de incidentes (“Empresa Consultora en seguridad”, 2024; “mediana empresa de tecnología”, 2024, Gestión de Incidentes de SI).

Por último, el análisis de la evaluación interna de protección de datos personales mostró una alta participación y un buen nivel de aciertos en conceptos básicos (habeas data, definición de dato personal), pero también una brecha específica: aproximadamente el 25 % de los colaboradores presentó un desempeño bajo en temas críticos como sanciones, principio de responsabilidad demostrada y claridad sobre los responsables internos de protección de datos, consolidando una cuarta brecha focalizada en el entendimiento profundo de obligaciones y consecuencias en materia de datos personales (“mediana empresa de tecnología”, 2024, informe ejecutivo evaluación protección datos personales).

La aplicación sistemática del enfoque propuesto por la NIST SP 800-50r1 permitió traducir estos hallazgos en cuatro brechas de concientización directamente vinculadas a políticas internas y controles ISO/IEC 27002 (escritorio limpio, uso de repositorios, comportamiento ante phishing y conocimientos sobre datos personales), dejando claramente definido el estado actual sobre el cual el PCSI debe actuar (NIST, 2024; ISO/IEC, 2022).

Resultados Frente al Objetivo 2: Lineamientos, Alcance, Responsabilidades y Audiencias del PCSI

El segundo objetivo específico buscaba definir los lineamientos, el alcance, las responsabilidades y las audiencias del PCSI como base para su diseño e implementación futura. Los resultados obtenidos se concretan en un bloque normativo y de gobernanza que traduce las recomendaciones del NIST SP 800-50r1 y los requisitos de ISO/IEC 27001/27002 en un marco claro para la “mediana empresa de tecnología” (NIST, 2024; ISO/IEC, 2022; ISO/IEC 27002:2022).

En primer lugar, se definió el propósito y el alcance organizacional del PCSI, estableciendo que cubre a todo el personal y terceros con acceso a activos de información, con segmentación por rol y exposición al riesgo (usuarios generales, responsables de datos sensibles, personal técnico/Infraestructura y mandos/terceros críticos). Esto permite que la concientización se enfoque en comportamientos relevantes y diferenciados, tal como sugiere NIST al hablar de segmentación por audiencias y alineación con el contexto del negocio (NIST, 2024).

En segundo lugar, se formalizaron políticas específicas que rigen el PCSI: mandato y obligatoriedad para todo el personal; periodicidad (campaña anual, refuerzos semestrales y microcontenidos mensuales); integración del onboarding como punto de entrada para nuevos colaboradores; y coherencia entre canales (LMS, Teams/Viva Engage y cartelera digital) con registro oficial de cumplimiento concentrado en el LMS Proporcionado por la ARL. Estos lineamientos responden a las recomendaciones de ISO/IEC 27002:2022 sobre planificación, frecuencia y cobertura de actividades de concientización, y al énfasis del NIST en campañas continuas y multimodales (ISO/IEC, 2022; NIST, 2024).

En tercer lugar, se definió una estructura clara de roles y responsabilidades para la gobernanza del PCSI: la Dirección General como patrocinador y aprobador del plan y los recursos; Transformación & Desarrollo como integrador del PCSI al sistema de formación institucional (incluido el procedimiento Capacitación y entrenamiento; Infraestructura Tecnológica/CISO como responsable del contenido temático y de la alineación con el SGSI; Mercadeo como líder de la comunicación y el diseño de piezas; y los usuarios como responsables de completar rutas, aplicar prácticas seguras y reportar incidentes. Este esquema se complementó con una matriz RACCI que detalla quién aprueba, ejecuta, consulta e informa en cada actividad clave del ciclo de vida del PCSI (“mediana empresa de tecnología”, 2024, Capacitación y entrenamiento; NIST, 2024).

Por último, se elaboró una síntesis de audiencias donde se describe para cada grupo: su rol, principales riesgos asociados, tipo de material requerido y prioridad, lo que facilita la trazabilidad entre las brechas identificadas, las necesidades de concientización y las intervenciones propuestas, tal como recomienda la NIST SP 800-50r1 en su fase de análisis de audiencias (NIST, 2024).

Resultados Frente al Objetivo 3: Diseño de la Estructura Anual del PCSI

El tercer objetivo buscaba diseñar la estructura anual del PCSI, definiendo campañas, acciones de refuerzo y microcontenidos para fortalecer la cultura de seguridad de la información. El resultado principal es un cronograma de 12 meses que integra, de forma coherente, contenidos en LMS, simulaciones de phishing, carteleras digitales y microcontenidos, todos mapeados a brechas específicas, audiencias y KPIs (NIST, 2024).

En este diseño se estructuraron cuatro capítulos de contenido para el curso principal en el LMS (concientización básica, buenas prácticas y controles, manejo de incidentes y reporte, y principios de tratamiento de datos personales), cada uno con subcapítulos que responden directamente a las brechas detectadas: por ejemplo, “Escritorio y pantalla limpia” orientado a cerrar la Brecha 1; “Uso correcto de repositorios institucionales” para la Brecha 2; “Manejo seguro del correo y reconocimiento de phishing” para la Brecha 3; y “Tratamiento de datos personales” para la Brecha 4 (“empresa auditora”, 2024; “Empresa Consultora en seguridad”, 2024; “mediana empresa de tecnología”, 2024, Política de tratamiento de datos personales y Tratamiento de Datos Personales).

El cronograma anual fija, mes a mes, el avance esperado en el LMS (porcentaje de finalización mínimo por capítulo), la ejecución de al menos una simulación de phishing, la publicación de microcontenidos mensuales alineados al tema del mes y dos campañas de cartelera digital de seis meses cada una. Esta planificación incorpora de manera explícita los principios de repetición espaciada y refuerzo contextual que NIST considera buenas prácticas para consolidar hábitos, sin exceder las capacidades presupuestales de la “mediana empresa

de tecnología” al apoyarse en herramientas ya disponibles (Microsoft 365, Proporcionado por la ARL, TVBox y software libre como GoPhish) (NIST, 2024).

Además, se diseñaron documentos específicos de apoyo: un documento de diseño instruccional para el curso en LMS, que detalla objetivos, estructura por capítulos, estrategia de instrucción, modalidad de entrega y configuración de evaluaciones; y un documento de diseño para los materiales de refuerzo (videos de cartelera y microcontenidos), que define objetivos, mensajes clave, estilo visual y plan de exhibición, asegurando la coherencia entre el curso formal, los refuerzos visuales y las políticas internas de la “mediana empresa de tecnología” (“mediana empresa de tecnología”, 2024, Capacitación y entrenamiento; ISO/IEC, 2022; NIST, 2024).

Resultados Frente al Objetivo 4: Metodología de Evaluación y KPIs del PCSI

El cuarto objetivo específico consistía en establecer la metodología de evaluación del PCSI, de manera que la organización cuente con una base para valorar su desempeño en el tiempo. Como resultado, se definió un conjunto de indicadores clave (KPIs) y criterios de evaluación alineados con las recomendaciones de la NIST SP 800-50r1 para medir participación, aprendizaje, comportamiento y resultados, así como con los requisitos de medición y evaluación del desempeño de ISO/IEC 27001:2022 (NIST, 2024; ISO/IEC, 2022).

Se definieron, entre otros, los siguientes KPIs directamente vinculados a las brechas identificadas:

CTR (tasa de clics en simulaciones de phishing). con línea base del 4 % y meta de reducción por debajo de ese valor, para evidenciar mejora en la capacidad de reconocer y evitar correos maliciosos.

Reportes de Incidentes por Pruebas de Phishing. con línea base 0 % y meta “> 0 %”, para impulsar la cultura de reporte.

Hallazgos por uso de Herramientas no Autorizadas. con base en el 10 % de hallazgos en auditoría y meta de reducción por debajo de ese valor.

Hallazgos de Escritorio y Pantalla Limpia. también con una línea base del 10 % y meta de reducción por debajo de ese umbral.

% de Finalización de la Capacitación en el LMS. con meta del 100 % para la población objetivo, como indicador de cobertura del PCSI (“Empresa Consultora en seguridad” S.A., 2024; “empresa auditora”, 2024; “mediana empresa de tecnología”, 2024).

Adicionalmente, se propuso una metodología de evaluación que combina: a) exámenes autocalificables por unidad en el LMS con umbral de aprobación del 80 %; b) análisis de métricas de participación y avance (inscritos, finalización, intentos, tiempos); y c) consolidación periódica de resultados en tableros de seguimiento para la revisión por la dirección, en línea con el enfoque de NIST de medir tanto insumos de aprendizaje como cambios de comportamiento y resultados en el riesgo (NIST, 2024).

Esta metodología quedó organizada dentro de una fase de “Evaluación y mejora” del ciclo de vida del PCSI, con actividades y horas-hombre asociadas (diseño y actualización de cuestionarios, consolidación de resultados, definición de indicadores y elaboración de informe ejecutivo anual), lo que facilita su ejecución futura y su integración con las revisiones del SGSI (“mediana empresa de tecnología”, 2024, Capacitación y entrenamiento; ISO/IEC, 2022).

Resultados Frente al Objetivo 5: Propuesta de Plan de Implementación del PCSI

El quinto objetivo específico buscaba elaborar una propuesta de plan de implementación para el PCSI, organizada de forma estructurada y coherente con el diseño, teniendo en cuenta las restricciones presupuestales de la “mediana empresa de tecnología”. El resultado más visible es la estimación de un presupuesto en horas-hombre, desagregado por fases del ciclo de vida del programa (planeación, análisis y diseño, desarrollo e implementación, evaluación y mejora), que suma 146 horas-hombre anuales distribuidas de la siguiente manera: 5 % planeación y estrategia, 10 % análisis y diseño, 71 % desarrollo e implementación y 14 % evaluación y mejora (NIST, 2024).

Este desglose muestra que la mayor inversión de tiempo se concentra en la ejecución sostenida del programa (sesiones, campañas, simulación de phishing, gestión de convocatorias y archivo de evidencias), coherente con la visión de NIST de que un PCSI efectivo es un sistema vivo que requiere operación continua más que esfuerzos puntuales (NIST, 2024). Al mismo tiempo, la explicitación de roles responsables en cada actividad hace posible que la "mediana empresa de tecnología" pueda priorizar y calendarizar las cargas de trabajo de TI, T&D, A&F y líderes de proceso.

Complementariamente, se documentaron instrucciones operativas para la configuración del curso en el LMS proporcionado por la ARL (creación de curso, registro de objetivos, capítulos y unidades, configuración de exámenes y criterios de aprobación) y para la publicación de videos en las carteleras digitales usando la plataforma de administración de dispositivos (MDM Scalefusion), de forma que la transición del diseño a la ejecución cuente con pasos concretos y repetibles ("mediana empresa de tecnología", 2024, Capacitación y entrenamiento; ISO/IEC, 2022).

En conjunto, estos elementos constituyen un plan de implementación de bajo costo monetario, que se apalanca en herramientas ya existentes y deja claramente definidos los esfuerzos en tiempo humano requeridos para poner en marcha el PCSI sin depender de adquisiciones tecnológicas adicionales, respetando las restricciones financieras señaladas para el periodo 2025 ("mediana empresa de tecnología", 2024; NIST, 2024).

Contrastación de la Hipótesis de Investigación

La hipótesis de investigación h1 plantea que el diseño de un plan de concientización en seguridad de la información, fundamentado en la guía NIST SP 800-50r1 y en evidencias internas sobre brechas de comportamiento de los colaboradores de la "mediana empresa de tecnología", permite que, al ejecutar las fases de planeación, análisis y diseño, se definan claramente los objetivos, las audiencias, los contenidos y las métricas iniciales necesarias para estructurar la implementación y evaluación futura del plan. Esta contrastación se realiza sin

considerar fases más allá del alcance del proyecto como desarrollo, implementación ni evaluación empírica (NIST, 2024).

En primer lugar, el documento demuestra que el diseño del PCSI se fundamenta explícitamente en la guía NIST SP 800-50r1, adoptando su enfoque de programa de aprendizaje en ciberseguridad y privacidad, así como el ciclo de vida basado en las fases de planificar, analizar y diseñar, que constituyen el alcance de la investigación. La guía orienta la definición de objetivos de aprendizaje, la segmentación de audiencias, la identificación de brechas y la propuesta de métricas, lo que permite afirmar que el marco metodológico del plan está alineado con las recomendaciones de NIST para la planificación y el diseño de programas de concientización (NIST, 2024).

En segundo lugar, el proyecto utiliza evidencias internas para identificar brechas de comportamiento en temas críticos como escritorio y pantalla limpia, uso de repositorios no oficiales, respuesta ante correos maliciosos y protección de datos personales. Estas evidencias provienen de informes de auditoría, campañas de phishing y evaluaciones de capacitación, que se analizan mediante técnicas descriptivas y análisis de brechas. A partir de ellas se derivan necesidades formativas concretas, que sirven de base para definir los objetivos del PCSI y la estructura de contenidos, cumpliendo así con la parte de la hipótesis que alude al uso de evidencias internas sobre brechas de comportamiento (“empresa auditora”, 2024; “Empresa Consultora en seguridad”, 2024; “mediana empresa de tecnología”, 2024; NIST, 2024).

En tercer lugar, los resultados muestran que, durante las fases de planeación, análisis y diseño, se logra definir de manera explícita y documentada los objetivos del plan, la segmentación de audiencias, los contenidos generales y un conjunto de métricas iniciales. El plan incluye objetivos generales y específicos del PCSI, objetivos de aprendizaje del curso en el LMS, la caracterización de audiencias según rol y exposición al riesgo, un mapa de capítulos y unidades temáticas, y la propuesta de KPIs asociados a las brechas identificadas, como el CTR de phishing y la reducción de hallazgos en auditoría. Estos elementos dejan preparado un

marco estructural que permite a la “mediana empresa de tecnología” organizar, en fases futuras, la implementación y evaluación del plan, aunque dichas fases no forman parte del alcance de esta investigación (NIST, 2024).

En consecuencia, la hipótesis se sostiene en el nivel de diseño: la investigación demuestra que, apoyándose en NIST SP 800-50r1 y en evidencias internas, es posible definir con claridad los componentes estructurales del PCSI necesarios para orientar una implementación y evaluación posterior del plan de concientización en seguridad de la información de la “mediana empresa de tecnología”.

Síntesis Integradora de los Resultados

En síntesis, los resultados de esta investigación aplicada muestran que es posible, a partir de evidencias internas y marcos de referencia internacionales, construir un PCSI robusto y alineado con el SGSI de la “mediana empresa de tecnología”, aun en un contexto de restricciones presupuestales. Se logró pasar de un conjunto disperso de hallazgos (phishing, auditorías, evaluaciones de datos personales) y documentos internos a un plan de concientización planificado, con objetivos claros, lineamientos formales, estructura anual de actividades, metodología de evaluación y plan de implementación en horas-hombre (“Empresa Consultora en seguridad”, 2024; “empresa auditora”, 2024; “mediana empresa de tecnología”, 2024; NIST, 2024).

El aporte central del proyecto radica en haber convertido la concientización en seguridad de la información en un proceso estratégico, medible y adaptable, tal como propone la NIST SP 800-50r1, y en haberlo integrado explícitamente con las exigencias de ISO/IEC 27001:2022 e ISO/IEC 27002:2022 sobre competencias, toma de conciencia, documentación y mejora continua, dejando a la “mediana empresa de tecnología” con un mapa claro para avanzar de la fase de diseño a la ejecución y a la posterior evaluación de resultados (NIST, 2024; ISO/IEC 27001:2022; ISO/IEC 27002:2022).

Conclusiones y Recomendaciones

Conclusiones

La Guía NIST SP 800-50r1 es Adecuada Como Marco para el Diseño del PCSI de La "mediana empresa de tecnología"

El uso sistemático de la NIST SP 800-50r1 permitió estructurar el proceso de planeación, análisis y diseño del Plan de Concientización en Seguridad de la Información (PCSI) de forma coherente, trazable y alineada con el riesgo, integrando diagnóstico, segmentación de audiencias, definición de contenidos, selección de métricas y planificación de la mejora continua (NIST, 2024).

Se comprobó que el enfoque propuesto por este marco facilita pasar de hallazgos dispersos (phishing, auditorías, evaluaciones internas) a un programa de aprendizaje organizado, con objetivos claros y actividades encadenadas, lo que respalda la hipótesis de que su adopción permite definir el alcance, objetivos, requisitos, cobertura y brechas que el plan busca mitigar.

La Organización Cuenta con Evidencias Suficientes para Orientar un PCSI Basado en Riesgos

El análisis de la información disponible (campaña de phishing, auditoría, evaluación de protección de datos personales, controles y políticas internas) permitió identificar cuatro brechas de concientización directamente relacionadas con comportamientos críticos: incumplimiento de escritorio y pantalla limpia, uso de repositorios no oficiales, respuesta inadecuada ante correos maliciosos y lagunas en temas clave de datos personales ("empresa auditora", 2024; "Empresa Consultora en seguridad", 2024; "mediana empresa de tecnología", 2024).

Este resultado demuestra que la "mediana empresa de tecnología" dispone de insumos suficientes para orientar el PCSI hacia problemas reales y medibles, cumpliendo con la recomendación de NIST de construir el programa de aprendizaje sobre el contexto y los riesgos específicos de la organización (NIST, 2024).

El Diseño del PCSI Está Alineado con ISO/IEC 27001:2022 e ISO/IEC 27002:2022

El PCSI se estructuró de forma consistente con los requisitos de competencia, concientización, documentación y mejora continua de ISO/IEC 27001:2022, así como con el control 6.3 de ISO/IEC 27002:2022 sobre concientización, educación y capacitación en seguridad de la información (ISO/IEC, 2022).

Esta alineación se evidencia en:

La definición de objetivos medibles y vinculados al SGSI.

La integración con el procedimiento institucional de capacitación (Capacitación y entrenamiento).

La existencia de contenidos mapeados a políticas y controles internos.

La inclusión de métricas y evidencias aptas para auditoría.

Lo anterior permite afirmar que el PCSI diseñado puede operar como un mecanismo de soporte directo al SGSI y a los procesos de revisión por la dirección y auditoría interna.

Es Posible Estructurar un PCSI de Bajo Costo Aprovechando Capacidades Existentes

El proyecto demostró que, aun en un escenario financiero retador, es viable diseñar un PCSI robusto sin requerir inversiones significativas en nuevas herramientas, aprovechando: el LMS Proporcionado por la ARL, la suite Microsoft 365, la video cartelera existente y herramientas libres como GoPhish y editores de video (“mediana empresa de tecnología”, 2024).

El presupuesto en horas-hombre (146 horas anuales) mostró que la principal inversión recae en la operación sostenida (ejecución de actividades, campañas, simulaciones y gestión de evidencias), más que en el diseño puntual, coherente con la visión de la NIST SP 800-50r1 de un programa de aprendizaje vivo y continuo (NIST, 2024).

El PCSI Queda Preparado para Medir su Propio Desempeño e Integrarse al Ciclo de Mejora Continua

La definición de KPIs específicos (CTR de phishing, reportes, hallazgos de escritorio y repositorios, finalización de cursos) y de una metodología de evaluación que combina resultados del LMS, auditorías, simulaciones y reportes de incidentes deja a la “mediana empresa de tecnología” en condiciones de evaluar la efectividad del PCSI una vez sea implementado (“Empresa Consultora en seguridad” S.A., 2024; “empresa auditora”, 2024; “mediana empresa de tecnología”, 2024; NIST, 2024, NIST SP 800-50r1, secc. 5.1–5.3).

Aunque en esta etapa no se ejecuta la implementación ni se miden cambios de comportamiento, el diseño deja establecidos los mecanismos necesarios para cerrar el ciclo de mejora continua exigido por ISO/IEC 27001:2022 y recomendado por NIST (ISO/IEC, 2022; NIST, 2024).

La Hipótesis de Investigación se Sostiene en el Nivel de Diseño

La investigación confirma que el diseño de un Plan de Concientización en Seguridad de la Información (PCSI) para la “mediana empresa de tecnología” es viable y efectivo en sus fases de planeación, análisis y diseño. Al fundamentarse en la guía NIST SP 800-50r1 y en un riguroso análisis de evidencias internas sobre brechas de comportamiento de los colaboradores, el proyecto logró definir con claridad los elementos estructurales esenciales del PCSI. Esto incluye la formulación precisa de objetivos, la identificación y segmentación de audiencias clave, la estructuración de contenidos temáticos relevantes y la propuesta de métricas iniciales pertinentes. Estos resultados demuestran que el diseño elaborado proporciona una base sólida y bien articulada, indispensable para orientar y facilitar la futura implementación y evaluación del plan de concientización. Así, la hipótesis se valida plenamente en el ámbito del diseño, estableciendo un marco robusto para las etapas subsiguientes del ciclo de vida del PCSI (NIST, 2024).

Recomendaciones

Priorizar la Implementación del PCSI Como Iniciativa Estratégica del SGSI

Se recomienda que la alta dirección formalice la implementación del PCSI como una iniciativa prioritaria dentro del plan de trabajo del SGSI, vinculándolo explícitamente a los resultados de riesgo, cumplimiento y satisfacción de partes interesadas. Esto incluye aprobar el plan anual, asignar las horas-hombre estimadas y establecer su seguimiento en las revisiones por la dirección, tal como sugieren ISO/IEC 27001:2022 y NIST (ISO/IEC, 2022; NIST, 2024).

Implementar el PCSI de Forma Incremental, Empezando por las Brechas más Críticas

Dado que las brechas de escritorio y pantalla limpia, uso de repositorios no oficiales y comportamiento ante phishing están directamente asociadas a hallazgos de auditoría y a resultados de simulaciones, se sugiere que la primera oleada de implementación del PCSI se concentre en:

Desplegar los capítulos 1 y 2 del curso en LMS.

Ejecutar la primera simulación de phishing tomando la línea base ya existente.

Lanzar campañas y microcontenidos sobre phishing, escritorio limpio y repositorios oficiales.

Este enfoque incremental permite concentrar esfuerzos en los vectores de mayor impacto y demostrar resultados tempranos para generar confianza y apoyo interno, siguiendo el principio de priorización por riesgo propuesto por NIST (NIST, 2024).

Integrar el PCSI de Manera Explícita al Procedimiento Institucional de Capacitación

Es recomendable actualizar o complementar el procedimiento de Capacitación y entrenamiento (Capacitación y entrenamiento) para que el PCSI quede reconocido como un programa formal dentro del sistema de formación, incluyendo:

La obligatoriedad de los módulos de seguridad de la información en el onboarding.

La periodicidad de refuerzos y reinducciones en temas de seguridad.

La incorporación de KPIs del PCSI a los indicadores de capacitación (cobertura, calificación, cumplimiento del plan).

Esta integración asegurará coherencia entre el sistema de gestión de calidad, el SGSI y el PCSI, en línea con las expectativas de ISO/IEC 27001:2022 sobre competencia y toma de conciencia (“mediana empresa de tecnología”, 2024; ISO/IEC, 2022).

Consolidar la Gobernanza del PCSI Mediante un Comité Periódico

Se recomienda establecer un comité del PCSI con participación de Dirección General, CISO/Infraestructura, T&D y Mercadeo, que se reúna al menos trimestralmente para:

Revisar indicadores del PCSI (participación, resultados de evaluaciones, CTR de phishing, hallazgos de auditoría relacionados con conducta).

Analizar incidentes, vulnerabilidades y cambios normativos que deban reflejarse en contenidos.

Aprobar ajustes a cronogramas, campañas y materiales.

Este comité debe articularse con los espacios existentes de revisión del SGSI y del SGC, reforzando el liderazgo visible y la mejora continua que exigen tanto ISO/IEC 27001:2022 como NIST SP 800-50r1 (ISO/IEC, 2022; NIST, 2024).

Asegurar la Calidad Pedagógica y Técnica de los Contenidos Antes de su Publicación

Previo a la publicación de los cursos en LMS, videos de cartelera y microcontenidos, se recomienda implementar una doble revisión:

Revisión técnica, a cargo del CISO/Infraestructura, para garantizar la precisión de los conceptos, la alineación con políticas internas y la ausencia de información sensible.

Revisión pedagógica/comunicacional, liderada por T&D y Mercadeo, para asegurar claridad, lenguaje accesible, pertinencia para la audiencia y coherencia visual del PCSI.

Este control cruzado está en consonancia con las buenas prácticas de diseño instruccional y de concientización planteadas por NIST y por ISO/IEC 27002:2022 (NIST, 2024; ISO/IEC, 2022).

Vincular el Desempeño en el PCSI con Otros Procesos de Gestión de Personas y Seguridad

Se sugiere que los resultados del PCSI (participación, finalización, desempeño en evaluaciones y simulaciones) se utilicen como insumo para:

Retroalimentar evaluaciones de desempeño cuando existan incumplimientos reiterados e injustificados.

Priorizar intervenciones adicionales en áreas con mayor brecha de comportamiento.

Alimentar la gestión de riesgos, incidentes y planes de tratamiento.

Esta recomendación busca que el PCSI no se perciba como un ejercicio aislado, sino como un componente del sistema de gestión integral, en línea con el enfoque de responsabilidad demostrada y de integración con la gestión de riesgos planteado por ISO/IEC y NIST (ISO/IEC, 2022; NIST, 2024).

Planear Desde Ahora una Evaluación de Impacto a Mediano Plazo

Finalmente, se recomienda que, una vez implementado el PCSI durante al menos un ciclo anual completo, se diseñe una evaluación específica de impacto que compare:

Resultados de nuevas campañas de phishing frente a la línea base (CTR y reportes).

Evolución de hallazgos de escritorio limpio y uso de repositorios en auditorías.

Cambios en resultados de evaluaciones de datos personales.

Esta evaluación permitiría, por un lado, validar empíricamente el impacto del PCSI sobre el riesgo humano y, por otro, alimentar investigaciones futuras que profundicen en la eficacia de programas de concientización basados en NIST SP 800-50r1 en organizaciones de características similares (NIST, 2024; ISO/IEC, 2022).

Estándares

ISO 27001:2022 Anexo A.6.3, Information security, cybersecurity and privacy protection, Information security management systems, Requirements

ISO 27002:2022 sección 6.3, Information security, cybersecurity and privacy protection, Information security controls

NIST SP800.50r1, Building a Cybersecurity and Privacy Learning Program

Referencias

“empresa auditora” para la “mediana empresa de tecnología”. (2024). INFORME Sistemas de Información –“mediana empresa de tecnología” – 2024. Noviembre 2024.

Cybersecurity and Infrastructure Security Agency (CISA). (s. f.). *Cross-Sector Cybersecurity Performance Goals (CPGs)*. Recuperado de https://www.cisa.gov/cross-sector-cybersecurity-performance-goals-cpgs

European Union Agency for Cybersecurity (ENISA). (2025). *Off the Hook – Don’t be Phished this Cybersecurity Month!* Recuperado de https://www.enisa.europa.eu/news/off-the-hook-dont-be-phished-this-cybersecurity-month

“mediana empresa de tecnología”. (2021a). Política de uso de activos y recursos de teleinformática. Sharepoint de la “mediana empresa de tecnología”, https://nfotrack.sharepoint.com/

“mediana empresa de tecnología”. (2021b). Política de respaldo de información de la “mediana empresa de tecnología”. Sharepoint de la “mediana empresa de tecnología”, https://nfotrack.sharepoint.com/

“mediana empresa de tecnología”. (2022). Caracterización Infraestructura Tecnológica. Sharepoint de la “mediana empresa de tecnología”, https://nfotrack.sharepoint.com/

“mediana empresa de tecnología”. (2023). Política de escritorio y pantalla limpia. Sharepoint de la “mediana empresa de tecnología”, https://nfotrack.sharepoint.com/

“mediana empresa de tecnología”. (2024a). Procedimiento Gestión de Incidentes de SI. Sharepoint de la “mediana empresa de tecnología”, https://nfotrack.sharepoint.com/

“mediana empresa de tecnología”. (2024b). Capacitación y entrenamiento – Capacitación y entrenamiento. Sharepoint de la “mediana empresa de tecnología”, https://nfotrack.sharepoint.com/

“mediana empresa de tecnología”. (2025a). Política de contraseñas seguras. Sharepoint de la “mediana empresa de tecnología”, https://nfotrack.sharepoint.com/

“mediana empresa de tecnología”. (2025b). Gestión de Incidentes de SI. Sharepoint de la “mediana empresa de tecnología”, https://nfotrack.sharepoint.com/

“mediana empresa de tecnología”. (2025c). Procedimiento Gestión de vulnerabilidades técnicas. Sharepoint de la “mediana empresa de tecnología”, https://nfotrack.sharepoint.com/

International Organization for Standardization. (2022a). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). International Organization for Standardization.

International Organization for Standardization. (2022b). Information security, cybersecurity and privacy protection — Information security controls (ISO/IEC 27002:2022). International Organization for Standardization.

National Institute of Standards and Technology. (2024). Developing a cybersecurity and privacy learning program (NIST Special Publication 800-50r1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-50r1.

“Empresa Consultora en seguridad” para la “mediana empresa de tecnología”. (2024). INFORME Ingeniería Social - Phishing – La “mediana empresa de tecnología”– 2024. Enero 2024.

Verizon. (2024, May 1). 2024 Data Breach Investigations Report: Vulnerability exploitation boom threatens cybersecurity. https://www.verizon.com/about/news/2024-data-breach-investigations-report-vulnerability-exploitation-boom

World Economic Forum. (2022). Digital dependencies and cyber vulnerabilities (Global Risks Report 2022, Chapter 3). https://www.weforum.org/publications/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/

Glosario

Administrativo & Financiero (A&F): Proceso de la “mediana empresa de tecnología” que incluye al Director General y es responsable de aprobar el PCSI, asignar recursos y comunicar el compromiso de la alta dirección con la seguridad de la información.

Concientización en seguridad de la información: Proceso para que las personas identifiquen riesgos, comprendan políticas del SGSI y adapten su comportamiento para reducir incidentes.

CPLP (Programa de Aprendizaje en Ciberseguridad y Privacidad): Marco de NIST SP 800-50r1 para estructurar actividades de concientización y capacitación en ciberseguridad y privacidad.

Datos personales: Información asociada a una persona natural, cuyo tratamiento en la “mediana empresa de tecnología” sigue políticas internas y normativa aplicable.

Escritorio y pantalla limpia: Prácticas para prevenir accesos no autorizados o exposición de información, mediante resguardo de documentos y bloqueo de sesión.

LMS Proporcionado por la ARL: Plataforma de la “mediana empresa de tecnología” para alojar el curso principal de concientización, registrar participación y aplicar evaluaciones.

Microcontenidos del PCSI: Contenidos breves para reforzar mensajes clave y mantener la cultura de seguridad en el flujo de trabajo.

NIST (National Institute of Standards and Technology): Instituto federal de Estados Unidos que desarrolla estándares y guías de ciberseguridad, incluyendo la serie de publicaciones especiales SP 800 que orientan la gestión de riesgos y programas de concientización.

PCSI (Plan de Concientización en Seguridad de la Información): Programa de la “mediana empresa de tecnología” para transformar políticas y riesgos en comportamientos seguros y medibles, alineado con NIST SP 800-50r1 e ISO/IEC 27001:2022.

Phishing: Técnica de ingeniería social para obtener información sensible mediante comunicaciones fraudulentas.

SGSI (Sistema de Gestión de Seguridad de la Información): Conjunto de políticas y procesos de la “mediana empresa de tecnología” para gestionar riesgos sobre la confidencialidad, integridad y disponibilidad de la información, alineado con ISO/IEC 27001:2022.

Transformación & Desarrollo (T&D): Proceso de la “mediana empresa de tecnología” responsable de la gestión de capacitación y desarrollo organizacional, integrando el PCSI al procedimiento institucional de formación.

Anexo A.

Instructivo para la creación de un curso en el LMS Colegio Sura de la ARL Sura

El siguiente instructivo se creó por parte de los autores tomando la información que la ARL SURA pone a disposición de los usuarios de la plataforma diseñada para le gestión de cursos o LMS; las imágenes incluidas fueron tomadas directamente de la plataforma.

INSTRUCTIVO LMS COLEGIO SURA

Manual para la creación de cursos en el LMS colegio SURA

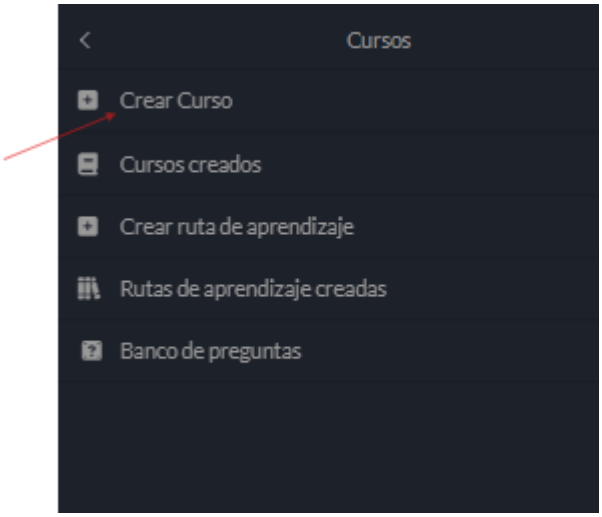
Este manual explica paso a paso cómo crear, diseñar, publicar y administrar un curso en el LMS colegio SURA y su integración con Chat Zeta. Cada sección sigue el mismo orden del formulario HTML de la plataforma y se apoya en capturas de pantalla numeradas (Figuras) que muestran los campos reales.

Información básica del curso

Ingresar a la página colegiosura.com, solicitando previamente el acceso al administrador del colegio Sura en Infotrack S.A.S

En el panel lateral desplegar el menú cursos

Seleccione crear curso para acceder a la sección de información básica.



Al iniciar la creación de un curso en el LMS colegio SURA, se muestra un panel lateral con las secciones Información básica, Objetivos, Diseño del curso, Marketing del curso y Publicar curso. Este panel refleja el mismo flujo que se describe en este manual.

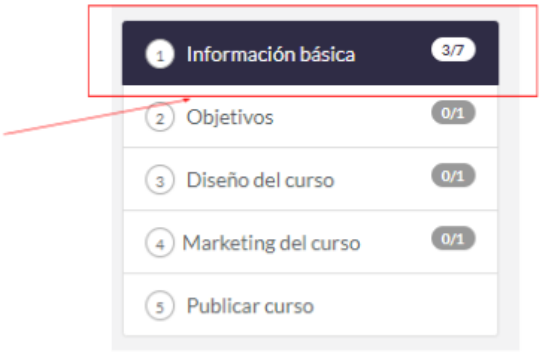


Figura 1. Panel lateral con los pasos del proceso de creación del curso.

1.1 Datos generales del curso

En esta subsección se define la información principal con la que se identificará el curso en la plataforma.

Título del curso: escribe un nombre claro y representativo.

Figura 2. Campo «Título» del curso.

Descripción: resume los contenidos y beneficios del curso en uno o dos párrafos.

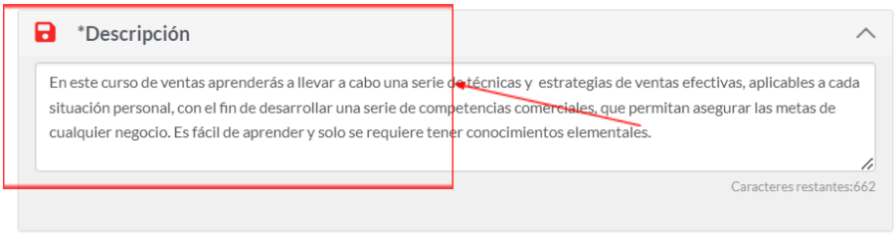


Figura 3. Campo «Descripción» del curso.

Modalidad: selecciona si el curso será virtual o presencial.

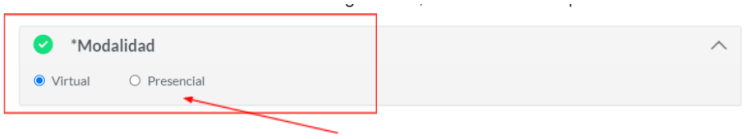


Figura 4. Selección de la modalidad (virtual o presencial).

Tipo: indica si se trata de un curso, diplomado, taller, seminario u otra opción.

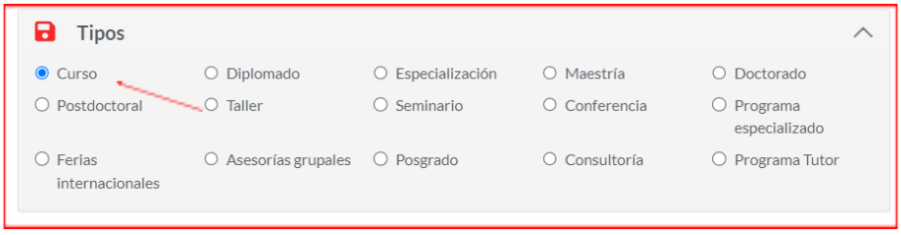


Figura 5. Tipos de oferta académica disponibles.

Nivel: define si el curso es básico, intermedio o avanzado.

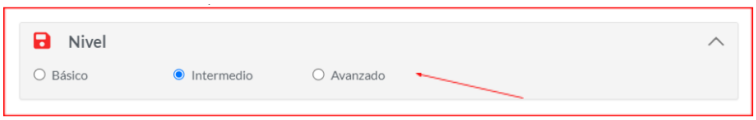


Figura 6. Selección del nivel del curso.

Categoría: clasifica el curso dentro de una categoría temática.

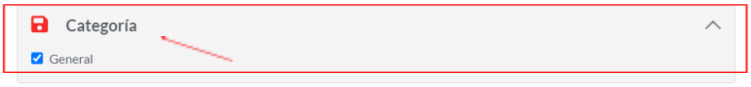


Figura 7. Campo «Categoría» del curso.

Pre-requisitos: especifica los conocimientos o condiciones previas recomendadas.

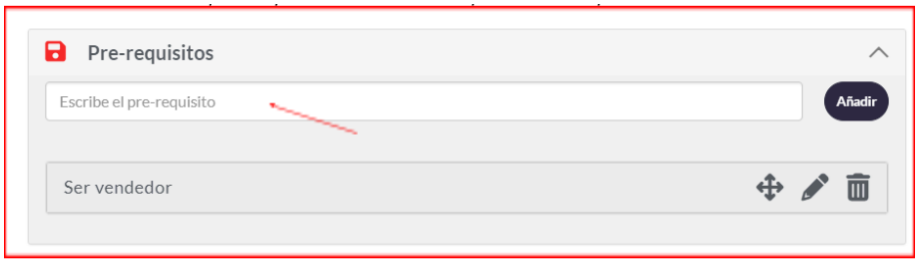


Figura 8. Registro de pre-requisitos del curso.

1.2 Imágenes principales del curso

En el LMS colegio SURA permite cargar diferentes imágenes para hacer más atractivo el curso en el catálogo.

Encabezado del curso (imagen panorámica recomendada 1920x1080).

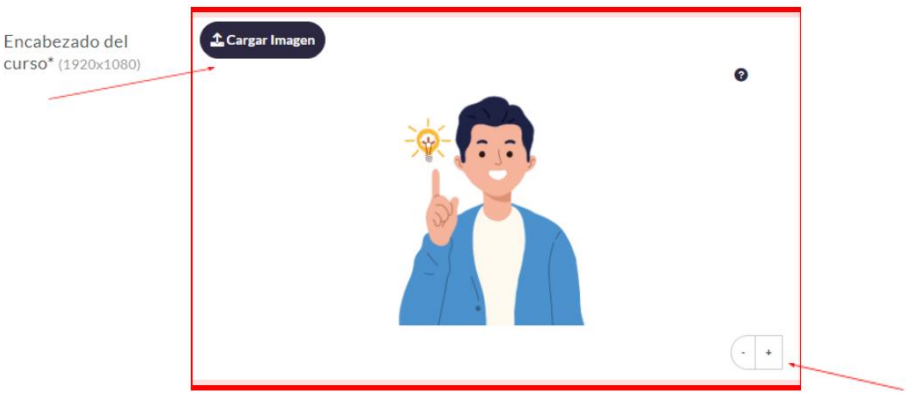


Figura 9. Encabezado del curso (imagen panorámica recomendada 1920x1080).

Imagen destacada que se muestra en el listado de cursos (720x375).

Figura 10. Imagen destacada que se muestra en el listado de cursos (720x375).

Imagen del chatbot asociado al curso (100x100).

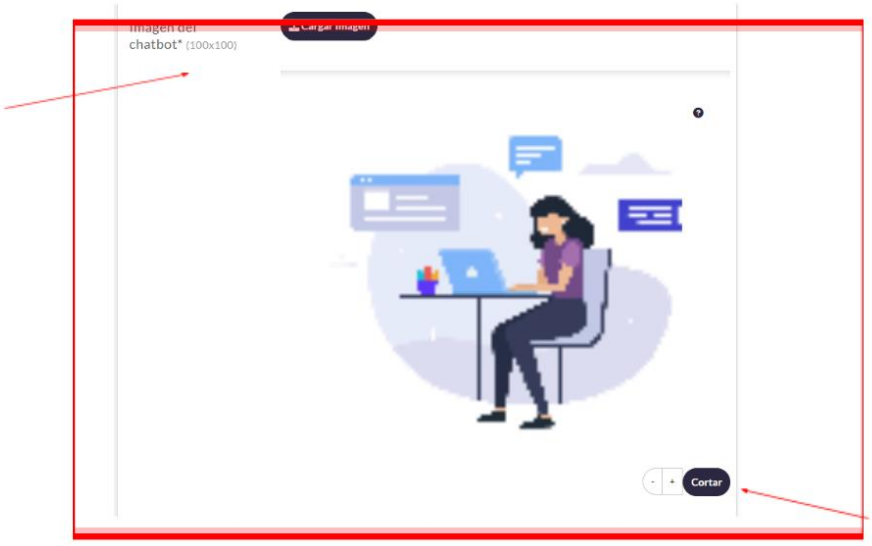


Figura 11. Imagen del chatbot asociado al curso (100x100).

1.3 Configuración del chatbot y visualización

Nombre del chatbot: define el nombre con el que los usuarios verán el asistente del curso.

Figura 12. Campo «Nombre del chatbot».

Visualización: indica si el curso se mostrará el LMS colegio SURA, en Chat Zeta o en ambos.

Figura 13. Opciones de visualización en el LMS colegio SURA y Chat Zeta.

Palabras claves: agrega de 2 a 3 palabras o frases que faciliten la búsqueda del curso.

Figura 14. Campo para registrar palabras clave del curso.

1.4 Docente, colaboradores y bibliografía

Sección «Profesor» donde se configura el responsable del curso.

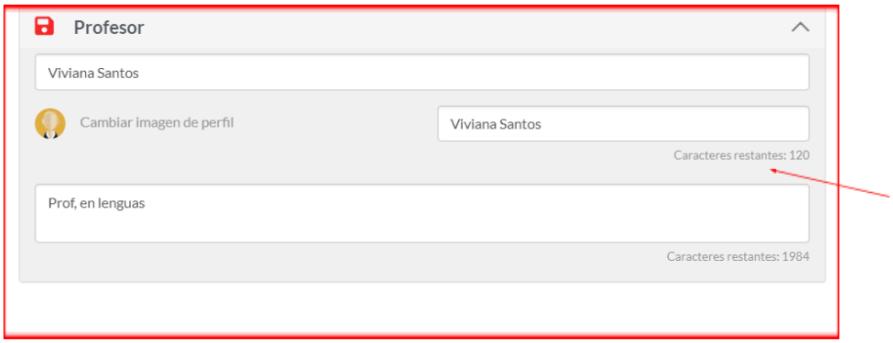


Figura 15. Sección «Profesor» donde se configura el responsable del curso.

Sección «Colaboradores» para asignar permisos a otros usuarios.

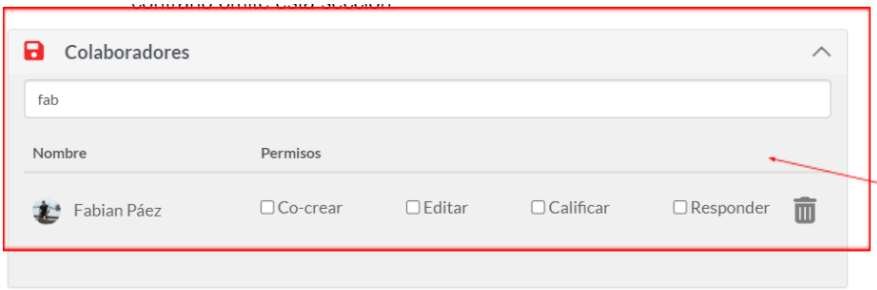


Figura 16. Sección «Colaboradores» para asignar permisos a otros usuarios.

Sección «Bibliografía o fuentes» para registrar referencias.

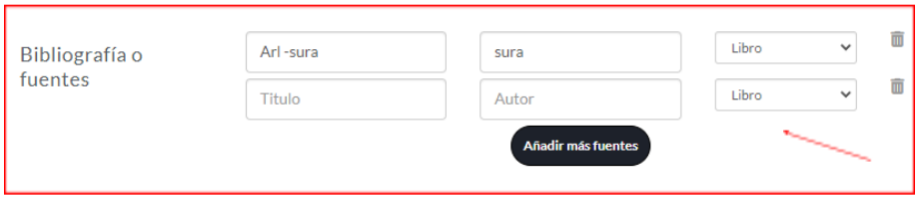


Figura 17. Sección «Bibliografía o fuentes» para registrar referencias.

Al final de la sección de información básica se encuentran los botones para previsualizar, guardar el avance y continuar al siguiente paso.

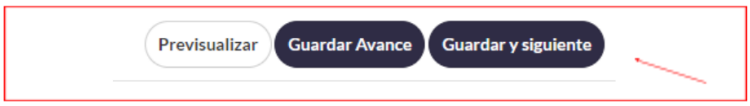


Figura 18. Botones «Previsualizar», «Guardar avance» y «Guardar y siguiente».

2. Objetivos del curso

En este paso se define el propósito general del curso y los objetivos específicos que se abordarán en las diferentes unidades.

2.1 Objetivo general

Campo donde se describe el objetivo global del curso.

Figura 19. Campo donde se describe el objetivo global del curso.

2.2 Objetivos específicos

Sección para añadir varios objetivos específicos.

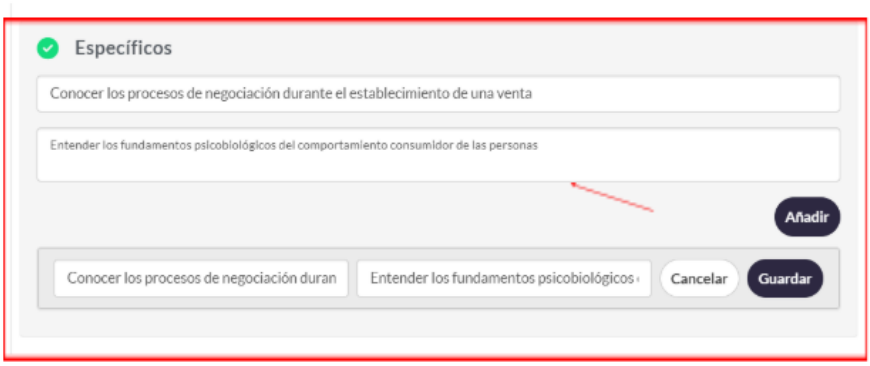


Figura 20. Sección para añadir varios objetivos específicos.

2.3 Relación entre objetivos y unidades

Vista donde se observa cada objetivo específico con sus unidades asociadas.

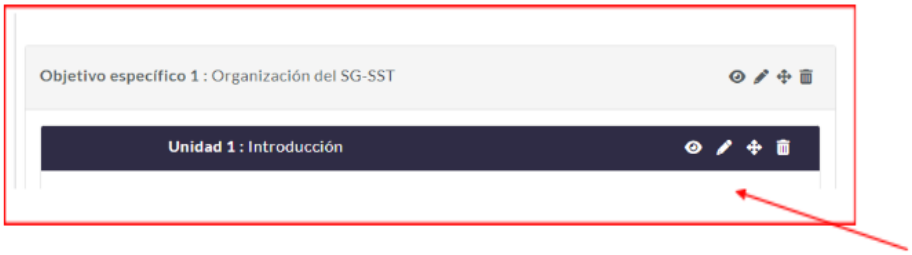


Figura 21. Vista donde se observa cada objetivo específico con sus unidades asociadas.

3. Diseño del curso

En el diseño del curso se crean las unidades y se añaden los diferentes tipos de contenidos y actividades.

3.1 Agregar unidades a un objetivo específico

Formulario para crear una nueva unidad dentro de un objetivo específico.

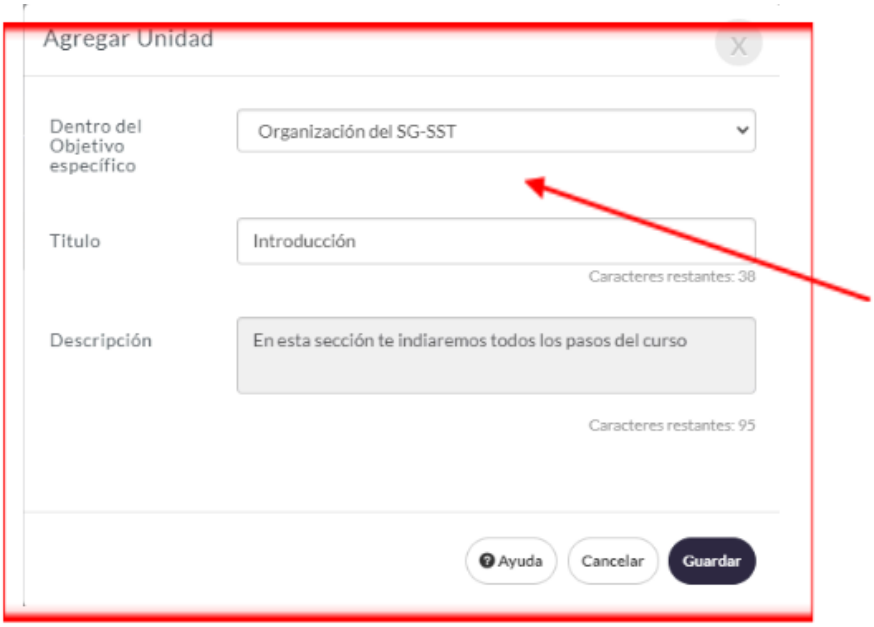


Figura 22. Formulario para crear una nueva unidad dentro de un objetivo específico.

3.2 Guardar cambios de la unidad

Botones para volver, guardar y avanzar al siguiente paso en el diseño.

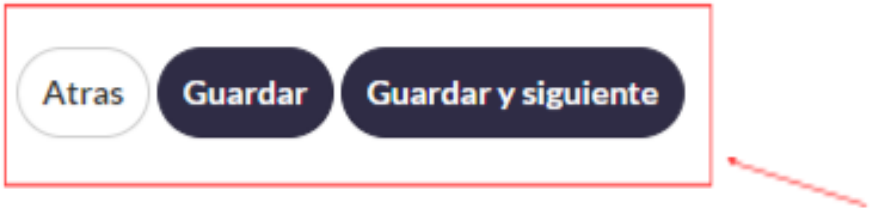


Figura 23. Botones para volver, guardar y avanzar al siguiente paso en el diseño.

3.3 Elementos de contenido

Opciones para añadir audio, medios, lecturas, documentos o imágenes.

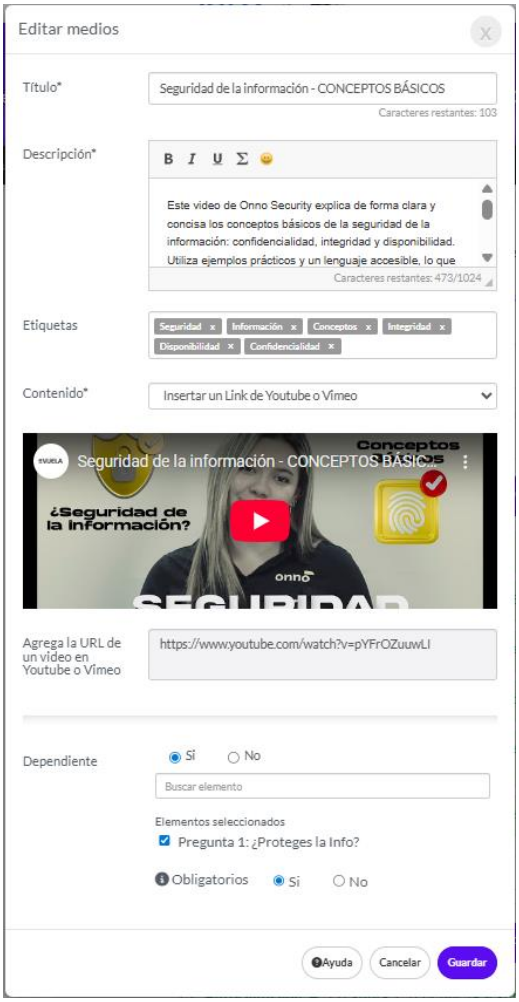


Figura 24. Opciones para añadir audio, medios, lecturas, documentos o imágenes.

3.4 Elementos colaborativos

Opciones para añadir wikis y foros.

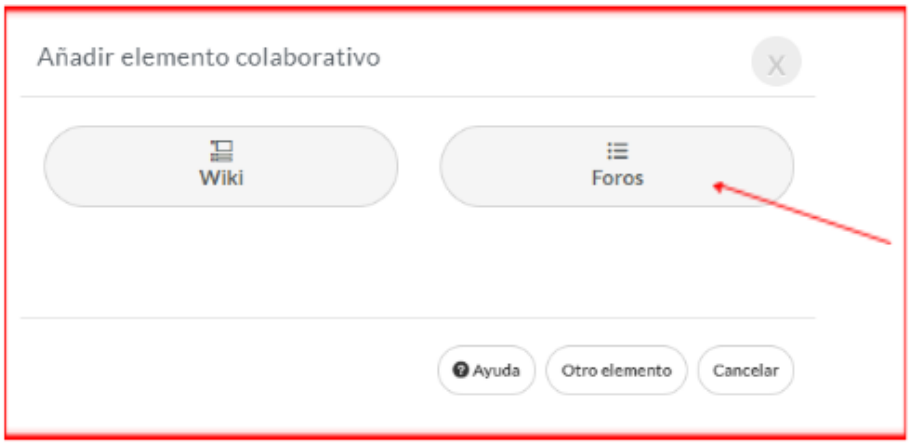


Figura 25. Opciones para añadir wikis y foros.

3.5 Elementos de doble vía

Opciones para añadir proyectos o preguntas abiertas.

Figura 26. Opciones para añadir proyectos o preguntas abiertas.

3.6 Elementos autocalificables

Opciones para añadir selección múltiple, ordenamiento, falso/verdadero o respuesta numérica.

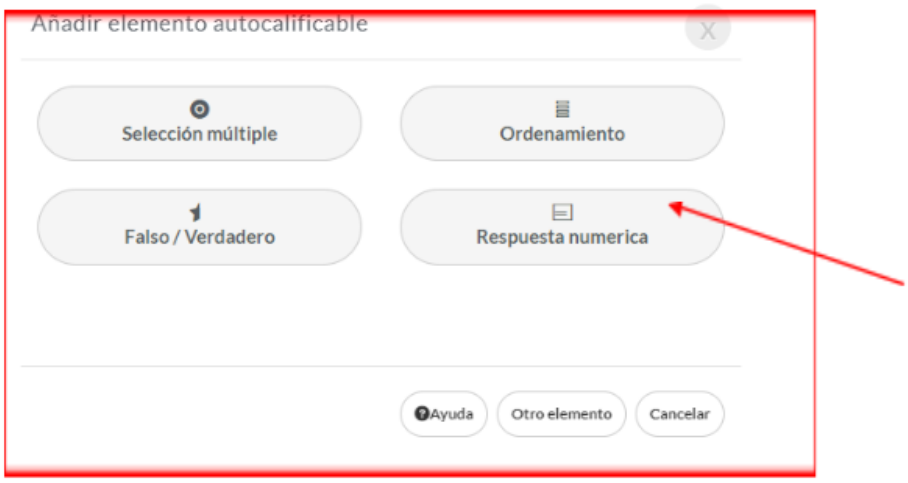


Figura 27. Opciones para añadir selección múltiple, ordenamiento, falso/verdadero o respuesta numérica.

3.7 Exámenes

Botón para crear evaluaciones tipo examen dentro de la unidad.

Figura 28. Botón para crear evaluaciones tipo examen dentro de la unidad.

3.8 Ventana general «Añadir elemento»

Resumen de las categorías de elementos que se pueden agregar a una unidad.

Figura 29. Resumen de las categorías de elementos que se pueden agregar a una unidad.

4. Marketing del curso

En esta sección se configuran los vídeos o imágenes promocionales que acompañarán al curso en el catálogo y dentro del aula.

4.1 Video o imagen promocional

Configuración del contenido promocional principal del curso.

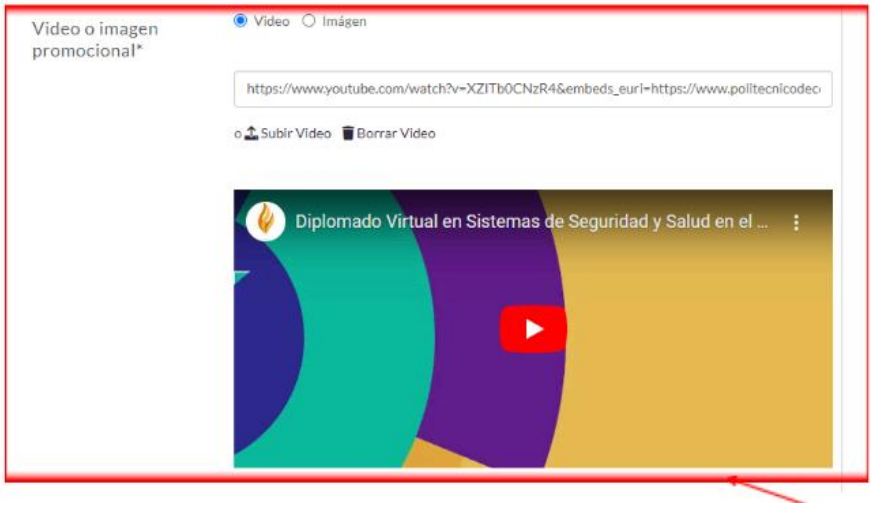


Figura 30. Configuración del contenido promocional principal del curso.

4.2 Video introductorio

Video inicial que da la bienvenida y explica el curso.

Figura 31. Video inicial que da la bienvenida y explica el curso.

4.3 Video de cierre

Video final para despedida, retroalimentación o cierre del proceso.

Figura 32. Video final para despedida, retroalimentación o cierre del proceso.

5. Publicar el curso

Finalmente, se configuran los aspectos de certificación, aprobación, pago y visibilidad antes de publicar el curso.

5.1 Certificado del curso

Activar o desactivar el certificado y acceder a su edición.

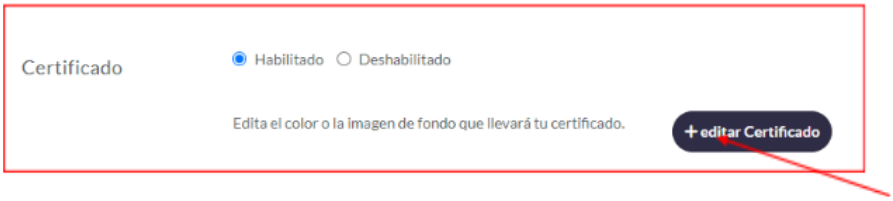


Figura 33. Activar o desactivar el certificado y acceder a su edición.

5.2 Requisitos para aprobar

Definir el porcentaje mínimo requerido para aprobar el curso.

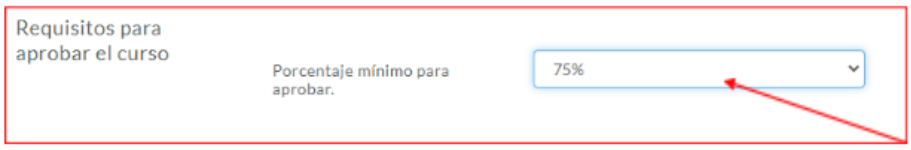


Figura 34. Definir el porcentaje mínimo requerido para aprobar el curso.

5.3 Método de pago

Elegir si el curso será gratuito o de pago.

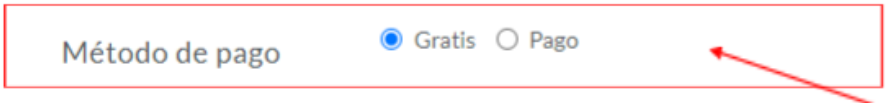


Figura 35. Elegir si el curso será gratuito o LMS de pago.

5.4 Forma de recaudo

Definir si el recaudo será virtual o presencial.

Figura 36. Definir si el recaudo será virtual o presencial.

5.5 Visualización del curso

Configurar si el curso será público o privado.

Figura 37. Configurar si el curso será público o privado.

5.6 Enlace del curso en Chat Zeta

Enlace que se habilita cuando el administrador aprueba el curso.

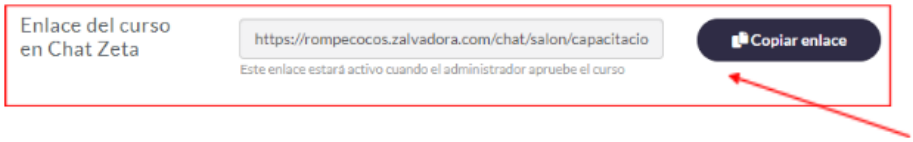


Figura 38. Enlace que se habilita cuando el administrador aprueba el curso.

5.7 Botones finales

Botones para volver, previsualizar, guardar y editar el certificado antes de finalizar.

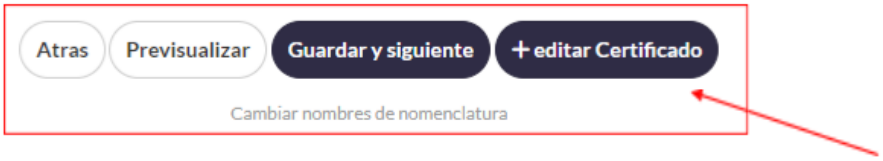


Figura 39. Botones para volver, previsualizar, guardar y editar el certificado antes de finalizar.

Anexo B.

Cronograma del PCSI para La “mediana empresa de tecnología”

En la tabla 10 se resume el cronograma detallado para la implementación del PCSI para 12 meses, capitulo por capitulo, brecha atacada y audiencia.

Tabla 10

Cronograma consolidado PCSI

Mes	Capítulo	Subcapítulo / Tema	Brecha atacada	Audiencia
1	5 - Formación PCSI	Roles y responsabilidades PCSI - Formación para líderes: métricas y gobernanza del PCSI	N/A (Gobernanza)	Audiencia 4 (Líderes)
2	Preparación	Preparación de contenidos Cap. 1 y 2 en LMS	N/A (Preparación)	Equipo T&D y TI/CISO
3	1 - Concientización Básica en Seguridad Informática	Conceptos básicos de seguridad de la información - Contextualización en seguridad	1, 2, 4	Grupos Usuarios generales
4	1 - Concientización Básica en Seguridad Informática	Importancia de la seguridad en el entorno laboral - Reconocimiento de impacto organizacional	1, 4	Grupos Usuarios generales
5	1 - Concientización Básica en Seguridad Informática	Principales tipos de ataque - Conceptualización de exposición	3	Grupos Usuarios generales
6	2 - Aplicar buenas prácticas y controles básicos	Gestión de contraseñas y autenticación - Gestión de credenciales y MFA	3	Grupos Usuarios generales
7	2 - Aplicar buenas prácticas y controles básicos	Manejo seguro del correo electrónico y navegación - Reconocimiento y reporte de phishing	3	Grupos Usuarios generales
8	2 - Aplicar buenas prácticas y controles básicos	Protección de la información en dispositivos y red - Proteger la información en dispositivos móviles y redes	1, 2, 3	Grupos Usuarios generales
9	3 - Manejo de incidentes y reporte	Reconocer un incidente y pasos iniciales - Respuesta inicial a incidentes y reportes	3, 4	Grupos Usuarios generales
10	4 - Principios del tratamiento de datos personales	Políticas y normativas internas - Uso correcto de repositorios autorizados (OneDrive/SharePoint)	1, 2	Grupos Usuarios generales
11	4 - Principios del tratamiento de datos personales	Políticas y normativas internas - Escritorio y pantalla limpia	1	Grupos Usuarios generales
12	4 - Principios del tratamiento de datos personales + 5 - Formación PCSI	Tratamiento de datos personales - Protección de datos personales (principios y obligaciones) + Revisión anual del PCSI	4	Grupos Usuarios generales + Audiencia 4

Nota. Fuente: Los autores

Anexo B

Cronograma del PCSI para La “mediana empresa de tecnología”

En la tabla 11 a continuación se relacionan los contenidos del PCSI para 12 meses, capitulo por capítulo del LMS, con sus respectivos contenidos para cartelera digital y microcontenidos, con las actividades necesarias para la implementación y cada KPI impactado.

Tabla 11

Consolidado presupuesto actividades y responsables del PCSI.

Mes	Avance	Cartelera Digital (6 meses totales)	Microcontenidos (Teams/Viva Engage)	Resumen actividades	Indicadores / KPI
1	Montaje en curso	No	No	*Capacitación dirigida a líderes sobre gobernanza del PCSI *Preparación de contenidos Cap. 1 y 2.	Revisiones al PCSI (>=1 anual)
2	Montaje en curso	Inicia 1.ª campaña	No	*Preparación de contenidos Cap. 3 y 4. *Planificación de refuerzos.	N/A
3	Mes 3	1.ª campaña en curso	Sí - "¿Qué es la seguridad de la información en La “mediana empresa de tecnología”?"	*Inicio de microcontenidos mensuales *Inicio de 1.ª campaña de cartelera	Tasa de finalización > 10%
4	Mes 4	1.ª campaña en curso	Sí - "Qué pasa si falla la seguridad en La “mediana empresa de tecnología”"		Tasa de finalización > 20%
5	Mes 5	1.ª campaña en curso	Sí - "3 ataques que todo colaborador debe conocer"		Tasa de finalización > 30%
6	Mes 6	1.ª campaña en curso	Sí - "3 reglas para una contraseña segura"		Tasa de finalización > 40%
7	Mes 7	Cierra 1.ª campaña (Mes 2-4)	Sí - "Antes de hacer clic: 3 preguntas que debes hacerte"	*Simulación de phishing *Cierre de 1.ª campaña de cartelera	Tasa de finalización > 50%; CTR phishing < 4%
8	Mes 8	Inicia 2.ª campaña	Sí - "Qué hacer si pierdes tu equipo de trabajo"	Inicio de 2.ª campaña de cartelera	Tasa de finalización > 60%
9	Mes 9	2.ª campaña en curso	Sí - "¿Qué es un incidente y cómo lo reportas?"		Tasa de finalización > 70%; Reportes phishing > 0%
10	Mes 10	2.ª campaña en curso	Sí - "Dónde sí y dónde no guardar información de La “mediana empresa de tecnología”"		Tasa de finalización > 80%; Hallazgos auditoría < 10%
11	Mes 11	2.ª campaña en curso	Sí - "Lo que nunca deberías dejar a la vista en tu puesto"		Tasa de finalización > 90%; Hallazgos escritorio < 10%
12	Mes 12	Cierra 2.ª campaña (Mes 8-10)	Sí - "Datos personales: las 5 cosas que no puedes olvidar"	*Revisión y evaluación anual del PCSI con líderes *Cierre de 2.ª campaña de cartelera	Tasa de finalización 100%; Revisiones al PCSI año 2

Nota. Fuente: Los autores

Anexo C.

Consolidado Detallado Presupuesto Horas Hombre

En la tabla a continuación se consolida el listado de actividades y el responsable de cada actividad para la implementación del PCSI en la “mediana empresa de tecnología”.

Tabla 12

Consolidado presupuesto actividades y responsables del PCSI.

Fase	Actividad	Descripción	Responsable	Otros roles
1. Planeación y estrategia	Definición y actualización anual del PCSI	Reunión de trabajo para revisar riesgos de SI, incidentes del último período, prioridades de negocio y actualizar el plan anual de PCSI (temas, poblaciones objetivo y actividades principales)	Líder TI	Director A&F, Líder TI, Líder T&D
1. Planeación y estrategia	Revisión semestral de avance y ajuste del PCSI	Seguimiento formal al avance del plan, revisión rápida de indicadores, incidentes y desviaciones, y definición de ajustes operativos	Líder TI	Líder TI, Líder T&D
2. Análisis y diseño	Diseño macro del currículo de concientización (segmentación por roles y temas)	Identificación de grupos de audiencia (todo el personal, TI, líderes, personal con acceso a información sensible) y definición de temas mínimos por cada segmento	Líder T&D	Líder TI
2. Análisis y diseño	Actualización de contenidos (presentaciones, guiones, cuestionarios)	Revisión de materiales digitales existentes, incorporación de cambios normativos y adición de ejemplos tomados de incidentes o hallazgos reales de La “mediana empresa de tecnología”	Líder T&D	Líder TI
3. Desarrollo e implementación	Sesión virtual de concientización básica para personal nuevo	Sesión digital de inducción en seguridad de la información para las personas que ingresan a la organización, integrada a la inducción corporativa	Líder T&D	Líder TI
3. Desarrollo e implementación	Refuerzo anual de concientización básica a todo el personal	Sesión digital de actualización general, realizada en grupos por áreas o equipos, reforzando mensajes clave del PCSI	Líder TI	Líder T&D, Líderes de proceso
3. Desarrollo e implementación	Taller anual para líderes de proceso sobre responsabilidades en SI	Taller digital donde se aclaran expectativas de liderazgo, responsabilidades sobre información de su proceso y rol en la ejecución del PCSI	Líder TI	Director A&F, Líder T&D
3. Desarrollo e implementación	Sesiones trimestrales breves para el equipo de TI	Encuentros digitales sobre prácticas seguras específicas (gestión de accesos, copias de seguridad, incidentes, vulnerabilidades)	Líder TI	Líder TI
3. Desarrollo e implementación	Planificación y redacción de campañas internas digitales	Definición de tema del período, mensajes clave, piezas breves y calendario de envíos	Líder T&D	Líder TI - Mercadeo
3. Desarrollo e implementación	Difusión de mensajes por canales digitales	Publicación y envío de correos, avisos en intranet o herramientas colaborativas, y seguimiento básico de visualización	Líder T&D	Líder TI - Mercadeo

Fase	Actividad	Descripción	Responsable	Otros roles
3. Desarrollo e implementación	Diseño y ejecución de una campaña de phishing simulado	Diseño de correos simulados, configuración de herramienta, ejecución de la campaña y consolidación de resultados	Líder TI	Líder TI, Líder A&F
3. Desarrollo e implementación	Sesiones de retroalimentación post-phishing	Breves reuniones digitales con las áreas más impactadas por la campaña para explicar resultados y reforzar buenas prácticas	Líder TI	Líderes de proceso
3. Desarrollo e implementación	Gestión de convocatorias, inscripciones y recordatorios	Envío de invitaciones digitales, seguimiento a confirmaciones y recordatorios para sesiones y evaluaciones	Líder T&D	Asistente T&D
3. Desarrollo e implementación	Archivo y organización digital de evidencias	Clasificación y almacenamiento en repositorios digitales de actas, presentaciones, grabaciones, informes y reportes de campañas	Líder T&D	Líder TI
4. Evaluación y mejora	Diseño y actualización anual de cuestionarios de evaluación	Revisión y ajuste de bancos de preguntas digitales según incidentes, políticas internas y contenidos impartidos	Líder T&D	Líder TI
4. Evaluación y mejora	Consolidación de resultados	Habilitar las evaluaciones, acompañar a los participantes en caso de dudas técnicas y consolidar resultados por área y rol	Líder T&D	Líder TI
4. Evaluación y mejora	Definición y revisión anual de indicadores del PCSI	Selección o ajuste de indicadores clave (participación, resultados de pruebas, incidentes ligados a fallo humano) y formalización de fichas de indicador	Líder TI	Director A&F, Líder T&D
4. Evaluación y mejora	Consolidación de resultados y reporte a la dirección	Elaboración de un informe ejecutivo anual del PCSI, presentando logros, brechas y recomendaciones de mejora	Líder TI	Director A&F

Nota. Fuente: Los autores

Anexo C.

Consolidado Detallado Presupuesto Horas Hombre

En la tabla a continuación se consolida el presupuesto hora-hombre requerido para la implementación del PCSI en la “mediana empresa de tecnología”

Tabla 13

Consolidado presupuesto horas-hombre

Fase	Frecuencia / Momento	Horas por evento	Nº eventos año	Horas-hombre anuales
1. Planeación y estrategia	1 vez al año (inicio del ciclo)	4	1	4
1. Planeación y estrategia	2 veces al año	2	2	4
2. Análisis y diseño	1 vez al año, con ajustes menores según necesidad	6	1	6
2. Análisis y diseño	2 veces al año (ajustes semestrales)	4	2	8
3. Desarrollo e implementación	Mensual (12 veces al año)	1,5	12	18
3. Desarrollo e implementación	4 eventos para cubrir toda la organización	2	4	8
3. Desarrollo e implementación	1 vez al año	3	1	3
3. Desarrollo e implementación	Trimestral (4 veces al año)	1,5	4	6
3. Desarrollo e implementación	Trimestral (4 campañas al año)	3	4	12
3. Desarrollo e implementación	24 acciones significativas en el año (semanal o quincenal dentro de cada campaña)	0,5	12	6
3. Desarrollo e implementación	1 vez al año (prueba inicial de madurez)	6	1	6
3. Desarrollo e implementación	1 sesiones tras la campaña	1	2	2
3. Desarrollo e implementación	12 ciclos de convocatoria relevantes en el año	2	12	24
3. Desarrollo e implementación	Mensual	1	12	12
4. Evaluación y mejora	1 vez al año	4	1	4
4. Evaluación y mejora	1 ciclo principal anual	8	1	8
4. Evaluación y mejora	1 vez al año	3	1	3
4. Evaluación y mejora	1 informe anual consolidado	6	1	6

Nota. Fuente: Los autores

Anexo D.

Consolidado Alineación Plan de Concientización

De acuerdo con la NIST SP 800-50r1, la identificación de audiencias, la identificación de necesidades y la determinación de brechas, deben confluir para establecer una visión clara para los próximos pasos del desarrollo del PCSI ([NIST], 2024). La tabla a continuación resume y alinea los parámetros identificados y definidos en la etapa de análisis del proyecto.

Tabla 14

Consolidado alineación plan de concientización

Capítulo	Subcapítulo	Tema	Brechas
1 - Concientización Básica en Seguridad Informática	Conceptos básicos de seguridad de la información	Contextualización en seguridad	1, 2 y 4
1 - Concientización Básica en Seguridad Informática	Importancia de la seguridad en el entorno laboral	Reconocimiento de impacto organizacional	1 y 4
1 - Concientización Básica en Seguridad Informática	Principales tipos de ataque	Conceptualización de exposición	3
2 - Aplicar buenas prácticas y controles básicos	Gestión de contraseñas y autenticación	Gestión de credenciales y MFA	3
2 - Aplicar buenas prácticas y controles básicos	Manejo seguro del correo electrónico y navegación	Reconocimiento y reporte de phishing	3
2 - Aplicar buenas prácticas y controles básicos	Protección de la información en dispositivos y red	Proteger la información de la empresa en dispositivo móviles	1, 2 y 3
3 - Manejo de incidentes y reporte	Reconocer un incidente y pasos iniciales	Respuesta inicial a incidentes y reportes	3 y 4
4 - Principios del tratamiento de datos personales	Políticas y normativas internas	Uso correcto de repositorios autorizados (OneDrive/SharePoint)	1 y 2
4 - Principios del tratamiento de datos personales	Políticas y normativas internas	Escritorio y pantalla limpia	1
4 - Principios del tratamiento de datos personales	Tratamiento de datos personales	Protección de datos personales (principios y obligaciones)	4
5 - Formación PCSI	Roles y responsabilidades PCSI	Formación para líderes: métricas y gobernanza del PCSI	N/A
Capacitaciones especializadas con fabricantes.	Está fuera del alcance del PCSI por tratarse de capacitaciones especializadas	Formación técnica avanzada: gestión de vulnerabilidades y respaldos	N/A

Nota. Fuente: Los autores

Anexo D.

Consolidado Alineación Plan de Concientización

De acuerdo con la NIST SP 800-50r1, la identificación de audiencias, la identificación de necesidades y la determinación de brechas, deben confluir para establecer una visión clara para los próximos pasos del desarrollo del PCSI ([NIST], 2024). La tabla a continuación resume y alinea los parámetros identificados y definidos en la etapa de análisis del proyecto.

Tabla 15

Consolidado alineación plan de concientización

Subcapítulo	Audiencia	Formato	Duración	Cadencia
Conceptos básicos de seguridad de la información	Grupos Usuarios generales	LMS (Escuela Sura)	12 meses	Mes 3
Importancia de la seguridad en el entorno laboral	Grupos Usuarios generales	LMS (Escuela Sura)	12 meses	Mes 4
Principales tipos de ataque	Grupos Usuarios generales	LMS (Escuela Sura)	12 meses	Mes 5
Gestión de contraseñas y autenticación	Grupos Usuarios generales	LMS (Escuela Sura) + Cartelera digital + Microcontenidos	12 meses + 6 meses + 1 mes	Mes 6
Manejo seguro del correo electrónico y navegación	Grupos Usuarios generales	LMS (Escuela Sura) + simulación de phishing	12 meses + simulación puntual	Mes 7
Protección de la información en dispositivos y red	Grupos Usuarios generales	LMS (Escuela Sura) + Cartelera digital + Microcontenidos	12 meses + 6 meses + 1 mes	Mes 8
Reconocer un incidente y pasos iniciales	Grupos Usuarios generales	LMS (Escuela Sura) + On-Bording	12 meses + 1 día	Mes 9
Políticas y normativas internas	Grupos Usuarios generales	LMS (Escuela Sura) + On-Bording	12 meses + 1 día	Mes 10
Políticas y normativas internas	Grupos Usuarios generales	LMS (Escuela Sura) + Cartelera digital + Microcontenidos	12 meses + 6 meses + 1 mes	Mes 11
Tratamiento de datos personales	*Grupos Usuarios generales *Audiencia 2	*LMS (Escuela Sura) + On-Bording *Capacitación dirigida	*12 meses + 1 día *1 día	* Mes 12 * Mes 1
Roles y responsabilidades PCSI	Audiencia 4	Capacitación dirigida	1 día	Mes 1 y Mes 12
Está fuera del alcance del PCSI por tratarse de capacitaciones especializadas	Audiencia 3	N/A	N/A	N/A

Nota. Fuente: Los autores

Anexo D.

Consolidado Alineación Plan de Concientización

De acuerdo con la NIST SP 800-50r1, la identificación de audiencias, la identificación de necesidades y la determinación de brechas, deben confluir para establecer una visión clara para los próximos pasos del desarrollo del PCSI ([NIST], 2024). La tabla a continuación resume y alinea los parámetros identificados y definidos en la etapa de análisis del proyecto.

Tabla 16

Consolidado alineación plan de concientización

Subcapítulo	Indicadores	KPI	Fórmula	Meta KPI
Conceptos básicos de seguridad de la información	Tasa de finalización (%) > 10%	N/A	N/A	N/A
Importancia de la seguridad en el entorno laboral	Tasa de finalización (%) > 20%	N/A	N/A	N/A
Principales tipos de ataque	Tasa de finalización (%) > 30%	N/A	N/A	N/A
Gestión de contraseñas y autenticación	Tasa de finalización (%) > 40% + 2 campañas + 12 publicaciones	N/A	N/A	N/A
Manejo seguro del correo electrónico y navegación	Tasa de finalización (%) > 50% + 1 prueba	CTR (tasa de clics) en simulaciones phishing	# clic / población prueba	< 4%
Protección de la información en dispositivos y red	Tasa de finalización (%) > 60% + 2 campañas + 12 publicaciones	N/A	N/A	N/A
Reconocer un incidente y pasos iniciales	Tasa de finalización (%) > 70% + Evaluación de inducción	Reportes de incidentes por pruebas de phising	# reportes / población prueba	> 0%
Políticas y normativas internas	Tasa de finalización (%) > 80% + Evaluación de inducción	Uso de herramientas no autorizadas para gestión de información en auditoría	# Hallazgos / población muestra	< 10%
Políticas y normativas internas	Tasa de finalización (%) > 90% + 2 campañas + 12 publicaciones	Reducción de hallazgos de escritorio en auditoría	# Hallazgos / población muestra	< 10%
Tratamiento de datos personales	Tasa de finalización (%) > 100% + Evaluación datos personales	% Finalización capacitación en LMS	# finalización / # Inscritos	100%
Roles y responsabilidades PCSI	Evaluación capacitación	Revisiones al PCSI	# Revisiones anuales realizadas	>=1
Está fuera del alcance del PCSI por tratarse de capacitaciones especializadas	Fuera del alcance	Fuera del alcance	N/A	N/A

Nota. Fuente: Los autores