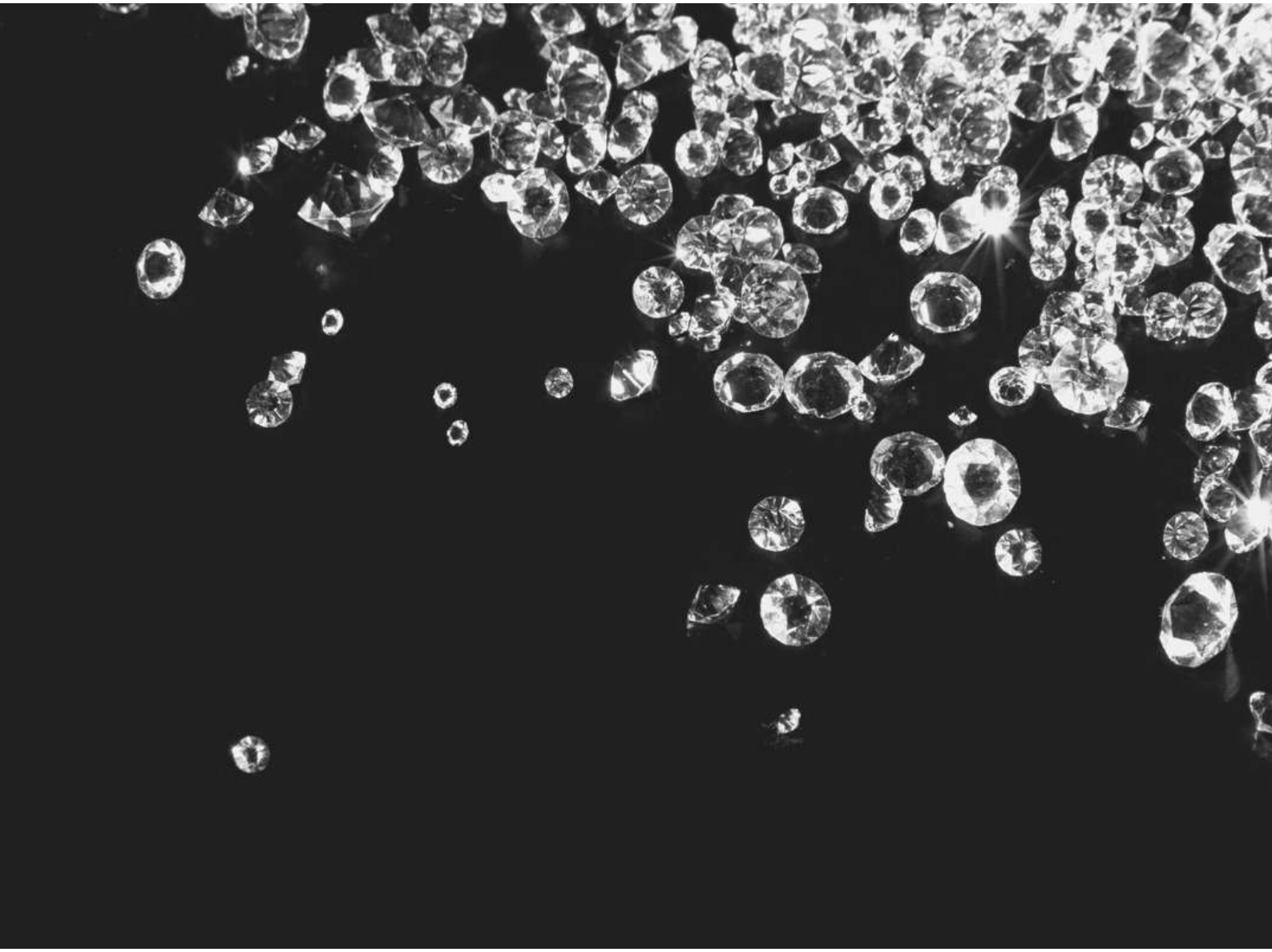
NOVIEMBRE 2023

ÁREA DE ESTRATÉGICA



IMPORTANCIA

DE LA CIBERSEGURIDAD

la seguridad convertida en Prioridad

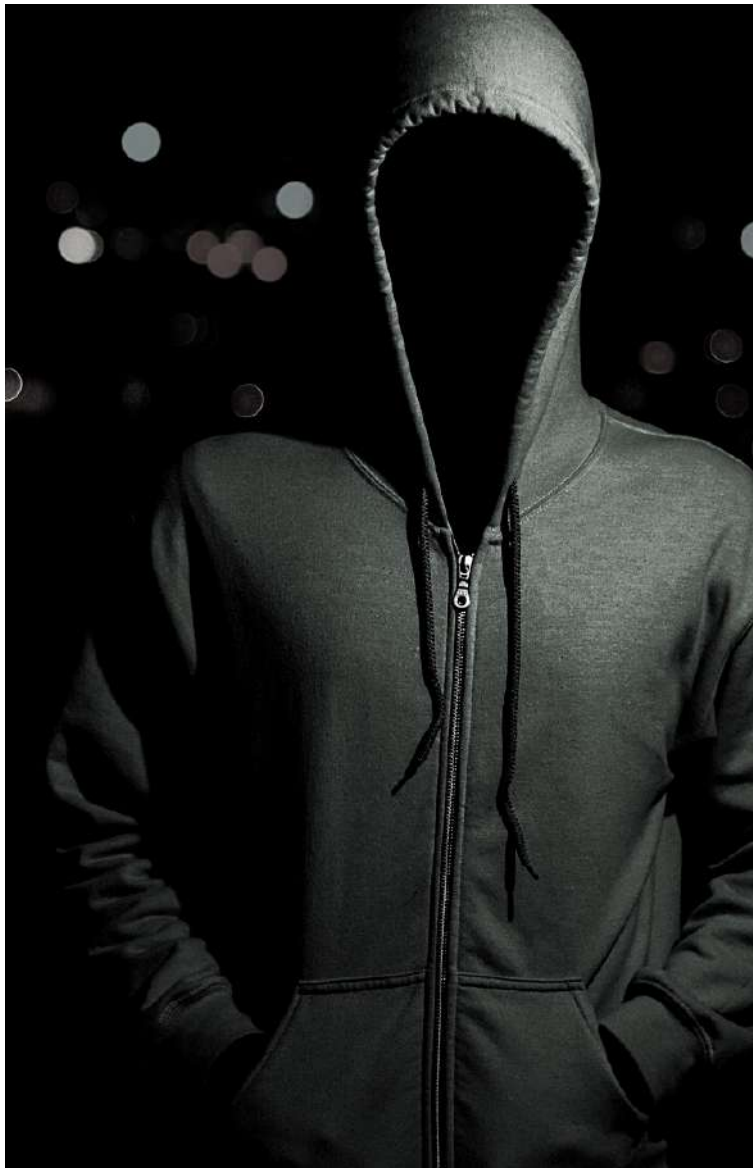
COS BIOCUBAFARMA + IA

https://csirt.biocubafarma.cu

EL CONCEPTO HUMANIZADO

Práctica crucial para proteger la información y los activos digitales de individuos y organizaciones contra las amenazas cibernéticas.

" Elemento fundamental para la estrategia de negocio de toda organización."



- se adapta a las nuevas amenazas y a los avances tecnológicos, ofreciendo soluciones específicas y vinculadas a las necesidades de cada organización.

- sus desafíos más comunes se caracterizan por la implementación de políticas de ciberseguridad que incluyan la gestión de riesgos, la adopción de nuevas tecnologías y la formación de los empleados.

HACIA DONDE SE DIRIGEN LOS CIBERATAQUES

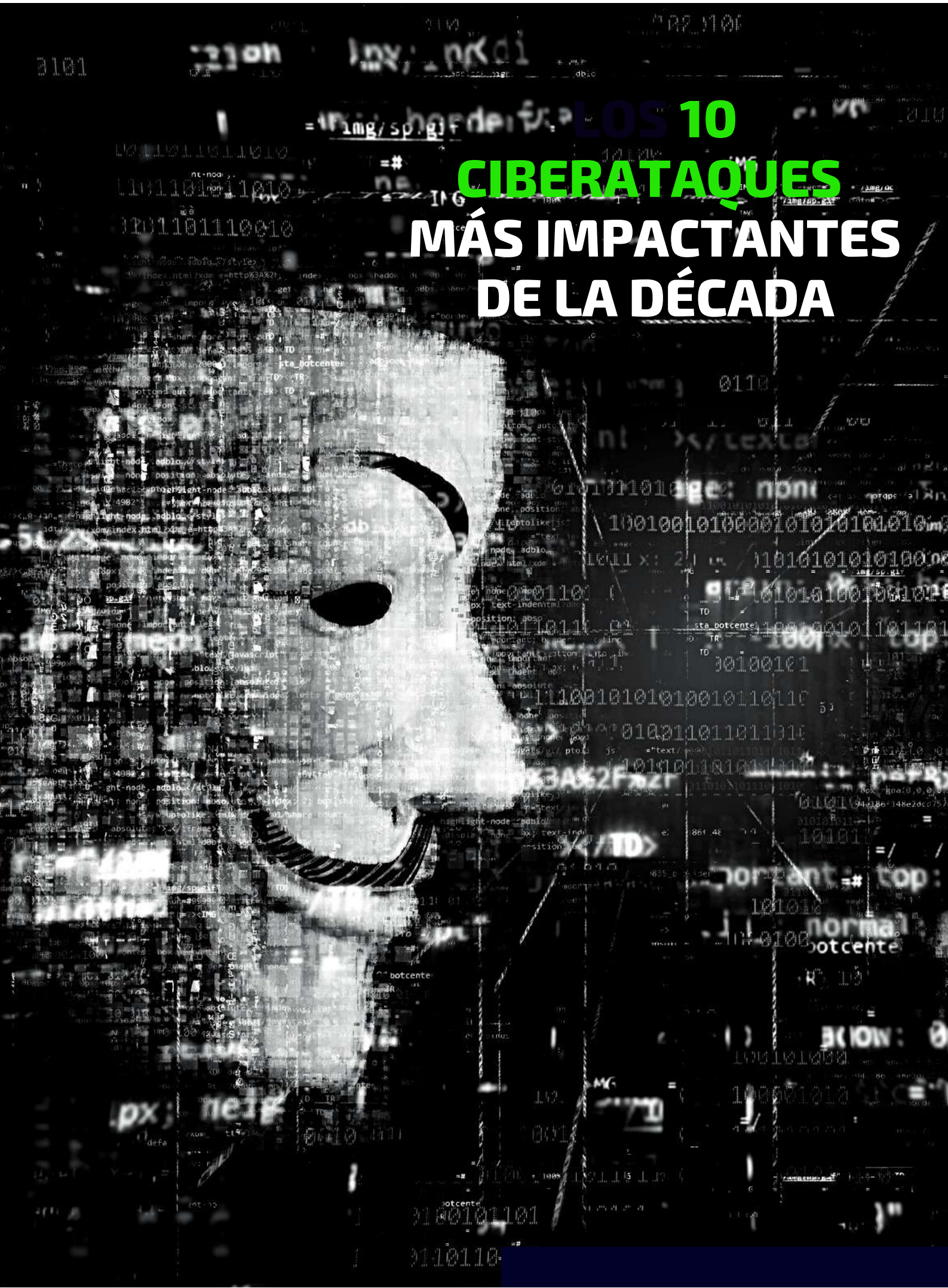
La implementación y despliegue de medidas de seguridad digital tiene como contexto actual el aumento masivo de más dispositivos conectados que personas, y los atacantes son cada vez más creativos y arriesgados.Los ciberataques están dirigidos al acceso, modificación, eliminación y venta la información confidencial. Los modelos de negocios híbridos, señalan a la extorsión constante de usuarios y organizaciones.

EL VERDADERO DOLOR DE CABEZA

El ciberespacio es un entorno hostil debido a la facilidad y bajo costo con el que se pueden llevar a cabo ataques cibernéticos. Este entorno ha evolucionado para convertirse en un escenario en el que las organizaciones deben defender intereses propios. La amenaza de ataques cibernéticos está siempre presente, ya que surgen constantemente nuevas vulnerabilidades y se desarrollan técnicas más sofisticadas.

La fértilidad y auge de los ciberataques responde a varios factores. En primer lugar, los ciberataques son cada vez más frecuentes y sofisticados, lo que hace que las empresas sean vulnerables a una amplia gama de amenazas cibernéticas. En segundo lugar, los ciberataques pueden tener un impacto económico significativo en las organizaciones, lo que representa una carga significativa para las empresas. En tercer lugar, los riesgos de ciberseguridad a los que se enfrentan las empresas aumentaron por cuenta de la pandemia, la cual forzó a muchas organizaciones a migrar a modelos de trabajo remoto y a implementar nuevas herramientas digitales para mantener sus operaciones activas. En cuarto lugar la complejidad de las políticas de ciberseguridad es una tarea desafiante, ya que las organizaciones deben abordar una amplia gama de amenazas y riesgos, y adaptarse a los rápidos cambios en las tecnologías de la información y las prácticas de seguridad.

LOS 10 CIBERATAQUES MÁS IMPACTANTES DE LA DÉCADA



1. Target | Diciembre 2013

El gigante estadounidense de venta minorista Target fue objeto de un ataque histórico en 2013 que afectó a 70 millones de clientes. Además del robo de información personal (nombres, direcciones, números de teléfono y correos electrónicos), hubo al menos 40 millones de víctimas que también vieron cómo les robaban sus datos bancarios.

2. eBay | Mayo 2014

En mayo de 2014, eBay emitió un comunicado en el que pedía a sus 145 millones de usuarios que cambiaran su contraseña tras descubrir que su red había sido objeto de un ciberataque. Los piratas informáticos se hicieron con nombres de clientes, contraseñas cifradas, correos electrónicos, direcciones, números de teléfono y fechas de nacimiento.

3. Elecciones en los Estados Unidos | Diciembre 2015.

La información de 191 millones de votantes estadounidenses, alrededor del 60% de la población, fue expuesta en Internet debido al error de una empresa de marketing contratada por el Comité Nacional Republicano durante la campaña de Donald Trump.

4. Friend Finder | Noviembre 2016

El caso se hizo público por LeakedSource, que lo clasificó en su momento como el mayor robo de datos de la historia. Más de 412 millones de cuentas en la red de sitios para adultos y pornografía Friend Finder fueron expuestas en el mercado negro, incluyendo correos electrónicos y contraseñas. Como estos datos estaban asociados a sitios de contenido para adultos, el impacto del ataque también implicó la extorsión y vergüenza de los usuarios implicados.

5. Ataque WannaCry| Mayo 2017

El ransomware WannaCry, se propagó afectando a más de 200.000 equipos informáticos en más de 150 países. El cual, exigieron un rescate de una cantidad de 8 mil millones de dólares. WannaCry fue un malware creado por cibercriminales para bloquear accesos a ordenadores y atacar a archivos valiosos con el sistema operativo de Microsoft Windows.

6. Uber | Noviembre 2017

La noticia destacó en los medios de comunicación, no sólo por el número de víctimas afectadas, 57 millones, sino también porque Uber pagó cien mil dólares a dos

hackers para eliminar los datos robados y ocultar el ciberataque, manteniéndolo en secreto.

7. Cambridge Analytica | Marzo 2018

Cambridge Analytica mostró al mundo cómo el robo de datos puede ser usado en política: en este caso, para influir en las elecciones presidenciales de EE.UU. en 2016. Cambridge Analytica - una empresa de análisis de datos que trabajó con el equipo de Donald Trump - utilizó sin consentimiento la información de 50 millones de perfiles de Facebook para identificar los patrones de comportamiento y gustos de los usuarios y utilizarlos en la difusión de propaganda política.

8. Facebook | Marzo 2019

Facebook se vio involucrado una vez más en un caso de exposición de datos. Cerca de 419 millones de números de teléfono y de identificación de usuario en Facebook fueron almacenados en un servidor online que no estaba protegido por contraseña.

9. SolarWinds y agencias de Estados Unidos| Dic 2020

Los sistemas informáticos de varias agencias gubernamentales, incluidos los Departamentos del Tesoro y del Comercio, fueron hackeados por ciberdelincuentes que actuaban en nombre de un gobierno extranjero, apuntando a Rusia. Los atacantes consiguieron interceptar paquetes de actualización de software de Microsoft preparados por SolarWinds, logrando acceder a través de este software a los sistemas de los Departamentos de Justicia y Tesoro de Estados Unidos.

10.Oleoducto Colonial Pipeline | Mayo 2021

La organización de hackers DarkSide parece atribuirse la responsabilidad del ataque de ransomware que provocó que Colonial Pipeline parara su actividad como medida de precaución.
En el caso del sector energético, al contar con datos altamente sensibles y una infraestructura crítica, este se convierte en una industria extremadamente sensible y valiosa para los hackers.

REPORTE 2023 DEL LATAM CISO

PRINCIPALES CIBERATAQUES EN AMÉRICA LATINA

- RANSOMWARE: *EL SECUESTRO COMO NEGOCIO RENTABLE*
- *PHISHING: INGENIERÍA SOCIAL SOFISTICADA*
- *ATAQUES CON INTELIGENCIA ARTIFICIAL: HACKEOS A TRAVÉS DE BOTS*

EL METAVERSO

El metaverso plantea nuevos desafíos en términos de ciberseguridad, ya que representa una nueva superficie de ataque y un entorno digital en constante expansión. La integración de la ciberseguridad en el metaverso requiere un enfoque multifacético que considere cómo se conectan los mundos real y virtual, así como la adopción de tecnologías emergentes para abordar las amenazas emergentes en este nuevo ámbito digital. La gestión de la seguridad del metaverso, o "***metaseguridad***", implica abordar las amenazas emergentes en este nuevo ámbito digital, mientras se adopta un enfoque multifacético para considerar cómo se conectan los mundos real y virtual.
Las principales preocupaciones de ciberseguridad para el metaverso incluyen la existencia de brechas y robos de identidad, la falta de un proceso claro relacionado con la privacidad de datos, la escasez de profesionales de seguridad con experiencia para proteger el metaverso, y la necesidad de integrar la seguridad en todo el proceso de desarrollo para proteger adecuadamente cada transacción en toda la plataforma Además, se destaca la importancia de desarrollar un marco de seguridad cibernética antes de ofrecer servicios en un entorno virtual como el metaverso, así como la necesidad de educación y prevención para evitar ser presa de los ciberdelincuentes en este nuevo entorno digital.
El desafío requiere un enfoque integral, la adopción de tecnologías emergentes y la conciencia sobre las amenazas evolutivas en este nuevo ámbito digital.

SOBRE NUESTRO COLABORADOR

La integración de la inteligencia artificial (IA) en el ámbito de la ciberseguridad ofrece un potencial significativo para fortalecer las capacidades de defensa cibernética. La IA ha demostrado ser una aliada valiosa en la mejora de la ciberseguridad, ya que mediante algoritmos avanzados y análisis predictivos, puede detectar y prevenir ataques cibernéticos de manera más eficiente.

La integración de la IA en el ámbito de la ciberseguridad gubernamental ofrece la oportunidad de ***fortalecer las capacidades de defensa cibernética, automatizar tareas críticas, mejorar la eficiencia operativa y proteger los activos digitales*** del gobierno contra las crecientes amenazas en el ciberespacio.

La inteligencia artificial (IA) se puede utilizar para mejorar la ciberseguridad de diversas maneras, incluyendo el monitoreo del tráfico de red, la identificación de amenazas desconocidas, la gestión de vulnerabilidades y la detección de anomalías. Además, la IA puede ayudar a automatizar la detección de amenazas y a responder más rápidamente que las tácticas convencionales basadas en software, lo que resulta fundamental en el contexto de los ciberataques en constante evolución. Sin embargo, es importante tener en cuenta que la implementación de la IA en ciberseguridad también conlleva desafíos, como la necesidad de abordar las desventajas y limitaciones de esta tecnología en el contexto de la ciberseguridad.

NUESTRAS LÍNEAS DE MENSAJE

- A MEDIDA QUE LOS CIBERCRIMINALES CONTINÚAN EVOLUCIONANDO SUS TÉCNICAS, DEBEMOS ADAPTARNOS Y MEJORAR NUESTRAS MEDIDAS DE CIBERSEGURIDAD.

- NO ES CUESTIÓN DE "SI" NOS VAMOS A VER AFECTADOS POR UN CIBERATAQUE, SINO "CUÁNDO". LA PREVENCIÓN ES FUNDAMENTAL PARA MINIMIZAR LOS RIESGOS Y POSIBLES CONSECUENCIAS.

- ESTAMOS EN UNA CARRERA CONSTANTE CONTRA LOS CIBERCRIMINALES. A MEDIDA QUE ELLOS NOS ADELANTAN, DEBEMOS ESFORZARNOS POR MANTENERNOS AL DÍA Y SER PROACTIVOS EN NUESTRAS ESTRATEGIAS DE DEFENSA.

- ADOPTAR UNA POSTURA RESILIENTE Y ADAPTATIVA EN LA ADOPCIÓN DE LA CIBERSEGURIDAD PUEDE MARCAR LA DIFERENCIA ENTRE ÉXITO Y FRACASO EN EL ÁMBITO EMPRESARIAL.

- ESTAMOS COMPROMETIDOS CON LA ADOPCIÓN DE PRÁCTICAS DE CIBERSEGURIDAD DE VANGUARDIA PARA PROTEGER NUESTROS ACTIVOS Y MANTENER LA CONFIANZA DE NUESTROS CLIENTES.

#CiberseguridadParaTodos

NOVIEMBRE 2023

ÁREA DE ESTRATÉGICA

IMPORTANCIA
DE LA CIBERSEGURIDAD

la seguridad convertida en Prioridad

COS BIOCUBAFARMA + IA

https://csirt.biocubafarma.cu