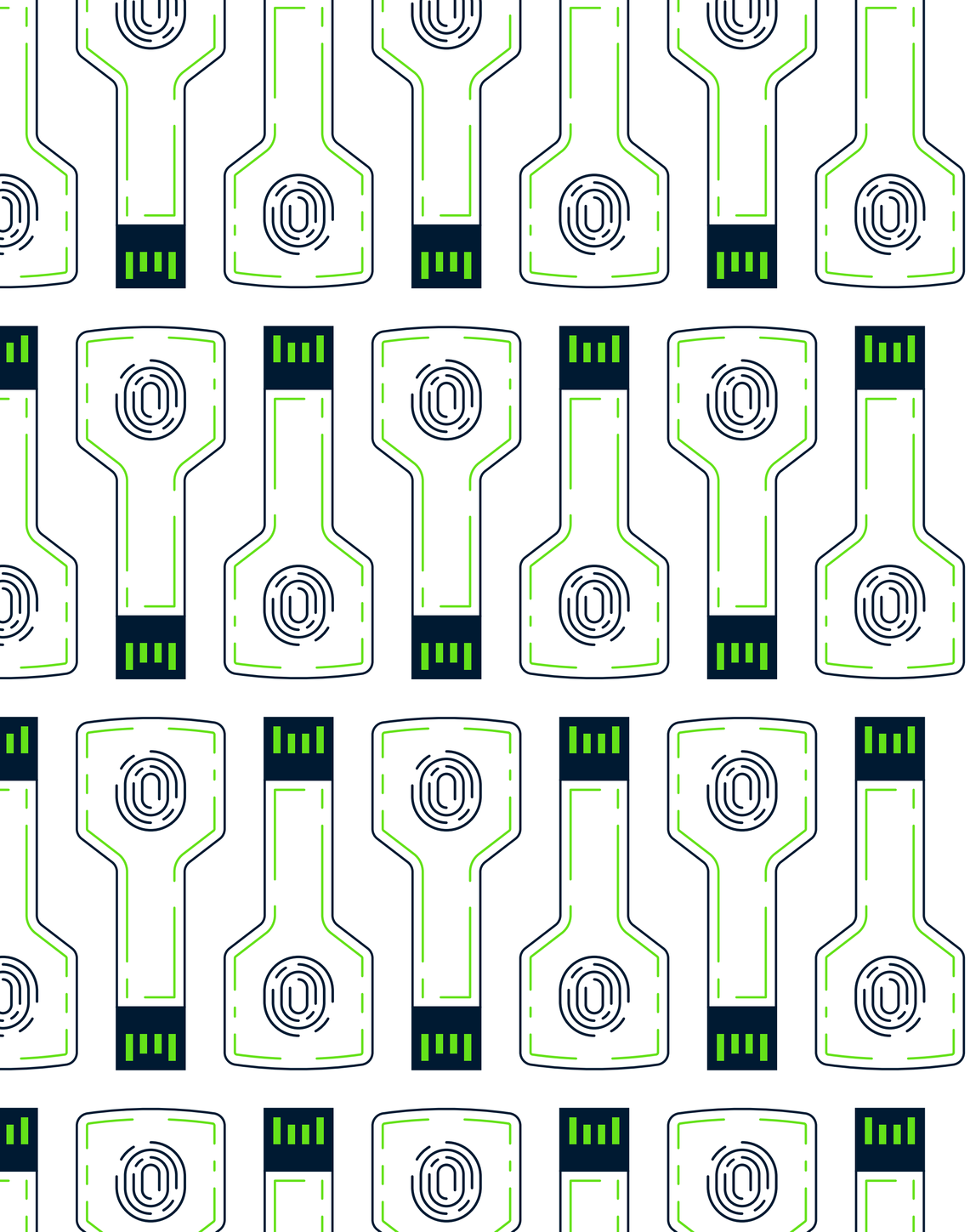
eti Tecnologías de la Información BioCubaFarma

ideas frescas

CIBER-SEGURIDAD



DIVISIÓN DE CIBERSEGURIDAD

Nuestra misión es garantizar la seguridad de la infraestructura de infocomunicaciones; brindando soporte y asesoría dentro del Grupo de las Industrias Biotecnológica y Farmacéutica de Cuba y a terceros que requieran de nuestros servicios.

NUESTROS ESPECIALISTAS CALIFICADOS

Se distinguen por su experiencia en el campo de la Seguridad Informática.

MAESTRÍAS EN:

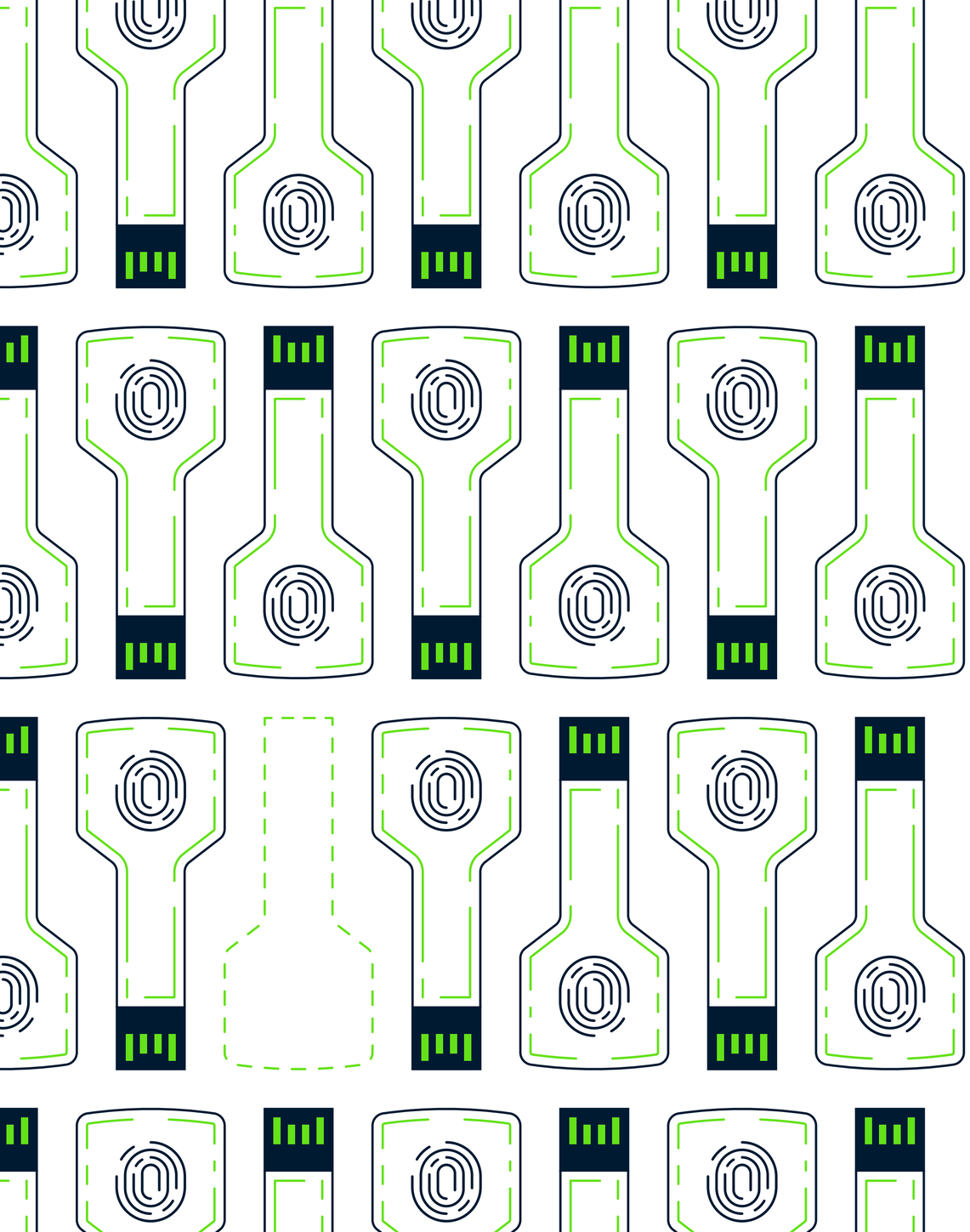
- Ingeniería en Aplicaciones Criptográficas.
- Sistemas de Telecomunicaciones.
- Seguridad Informática.
- Informática Aplicada.
- Análisis de Información y Prospectiva.

CERTIFICACIONES INTERNACIONALES EN:

- Ciberataques y Técnicas de Prevención.
- Hacking Ético.

COLABORADORES:

OSRI / MINCOM / MININT



NUESTROS SERVICIOS:

CS1.
DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA.

CS2.
PROTECCIÓN CRIPTOGRÁFICA.

CS3.
ANÁLISIS DE TRAZAS.

CS4.
ESCANEO PROFUNDO DE SITIOS WEB.

CS5.
SERVICIOS DE MONITOREO DE EVENTOS DE SEGURIDAD Y SOLUCIÓN PARA ANÁLISIS DE TRAZAS EN SEGURIDAD INFORMÁTICA.

CS6.
CONSULTORÍA PARA LA GESTIÓN SEGURA DE REDES.

CS7.
SERVICIOS ESPECIALIZADOS.

CS8.
CIBERSEGURIDAD COMO SERVICIO.

CS9.
IMPLEMENTACIÓN DE UNA INFRAESTRUCTUR DE LLAVE PÚBLICA.

CS10.
ADIESTRAMIENTO ONLINE.

CS1.
DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA.

Permite realizar un **ANÁLISIS DE LA SEGURIDAD DE LA RED** para identificar los riesgos, las amenazas y las vulnerabilidades de los activos, sistemas y servicios de la infraestructura tecnológica con impacto en las operaciones de negocio.

- Revisión de la infraestructura de Infocomunicaciones.
- Revisión de la protección perimetral en la red.
- Revisión de la infraestructura de virtualización.
- Revisión de las políticas de filtrado implementadas.
- Identificación y detección de vulnerabilidades de los servicios y sistemas desplegados en la infraestructura tecnológica.
- Revisión de las políticas implementadas para la actualización de los parches de seguridad para sistemas operativos y la actualización de los sistemas antivirus empleados.

Contempla, además, **ANÁLISIS DEL SISTEMA DE GESTIÓN DOCUMENTAL DE LA SEGURIDAD DE LA INFORMACIÓN** para la identificación de medidas de acción preventivas y correctivas para minimizar los riegos.

- Evaluación del Sistema de Gestión de la Seguridad Informática (SGSI).
- Levantamiento y caracterización del Sistema Informático.
- Análisis y Cálculo de Riesgos.
- Elaboración, actualización o derogación de las Políticas, Medidas y Procedimientos.
- Elaboración del Plan de Contingencia.
- Elaboración del Plan de Seguridad Informática.

CS2.
PROTECCIÓN CRIPTOGRÁFICA.

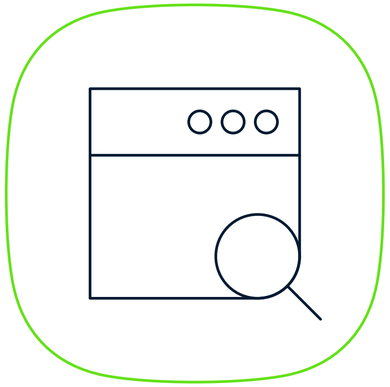
INSTALACIÓN, CONFIGURACIÓN Y CAPACITACIÓN para el empleo de sistemas criptográficos que garanticen la integridad, confiabilidad y seguridad de la información.

- Solución **ECIF** para la protección de la información basado en el cifrado de ficheros y documentos clasificados para su transmisión por canales no seguros.
- Solución **VIPNET**, aprobada por el MININT para el establecimiento de una Red Privada Virtual (VPN) que garantice la transmisión por canales seguros de datos empleando sistemas criptográficos.
- Solución para garantizar **AUTENTICACIÓN SEGURA EN LA ADMINISTRACIÓN DE SERVIDORES** basada en la generación de llaves criptográficas.

CS3.
ANÁLISIS DE TRAZAS.

ANÁLISIS DE LAS TRAZAS DE NAVEGACIÓN DE INTERNET DE LOS USUARIOS que emplean el servicio, reflejando información estadística de los principales usuarios que utilizan el servicio, acceso a sitios no permitidos, así como los sitios web más visitados, el número de sesiones y el tiempo de duración de cada una.

Adicionalmente se brinda el servicio de **ANÁLISIS DE LAS TRAZAS DE SISTEMAS Y SERVICIOS** para el análisis de incidentes de seguridad.



CS4.
ESCANEO PROFUNDO DE SITIOS WEB.

Empleo de herramientas para la **EVALUACIÓN INTEGRAL DE LA SEGURIDAD DEL SERVICIO WEB** permitiendo medir el grado de optimización del sitio hospedado y detectar vulnerabilidades que puedan comprometer el correcto funcionamiento del sistema y que pongan en riesgo la integridad del mismo.

- Verificación de los tiempos de respuesta de la aplicación.
- Análisis de errores en el código de programación y enlaces truncados.
- Verificación de la aplicación de filtro de caracteres a formularios de búsquedas.
- Verificación de la autenticación basada en Token de la aplicación web.
- Verificación de vulnerabilidades XSS, CSRF, etc.
- Búsqueda de formularios de autenticación con auto-completamiento activados.
- Búsqueda de lazos o bucles en el código de la aplicación web.

Se brinda además un servicio de **RE-ESCANEO DE SITIOS WEB**, una vez culminado el proceso de corrección de deficiencias identificadas en el Escaneo Profundo del Sitio Web, para comprobar si fueron corregidas las vulnerabilidades anteriormente señaladas e identificar nuevas amenazas.

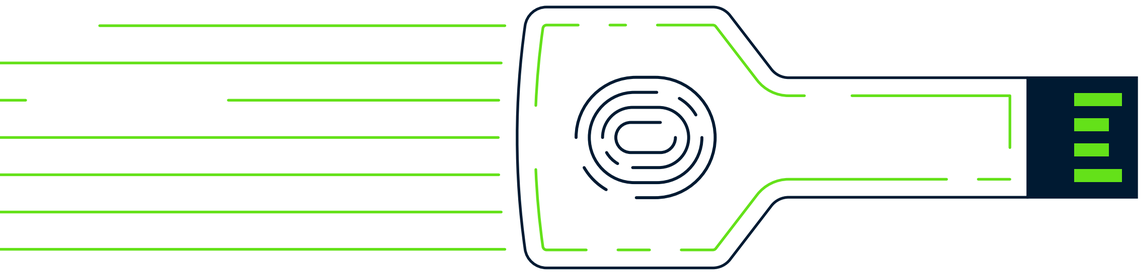
- Re-escaneo del sitio Web para verificar la solución de las vulnerabilidades detectadas en el escaneo anterior.
- Identificación de nuevas amenazas.

CS5.
SERVICIOS DE MONITOREO DE EVENTOS DE SEGURIDAD Y SOLUCIÓN PARA ANÁLISIS DE TRAZAS EN SEGURIDAD INFORMÁTICA.

La plataforma para la Gestión de Eventos e Información de Seguridad Open Source (OSSIM, por sus siglas en inglés) es una solución SIEM (Security Information and Event Managent) que permite centralizar incidentes de seguridad. Su arquitectura está conformada por dos componentes principales: Sensor y Servidor. El Sensor permite la detección de activos de la red, evaluación de vulnerabilidades, recolección de flujo de tráfico y detección de incidentes. El Servidor tiene la función de centralizar y procesar la información enviada por el (los) sensor(es) desplegados en la red, correlacionar eventos, dar seguimiento a incidentes de seguridad a través de un sistema de gestión de tickets, definir prioridades a los diferentes eventos detectados y visualizar de forma amigable toda la información recibida para su posterior análisis. Esta solución integra un conjunto de herramientas de seguridad que de una forma armónica e integradora permite detectar incidentes de seguridad a través de la habilitación o despliegue de nuevos plugins encontrándose entre los más empleados el Sistema de Detección de Intrusos de Red (NIDS) Suricata y el Sistema de Detección de Intrusos de Host (HIDS) OSSEC. Su flexibilidad radica principalmente en la posibilidad que brinda la plataforma para desarrollar nuevos plugins que tributen información acerca de un evento determinado que se desee alertar.

A PARTIR DE LA IMPLEMENTACIÓN DE ESTE SERVICIO ES POSIBLE:

- Notificar incidentes de seguridad reportados por la plataforma de monitoreo que pongan en riesgo la seguridad de la infraestructura tecnológica de su entidad.
- Brindar informes periódicos acerca de las vulnerabilidades de los sistemas, plataformas y servicios de la entidad incluidos en el presente contrato.
- Análisis en tiempo real de las trazas de los distintos sistemas.



CS6.
CONSULTORÍA PARA LA GESTIÓN SEGURA DE REDES.

COMPRENDE LAS SIGUIENTES ACTIVIDADES:

1. Diseño de arquitectura para el despliegue de sensores OSSIM.
2. Instalación, configuración y administración de sensores OSSIM.
3. Monitoreo de eventos de seguridad.
4. Notificación de alertas generadas por la Plataforma OSSIM.
5. Escaneo de vulnerabilidades que incluye hasta 12 sistemas o servicios y una vez solucionadas las vulnerabilidades identificadas se realizará un re-escaneo.
6. Instalación, configuración y administración del servidor Splunk.
7. Creación de dashboard personalizados y generación de reportes.
8. Capacitación para el empleo de la herramienta Splunk.

Asesoramiento en temas de ciberseguridad para la concientización del personal que trabaja en temas vinculados a la informática y las comunicaciones, que contribuyan de manera efectiva al despliegue seguro de nuevos servicios.

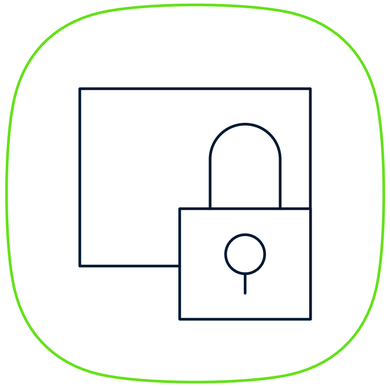
Eventos en temas de ciberseguridad.

CS7.
SERVICIOS ESPECIALIZADOS.

Servicios Especializados que complementan los niveles de seguridad de los sistemas y servicios desplegados en la infraestructura de infocomunicaciones que garanticen en gran medida la confidencialidad, integridad y disponibilidad de la información.

SERVICIOS BRINDADOS:

- Habilitación de los registros de la auditoría SQL.
- Instalación y configuración de filtros de contenido integrado a servidores proxy.
- Instalación y configuración básica de sensores OSSIM.
- Configuración de firewall de aplicación Mod-Security con reglas de filtrado específicas.
- Configuración segura de servidores web (servicio HTTPS).
- Análisis de flujo de tráfico de red.
- Detección y descontaminación de virus informáticos.
- Instalación, configuración y puesta en marcha del KAV y WSUS.



CS8.
CIBERSEGURIDAD COMO SERVICIO.

Gestión automatizada de eventos de seguridad empleando la plataforma para la Gestión de Eventos e Información de Seguridad Open Source (OSSIM) para el monitoreo de eventos de seguridad, levantamiento de activos, correlación de incidentes de seguridad y detección de vulnerabilidades.

PLATAFORMA DE EVENTO DE SEGURIDAD EN LA NUBE.

A PARTIR DE LA IMPLEMENTACIÓN DE ESTE SERVICIO ES POSIBLE:

- Ahorro de recursos tecnológicos, los cuales pueden ser destinados para otras funciones.
- Disminución del tiempo para comenzar con el empleo de la plataforma.
- Contar con especialistas encargados de la administración y configuración óptima de la plataforma garantizando así:
  - Proceso de actualización de la plataforma de supervisión hacia nuevas versiones.

- Actualización automática de las reglas empleadas por el Sistema de Detección de Intrusos de Red.
- Bases de datos de vulnerabilidades actualizadas.

- Se garantiza comunicación encriptada entre el sensor y el servidor.
- Manejo seguro de las credenciales de usuarios.
- Identificación y protección de los datos sensibles a partir del establecimiento de mínimos privilegios.
- Configuración y empleo del módulo de Intercambio de Amenazas (OTX) para la generación de eventos en tiempo real basados en nuevas amenazas.
- Contar con sistema de salva automática que garantice un respaldo de la información ante fallas técnicas.
- Preparación de los especialistas designados para el empleo de la plataforma.
- Contratación de nuevos servicios para la integración de la plataforma con servicios y sistemas desplegados en la infraestructura tecnológica, acorde a las características de la entidad.
- Retroalimentación de la información brindada por la Base de Datos del Conocimiento por los especialistas del Grupo de Ciberseguridad.

COMPRENDE LAS SIGUIENTES ACTIVIDADES:

1. Elaboración del proyecto:
   - Acta de Inicio.
   - Identificación de la red LAN.
   - Confección del Proyecto Final.
   - Discusión del Proyecto con el cliente.
2. Implementación y Configuración:
   - Instalación de sensores.
   - Configuración básica de sensores.
   - Habilitación de plugins.
   - Configuración de plugins.
3. Preparación:
   - Capacitar al cliente para el empleo de la plataforma.
4. Monitoreo de Eventos.
   - Creación de los grupos de redes.
   - Levantamiento de activos.
   - Configuración de tareas de escaneo de vulnerabilidades de los sistemas.
   - Creación de politicas personalizadas para eliminar falsos positivos.

PLATAFORMA DE ANÁLISIS DE TRAZAS EN LA NUBE basado en la solución Splunk.

Acceder a un sistema que gestiona de forma centralizada, y en tiempo real, las trazas de los sistemas, servicios y aplicaciones desplegadas en la infraestructura tecnológica.

CS9. IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE LLAVE PÚBLICA.

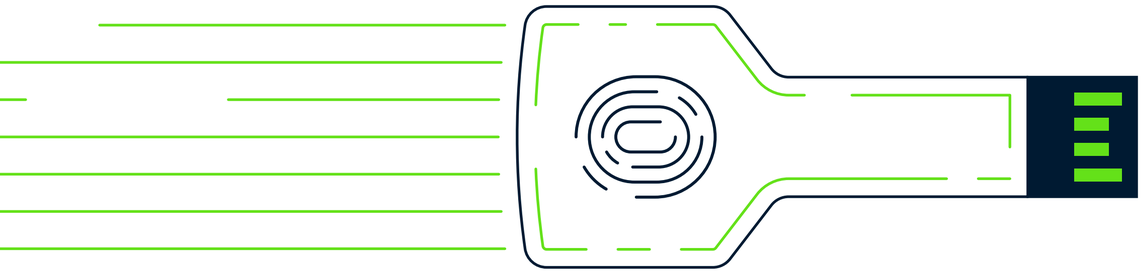
Gestión personalizada de una PKI a partir de la implementación de una estrategia de transformación digital de la información en el sector empresarial.

A PARTIR DE LA EJECUCIÓN DE ESTE SERVICIO ES POSIBLE:

- Autenticar usuarios, máquinas y servidores dentro de la propia organización.
- Aumentar el nivel de cifrado y recursos de valor agregado para asegurar que el sitio web este protegido, y este al día con las necesidades actuales de los sitios web modernos. Clientes y visitantes sabrán que la navegación en el sitio es seguro y que los detalles de pago e informaciones personales están protegidos y cifrados.
- Tener una manera fácil de implementar y económica de agregar firmas digitales a los procesos, ofreciendo mayor seguridad en torno a la identidad del suscriptor, autenticidad de la firma e integridad del contenido.

COMPRENDE LAS SIGUIENTES ACTIVIDADES:

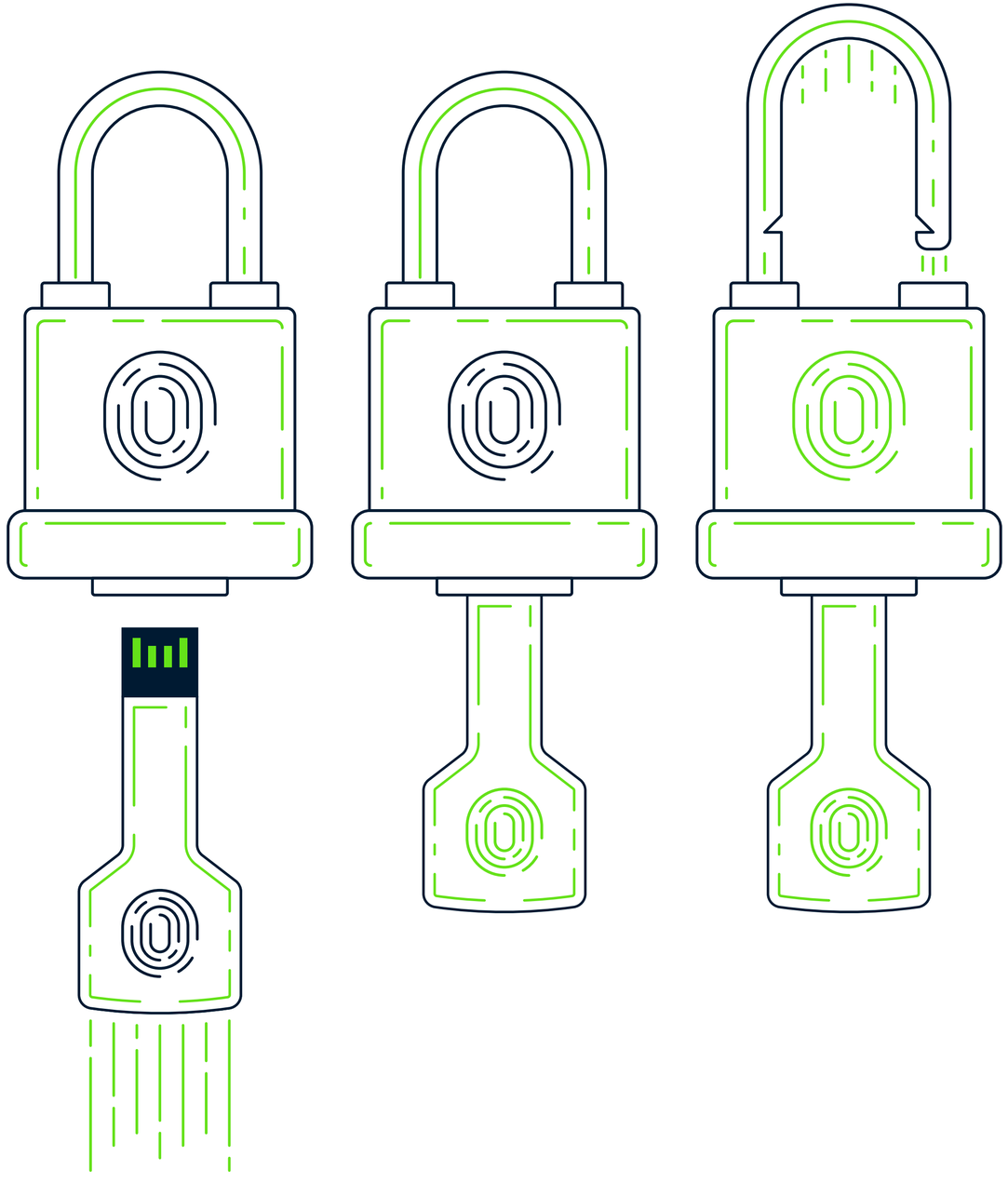
1. Capacitación de directivos enfocada al establecimiento de una jerarquía para la administración y gestión del contenedor criptográfico.
2. Diseño de una estrategia ordenada y hábil vinculada a la transformación digital de la información.
3. Definición de las acciones contractuales para la conformación de un Cronograma General para implantar Firma Digital y sus responsables.
4. Definición de Requisitos operacionales para el ciclo de vida de los Certificados Digitales con el objetivo de integrar toda la información generada con acciones específicas de las figuras representativas que intervienen en el ciclo de vida de los Certificados Digitales.
5. Análisis General para el almacenamiento y conservación de las claves.
6. Establecimiento de principios para la firma digital del correo electrónico usando los certificados personales de usuarios emitidos por una Autoridad Certificadora Intermedia.
7. Gestión de certificados digitales de firma y SSL para sitios web.



CS10.
ADIESTRAMIENTO ONLINE.

A partir de la implementación de este servicio con la utilización de la Plataforma Educativa Moodle es posible:

- Interactuar con una interfaz de navegación sencilla, ligera y eficiente.
- Proporcionar un entorno de aprendizaje y trabajo colaborativo.
- Ofrecer una serie de actividades para los cursos: consulta, tarea, diálogo, chat, foro, glosario, cuestionario, reunión, descarga de materiales educativos, entre otros.
- Todas las calificaciones para los foros, diarios, cuestionarios y tareas pueden verse y descargarse como un archivo con formato de hoja de cálculo o archivo de texto.
- Integración del correo. Pueden enviarse al correo electrónico copias de los mensajes enviados a un foro, los comentarios de los profesores, etc. en formato HTML o de texto.

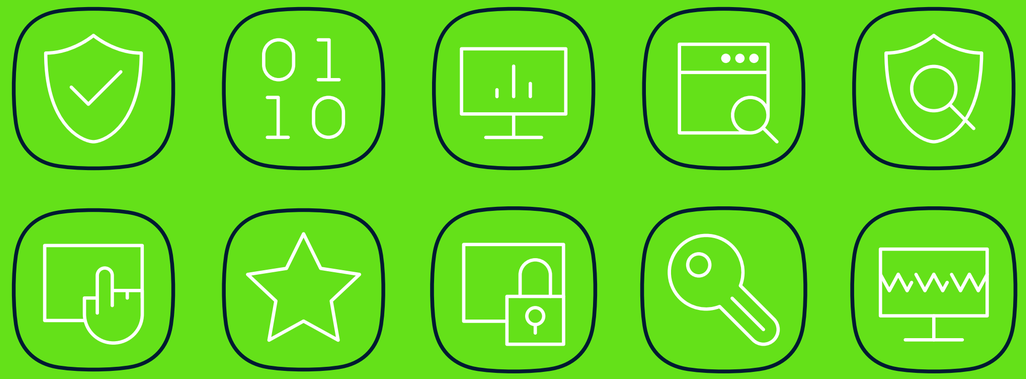


CONTACTOS

(+53) 7 2152142 / (+53) 7 2152152 / (+53) 7 2152187
comercial@eti.biocubafarma.cu
Calle 18 N°4310 e/ 43 y 47, Miramar.
La Habana, Cuba.

eti
Tecnologías de
la Información
BioCubaFarma

ideas frescas



CIBER-
-SEGURIDAD