

Agrupación 31 Tte. Américo Pico



COMCOME

CiberDefensa

Gma. de Reserva Magno D. Ayala R.
Ing. en Ciencias de la Informática
Especialista en C.C.E.

[Perfil LinkedIn](#)





CIBERSEGURIDAD

CIBERDEFENSA

CIBERSOLDADO?

CiberSeguridad

La **Ciberseguridad** es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

CiberSeguridad



La **Ciberseguridad** o seguridad de las Tecnologías de la Información y Comunicación es el área de la informática que se encarga de proteger la integridad de la infraestructura computacional y la información que se almacena en ella.

CiberSeguridad

La definición de ciberseguridad por parte de ISACA (*Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información*) es la “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.

ISO 27001 define *Activo de la Información* como “conocimientos o datos que tienen valor para una organización”, y *Sistemas de Información* como “los que comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma”.

<https://www.esic.edu/rethink/tecnologia/definicion-ciberseguridad-riesgo>

CiberSeguridad

Responsables (entidades)

CISO: encargado de alinear la estrategia de ciberseguridad con los objetivos de la organización.

CSO: responsable de la seguridad interna de la empresa.

DPO: tiene un perfil jurídico y de cumplimiento normativo.

Analistas de seguridad:

Arquitecto de seguridad:

Hacker ético:

Especialista forense:

Especialistas de incidencias:

Responsables de inteligencia:

<https://www.pmg-ssi.com/2018/04/responsables-de-la-ciberseguridad/>

CiberSeguridad



Responsables (gobierno)

- MITIC/CSIRT
- Ministerio Publico/Fiscalía de delitos informáticos
- Ministerio del Interior/Policía Nacional

Elementos:

- CN
- CP
- CPP
- Leyes especiales

CiberDefensa



El ciberespacio ya no es un dominio “emergente”, sino un potencial teatro de guerra donde todas las naciones soberanas podrían participar activa y continuamente. En todo el mundo, los actores gubernamentales y no gubernamentales han desarrollado capacidades cibernéticas, ofensivas y defensivas, que han allanado el camino para una reevaluación de los conocimientos tradicionales del poder global, su influencia e incluso la guerra.

CiberDefensa



Ciberdefensa: Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.

CiberDefensa

Ciberdefensa es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformaticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos.

CiberDefensa



CIBERESPACIO, es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan.

CiberDefensa



Desmitificar la Red

- La red no es gratis, es un negocio
- No es el paradigma de la democracia directa
- La libertad en la red no existe.
- No existe la vigilancia perfecta.
- La privacidad es prácticamente nula (cada vez menor)
- Riesgos de la regulación (Regular que y como)

https://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

CiberDefensa

Responsables:

- Ministerio de Relaciones Exteriores (MRE)
- Ministerio de Defensa Nacional (MDN)
- Fuerzas Militares (FFMM)
- Comando Conjunto de Ciberdefensa
- Ministerio del Interior (MI)
- Secretaría Nacional de Inteligencia (SNI)

Elementos:

- **CN**
- **Libro Blanco de la Defensa Nacional**
- **Política de Defensa**
- **Leyes especiales**

CiberSoldado?

En informática, un usuario es una persona que utiliza una computadora o un servicio de red. Los usuarios de sistemas informáticos y productos de software generalmente carecen de la experiencia técnica necesaria para comprender completamente cómo funcionan.

[https://es.wikipedia.org/wiki/Usuario_\(inform%C3%A1tica\)](https://es.wikipedia.org/wiki/Usuario_(inform%C3%A1tica))

CiberSoldado?

En cambio, los programadores y todo profesional técnico no pueden ser considerados como usuarios cuando trabajan con la computadora a nivel profesional.

Un usuario generalmente se identifica frente al sistema o servicio utilizando un nombre de usuario (nick) y generalmente una contraseña segura, este tipo es llamado usuario registrado. Por lo general un usuario se asocia a una única cuenta de usuario, en cambio, una persona puede llegar a tener múltiples cuentas en un mismo sistema o servicio (si eso está permitido).

Un usuario registrado accede a un servicio a través de un login luego de su autenticación.

CiberSoldado?

El mayor punto débil de tu seguridad eres tú:

Cuando pensamos en la gente que suele realizar ataques informáticos, lo primero que nos viene a la mente suele ser un experto informático capaz de descifrar la mejor de las contraseñas o aprovecharse de vulnerabilidades desconocidas para el común de los mortales. Pero por lo general, para robarle la cuenta de Facebook o Gmail **ni siquiera hay que tener grandes conocimientos informáticos**, vale con esperar a que tal persona se las dé amablemente.

<https://www.genbeta.com/a-fondo/el-mayor-punto-debil-de-tu-seguridad-eres-tu-asi-te-pueden-atacar-con-la-ingenieria-social>

CiberSoldado?

El aspecto más inmediato, sentido y urgente de la SEGURIDAD, como condición para el desarrollo individual y colectivo, es la SEGURIDAD CIUDADANA que si bien sigue teniendo como principal amenaza el crimen común, de persecución fiscal policial y definición judicial, se ve hoy día aún más perturbada por efecto de las nuevas amenazas; que, a diferencia de aquellos delitos contra el orden público, tienen motivaciones, propósitos, alcances y distintos medios mucho más expandidos.

https://www.mdn.gov.py/application/files/7415/6415/4362/Politica_de_Defensa_Nacional_2019-2030.pdf

CiberSoldado?

La ingeniería social, una técnica de ataque muy utilizada debido a su alto nivel de eficacia. Parte de la base de que **las personas somos el eslabón más débil** de un sistema de seguridad, y ya sea mediante labia o automatismos intenta engañarnos para que acabemos revelando datos claves para comprometer nuestros sistemas.

CiberSoldado?

- El atacante puede jugar con las emociones de la víctima
- Muchas entidades no establecen barreras de acceso a datos y sistemas importantes
- Intentan engañar a los usuarios para que abran un fichero o pulsen sobre un enlace
- Llegan a suplantar a proveedores de la entidad
- Intentaran hacerse pasar por ti
- Ser conscientes de qué tipo de información compartimos
- USB's con contenidos que puedan ser de interés para la víctima

CiberSoldado?

El ser humano es el punto más débil de la ciberseguridad y eso supone un problema de difícil solución para las personas/empresas/países.

El 71% de todos los incidentes registrados el pasado comenzó como un ataque de suplantación de identidad (phishing). Así lo asegura un nuevo informe de BAE Systems

<https://www.businessinsider.es/ser-humano-punto-debil-ciberseguridad-385816>

CiberSoldado?

Compromiso

Es tarea y compromiso de esta Agrupación 31 coadyuvar en la preparación y capacitación tanto del personal militar como cualquier ciudadano que quiera colaborar en la defensa cibernética.

El ultimo eslabón de la defensa cibernética es el ciudadano y el mas vulnerable, por lo tanto, capacitar y preparar convenientemente a la población es una tarea necesaria.

La forma de implementacion es un tema para otra charla.

CiberSoldado?

CONCLUSIÓN

La seguridad cibernética en las Américas

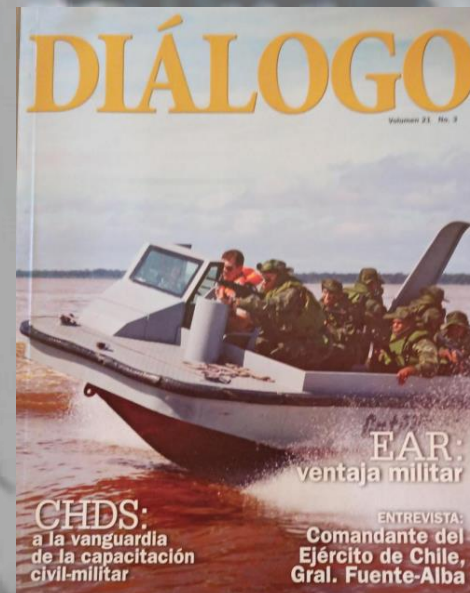
“Es imperativo exponer la necesidad de educar al usuario final y la necesidad de articulación y cooperación, en los niveles interno y externo, entre los actores nacionales responsables de administrar las amenazas de ciberespacio.”

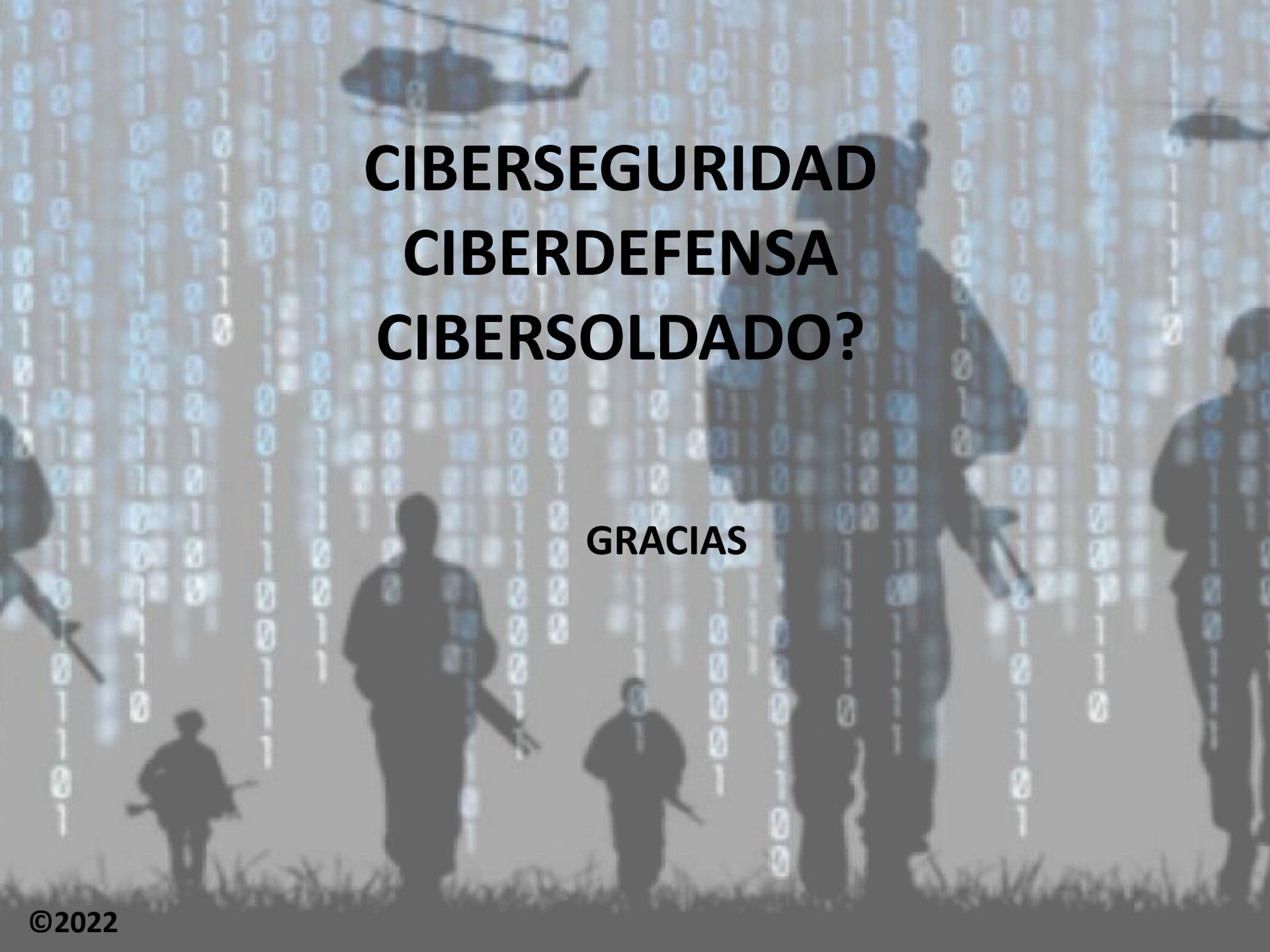
Omar J. Alvarado

Coordinador General CSIRT Venezuela

Boletín de la OEA junio 2010

Dialogo Vol. 21, N° 3



The background features a light blue and grey color scheme with vertical columns of binary code (0s and 1s) falling from the top, reminiscent of the 'Matrix' effect. Silhouettes of soldiers in various poses, some holding rifles, and a helicopter are scattered across the scene, suggesting a military or defense context.

CIBERSEGURIDAD CIBERDEFENSA CIBERSOLDADO?

GRACIAS