

# CONSIST

*Business Information Technology*

Soluciones inteligentes para un mundo digital

## Gestión de Riesgos Internos

(Monitorización | Control de Acceso | Respuesta ante incidentes)

## Consist España es parte de Consist Worldwide Software Solution group



- Mas 1000 empleados en todo el mundo
- 50 años de experiencia; 28 años en España
- Presencia multinacional
- Mas de 1400 clientes



(Ekran System)

# Gestión de Riesgos Internos

(Monitorización | Control de Acceso | Respuesta ante incidentes)

# Syteca® graba la actividad del usuario. Analiza y audita

Software de monitorización de la actividad de los usuarios que ayuda a todo tipo de empresas, a detectar amenazas internas y cumplimiento normativo.

- ✓ Compatibilidad total con sistemas operativos de escritorio y servidores
- ✓ Agente de software ligero y formatos altamente optimizados para el almacenamiento de datos
- ✓ Alertas y respuestas ante incidentes de seguridad
- ✓ Gestión de accesos e identidades
- ✓ Bajo costo total de adquisición

The screenshot displays the Syteca software interface. On the left, a 'RISK SCORE' chart shows various user activity levels from 0% to 100%. In the center, a window titled 'Budget\_plans(Finder) - 13/07/2018 19:37:23' shows a Finder window with files like 'SugarFish-budget-21Tables', 'SugarFish-budget-21Tables', and 'SugarFish-budget-21Tables'. The desktop background is a scenic landscape. On the right, a detailed log table lists numerous user activities, including file operations like 'Budget\_plans' in 'Finder' and 'Preview' applications, as well as browser sessions in 'Safari' and 'Casino Gam...'. The log includes columns for ACTI..., ACTI..., APPL..., and TI....

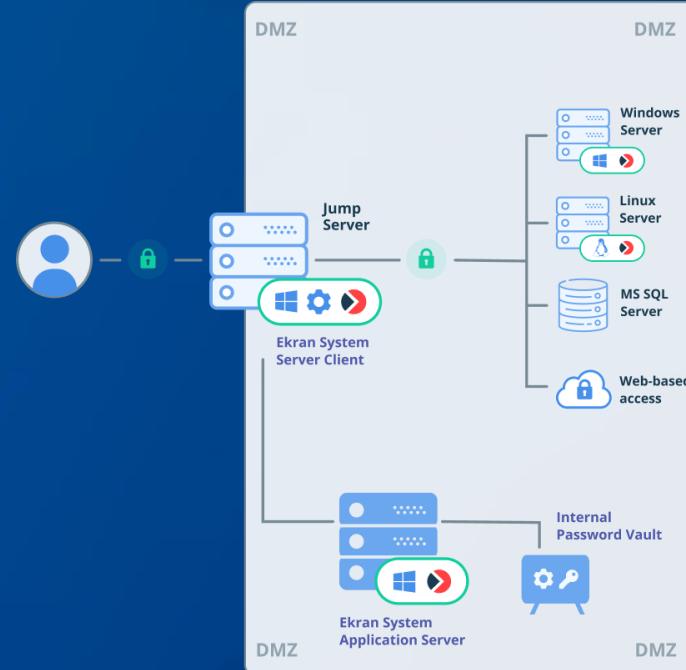
## Plataformas compatibles

	macOS	SELinux® / Linux	UNIX®
vmware®	aws	cITRIX®	

# Syteca® Gestión de Acceso Privilegiado (PAM)

Los privilegios sin control son peligrosos. Con la gestión de acceso privilegiado (PAM) de Syteca, se obtienen los controles necesarios para abordar los retos siguientes:

- ✓ Asegurar los puntos de conexión críticos
- ✓ Obtener visibilidad de todas las cuentas privilegiadas.
- ✓ Control minucioso de los permisos de acceso
- ✓ Auditar y monitorizar la actividad privilegiada
- ✓ Asegurar el cumplimiento



## Funcionalidades

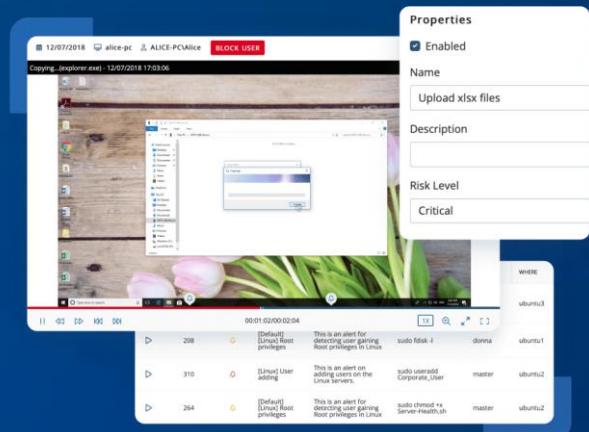
- Gestión de acceso y sesiones mediante un servidor de salto.
- Gestión y comprobación de contraseñas.
- Flujo de trabajo y aprobación de acceso.
- Doble factor de autenticación.
- Monitorización continua de las cuentas privilegiadas.
- Alertas y respuesta ante incidentes en tiempo real.

# Syteca® Detección de amenazas y respuesta en tiempo real

Detección de incidentes basada en reglas.

Grupo de reglas para cubrir los indicadores de amenazas internas más comunes. Además, permite definir reglas utilizando diversos parámetros como nombres de procesos, direcciones web abiertas, dispositivos USB conectados, pulsaciones de teclas o comandos Linux ejecutados, etc.

The screenshot shows the Syteca alert management interface. On the left, there's a list of alerts with columns for Name, Description, Assigned To, State, Notification, and Email Recipient. One alert is selected, showing its properties: Name is 'Unusual working hours', Conditions are 'Unusual work hours', and State is 'High'. On the right, there's a section for 'Email Notifications' with options like 'Send notification on detected anomalies for a finished session', 'Send instant notification on detected anomalies', 'Send total session risk score in case of no anomalies', and 'Send email notification'. Below that is an 'Additional Actions' section with options like 'Show warning message to user' and 'Block user in the current session'.



## Análisis del comportamiento de usuarios y entidades (UEBA)

El sistema de alertas incluye un módulo de inteligencia artificial que compara el comportamiento de los usuarios con múltiples factores para detectar actividades anómalas de los usuarios y posibles cuentas comprometidas

The screenshot shows the Syteca endpoint access control interface. At the top, there are tabs for 'ACCESS REQUESTS', 'TWO-FACTOR AUTHENTICATION', and 'ENDPOINT ACCESS CONTROL'. A search bar is at the top right. Below, a table lists access requests with columns for Status, Request type, User, Client, Processed by, Request time, and Processed time. The first request is from 'Comp10\BenjaminTeel' on 'Comp10' requesting mass storage device access. The status is 'Pending' with a note 'please grant access according to ET-3633'. The second request is from 'Comp1\John Dean' on 'Comp1' requesting use of a flash drive. The third request is from 'Paul.Mac\Paul' on 'Comp1' requesting use of a flash drive. Approval status is shown in green bubbles: 'Approved by demo\_user\_First demo\_user\_Last' for the first two, and 'Approved by demo\_user\_First demo\_user\_Last' for the third.

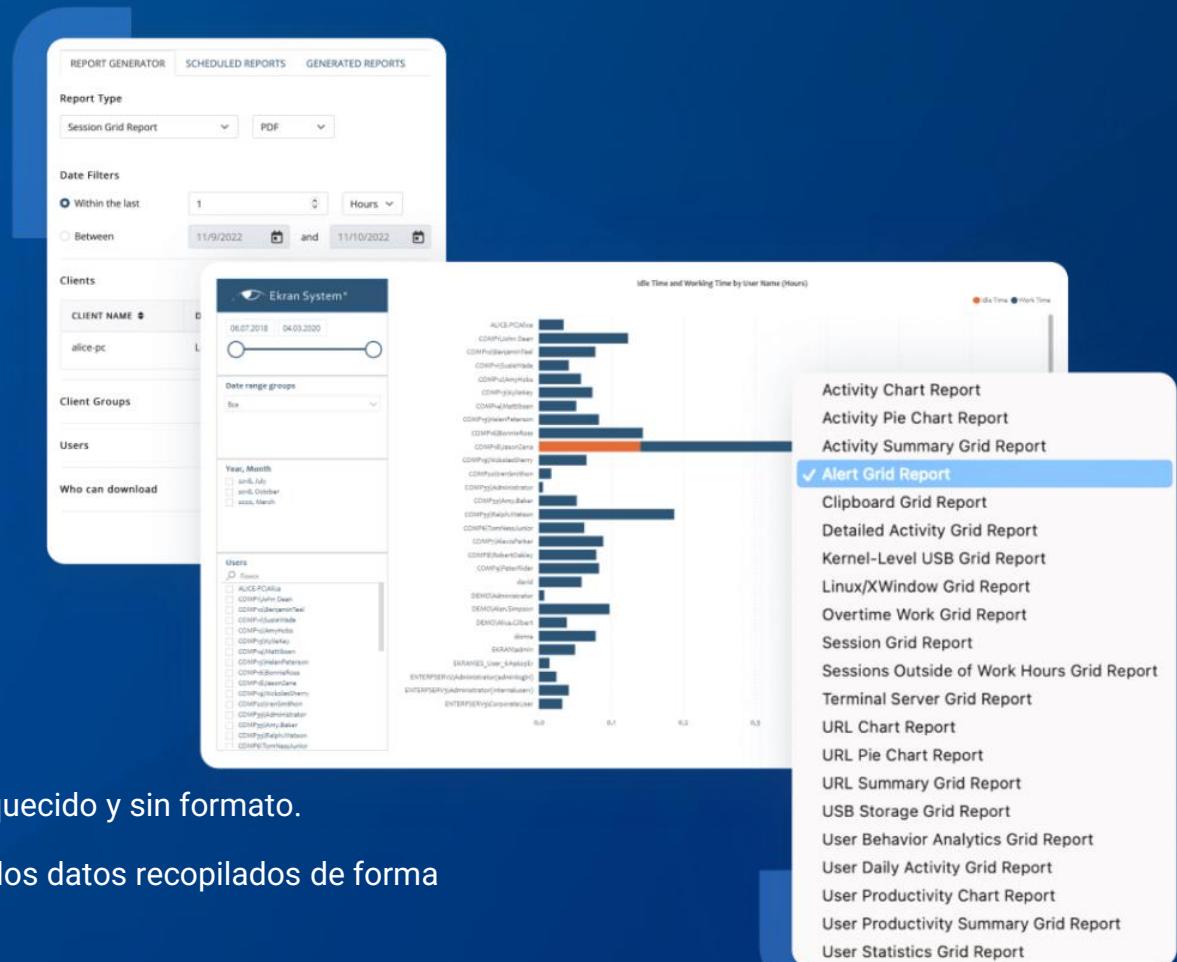
## Gestión de USB

Permite detectar y rastrear, pudiendo activar alertas al conectar varios tipos de dispositivos USB. También ofrece un conjunto de herramientas para bloquear dispositivos específicos, además de posibilitar su aprobación manual.

# Auditoría mejorada e informes de actividad de los usuarios

Con Syteca, puede generar informes detallados en múltiples formatos y analizar el panorama de amenazas durante períodos de tiempo específicos. Esto le ayudará a:

- ✓ Detectar a tiempo las amenazas internas
- ✓ Responder eficazmente ante incidentes
- ✓ Crear un rastro de auditoría claro y eficaz
- ✓ Ayudar al cumplimiento de TI



Generación de informes ad hoc manualmente o de forma automática

Creación de informes en diversos formatos, como PDF, HTML, Excel, CSV y texto enriquecido y sin formato.

Gracias a la API de Syteca se puede integrar con Microsoft Power BI, puede presentar los datos recopilados de forma personalizada, interactiva y fácil de usar.

# Syteca® le ayuda a cumplir con las siguientes normativas:

[ISO 27001](#)

[PCI DSS](#)

[SWIFT CSP](#)

[SOX](#)

[FISMA](#)

[GDPR](#)

[NIST 800-53](#)

[NIST 800-171](#)

[NERC](#)

[GLBA](#)

[NISPOM Change  
2 and H.R 666](#)

[SOC 2](#)

[HIPAA](#)

[DORA](#)

[NIS2](#)

# RESUMEN

Una visión y gestión unificada y simplificada del fraude y el riesgo en todos los canales y aplicaciones.

**Supervise las aplicaciones de una forma más avanzada de lo que nunca creyó posible.**



## Análisis en tiempo real

Capture el comportamiento de los usuarios en tiempo real en todos los sistemas



## Gestión de Acceso Privilegiado (PAM)

Obtener visibilidad absoluta de todas las cuentas privilegiadas



## Reproducción Visual

Audite el acceso de los usuarios sin invadir la privacidad de los empleados



## Investigaciones más rápidas

Reduzca costes con sólidas herramientas de investigación



## Seguridad Integral

Datos de todos los canales para análisis, informes y alertas

GRACIAS

# Soluciones Consist España y Portugal



Solución tecnológica que ofrece todas las facilidades para desarrollo, migración automática y modernización de aplicaciones ADABAS®/NATURAL®. Atiende todas las exigencias de las empresas que necesitan migración rápida y sin riesgo de sus aplicaciones corporativas con una reducción de costo representativa.



La forma más rápida de conectar vía APIs sus20. Diapositiva 20 sistemas Back-end centrales(sistemas legacy) con soluciones móviles, en la nube y web en tan solo unos minutos



Low Code application platform Lcap/NoCap que permite construir aplicaciones web o móviles en un entorno seguro y hasta un 80% más rápido que con desarrollo convencional.



Plataforma de comunicación digital omnicanal que permite a los clientes establecer una comunicación e interacción directas con el representante de una organización a través de diversos canales y plataformas -teléfonos inteligentes, tabletas y ordenadores-, proporcionándoles así una experiencia de atención al cliente innovadora, rápida y eficaz.



ETL basada en Apache Spark. Genera de forma automática y sin codificación procesos para suministrar información a herramientas BI. BigBI permite automatizar procesos para explotar la información almacenada en Data Lakes de forma ágil y rápida