
WWW.CYTE.CO

PRODUCTOS & SERVICIOS

cyte
We-know-how®

Empleamos criptografía post-cuántica en nuestros productos de seguridad cibernética.

Somos cyte, una empresa con más de 25 años en el mercado, expertos en el desarrollo de soluciones tecnológicas seguras, rápidas y eficientes; basadas en criptografía post-cuántica.

Fabricamos y desarrollamos productos innovadores, diseñados para resistir incluso a ataques cuánticos. Nos enfocamos en convertirnos en un aliado estratégico para las organizaciones, habilitando y promoviendo buenas prácticas para la implementación de nuestra tecnología.





PRODUCTOS

Nuestro portafolio consta de siete productos innovadores, diseñados con la criptografía y la criptografía post-cuántica en su núcleo, cada uno de estos es la demostración de nuestro compromiso con la vanguardia tecnológica y la seguridad cibernética.

CRYPTO-VAULT®

CRYPTO-VAULT®

Con Crypto-Vault® y un diagnóstico detallado de la infraestructura usamos cifrado y firma digital para proteger la información sensible de extremo a extremo. Así, nos comprometemos a garantizar la confidencialidad, integridad y seguridad de los datos que deban ser compartidos a nivel interno o con terceros, con el fin de evitar fraudes, alteración, riesgos o pérdida de la información.

CRYPTO-VAULT ULTRA®

Cuando la organización debe realizar múltiples procesos de cifrado y su administración se hace compleja y de gran responsabilidad, si necesitamos centralizarlo para su control y generar constantemente un número de operaciones de criptografía de manera automática y segura, esta herramienta es la indicada.

CRYPTO-VAULT-CLOUD®

Crypto-Vault-Cloud®, habilita las diferentes funcionalidades de Crypto-Vault®, a través de un REST API, el cual puede ser invocado para cifrado, firma digital y administración de llave. Dicho REST-API puede ser consumido desde cualquier lenguaje de programación, en caso de que se quieran procesos automatizados, o se puede consumir por medio de una interfaz gráfica Web que viene con el producto.

TOKENIZER®



Con Tokenizer® aseguramos la información sensible, que está almacenada en bases de datos o en reposo para prevenir fraudes, robos o modificaciones; y así garantizar la máxima seguridad, confidencialidad e integridad de la información, soportado con tecnología criptográfica.

Tokenización de
datos individuales

Integración con
hardware criptográfico

Tokenización de una
columna de un DB o archivo

Tokenización en
múltiples bases de datos

NOTYFIND®



Con Notyfind®, descubre y evita el vencimiento de certificados digitales mediante alertas oportunas que recuerdan su vencimiento. Además, realiza la renovación automática de certificados y dominios, para así garantizar la centralización, control y continuidad de la operación de las plataformas.

Descubrimiento

de Certificados SSL/TLS en la red de la organización.

Integración

con Windows Server Active Directory Certificate Service (ADCS).

Envío

de notificaciones a funcionarios encargados de la renovación.



WEB-ARMOR®



La información que es enviada desde el navegador o aplicación móvil de un usuario hasta el servidor, puede ser hurtada para cometer fraudes letales. Esta información suele protegerse, únicamente, con TLS (sucesor de SSL). Sin embargo, TLS y SSL tienen múltiples vulnerabilidades.

Dado que hay y seguirá habiendo muchas más vulnerabilidades, es esencial añadir una capa adicional de seguridad con criptografía, si el objetivo principal de tu organización es salvaguardar los datos.

Web-Armor® brinda una capa de cifrado adicional e impenetrable, ayudando a proteger la información que se transmite a través de un ambiente web, de riesgos, vulnerabilidades y ataques cibernéticos.



Las contraseñas suelen ser el eslabón más débil de la cadena de seguridad de una empresa, y tanto las aplicaciones de software como cuentas de usuario están en alto riesgo.

La administración corporativa de contraseñas mitiga el riesgo de filtración de datos, fortaleciendo el eslabón más débil y evitando fraudes causados por empleados despedidos, o por interrupciones debido a ausencias (salud, vacaciones o calamidades). Logrando así reducir todos los riesgos relacionados a contraseñas y, por defecto, se hacen cumplir las políticas recomendadas por los mejores estándares de seguridad.

Passguard®, centraliza las contraseñas de toda la organización, para resguardarlas y gestionarlas de forma segura y eficiente.



QUANTUMTALK®



VISUALIZACIÓN ÚNICA DE TRANSFERENCIAS DE ARCHIVOS

- Recibe la corriente de transferencia, procesándola únicamente en memoria, sin escribirla en disco.
- El contenido se muestra en un visor diseñado para prevenir la captura de pantalla.
- Cuando el visor se cierra o la aplicación cambia, el archivo se elimina de la RAM.
- En este punto, el archivo desaparece completamente del dispositivo.
- Esto lo hace muy difícil para el usuario acceder al archivo en el dispositivo.

RIESGOS: En todos los casos, si el usuario que recibe el archivo posee el hardware, él o ella podría hacer jailbreak para acceder al contexto de memoria de cualquier programa.

SERVICIOS

Servicios enfocados en el análisis, desarrollo y entrenamiento, con el propósito de reforzar tanto el conocimiento como los hábitos de seguridad dentro de la organización. Logramos que tus empleados sean más conscientes frente al riesgo y las consecuencias que conlleva un ataque cibernético, para así, crear hábitos de seguridad permanentes

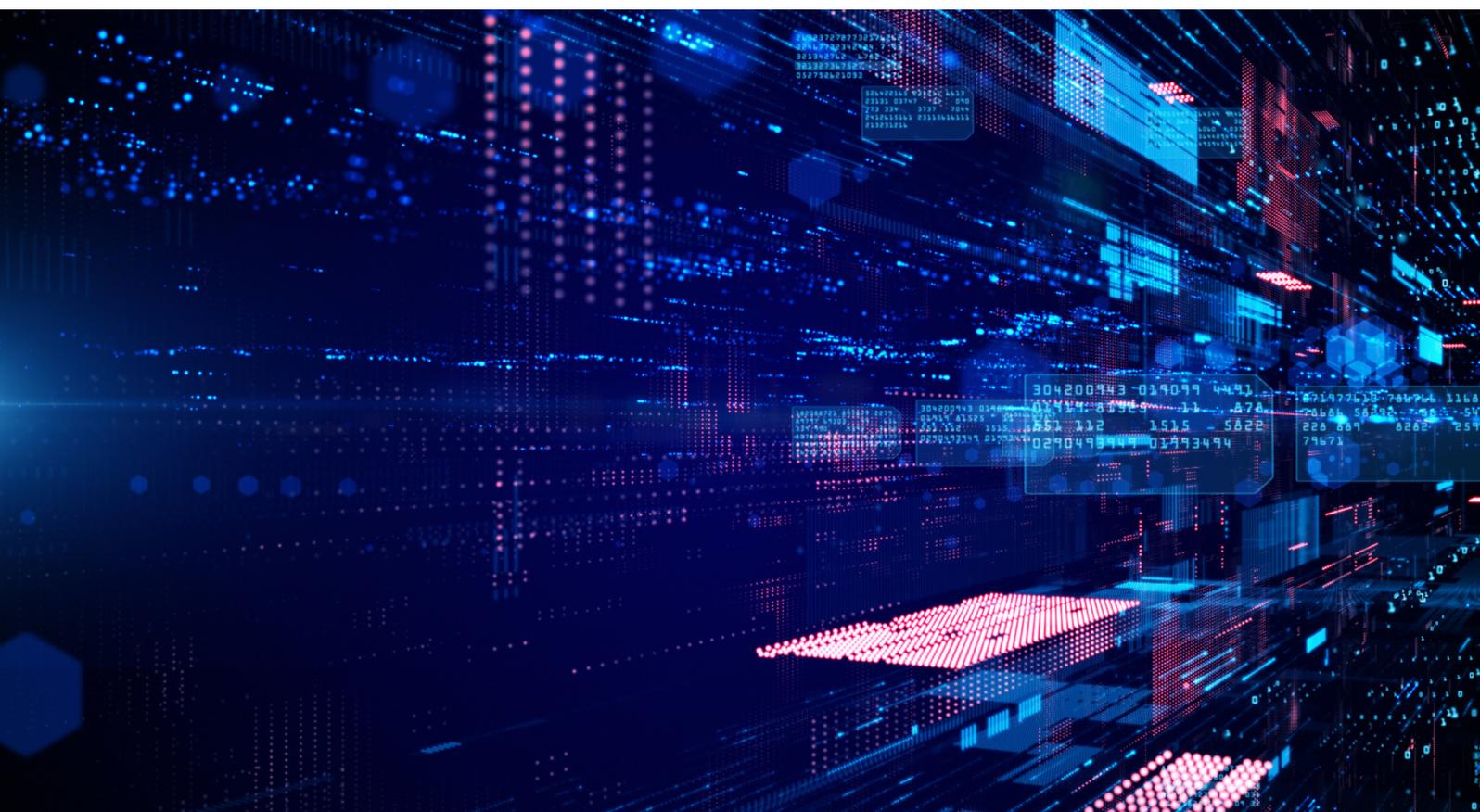
CONSULTORÍA

Nos enfocamos en realizar un análisis de riesgo informático donde podemos identificar las zonas en las cuales se requiere reforzar los procesos de seguridad en el software.

Adicionalmente, realizamos hacking ético, con un equipo de hackers con conocimiento mucho mas alto que el del promedio del mercado.

DESARROLLO DE APLICACIONES

Nuestro equipo de ingenieros de desarrollo se enfrentan a los retos del mercado desarrollando aplicaciones complejas que incorporan códigos de seguridad en cada uno de los pasos, haciéndolas seguras y confiables.





ENTRENAMIENTOS

Realizamos entrenamiento en ingeniería criptográfica, gestión y configuración de seguridad en redes, gerencia de seguridad y código seguro.

Cada uno de nuestros entrenamientos tiene como objetivo principal capacitar a los colaboradores sobre las posibles amenazas que pueden enfrentar y cómo pueden actuar para mantener seguros los datos.

Además el aprender y entender la importancia de la seguridad en cada uno de los procesos que se realicen en la organización dando pautas al personal, a nivel de ingeniería, para implementar dichas soluciones.

ETHICAL HACKING

Aplicaciones: web, escritorio, móviles

Infraestructura y redes: aplicaciones propias y de terceros

Previo a un release o posterior a la concepción Y sistemas en producción.

www.cyte.co

cyte
We-know-how®

¡Conoce más!

