Ficha técnica

Cognitus

Plataforma de Concientización en Ciberseguridad

Producto:	Cognitus LMS
Versión de documento:	1.0.0
Tipo de Documento:	Descripción de la solución
Fecha de elaboración:	11 de septiembre de 2025
Autor:	Postech

Conciencia activa, respuesta efectiva

COGNITUS

FICHA TÉCNICA

Plataforma de Concientización
en Ciberseguridad

Sistema de Gestión del Aprendizaje (LMS)
para la formación y evaluación en Seguridad de la Información

Producto:	Cognitus LMS
Versión de producto:	5.1
Tipo de Documento:	Ficha Técnica
Fecha:	21 de agosto de 2025
Clasificación:	Comercial
Contacto:	ventas@postech.us

"Conciencia activa, respuesta efectiva"

1. Tabla de contenido

1. INFORMACIÓN GENERAL Y ALCANCE

1.1 Nombre de la Solución

Nombre Comercial:	Cognitus LMS
Nombre Completo:	Cognitus - Plataforma de Concientización en Ciberseguridad
Versión Actual:	5.1
Tipo de Sistema:	Learning Management System (LMS)
Desarrollado por:	Postech

1.2 Descripción General

Cognitus es una plataforma integral de Sistema de Gestión del Aprendizaje (LMS) diseñada específicamente para transformar a los empleados de una organización en una línea de defensa activa contra amenazas cibernéticas.

La solución implementa el concepto de "Firewall Humano", reconociendo que el factor humano es tanto la mayor vulnerabilidad como la mejor defensa en ciberseguridad. A través de un programa estructurado de formación, Cognitus desarrolla competencias prácticas que permiten a los usuarios identificar, prevenir y reportar amenazas de seguridad en su día a día.

La plataforma combina contenido multimedia interactivo, evaluaciones automatizadas, simulaciones de phishing y herramientas de seguimiento que permiten medir el impacto real del programa en la reducción de riesgos de seguridad.

1.3 Objetivos del Programa

Objetivos Principales de Aprendizaje

✓ Reducir la tasa de clics en correos de phishing en al menos un 70%
✓ Fortalecer las prácticas de creación y gestión de contraseñas seguras
✓ Desarrollar capacidad para identificar intentos de ingeniería social
✓ Crear conciencia sobre clasificación y manejo de información sensible
✓ Establecer cultura de reporte inmediato de incidentes de seguridad
✓ Cumplir con requisitos normativos de capacitación (ISO 27001, LFPDPPP)
✓ Reducir incidentes de seguridad causados por error humano

✓ Desarrollar "champions" de seguridad en cada área de la organización

1.4 Audiencia Objetivo

Perfil	Descripción	Nivel Recomendado
Personal General	Todos los empleados sin conocimientos técnicos en seguridad	Nivel Básico (15 cursos)
Mandos Medios	Supervisores y gerentes con acceso a información sensible	Nivel Básico + Intermedio (24 cursos)
Alta Dirección	Directivos y ejecutivos responsables de decisiones estratégicas	Cursos selectos de gobernanza y riesgos
Personal de TI	Equipos técnicos de tecnología y sistemas	Programa completo (35 cursos)
Equipo de Seguridad	Especialistas en ciberseguridad y gestión de riesgos	Nivel Avanzado + Certificaciones
Nuevos Ingresos	Empleados en proceso de inducción	Programa de Onboarding (cursos esenciales)

2. COMPONENTES DE LA SOLUCIÓN (METODOLOGÍA)

2.1 Módulos de Formación

El programa de concientización está estructurado en 35 cursos organizados en tres niveles progresivos:

Nivel	Cursos	Duración	Enfoque
Básico	15	20-25 horas	Fundamentos de seguridad, amenazas comunes, buenas prácticas
Intermedio	9	15-18 horas	Gestión de seguridad, cumplimiento normativo, controles
Avanzado	11	25-30 horas	Gestión estratégica, respuesta a incidentes, continuidad

Formatos de Contenido

Formato	Descripción
Videos Interactivos	Presentaciones narradas con animaciones, ejemplos visuales y puntos de interacción. Duración promedio: 5-10 minutos por video.
Micro-Learning	Módulos cortos de 15-20 minutos diseñados para aprendizaje ágil sin interrumpir significativamente las actividades laborales.
Gamificación	Sistema de puntos, insignias, tablas de clasificación y logros que motivan la participación y el aprendizaje continuo.
Simulaciones	Escenarios interactivos donde el usuario toma decisiones y observa las consecuencias de sus acciones.
Casos de Estudio	Análisis de incidentes reales de la industria adaptados para el aprendizaje práctico.
Infografías	Resúmenes visuales de conceptos clave para referencia rápida y refuerzo.

2.2 Simulaciones de Phishing

La plataforma incluye capacidades para ejecutar campañas de simulación de phishing que permiten evaluar el comportamiento real de los usuarios:

Característica	Descripción
Frecuencia:	Configurable: semanal, quincenal, mensual o personalizada
Tipos de Ataques:	Email phishing, spear phishing, whaling, smishing (SMS), vishing
Plantillas:	Biblioteca de +50 plantillas basadas en ataques reales actualizadas constantemente
Personalización:	Adaptación con logos, nombres y contexto específico de la organización
Realismo:	URLs enmascaradas, dominios similares, técnicas de urgencia y autoridad
Respuesta Educativa:	Al hacer clic, el usuario recibe capacitación inmediata sobre la amenaza
Métricas:	Tasa de apertura, clics, reportes, tiempo de respuesta por usuario/área
Progresión:	Dificultad incremental basada en el desempeño del usuario

2.3 Refuerzo y Material de Apoyo

Para mantener la concientización continua más allá de los cursos formales, Cognitus proporciona materiales de refuerzo:

Material	Uso y Características
Posters Digitales	Gráficos de alto impacto para pantallas corporativas, comedores y áreas comunes. Temas: contraseñas, phishing, reportes. Personalizables con marca corporativa.
Banners Web	Imágenes para intranet, firma de correo y sitios internos con mensajes de concientización rotatorios.
Infografías	Guías visuales rápidas sobre temas específicos: cómo detectar phishing, crear contraseñas seguras, reportar incidentes.
Boletines Mensuales	Newsletter con alertas de nuevas amenazas, tips de seguridad, reconocimientos a usuarios destacados y recordatorios de cursos.
Videos Cortos	Cápsulas de 1-2 minutos para refuerzo rápido, ideales para reuniones de equipo o comunicados internos.
Guías de Bolsillo	Documentos PDF descargables con checklists y referencias rápidas para usuarios.

2.4 Evaluación y Tests

Sistema integral de evaluación para medir la retención de conocimiento y el desarrollo de competencias:

Tipo de Evaluación	Características
Examen Diagnóstico	Evaluación inicial para determinar nivel de conocimientos y personalizar ruta de aprendizaje. Cubre temas de los tres niveles.
Evaluaciones Formativas	Cuestionarios durante cada módulo con retroalimentación inmediata. No impactan calificación final. Permiten verificar comprensión.
Exámenes de Certificación	Evaluación final por curso. Banco de preguntas aleatorizado. Calificación mínima: 80%. Intentos limitados configurables.
Evaluaciones Prácticas	Escenarios simulados donde el usuario debe tomar decisiones. Miden capacidad de aplicar conocimientos en situaciones reales.
Retroalimentación	Explicación detallada de respuestas correctas e incorrectas. Referencias a material de estudio para refuerzo.

3. FUNCIONALIDADES TÉCNICAS Y DE PLATAFORMA

3.1 Administración y Gestión (Dashboard)

Panel de control centralizado para administradores de TI y Recursos Humanos:

Funcionalidad	Descripción
Gestión de Usuarios:	Alta, baja y modificación masiva. Importación desde CSV/Excel. Sincronización automática con directorio.
Gestión de Grupos:	Creación de cohortes por área, nivel jerárquico, ubicación o criterio personalizado.
Asignación de Cursos:	Asignación individual o masiva. Rutas de aprendizaje predefinidas por perfil. Fechas límite configurables.
Gestión de Roles:	Más de 8 roles predefinidos con permisos granulares. Creación de roles personalizados.
Notificaciones:	Configuración de alertas automáticas por correo. Recordatorios de cursos pendientes y vencidos.
Calendario:	Vista de eventos, fechas límite y campañas programadas.
Configuración:	Personalización de políticas de acceso, intentos de examen, vigencia de certificaciones.

3.2 Informes y Métricas (Reporting)

Tipo de Reporte	Contenido
Dashboard Ejecutivo	KPIs de alto nivel: % completitud, tasa de certificación, tendencias de riesgo, comparativas por área.
Reporte de Cumplimiento	Estado de cumplimiento normativo. Usuarios con capacitación completa, pendiente o vencida. Exportable para auditorías.
Reporte de Riesgo por Usuario	Puntuación de riesgo individual basada en desempeño en cursos y simulaciones de phishing. Identificación de usuarios de alto riesgo.
Reporte de Phishing	Resultados de campañas de simulación: tasas de apertura, clics, reportes. Tendencias por campaña y área.
Reporte de Progreso	Avance individual y grupal en rutas de aprendizaje. Tiempo invertido, módulos completados, calificaciones.
Exportación	Formatos: PDF, Excel, CSV. Programación de envío automático. API para integración con BI.

3.3 Integraciones

Integración	Soporte
Directorio Activo:	LDAP, Microsoft Active Directory, Azure AD
Single Sign-On (SSO):	SAML 2.0, OAuth 2.0, OpenID Connect
Provisioning:	SCIM 2.0 para sincronización automática de usuarios
Correo Electrónico:	SMTP para notificaciones. Integración con Exchange, Google Workspace
LTI:	Learning Tools Interoperability para integración con otros LMS
API REST:	API documentada para integraciones personalizadas y extracción de datos
Almacenamiento:	Microsoft OneDrive, Google Drive, Dropbox para recursos
BI/Analytics:	Webhooks y exportación para Power BI, Tableau, otros

3.4 Personalización (Branding)

Opciones para adecuar la plataforma a la imagen corporativa de cada organización:

Elemento	Personalización Disponible
Logo:	Logo principal, favicon e icono de aplicación móvil
Colores:	Paleta de colores corporativos (primario, secundario, acentos)
Tema Visual:	Temas prediseñados o CSS personalizado
Dominio:	Subdominio personalizado (empresa.cognitus.mx) o dominio propio
Correos:	Plantillas de notificación con imagen corporativa
Certificados:	Diseño de certificados con logo, firma y elementos corporativos
Contenido:	Posibilidad de incluir políticas y procedimientos propios en los cursos
Materiales:	Posters, infografías y boletines adaptables a la marca

4. TEMAS CUBIERTOS (CURRICULUM)

4.1 Phishing y Seguridad del Correo

Tema	Competencias Desarrolladas
Identificación de Phishing	Reconocer señales de correos maliciosos, URLs sospechosas, remitentes falsos
Spear Phishing y Whaling	Detectar ataques dirigidos personalizados contra individuos o ejecutivos
Manejo de Adjuntos	Verificar seguridad de archivos antes de abrir, identificar extensiones peligrosas
Verificación de Enlaces	Técnicas para validar URLs antes de hacer clic, identificar dominios falsos
Reporte de Incidentes	Proceso correcto para reportar correos sospechosos al equipo de seguridad

4.2 Higiene de Seguridad

Tema	Competencias Desarrolladas
Contraseñas Seguras	Crear contraseñas robustas, usar gestores de contraseñas, evitar reutilización
Autenticación Multifactor	Configurar y usar MFA en todas las cuentas críticas
Bloqueo de Equipos	Hábito de bloquear estación al alejarse, configuración de timeout automático
Actualizaciones	Importancia de mantener software actualizado, reconocer alertas legítimas
Escritorio Limpio	No dejar documentos sensibles expuestos, destrucción segura de información

4.3 Seguridad en Trabajo Remoto y Dispositivos

Tema	Competencias Desarrolladas
Redes Seguras	Riesgos de Wi-Fi público, uso de VPN, configuración segura de red doméstica
BYOD (Bring Your Own Device)	Políticas para uso de dispositivos personales, separación de datos, MDM
Seguridad Móvil	Configuración segura de smartphones, apps de fuentes confiables, permisos
Trabajo en Espacios Públicos	Shoulder surfing, protectores de pantalla, cuidado de dispositivos
Almacenamiento en la Nube	Servicios autorizados vs. shadow IT, compartir archivos de forma segura

4.4 Protección de Datos Personales y Confidenciales

Tema	Competencias Desarrolladas
Clasificación de Datos	Identificar niveles de sensibilidad: público, interno, confidencial, secreto
Manejo de Datos Personales	Principios de la LFPDPPP, derechos ARCO, avisos de privacidad
Transferencia Segura	Métodos seguros para compartir información sensible, cifrado
Retención y Destrucción	Políticas de retención, métodos de destrucción segura de datos
Propiedad Intelectual	Protección de información propietaria, acuerdos de confidencialidad

5. CUMPLIMIENTO NORMATIVO Y SOPORTE

5.1 Alineación con Estándares y Regulaciones

Estándar/Regulación	Cobertura en Cognitus
NIST 800-50	Guía para programas de concientización en seguridad. Cognitus cubre todos los componentes recomendados: análisis de necesidades, desarrollo de materiales, implementación y evaluación.
NIST 800-16	Requisitos de capacitación en seguridad de TI. El programa incluye cursos específicos para diferentes roles según lo especificado en este estándar.
ISO 27001	Requisitos de concientización y capacitación del Anexo A (A.7.2.2). Cognitus proporciona evidencia documentada de cumplimiento para auditorías de certificación.
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Curso específico sobre la ley y sus implicaciones para el manejo de datos.
RGPD/GDPR	Reglamento General de Protección de Datos europeo. Contenido adaptable para organizaciones con operaciones en la UE.
PCI-DSS	Requisito 12.6 de capacitación en seguridad para personal con acceso a datos de tarjetas. Cursos específicos disponibles.
SOX	Sarbanes-Oxley. Documentación de controles de capacitación para auditorías de cumplimiento.

5.2 Idiomas Disponibles

Componente	Idiomas
Interfaz de Plataforma:	Español (México), Español (España), Inglés, Portugués + 100 paquetes de idioma adicionales
Contenido de Cursos:	Español (México) nativo. Inglés disponible. Otros idiomas bajo solicitud.
Materiales de Apoyo:	Español e Inglés. Adaptables a otros idiomas.
Soporte Técnico:	Español e Inglés

5.3 Soporte Técnico y Actualizaciones

Servicio	Descripción
Mesa de Ayuda:	Soporte por correo electrónico y sistema de tickets. Tiempo de respuesta: 4-8 horas hábiles.
Horario de Soporte:	Lunes a Viernes, 9:00 - 18:00 hrs (Ciudad de México). Soporte extendido disponible.
Actualizaciones de Plataforma:	Actualizaciones de seguridad mensuales. Nuevas funcionalidades trimestrales.
Actualización de Contenido:	Contenido actualizado cada 2-3 meses con nuevas amenazas, técnicas y casos de estudio.
Alertas de Seguridad:	Notificaciones de nuevas amenazas relevantes para usuarios y administradores.
Documentación:	Base de conocimientos, guías de usuario, videos tutoriales, webinars periódicos.

6. . REQUISITOS DE IMPLEMENTACIÓN

6.1 Requisitos Técnicos

Requisitos del Cliente (Usuario Final)

Componente	Requisito
Navegadores Web:	Google Chrome 90+, Mozilla Firefox 88+, Microsoft Edge 90+, Safari 14+
Aplicación Móvil:	Cognitus App para Android 8.0+ e iOS 14+
Conexión Internet:	Mínimo 1 Mbps (recomendado 5 Mbps para contenido multimedia fluido)
JavaScript:	Debe estar habilitado en el navegador
Cookies:	Deben estar habilitadas para el dominio de la plataforma
Resolución:	Mínimo 1024x768 (responsivo para dispositivos móviles)

Requisitos de Red (Para simulaciones de phishing)

Configuración	Detalle
Whitelisting de IPs:	Lista de IPs de servidores de simulación para evitar bloqueo por filtros de correo
Dominios:	Dominios de simulación a agregar en listas blancas de proxy/firewall
SPF/DKIM:	Configuración opcional para mejorar entregabilidad de correos de simulación
Excepciones de Gateway:	Reglas para permitir paso de correos de prueba sin alteración

Requisitos del Servidor (Instalación On-Premise - Opcional)

Componente	Especificación
Sistema Operativo:	Linux (Ubuntu 22.04 LTS, RHEL 8+), Windows Server 2019+
Servidor Web:	Apache 2.4+ o Nginx 1.18+ con soporte PHP
PHP:	Versión 8.1 mínimo (recomendado 8.2)
Base de Datos:	MySQL 8.0+ / MariaDB 10.6+ / PostgreSQL 13+
RAM:	Mínimo 4 GB (8 GB recomendado para >500 usuarios)
CPU:	4 cores mínimo (8 cores para alto volumen)
Almacenamiento:	50 GB mínimo (SSD recomendado)

6.2 Modelo de Licenciamiento

Modelo	Descripción	Ideal Para
Por Usuario	Licencia individual por usuario activo. Facturación mensual o anual.	Organizaciones con rotación de personal o crecimiento variable
Por Banda	Rangos de usuarios (50, 100, 250, 500, 1000+). Precio fijo por banda.	Organizaciones con plantilla estable que buscan costos predecibles
Suscripción Anual	Contrato anual con acceso completo a plataforma y actualizaciones.	Organizaciones que requieren presupuestos anuales definidos
Enterprise	Licencia corporativa ilimitada. Términos personalizados.	Grandes organizaciones con +5,000 usuarios

Todos los modelos incluyen: acceso completo al catálogo de cursos, actualizaciones de contenido, soporte técnico estándar y reportes básicos. Funcionalidades adicionales como simulaciones de phishing, API access, o personalización avanzada pueden requerir complementos.

7. RESUMEN DE CARACTERÍSTICAS

Característica	Cognitus LMS
Cursos de Concientización	✓ 35 cursos en 3 niveles
Simulaciones de Phishing	✓ +50 plantillas actualizadas
Contenido Multimedia (Videos, Gamificación)	✓ Incluido
Evaluaciones y Certificaciones	✓ Automatizadas
Dashboard de Administración	✓ Completo
Reportes en Tiempo Real	✓ Múltiples formatos
Métricas de Riesgo por Usuario	✓ Scoring individual
Integración SSO / LDAP	✓ SAML, OAuth, LDAP
API para Integraciones	✓ REST API documentada
Personalización de Marca	✓ Logo, colores, dominio
Aplicación Móvil	✓ iOS y Android
Soporte en Español	✓ Nativo
Cumplimiento ISO 27001	✓ Documentado
Actualizaciones de Contenido	✓ Incluidas
Materiales de Refuerzo	✓ Posters, infografías, boletines

Para más información o solicitar una demostración:

ventas@postech.us

"Conciencia activa, respuesta efectiva"