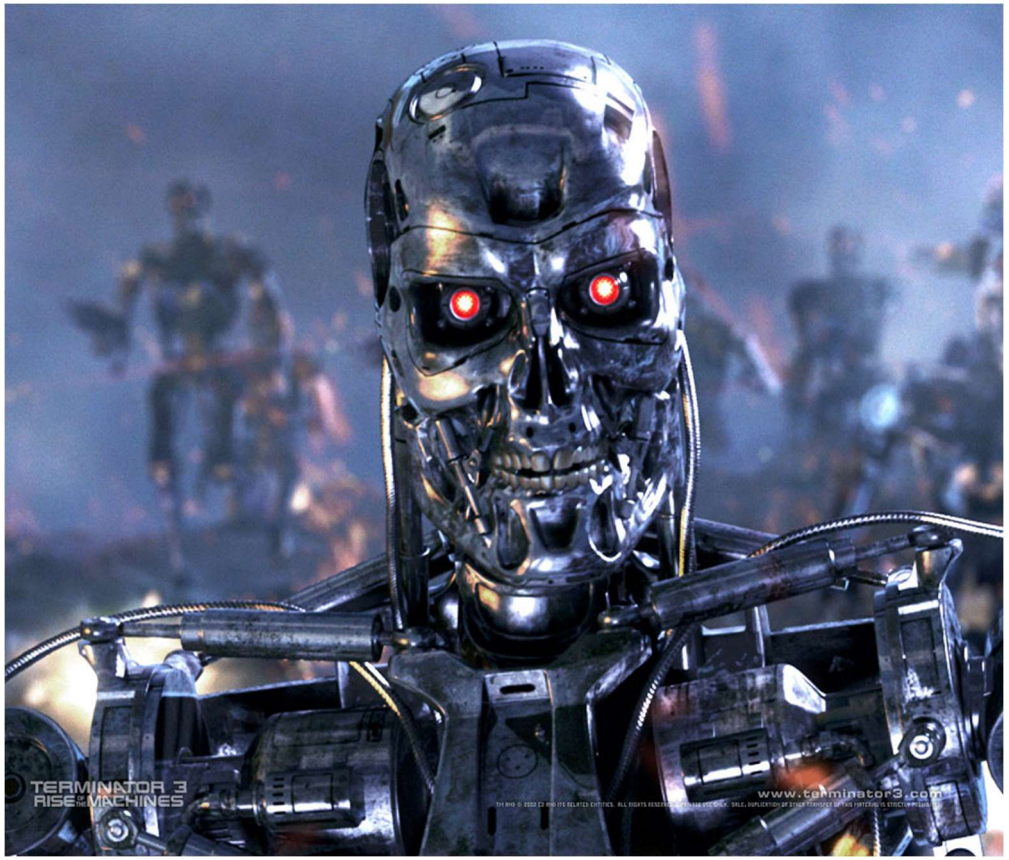
SEGURIDAD DE LA INFORMACIÓN

- Ciberseguridad
- Riesgo Operacional
- Infraestructuras Críticas
- COVID-19

MOORE

cyte

LO QUE NO ES CIBERSEGURIDAD



LO QUE SI ES CIBERSEGURIDAD

cyte

FUENTE: www.exordio.com

LO QUE SI ES CIBERSEGURIDAD

FUENTE: Wikipedia

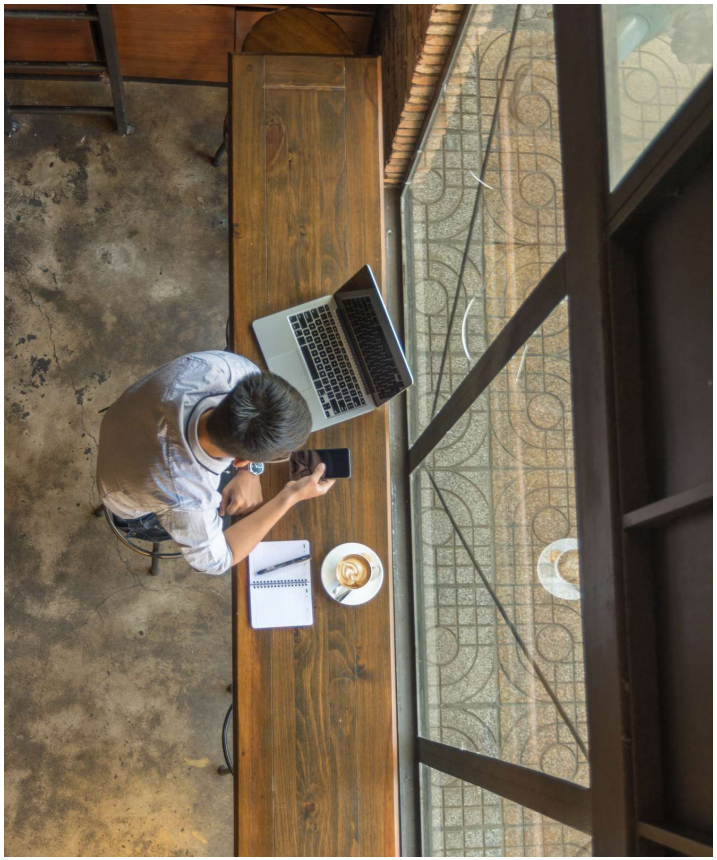
1982: EL GASODUCTO URENGOY–SURGUT–CHELYABINSK

- En la antigua Unión Soviética los servicios secretos eran muy buenos robando tecnología de occidente
  - Y la CIA siempre ha sido experta en operaciones encubiertas

- La Unión Soviética robó tecnología SCADA Canadiense para operar gasoductos,
  - La CIA introdujo una bomba lógica
  - La explosión fue equivalente a 3 kilotones de TNT
    - Véase el “The Farewell Dossier” y “At the Abyss”

SUN TZU Y CLAUSEWITZ

- Clausewitz:
  - “la guerra es un acto de fuerza para doblegar al enemigo”
- Sun Tzu:
  - “cien victorias en cien batallas no es lo ideal. Lo ideal es someter al enemigo sin luchar”
- La operación Bernhard pudo haber doblegado a Inglaterra utilizando un tipo diferente de fuerza:
  - La destrucción económica del país



GUERRA Y CIBER-GUERRA

- Si la guerra es una extensión de la política, la ciberguerra es simplemente un nuevo ámbito de la guerra tradicional,

- La ciberguerra produce una parálisis estratégica, se puede doblegar la voluntad del enemigo sin aplicación de la fuerza física

  {operación Bernhard}+

  - Las armas de ciberguerra son armas de interrupción masiva

GUERRA Y CIBER-GUERRA

cyte

CNET News

Iran's cyberwarfare czar is allegedly assassinated

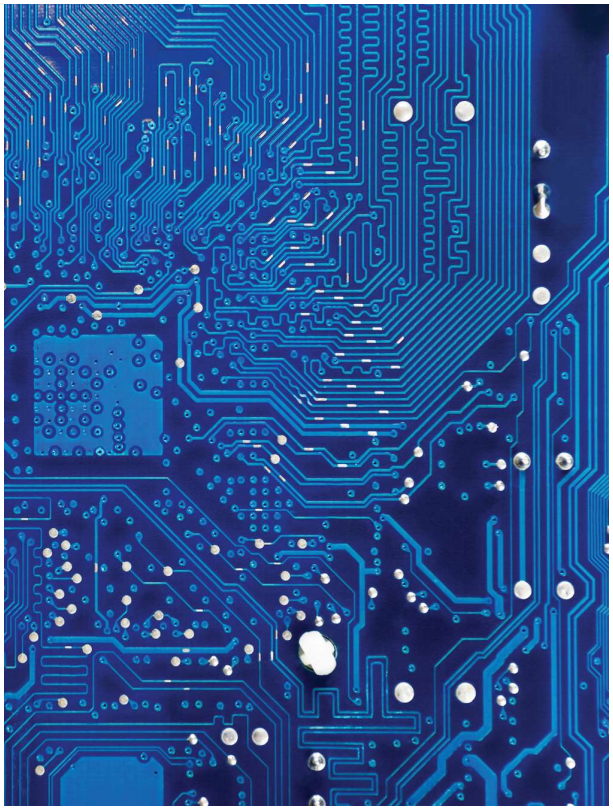
As the Middle East country beefs up its cyberforces, Mojtaba Ahmadi, the head of its Cyber War Headquarters, is said to be found with two bullet wounds near his heart.

by Dara Kerr | October 2, 2013 5:31 PM PDT

JUNIO 2010 - STUXNET

JUNIO 2010 - STUXNET

- Un ataque especialmente enfocado:
  - Irán, PLCs, equipos Siemens, centrifugadoras de Uranio enriquecido, auto-borrado el 24 de junio del 2012,
  - Dos servidores en Dinamarca y Malasia coordinaban el ataque
- Posiblemente elaborado por el gobierno Israelí (Mossad) y CIA – NSA,
- Se dañaron alrededor de 1000 centrifugadoras
  - Se retrasó el programa nuclear Iraní quizás en un año
- Duqu, septiembre 1 del 2011 a delincuencia común
- Flame, mayo del 2012 a delincuencia común



STUXNET, LO QUE FINALMENTE SE SUPO

Obama Ordered Wave of Cyberattacks Against Iran – NYTimes.com

www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0&pagewanted=print

Reader

Fab at MIT trendwatching AllThingsD Etsy Pin It Building & Hacking CrowdSourcing CryptoBoincRAR Format wars Homomorphic GPS Micromort Datamatrix Generator

Infosecurity – Encryption | Geeks are the New Guardia... | www.cl.cam.ac.uk/research... | Energy Department Confir... | Video Listing | Building an... | Obama Ordered Wave of C...

The New York Times

June 1, 2012

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

Told it was unclear how much the Iranians knew about the code, and offered evidence that it was still causing havoc, Mr. Obama decided that the cyberattacks should proceed. In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.

This account of the American and Israeli effort to undermine the Iranian nuclear program is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts. None would allow their names to be used because the effort remains highly classified, and parts of it continue to this day.

These officials gave differing assessments of how successful the sabotage program was in slowing Iran's progress toward developing the ability to build nuclear weapons. Internal Obama

FUENTE: www.nytimes.com

SUCESOS EN LA HISTORIA

cyte

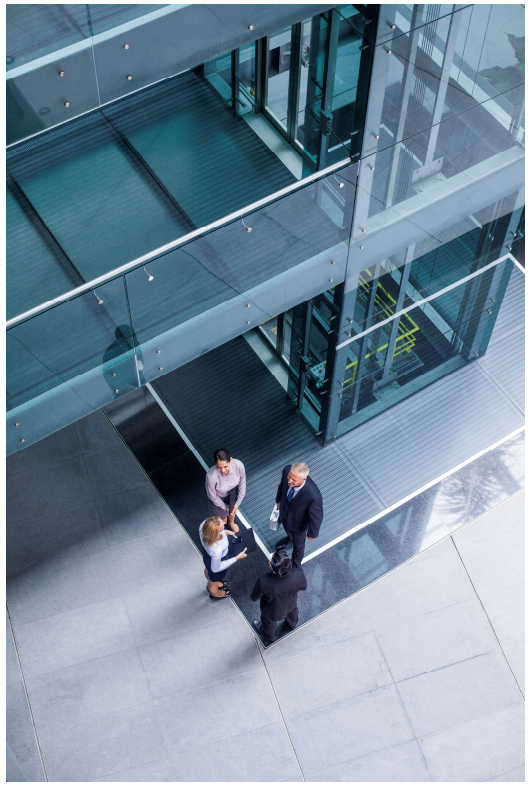
- Stuxnet (2010)
- Havex (2013)
- BlackEnergy (2015)
- CrashOverride (2016)
- Triton – Trisis (¿2018?) - Triconex safety controller model

MOORE

LAS ARMAS CIBERNÉTICAS SON ARMAS DE INTERRUPCIÓN MASIVA

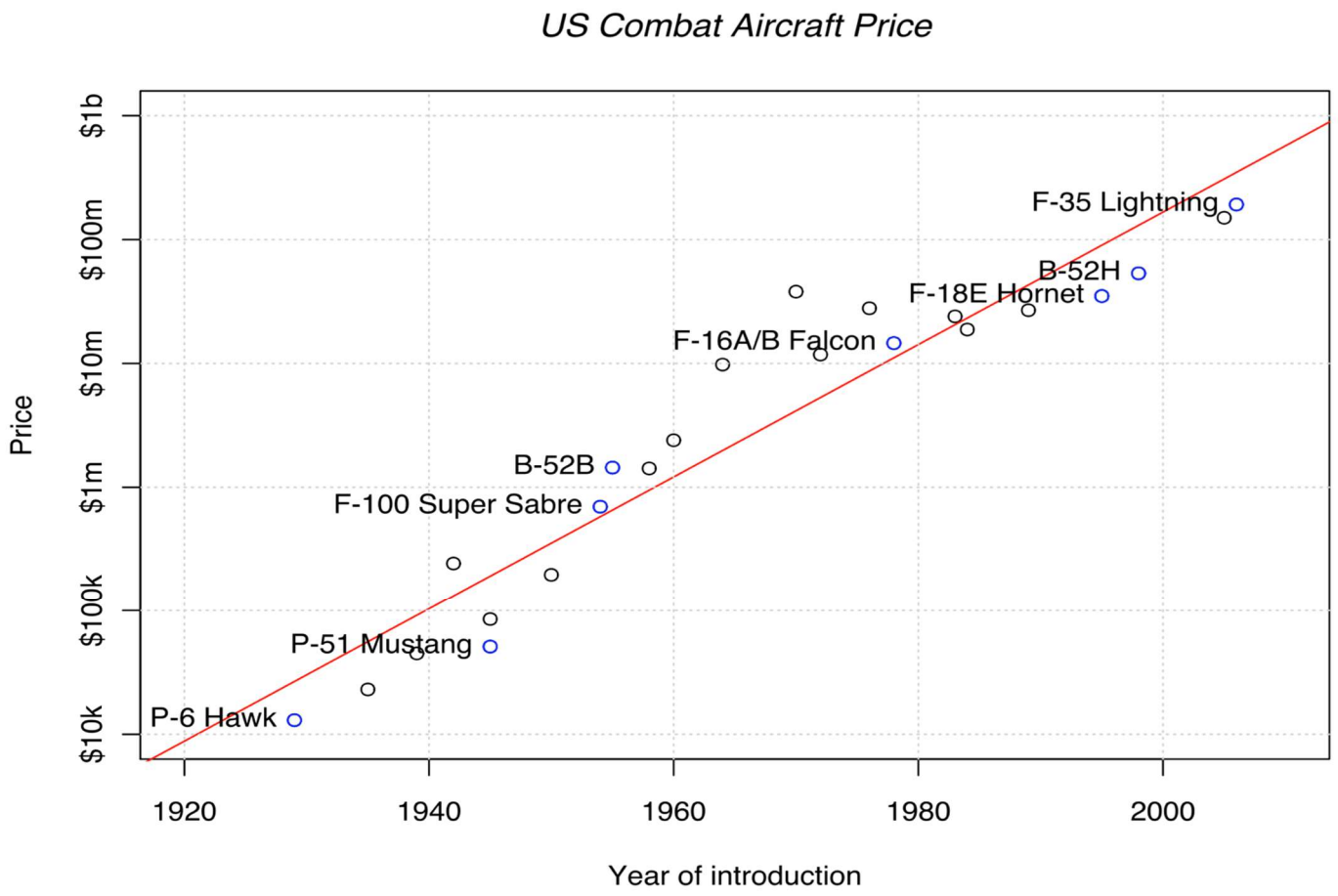
CARACTERÍSTICAS DE LAS CIBERARMAS

- Las víctimas son fundamentalmente población civil
- Bajo costo,
- Alto impacto,
- Sin fronteras,
- Difícil de rastrear la fuente,
  - No hay disuasión, no hay “destrucción mutua asegurada”
- Rápido o lento…
- Asimétrico
- Pasan fácilmente a la delincuencia común… y vuelven
- Requiere víctimas tecnológicamente sofisticadas



AUGUSTINE'S LAW NUMBER 16

cyte



MOORE

AUGUSTINE'S LAW NUMBER 16

"In the year 2054, the entire defense budget will purchase just one tactical aircraft. This aircraft will have to be shared by the Air Force and Navy 3½ days each per week except for leap year, when it will be made available to the Marines for the extra day"

UNA PARTE DE AL EN LA NOCHE

¿CÓMO DESAPARECER UN CONTAINER?

cyte

BBC NEWS

EUROPE

16 October 2013 Last updated at 05:08 GMT

Police warning after drug traffickers' cyber-attack

By Tom Bateman
Reporter, Today programme

The head of Europe's crime fighting agency has warned of the growing risk of organised crime groups using cyber-attacks to allow them to traffic drugs.

The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking business.

His comments follow a cyber-attack on the Belgian port of Antwerp.

Drug traffickers recruited hackers to breach IT systems that controlled the movement and location of containers.

Police carried out a series of raids in Belgium and Holland earlier this year, seizing computer-hacking equipment as well as large quantities of cocaine and heroin, guns and a suitcase full of cash.

Fifteen people are currently awaiting trial in the two countries.

¿CÓMO DESAPARECER UN CONTAINER?

cyte

EL ESPECTADOR

Imprimir aquí

Economía | Vie, 06/13/2014 - 21:38

Renuncia de Ortega a la DIAN, a la espera

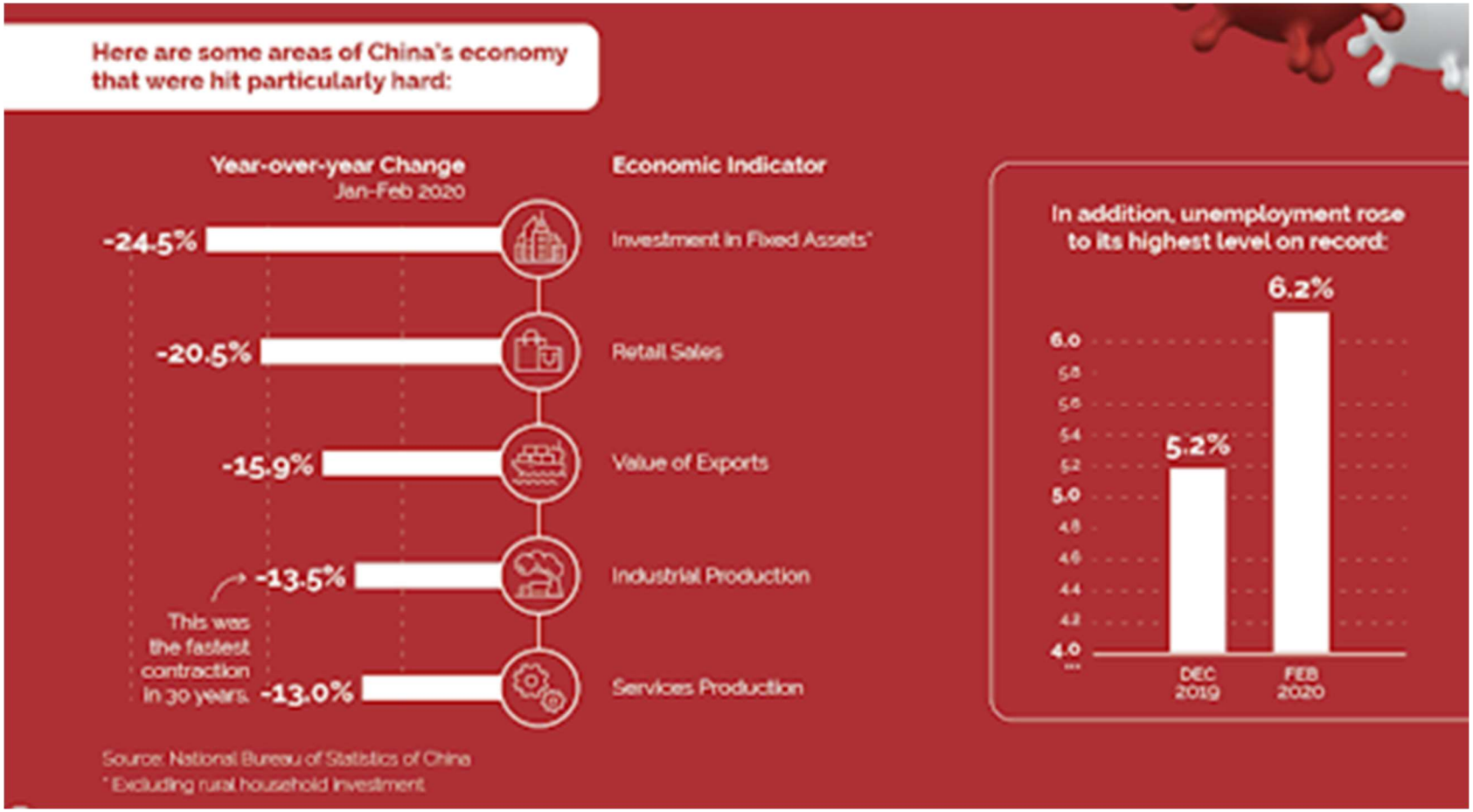
Por: Redacción Negocios

Amenazas y presiones políticas llevarían al jefe de la DIAN, Juan R. Ortega, a formalizar este lunes su dimisión ante el presidente Santos.

Desde que Juan Ricardo Ortega López, jefe de la Dirección de Impuestos y Aduanas Nacionales (DIAN), asumió su cargo el 7 de agosto de 2010, tenía claro que debía dar una lucha a brazo partido contra el contrabando, la evasión de impuestos, las estructuras para el lavado de activos, el fraude dentro de la entidad y muchos otros males que durante varias administraciones se han prolongado. Ahora, a un día de las elecciones presidenciales, su renuncia —que se venía dando como un hecho hasta hace pocas semanas en la Casa de Nariño— parece ser un hecho a punto de concretarse.

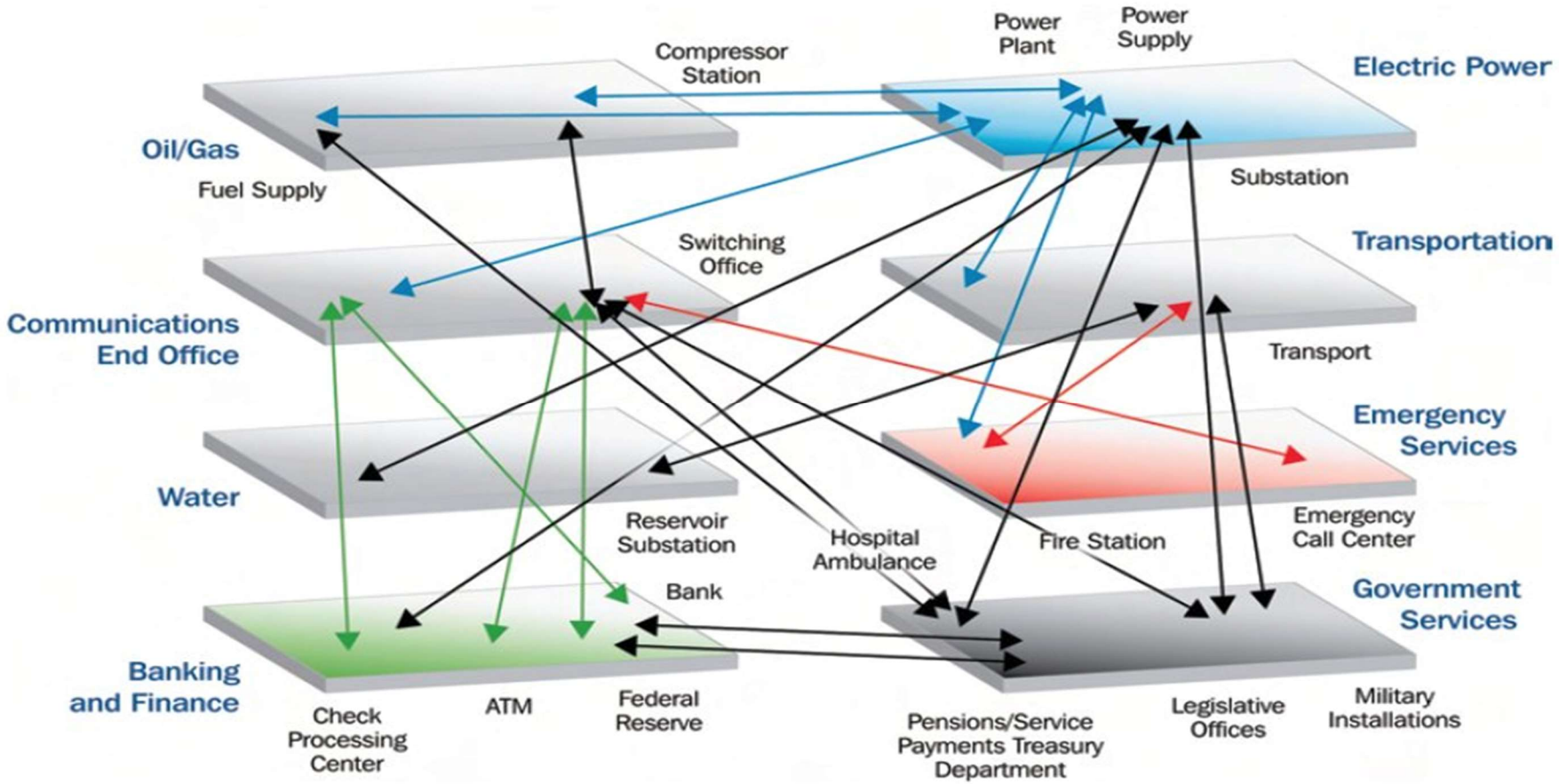

¿ESTAMOS TRATANDO DE RESOLVER UN PROBLEMA DEL SIGLO XXI, CON MENTALIDAD DEL SIGLO XX?

LA ECONOMÍA CHINA



COLOMBIA

EL APARATO PRODUCTIVO Y SUS DEPENDENCIAS

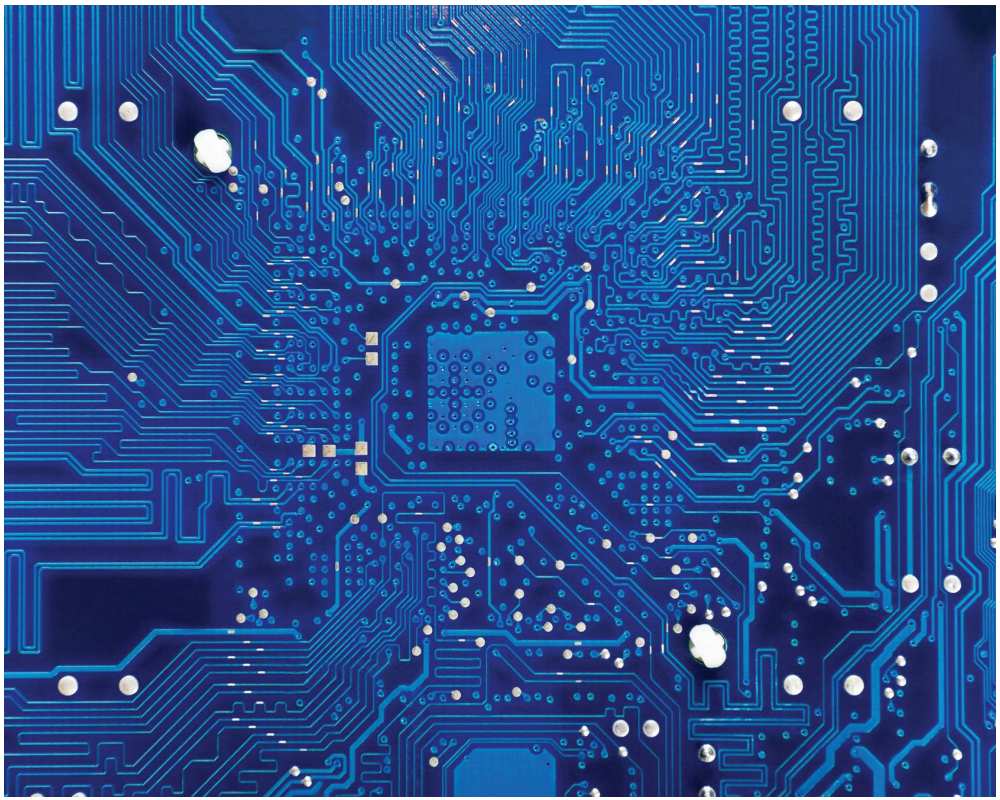


¿CÓMO PROTEGEMOS LA INFRAESTRUCTURA CRÍTICA?

¿CÓMO PROTEGER INFRAESTRUCTURA CRÍTICA?

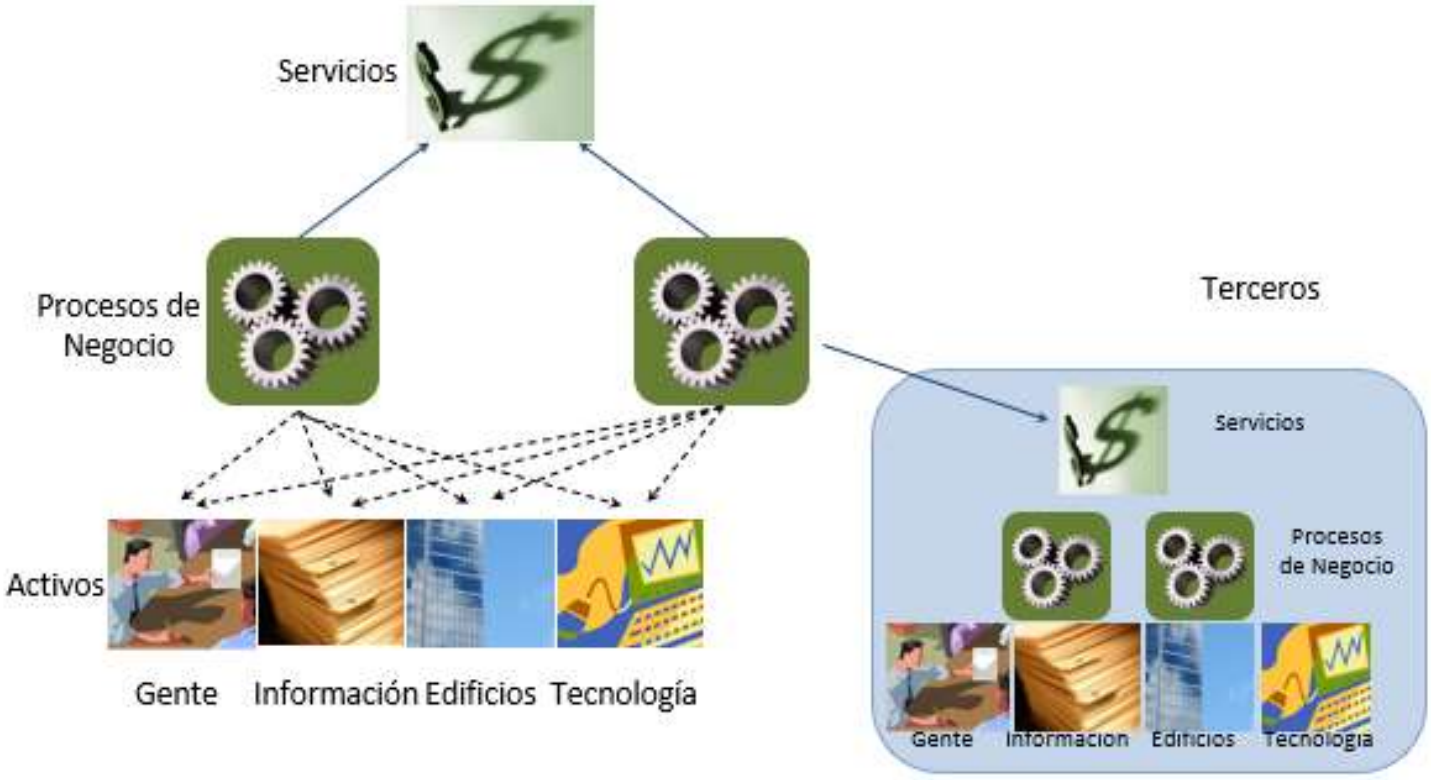
El esfuerzo gravita alrededor de Análisis de Riesgos

- Modelaje de amenazas,
- Modelaje de atacantes,
  - Recursos,
  - Motivación,
  - …

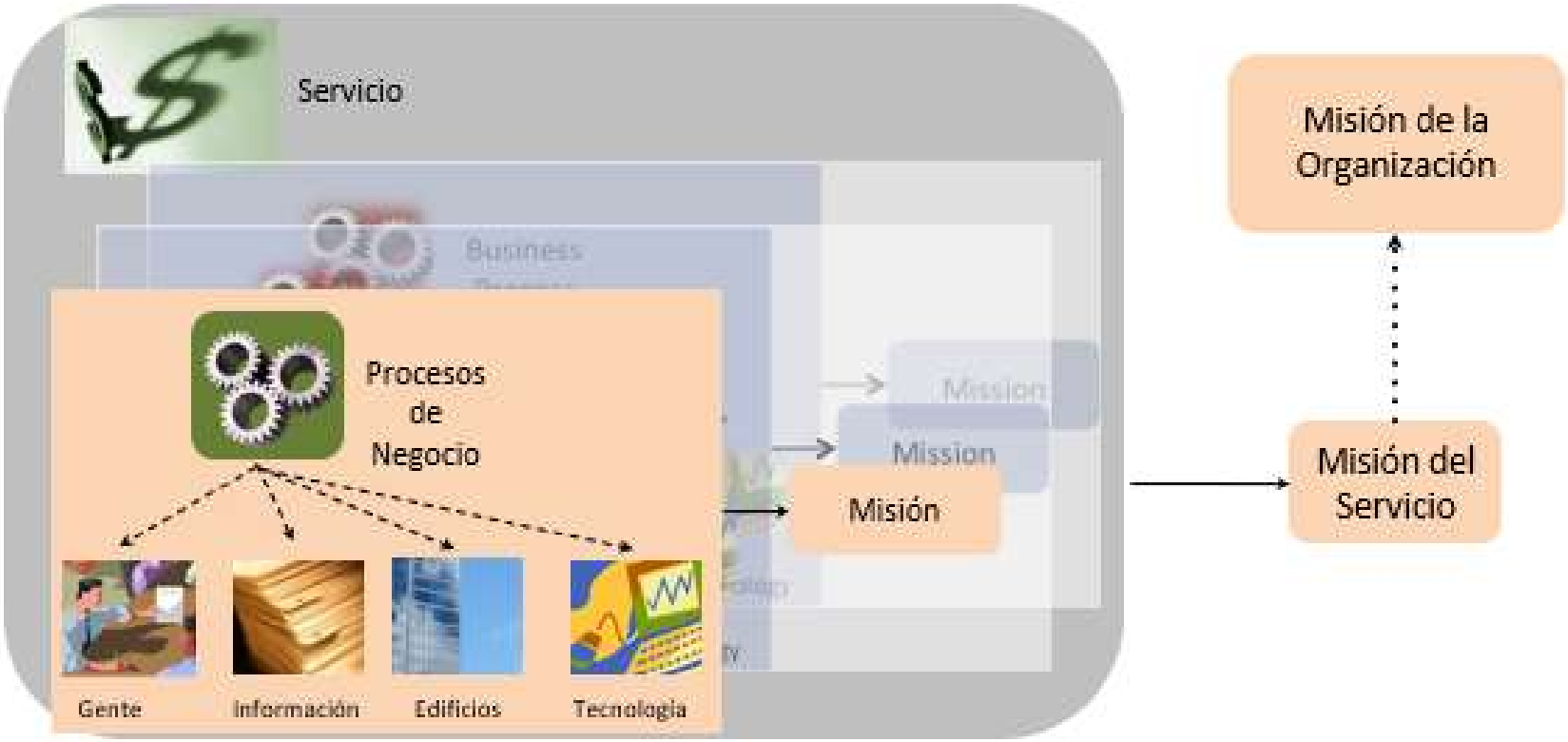


UNA ORGANIZACIÓN TÍPICA

Y SUS TERCEROS (OUT-SOURCING)

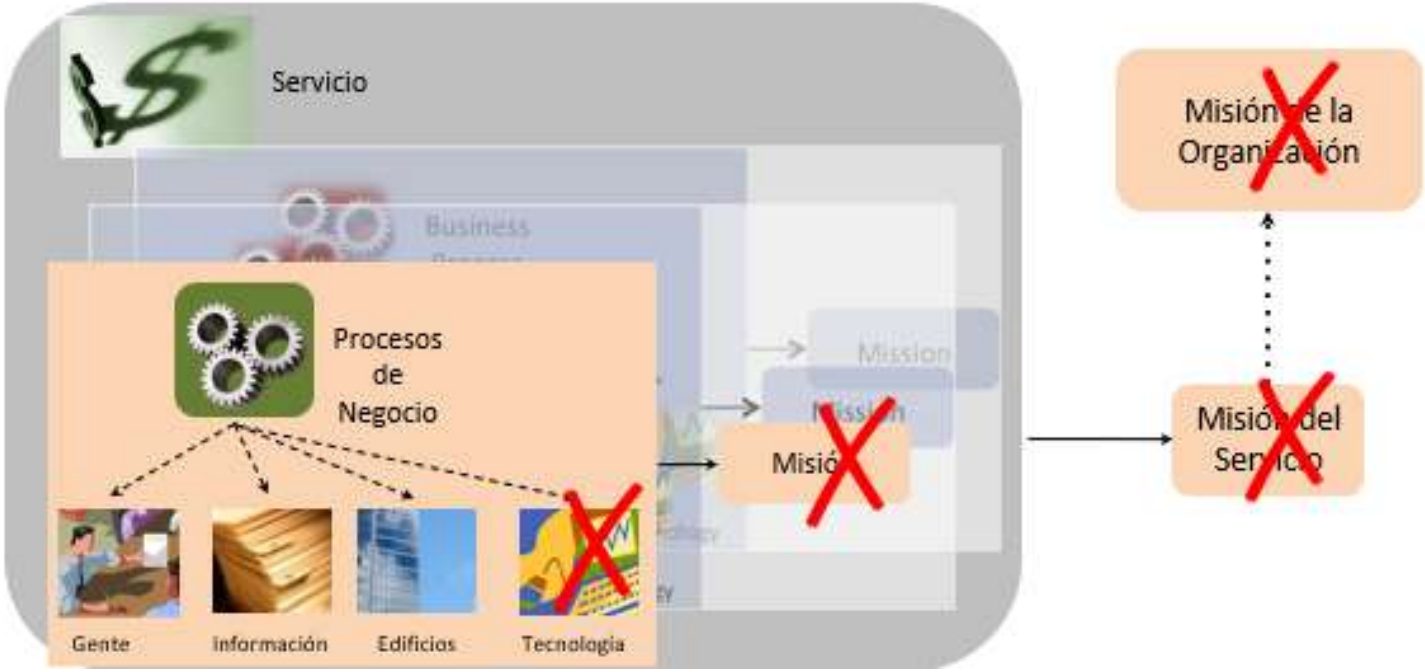


Y LA MISIÓN DE LA ORGANIZACIÓN



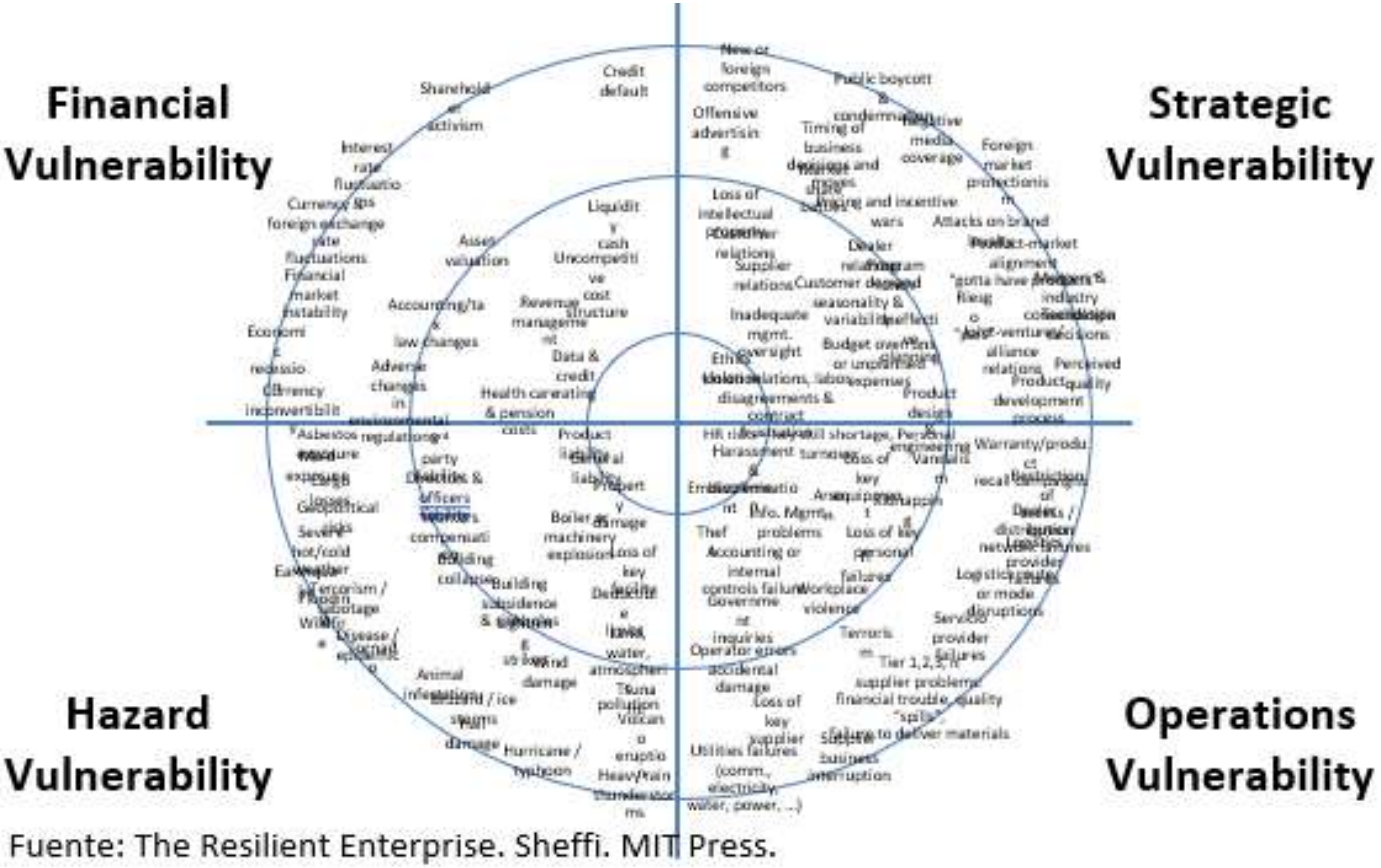
Y LA MISIÓN DE LA ORGANIZACIÓN

Un activo falla ➔ → efecto cascada



- ✕ Procesos
- ✕ Misión de la organización
- ✕ …
- ✕ El país

VULNERABILITIES



Fuente: The Resilient Enterprise. Sheffi. MIT Press.

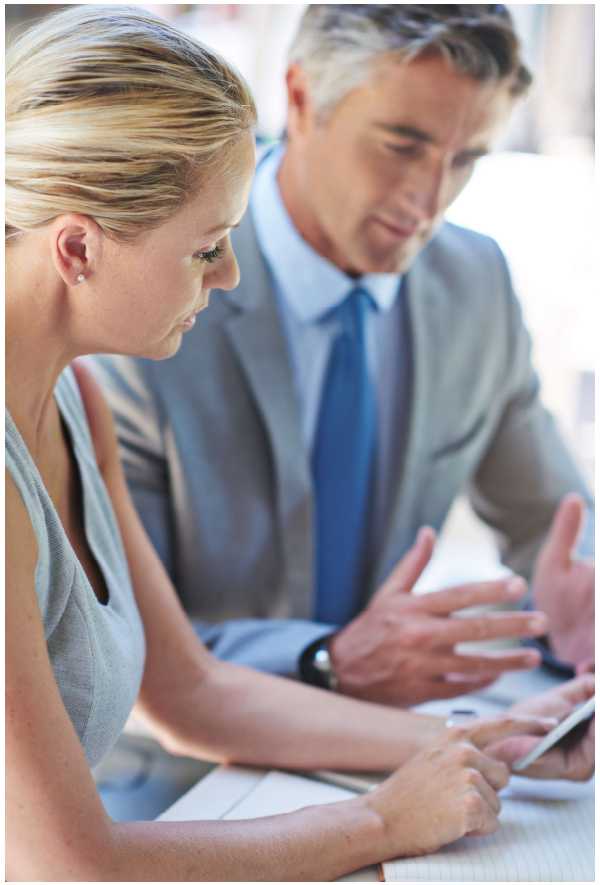
OPERATIONS VULNERABILITIES

HIPÓTESIS DE TRABAJO FRENTE A LA SEGURIDAD

Una región es resiliente a ciberguerra si su infraestructura crítica es resiliente a riesgo operacional

HIPÓTESIS DE TRABAJO FRENTE A LA SEGURIDAD

- Gestión de riesgos
- Gestión de continuidad
- Gestión de incidentes
- Gestión de activos
- Gestión de logs, monitoreo y mediciones
- Seguridad en el ciclo de vida del software
- Gestión de terceros
- Gestión de identidades
- Gestión de acceso
- Gestión de vulnerabilidades



¿QUÉ TAN BIEN PREPARADOS ESTÁBAMOS PARA COVID-19?

COVID-19 Y LA CONTINGENCIA TECNOLÓGICA MUNDIAL

RESILIENCIA ORGANIZACIÓN APALANCADA EN HERRAMIENTAS DE TI

CONTINGENCIAS TECNOLÓGICAS DESARROLLADAS

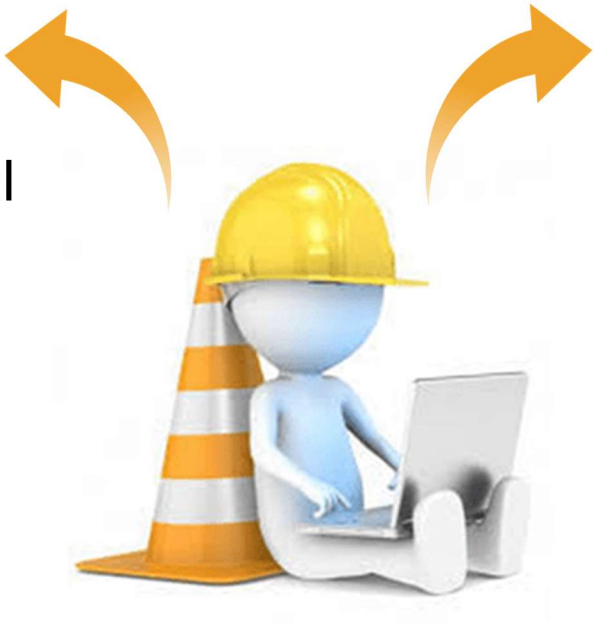
- Desarrollar acceso remoto a sistemas
- Cambios en los procesos internos y externos
- Implementación de nuevas herramientas de apoyo para desarrollar las tareas

PRINCIPALES PROBLEMAS EN LA CIBER CONTINGENCIA

- Ausencia de visión de riesgos al momento de desplegar las contingencias de TI
- Implementaciones de soluciones con brechas existentes
- Postura de gestión de riesgos reactiva y no preventiva

SITUACIONES A LAS QUE NOS EXPONEMOS

- Asignación de permisos no requeridos a personal
- No identificación e implementación de buenas prácticas de seguridad (Hardening)



- Vulnerabilidades de día Zero
- Tecnologías no seguras
- Uso de recursos de TI no corporativos

SITUACIONES A LAS QUE NOS EXPONEMOS

Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL

Inicio | CERT.PY | Servicios | Noticias | Estandares y Normas | Publicaciones | Informes | Contacto

Vulnerabilidad en Zoom permitiría a un atacante remoto obtener las credenciales de acceso de Windows

SITUACIONES A LAS QUE NOS EXPONEMOS

cyte

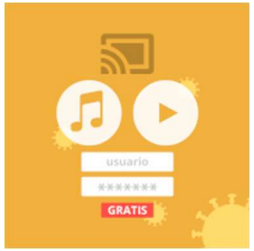
Cadenas retransmitidas por plataformas de chat

Phising tradicional

Smishing

Fake news

Suscripciones gratuitas

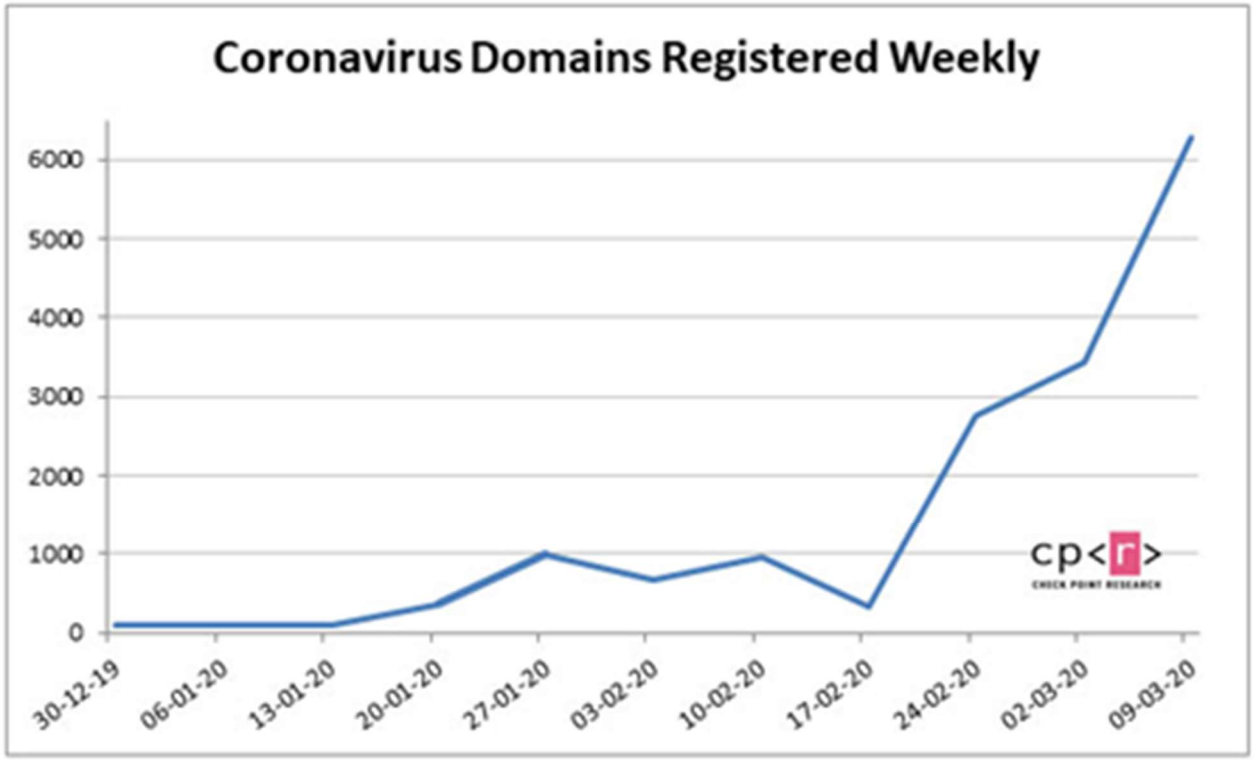


Compras online

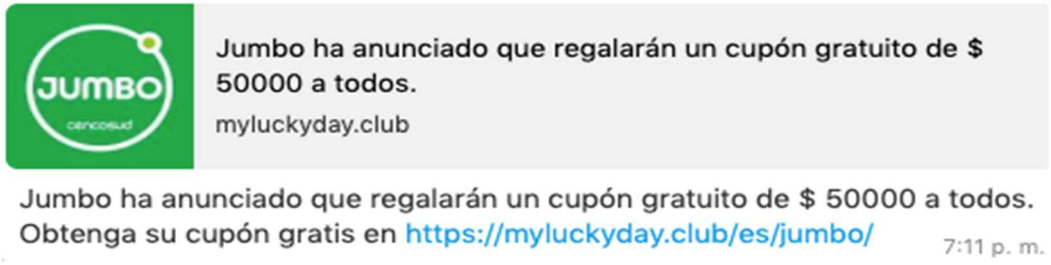
MOORE

DATO INTERESANTE

Cifra sobre dominios registrados relacionados con la palabra Coronavirus



EN COLOMBIA...



oogle.com/forms/d/e/1FAIpQLSfUEhQUHYFGWAa1Xkm1y3vMrxtKt0lbARBPmyke
/viewform --> *URL FRAUDULENTA*

ADMINISTRACIÓN

- Análisis de riesgo operacional y derivados
- Gestión de riesgos
- Evaluación de riesgos emergentes
- RIESGOS

HERRAMIENTAS

- Modelos de Criptografía
- Blockchain
- Herramientas de Hardening
- ……

Milton Quiroga
CYTE
mquiroga@cyte.co

Adriana Piñango
Gerente Consultoría Empresarial TI
apinango@moore-colombia.co