

Arquitectura:

PRODUCTO: EXÁMENES SEGUROS

MODELO: EDTEST.AI

MARCA: TERRITORIUM LIFE

Funcionalidades técnicas / Technical features

1. Personalización / Customization

- ⦿ Es posible personalizar el nombre de dominio de la plataforma mediante un esquema del tipo "white label"
- ⦿ Es factible reemplazar el icono de la plataforma con el logo institucional
- ⦿ Es posible agregar atributos adicionales a los usuarios de la plataforma para extender la identidad estándar
- ⦿ Es posible personalizar la interfaz de usuario a nivel plataforma para adaptarla al look and feel institucional
- ⦿ Es factible mapear la estructura de la organización en la plataforma (institución, campus, departamento)
- ⦿ Territorium ofrece herramientas de desarrollo (Developer Tools) para extender las funcionalidades de la plataforma (por ejemplo, SDK, toolkits, script blocks, plugins, add in's/add on's)
- ⦿ Es factible solicitar desarrollos a la medida (reportes, etc.)

2. Integración / Integration

- ⦿ Es posible integrar apps de diferentes tecnologías/proveedores con la plataforma
- ⦿ Es factible establecer un Single Sign On con el resto de las aplicaciones institucionales con el cliente a través del protocolo SAML 2.0
- ⦿ La plataforma ofrece un API para propósitos de integración con los estándares REST, SOAP)

3. Administración de roles / Roles management

- ⦿ La plataforma maneja roles distintos para cada perfil de usuario de la solución
- ⦿ El nivel de acceso de cada rol se puede personalizar para decidir lo que puede o no hacer en la plataforma.
- ⦿ La plataforma cuenta con un gestor de perfiles que permite granularizar permisos y privilegios. Se pueden agregar nuevos perfiles gestionando los permisos para cada nuevo perfil creado

4. Interfaz y experiencia de usuario / User interface & user experience

Se usan los estándares Web más conocidos y ampliamente utilizados son: HTML, XML y CSS. La plataforma está construida en su base respetando una ergometría visual.

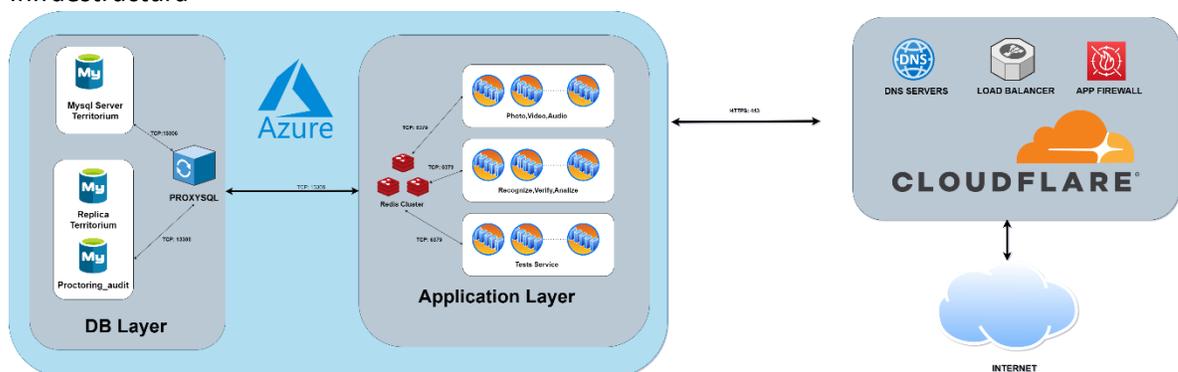
- ☉ Consistencia: El diseño es consistente a través de toda la aplicación. Tanto en las secuencias de acciones e identidad gráfica.
- ☉ Eficiencia: La interfaz debe permitir el uso eficiente del tiempo del usuario, cargando y presentando el contenido dentro un tiempo aceptable.
- ☉ Diseño: El diseño es atractivo. Esto ayuda al usuario a consumir los datos y minimizar el estrés, logrando el efecto de “sentirse bien”.
- ☉ Memoria: El uso de la memoria de los usuarios es minimizado.
- ☉ Ayuda contextual: Los recursos de ayuda deben ser visibles y estar siempre disponibles, sin interrumpir la navegación.
- ☉ Estructura y espacio: La interfaz considerara la posición de las manos, la movilidad de los dedos y el campo visual de los usuarios.
- ☉ La herramienta tiene soporte multi-plataforma y multi-dispositivo (ver tabla).

	Minimum device requirements								
	Lockdown Browser			Other Browsers					
	Desktop/Tower	Notebook/Laptop	iMac/Macbook	Desktop/Tower	Notebook/Laptop	iMac/Macbook	Apple iPad	Android Tablet	
Operating System	Windows 10, 8, and 7	Windows 10, 8, and 7	Mac Operating System 10.15 – 10.12; Mac OSX 10.11 and OSX 10.10	Windows 10, 8, and 7	Windows 10, 8, and 7	Mac Operating System 10.15 – 10.12; Mac OSX 10.11 and OSX 10.10	iPad iOS 11.0 and more recent are supported	Android version 8.0 and above.	
Browser	Lockdown Browser	Lockdown Browser	Lockdown Browser	Google Chrome 53+, Microsoft Edge +, Mozilla Firefox 42+, Opera 40+, Safari 11+	Google Chrome 53+, Microsoft Edge +, Mozilla Firefox 42+, Opera 40+, Safari 11+	Google Chrome 53+, Microsoft Edge +, Mozilla Firefox 42+, Opera 40+, Safari 11+	Google Chrome 53+, Microsoft Edge +, Mozilla Firefox 42+, Opera 40+, Safari 11+	Google Chrome 53+, Microsoft Edge +, Mozilla Firefox 42+, Opera 40+, Safari 11+	
Microphone	Microphone/Headset with mouth piece (inserted to aux point or sound input)	Microphone/Headset with mouth piece (inserted to aux point or sound input)	Microphone/Headset with mouth piece (inserted to aux point or sound input)	Microphone/Headset with mouth piece (inserted to aux point or sound input)	Microphone/Headset with mouth piece (inserted to aux point or sound input)	Microphone/Headset with mouth piece (inserted to aux point or sound input)	Microphone/Headset with mouth piece (inserted to aux point or sound input)	Microphone/Headset with mouth piece (inserted to aux point or sound input)	
Webcam/Camera	Minimum of 480p, however, 720p is recommended	Minimum of 480p, however, 720p is recommended	Minimum of 480p, however, 720p is recommended	Minimum of 480p, however, 720p is recommended	Minimum of 480p, however, 720p is recommended				
Memory (RAM)/Permanent Harddrive Space	Minimum memory (RAM) required is 75 MB	Minimum memory (RAM) required is 75 MB	Minimum memory/hard drive space is 120 MB	N/A	N/A	N/A	N/A	N/A	
Bandwidth/Internet line speed	512 kpbs (recommended 1 MB)	512 kpbs (recommended 1 MB)	512 kpbs (recommended 1 MB)	512 kpbs (recommended 1 MB)	512 kpbs (recommended 1 MB)				

- ☉ La plataforma soporta configuración multilinguaje para administrador y usuario final

5. Arquitectura / Architecture

- ⊗ La tecnología en la que está desarrollada la herramienta es PHP, Node JS CSS JavaScript, SQL Server, Mongo DB, Azure Cognitive Services de Microsoft
- ⊗ La instancia que se ofrece en la Nube de Microsoft es dedicada al Cliente para el desarrollo óptimo de la plataforma
- ⊗ La arquitectura cuenta con auto escalamiento. El escalado automático es una característica que está integrada en Cloud Services, Virtual Machines y Websites que ayuda a las aplicaciones a rendir de forma óptima cuando cambia la demanda. Por supuesto, el rendimiento significa cosas distintas, según la aplicación. Algunas aplicaciones están vinculadas a la CPU y otras a la memoria. Por ejemplo, puede que tenga una aplicación web que atienda millones de solicitudes durante el día, pero ninguna durante la noche. El escalado automático permite escalar el servicio en función de estas circunstancias o de cualquier otra métrica que defina.
- ⊗ No hay límite de almacenamiento para contenido (documentos, videos, recursos, etc.)
- ⊗ El servicio, cuenta con ambientes de desarrollo, pruebas y entrenamiento que se pueden compartir con el cliente.
- ⊗ No existe límite en la transferencia de datos.
- ⊗ Los centros de datos de Azure Microsoft para México se encuentran en las siguientes regiones:
 - Centro de EE. UU. Iowa
 - Centro-norte de EE. UU. Illinois
 - Centro-sur de EE. UU. Texas
 - Este de EE. UU. Virginia
 - Este de EE. UU. 2 Virginia
 - Oeste de EE. UU. California
 - West Central US Wyoming
 - West US 2 Washington
- ⊗ La arquitectura es multirregión para alta disponibilidad, y es configurable la elección del centro de datos.
- ⊗ Infraestructura



6. Licenciamiento / Licensing

- ⦿ Existen diferentes tipos de implementación (estándar, avanzada, empresarial) que impliquen acceso a funcionalidades diferenciadas dependiendo del esquema contratado.
- ⦿ El licenciamiento es por usuario o ilimitado.

7. Seguridad y mantenimiento / Security and maintenance

- ⦿ Se cuenta con distintas capas de seguridad, incluyendo soluciones como Cloudflare, que actúa como WAF a nivel DNS, previene ataques DDoS, y ayuda en la transferencia de datos, al actuar como un CDN. Por otro lado, se utiliza certificados SSL para el transporte de los datos, y en el caso de datos sensibles, los datos se transportan encriptados y se guardan encriptados. Cloudflare protege en varias vías: las vulnerabilidades OWASP, actúa como WAF, previene ataques DDoS, detiene acceso de intrusos, y permite controlar el acceso definiendo reglas que pueden utilizar la geolocalización.

⦿ **Comunicación Protegida**

La solución de Territorium protege todas las comunicaciones a través de Internet con la tecnología de seguridad de la capa de transporte (TLS). La TLS asegura que una comunicación no sea leída o modificada por otra entidad. Territorium Life utiliza la TLS para proteger las comunicaciones entre el servidor Web y el equipo del cliente; por ejemplo, un navegador.

La oferta SAAS requiere de manera predeterminada la tecnología de TLS en todo el sistema. La tecnología de TLS finaliza en el balanceador de carga LB de Azure. Los certificados de TLS requieren un cifrado de 2048 bits.

Azure Storage usa TLS 1.2 en puntos de conexión HTTP públicos. Sin embargo, TLS 1.0 y TLS 1.1 se siguen admitiendo gracias a la compatibilidad con versiones anteriores.

⦿ **Superficie de Ataque Mínimo.**

Las instancias de cliente de la oferta SAAS de Territorium finalizan la TLS en el balanceador de carga (LB) de Azure. Por lo tanto, los únicos activos con acceso de entrada son los LB. Los puertos disponibles son 80 (http) y 443 (https). El acceso al puerto 80 causa un redireccionamiento al puerto 443, lo cual significa que se protege la comunicación a través de la TLS. Todos los otros puertos son inaccesibles externamente, ya que Territorium aplica una política de Firewall con denegación predeterminada para la solución EDTEST de TerritoriumLife y aprovecha de esta manera toda la potencia de los grupos de seguridad de Azure Microsoft. Además, la solución EDTEST coloca toda la infraestructura no perteneciente al LB en una subred privada, completamente eliminada de Internet.

⦿ **Acceso de las aplicaciones**

Solo el personal autorizado de Territorium puede acceder a las instancias de la solución TerritoriumLife mediante la interfaz web, a través de la TLS.

🕒 **Acceso a back-end**

Una parte limitada del personal tendría acceso a la línea de comandos y back-end mediante el uso de claves SSH. El acceso solo es posible mediante claves SSH, un método de acceso más seguro en comparación con el ingreso de nombre de usuario y contraseñas. Las claves son administradas por un grupo pequeño y pueden ser revocadas en cualquier momento.

🕒 **Acceso a la consola**

El acceso de Territorium a la consola web de Azure de Microsoft requiere autenticación de factores múltiples (MFA).

🕒 **Auditoría de seguridad**

La solución de EDTEST aprovecha las potentes herramientas de auditoría de Azure, incluidas en Azure Active Directory.

🕒 **CLOUDFLARE para protección y gestionamiento DNS**

Protege en varias vías: las vulnerabilidades OWASP, actúa como WAF, previene ataques DDoS, detiene acceso de intrusos, y permite controlar el acceso definiendo reglas que pueden utilizar la geolocalización.

🕒 **Contramedidas de DDoS**

La colaboración con Azure de Microsoft para TerritoriumLife ofrece muchas ventajas en términos de escala, eficacia y seguridad. Una clara ventaja se presenta al aprovechar la infraestructura de alta disponibilidad en la que se basa Azure. Por ejemplo, la solución TerritoriumLife se beneficia a partir de las contramedidas de DDoS que los Azure proporcionaron en forma nativa.

🕒 **Capacidad de recuperación del sistema de archivos y las copias de seguridad**

La solución de EDTEST utiliza Azure Storage para realizar copias de seguridad de los datos esenciales del sistema de archivos. Se realizan copias de seguridad de estos datos cada 5 minutos. Azure Storage ofrece "**11 nueves**" de durabilidad de los datos.

🕒 **Alta disponibilidad**

La solución de EDTEST utiliza Azure. Garantizamos que las aplicaciones que se ejecutan en una suscripción de cliente estarán disponibles el **99,95 %** del tiempo.

🕒 Territorium cuenta con un plan de recuperación de desastres (DRP)

🕒 Seguimos las buenas prácticas y nuestro equipo está certificado en ITIL, PMI y somos compliant con GDPR en seguridad de datos. Nuestro sistema de calidad está basado en ISO 9000. Las certificaciones son heredadas por el uso de AZURE de Microsoft como proveedor de nube (ISO 27000, PCI-DSS)

🕒 La plataforma cuenta con métricas de uso (usuarios, sesiones, comportamiento, recursos accedidos, por hora, ubicación geográfica)

🕒 En caso de que la relación contractual se finalice, Territorium ofrece la opción de extraer la información generada por el cliente durante el tiempo que utilizó la herramienta

- ⦿ La información al término del contrato se entrega en formatos XML y SQL Dump. Vía SFTP.
- ⦿ Se realizan ejercicios sobre la detección de vulnerabilidades técnicas para minimizar los riesgos del tipo Ethical Hacking de forma constante realizadas por terceros.
- ⦿ La plataforma cumple con revisiones sobre el reporte TOP TEN de OWASP
- ⦿ Se cuenta con esquema de respaldos de información.
- ⦿ La plataforma esta sincronizada a un servicio de NTP
- ⦿ La plataforma cuenta con Endpoint Data Loss Prevention (DLP) Azure Microsoft. Se usa un tercero para azure que mejora las funciones de seguridad de la infraestructura de escritorio virtual (VDI) para incluir controles y acceso a datos basados en políticas. Nuestra prevención de pérdida de datos ayuda a descubrir, monitorear, auditar y hacer cumplir las políticas por igual en entornos físicos o virtuales. Esto nos permite monitorear y controlar consistentemente las transferencias de datos confidenciales entre la fuerza laboral interna, subcontratada, colaboradores externos y administradores de sistemas. Puede restringir accesos por dirección IP, geolocalización entre otros.
- ⦿ LA solución EDTEST Puede restringir accesos por IP, geolocalización (a nivel continente, país o estado). Esto se hace utilizando el servicio de Cloudflare, que permite configurar reglas en función de la geolocalización del usuario. Incluso se puede restringir acceso por agente(navegador), IP.

8. Ley de protección de datos personales / Personal data protection law

- ⦿ Sí, se siguen las prácticas de GDPR y han sido auditadas por múltiples clientes internacionales y en USA. Se adjuntan encabezados de los datos que se tienen, y política en el manejo de datos de Territorium.
- ⦿ Los datos son eliminados de todos lados, incluso del respaldo. Se pueden conservar hasta 6 meses después de terminado el contrato, si el cliente lo decide.

9. Soporte / Support

- ⦿ Se cuenta con los 3 niveles de soporte N1, N2 y N3. En el costo de uso de licencia se incluye nivel 2 a administradores del sistema, así como nivel 3. Si se requiere se entregue soporte directo a usuario se realiza una propuesta especial de soporte N1 según el nivel de concurrencia de usuarios esperado. Para ello se cuenta con una mesa de ayuda escalable con múltiples agentes disponibles y que ha sido utilizada con concurrencias de hasta 60,000 usuarios.
- ⦿ Se cuenta con varios canales de comunicación dependiendo el nivel de soporte: web, email, teléfono y videoconferencia durante la aplicación de las evaluaciones.
- ⦿ En tiempo de administración, el soporte es inmediato, abordándolo en una sala de videoconferencias con el equipo del cliente. En fallas críticas el tiempo de respuesta es 24/7 y en incidentes menores de lunes a viernes de 9 a 17:00 para México. RTO: menos de 24 horas. RPO: 1 hora o menos
- ⦿ Se asigna un ejecutivo de cuenta y un Project Manager exclusivo

MONTERREY HEADQUARTERS TERRITORIUM

Nogalar 208, Antiguo Nogalar, 66484 San Nicolás de los Garza,

Nuevo León, México Tel. (81) 1935 7560

CIUDAD DE MÉXICO TERRITORIUM

Hamburgo 254 esquina con Sevilla 28. Colonia Juárez. Alcaldía Cuauhtémoc
Despacho 101 y 102

SAN ANTONIO TERRITORIUM

8452 Fredericksburg Rd #045 San Antonio, Tx 78229

BOGOTÁ TERRITORIUM

CARRERA 15# 88-64 OFICINA 103 EDIFICIO ZIMMA