Technical specifications

Cognitus

Cybersecurity Awareness Platform

Product:	Cognitus LMS
Document version:	1.0.0
Document Type:	Solution description
Date of preparation:	September 11, 2025
Author:	Postech

PostecH

Conciencia activa, respuesta efectiva

COGNITUS

TECHNICAL SPECIFICATIONS

Awareness Platform
in Cybersecurity

Learning Management System (LMS)
for training and assessment in Information Security

Product:	Cognitus LMS
Product version:	5.1
Document Type:	Technical Specifications
Date:	August 21, 2025
Classification:	Commercial
Contact:	sales@postech.us

"Active awareness, effective response"

1. table of Contents

1. GENERAL INFORMATION AND SCOPE

1.1 Solution Name

Trade Name:	Cognitus LMS
Full Name:	Cognitus - Cybersecurity Awareness Platform
Current Version:	5.1
System Type:	Learning Management System (LMS)
Developed by:	Postech

1.2 General Description

Cognitus is a comprehensive Learning Management System (LMS) platform specifically designed to transform an organization's employees into an active line of defense against cyber threats.

The solution implements the concept of a "Human Firewall," recognizing that the human factor is both the greatest vulnerability and the best defense in cybersecurity. Through a structured training program, Cognitus develops practical skills that enable users to identify, prevent, and report security threats in their daily work.

The platform combines interactive multimedia content, automated assessments, phishing simulations, and tracking tools that allow measuring the program's real impact on reducing security risks.

1.3 Program Objectives

Main Learning Objectives
✓ Reduce the click-through rate on phishing emails by at least 70% ✓ Strengthen practices for creating and managing secure passwords ✓ Develop the ability to identify social engineering attempts ✓ Raise awareness about the classification and handling of sensitive information ✓ Establish a culture of immediate reporting of security incidents ✓ Comply with regulatory training requirements (ISO 27001, LFPDPPP) ✓ Reduce security incidents caused by human error ✓ Develop security "champions" in every area of the organization

1.4 Target Audience

Profile	Description	Recommended Level
General Staff	All employees without technical knowledge in security	Basic Level (15 courses)
Middle Management	Supervisors and managers with access to sensitive information	Basic + Intermediate Level (24 courses)
Senior Management	Managers and executives responsible for strategic decisions	Selected courses on governance and risk
IT Staff	Technical teams for technology and systems	Complete program (35 courses)
Safety Equipment	Cybersecurity and risk management specialists	Advanced Level + Certifications
New Admissions	Employees in the induction process	Onboarding Program (essential courses)

2. SOLUTION COMPONENTS (METHODOLOGY)

2.1 Training Modules

The awareness program is structured into 35 courses organized into three progressive levels:

Level	Courses	Duration	Approach
Essential	15	20-25 hours	Security fundamentals, common threats, best practices
Intermediate	9	15-18 hours	Security management, regulatory compliance, controls
Advanced	11	25-30 hours	Strategic management, incident response, continuity

Content Formats

Format	Description
Interactive Videos	Narrated presentations with animations, visual examples, and interactive elements. Average duration: 5-10 minutes per video.
Micro-Learning	Short 15-20 minute modules designed for agile learning without significantly disrupting work activities.
Gamification	A system of points, badges, leaderboards, and achievements that motivate participation and continuous learning.
Simulations	Interactive scenarios where the user makes decisions and observes the consequences of their actions.
Case Studies	Analysis of real industry incidents adapted for practical learning.
Infographics	Visual summaries of key concepts for quick reference and reinforcement.

2.2 Phishing Simulations

The platform includes capabilities to run simulated phishing campaigns that allow for the evaluation of real user behavior:

Feature	Description
Frequency:	Configurable: weekly, bi-weekly, monthly or custom
Types of Attacks:	Email phishing, spear phishing, whaling, smishing (SMS), vishing
Templates:	Library of 50+ templates based on real attacks, constantly updated
Personalization:	Adaptation with logos, names and specific context of the organization
Realism:	Masked URLs, lookalike domains, urgency techniques, and authority
Educational Response:	Upon clicking, the user receives immediate training on the threat
Metrics:	Open rate, clicks, reports, response time per user/area
Progression:	Incremental difficulty based on user performance

2.3 Reinforcement and Support Material

To maintain ongoing awareness beyond formal courses, Cognitus provides reinforcement materials:

Material	Use and Features
Digital Posters	High-impact graphics for corporate displays, cafeterias, and common areas. Topics: passwords, phishing, reports. Customizable with corporate branding.
Web Banners	Images for intranet, email signature and internal sites with rotating awareness messages.
Infographics	Quick visual guides on specific topics: how to detect phishing, create secure passwords, report incidents.
Monthly Newsletters	Newsletter with alerts on new threats, security tips, recognition of outstanding users, and course reminders.
Short Videos	1-2 minute capsules for quick reinforcement, ideal for team meetings or internal communications.
Pocket Guides	Downloadable PDF documents with checklists and quick references for users.

2.4 Assessment and Tests

Comprehensive assessment system to measure knowledge retention and skills development:

Type of Evaluation	Characteristics
Diagnostic Examination	Initial assessment to determine knowledge level and personalize learning path. Covers topics from all three levels.
Formative Assessments	Quizzes during each module with immediate feedback. They do not affect the final grade. They allow you to check your understanding.
Certification Exams	Final assessment per course. Randomized question bank. Minimum passing grade: 80%. Configurable limited attempts.
Practical Assessments	Simulated scenarios where the user must make decisions. They measure the ability to apply knowledge in real-life situations.
Feedback	Detailed explanation of correct and incorrect answers. References to study material for reinforcement.

3. TECHNICAL AND PLATFORM FEATURES

3.1 Administration and Management (Dashboard)

Centralized control panel for IT and HR administrators:

Functionality	Description
User Management:	Add, delete, and bulk modify. Import from CSV/Excel. Automatic directory synchronization.
Group Management:	Creation of cohorts by area, hierarchical level, location, or custom criteria.
Course Assignment:	Individual or bulk assignment. Predefined learning paths by profile. Configurable deadlines.
Role Management:	More than 8 predefined roles with granular permissions. Creation of custom roles.
Notifications:	Set up automatic email alerts. Reminders for pending and overdue courses.
Calendar:	View of events, deadlines, and scheduled campaigns.
Configuration:	Customization of access policies, exam attempts, validity of certifications.

3.2 Reporting and Metrics

Report Type	Content
Executive Dashboard	High-level KPIs: % completion, certification rate, risk trends, comparisons by area.
Compliance Report	Regulatory compliance status. Users with completed, pending, or expired training. Exportable for audits.
User Risk Report	Individual risk score based on performance in phishing courses and simulations. Identification of high-risk users.
Phishing Report	Simulation campaign results: open rates, clicks, reports. Trends by campaign and area.
Progress Report	Individual and group progress in learning paths. Time spent, modules completed, grades.
Export	Formats: PDF, Excel, CSV. Scheduled automatic sending. API for BI integration.

3.3 Integrations

Integration	Medium
Active Directory:	LDAP, Microsoft Active Directory, Azure AD
Single Sign-On (SSO):	SAML 2.0, OAuth 2.0, OpenID Connect
Provisioning:	SCIM 2.0 for automatic user synchronization
Email:	SMTP for notifications. Integration with Exchange and Google Workspace.
LTI:	Learning Tools Interoperability for integration with other LMS
REST API:	Documented API for custom integrations and data extraction
Storage:	Microsoft OneDrive, Google Drive, Dropbox for resources
BI/Analytics:	Webhooks and export for Power BI, Tableau, and others

3.4 Personalization (Branding)

Options to adapt the platform to the corporate image of each organization:

Element	Customization Available
Logo:	Main logo, favicon, and mobile app icon
Colors:	Corporate color palette (primary, secondary, accents)
Visual Theme:	Pre-designed themes or custom CSS
Domain:	Custom subdomain (company.cognitus.mx) or own domain
Mail:	Notification templates with corporate branding
Certificates:	Design of certificates with logo, signature and corporate elements
Content:	Possibility of including our own policies and procedures in the courses
Materials:	Posters, infographics and newsletters adaptable to the brand

4. TOPICS COVERED (CURRICULUM)

4.1 Phishing and Email Security

Issue	Skills Developed
Identifying Phishing	Recognize signs of malicious emails, suspicious URLs, fake senders
Spear Phishing and Whaling	Detecting targeted attacks specifically designed against individuals or executives
Handling Attachments	Verify file safety before opening; identify dangerous extensions.
Link Verification	Techniques for validating URLs before clicking, identifying fake domains
Incident Report	Correct procedure for reporting suspicious emails to the security team

4.2 Safety Hygiene

Issue	Skills Developed
Secure Passwords	Create strong passwords, use password managers, avoid reusing them
Multi-factor Authentication	Configure and use MFA on all critical accounts
Equipment Lockout	Habit of locking station when walking away, automatic timeout setting
Updates	Importance of keeping software updated, recognizing legitimate alerts
Clean Desk	Do not leave sensitive documents exposed; securely destroy information.

4.3 Security in Remote Work and Devices

Issue	Skills Developed
Secure Networks	Risks of public Wi-Fi, VPN use, secure home network setup
BYOD (Bring Your Own Device)	Policies for the use of personal devices, data separation, MDM
Mobile Security	Secure smartphone setup, apps from trusted sources, permissions
I work in public spaces	Shoulder surfing, screen protectors, device care
Cloud Storage	Authorized services vs. shadow IT, secure file sharing

4.4 Protection of Personal and Confidential Data

Issue	Skills Developed
Data Classification	Identify sensitivity levels: public, internal, confidential, secret
Handling of Personal Data	Principles of the LFPDPPP, ARCO rights, privacy notices
Secure Transfer	Secure methods for sharing sensitive information, encryption
Retention and Destruction	Data retention policies, secure data destruction methods
Intellectual Property	Protection of proprietary information, confidentiality agreements

5. REGULATORY COMPLIANCE AND SUPPORT

5.1 Alignment with Standards and Regulations

Standard/Regulation	Coverage on Cognitus
NIST 800-50	Guide for safety awareness programs. Cognitus covers all recommended components: needs analysis, materials development, implementation, and evaluation.
NIST 800-16	IT security training requirements. The program includes specific courses for different roles as specified in this standard.
ISO 27001	Awareness and training requirements of Annex A (A.7.2.2). Cognitus provides documented evidence of compliance for certification audits.
LFPDPPP	Federal Law on the Protection of Personal Data Held by Private Parties. Specific course on the law and its implications for data handling.
GDPR	European General Data Protection Regulation. Content adaptable for organizations with operations in the EU.
PCI-DSS	Requirement 12.6: Security training for personnel with access to card data. Specific courses available.
SOX	Sarbanes-Oxley. Documentation of training controls for compliance audits.

5.2 Available Languages

Component	Languages
Platform Interface:	Spanish (Mexico), Spanish (Spain), English, Portuguese + 100 additional language packs
Course Content:	Native Spanish (Mexico). English available. Other languages upon request.
Supporting Materials:	Spanish and English. Adaptable to other languages.
Technical Support:	Spanish and English

5.3 Technical Support and Updates

Service	Description
Help Desk:	Email and ticketing support. Response time: 4-8 business hours.
Support Hours:	Monday to Friday, 9:00 AM - 6:00 PM (Mexico City). Extended support available.
Platform Updates:	Monthly security updates. Quarterly new features.
Content Update:	Content updated every 2-3 months with new threats, techniques and case studies.
Security Alerts:	Notifications of new threats relevant to users and administrators.
Documentation:	Knowledge base, user guides, tutorial videos, regular webinars.

6. IMPLEMENTATION REQUIREMENTS

6.1 Technical Requirements

Customer (End User) Requirements

Component	Requirement
Web Browsers:	Google Chrome 90+, Mozilla Firefox 88+, Microsoft Edge 90+, Safari 14+
Mobile Application:	Cognitus App for Android 8.0+ and iOS 14+
Internet connection:	Minimum 1 Mbps (5 Mbps recommended for smooth multimedia content)
JavaScript:	It must be enabled in the browser.
Cookies:	They must be enabled for the platform domain
Resolution:	Minimum 1024x768 (mobile responsive)

Network Requirements (For phishing simulations)

Configuration	Detail
IP whitelisting:	List of IPs of simulated servers to avoid blocking by email filters

Domains:	Simulation domains to add to proxy/firewall whitelists
SPF/DKIM:	Optional configuration to improve deliverability of simulated emails
Gateway Exceptions:	Rules for allowing unaltered test emails to pass through

Server Requirements (On-Premise Installation - Optional)

Component	Specification
Operating System:	Linux (Ubuntu 22.04 LTS, RHEL 8+), Windows Server 2019+
Web Server:	Apache 2.4+ or Nginx 1.18+ with PHP support
PHP:	Version 8.1 minimum (8.2 recommended)
Database:	MySQL 8.0+ / MariaDB 10.6+ / PostgreSQL 13+
RAM:	Minimum 4 GB (8 GB recommended for >500 users)
CPU:	4 cores minimum (8 cores for high volume)
Storage:	50 GB minimum (SSD recommended)

6.2 Licensing Model

Model	Description	Ideal For
Per User	Individual license per active user. Monthly or annual billing.	Organizations with staff turnover or variable growth
By Band	User ranges (50, 100, 250, 500, 1000+). Fixed price per band.	Organizations with a stable workforce seeking predictable costs
Annual Subscription	Annual contract with full access to the platform and updates.	Organizations that require defined annual budgets
Enterprise	Unlimited corporate license. Custom terms.	Large organizations with 5,000+ users

All plans include: full access to the course catalog, content updates, standard technical support, and basic reports. Additional features such as phishing simulations, API access, or advanced customization may require add-ons.

7. SUMMARY OF FEATURES

Feature	Cognitus LMS
Awareness Courses	✓ 35 courses in 3 levels
Phishing Simulations	✓ +50 updated templates
Multimedia Content (Videos, Gamification)	✓ Included
Assessments and Certifications	✓ Automated
Administration Dashboard	✓ Complete
Real-Time Reports	✓ Multiple formats
Risk Metrics by User	✓ Individual scoring
SSO/LDAP Integration	✓ SAML, OAuth, LDAP
API for Integrations	✓ Documented REST API
Brand Personalization	✓ Logo, colors, domain
Mobile App	✓ iOS and Android
Support in Spanish	✓ Native
ISO 27001 Compliance	✓ Documented
Content Updates	✓ Included
Reinforcement Materials	✓ Posters, infographics, newsletters

For more information or to request a demonstration:

sales@postech.us

"Active awareness, effective response"