Enrique Fenollosa

Gerente General Sudamérica

enrique.fenollosa@s2grupo.com

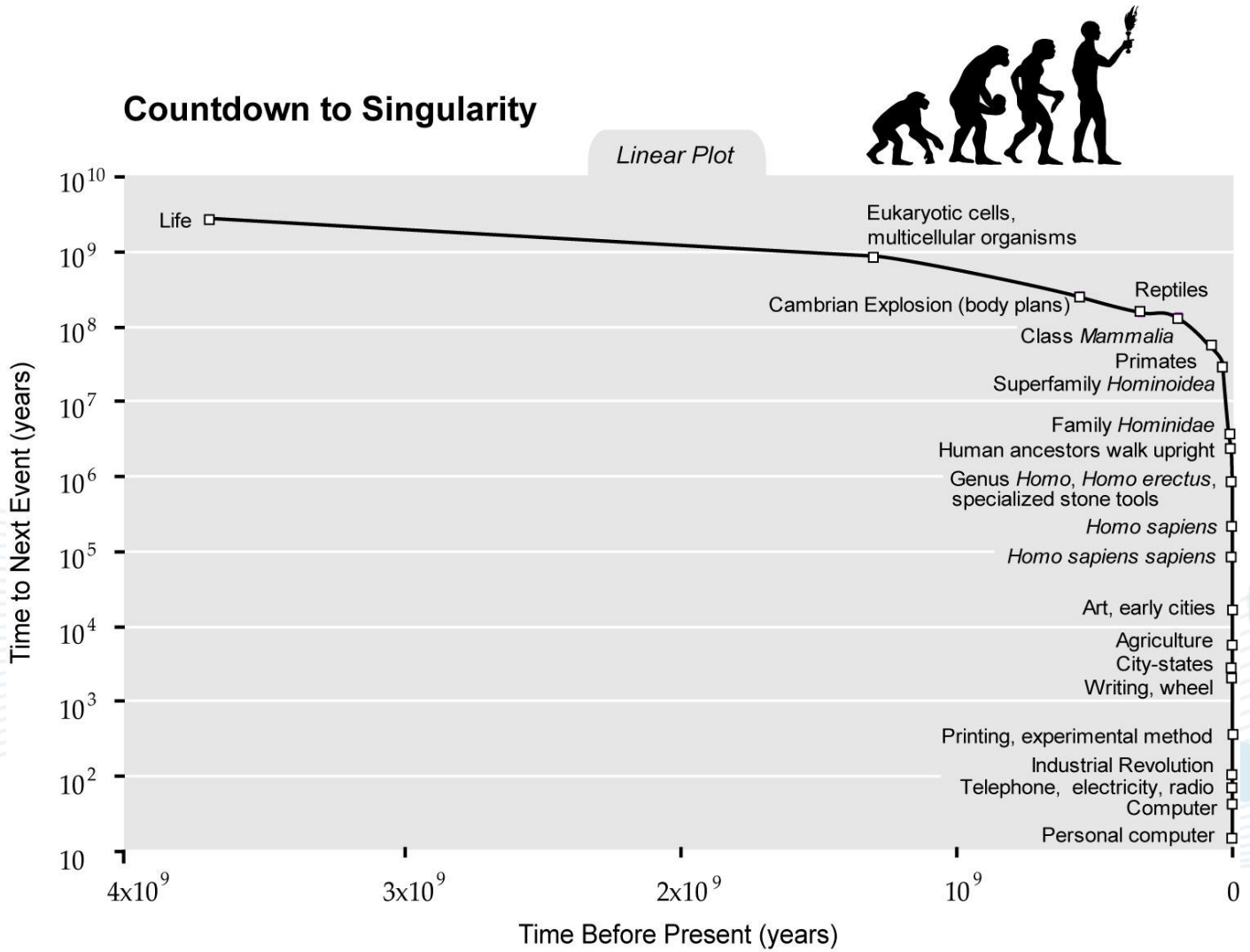
Ciberseguridad en tiempos de COVID-19

3/6/2020

ANTICIPANDO
UN MUNDO CIBERSEGURO

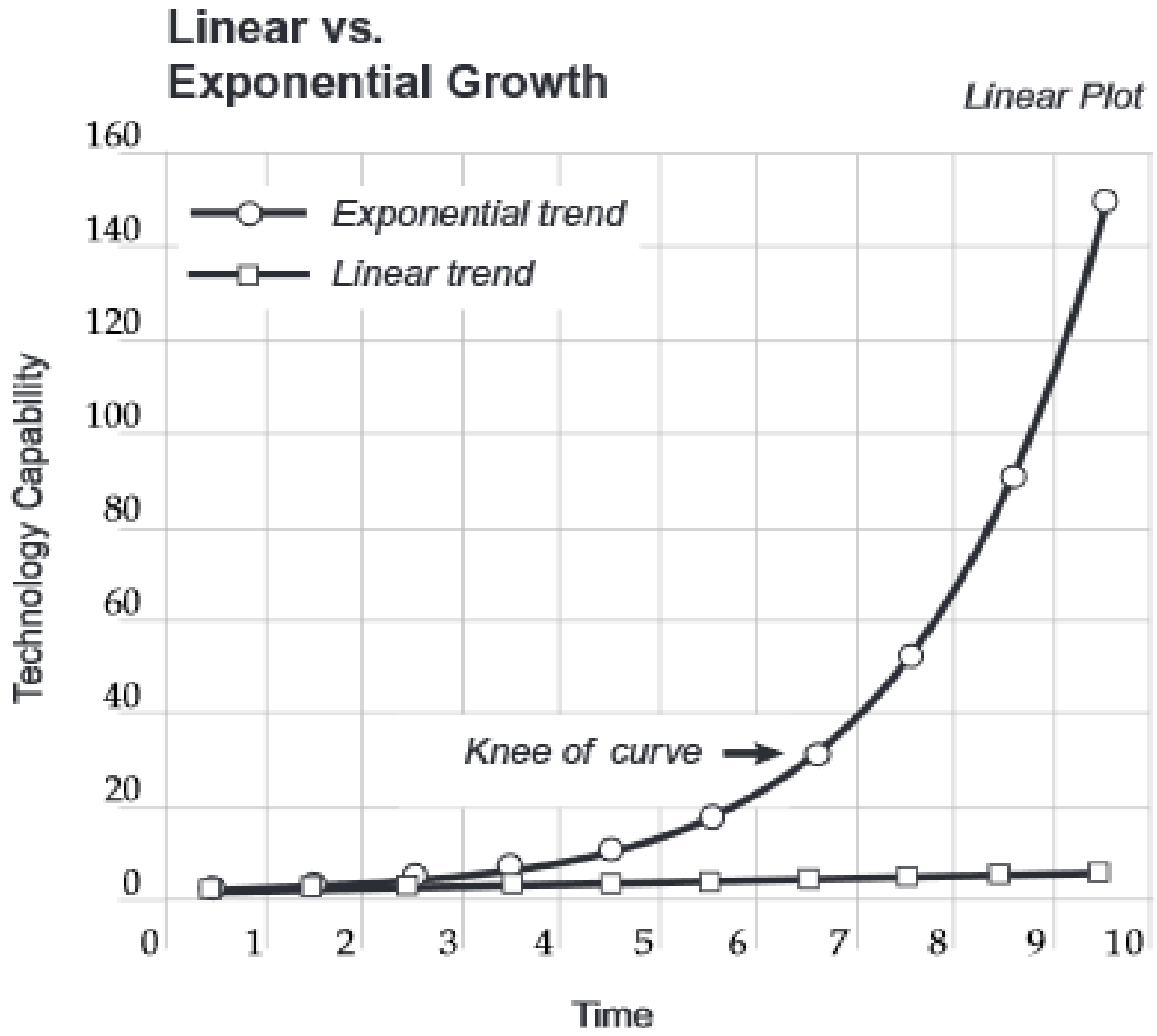

El mundo está
cambiando

Cada vez cambia más **rápido**



*El cambio está siendo **disruptivo***

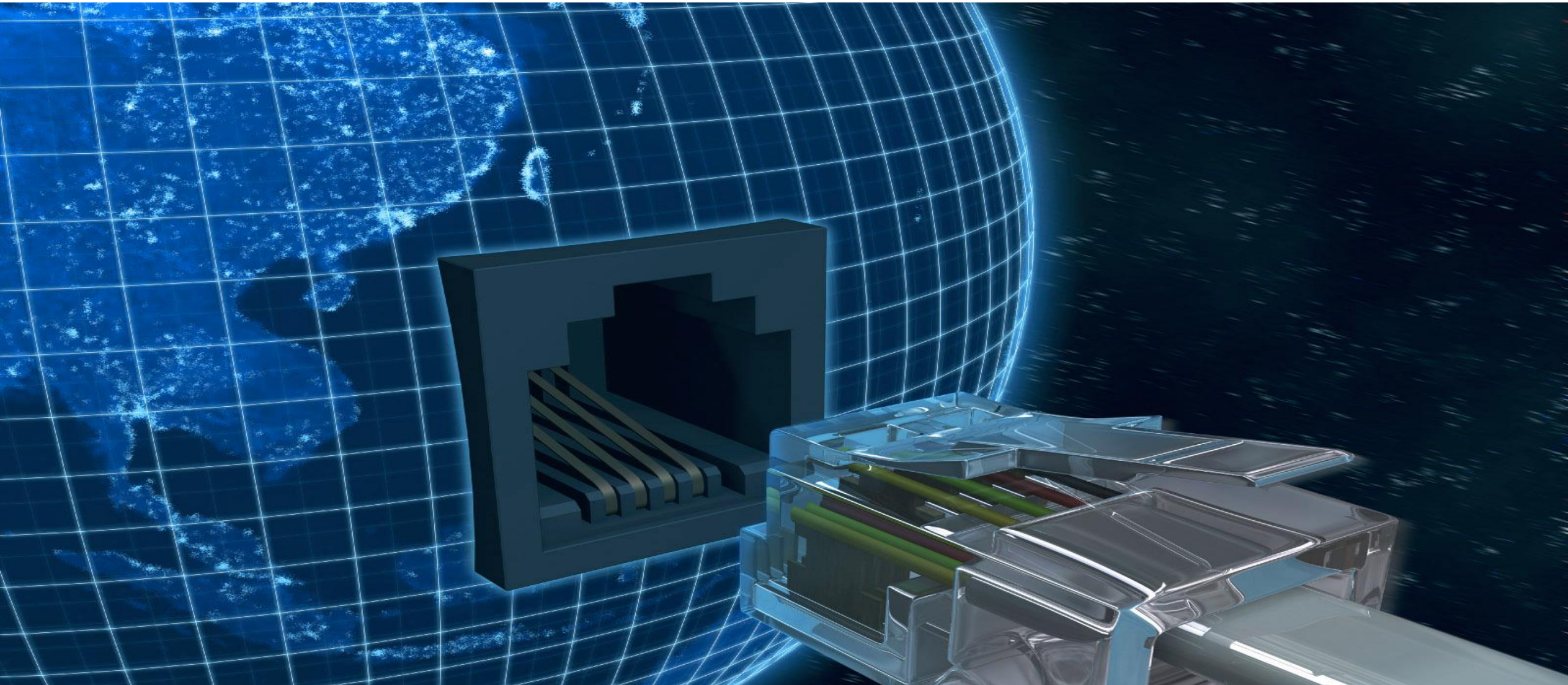
No estamos preparados para **crecimientos exponenciales**



*Miles de millones de nuevos **Ciudadanos Digitales** se van a incorporar a la **Sociedad Digital***

*La **Aceleración Tecnológica** está **revolucionando** todos los **procesos** cotidianos*

Lo hemos conectado TODO al ciberespacio, creando un
mundo Hiperconectado



Y también hemos conectado...



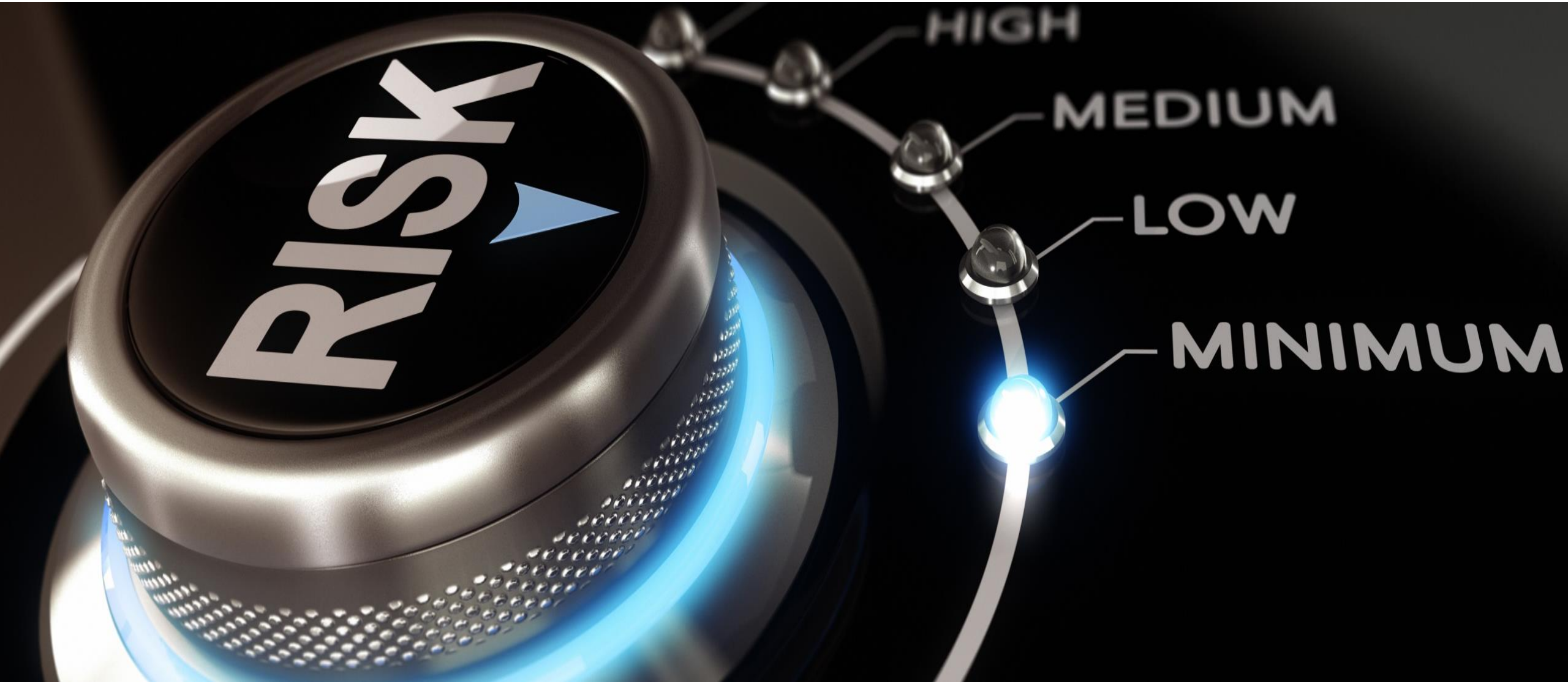




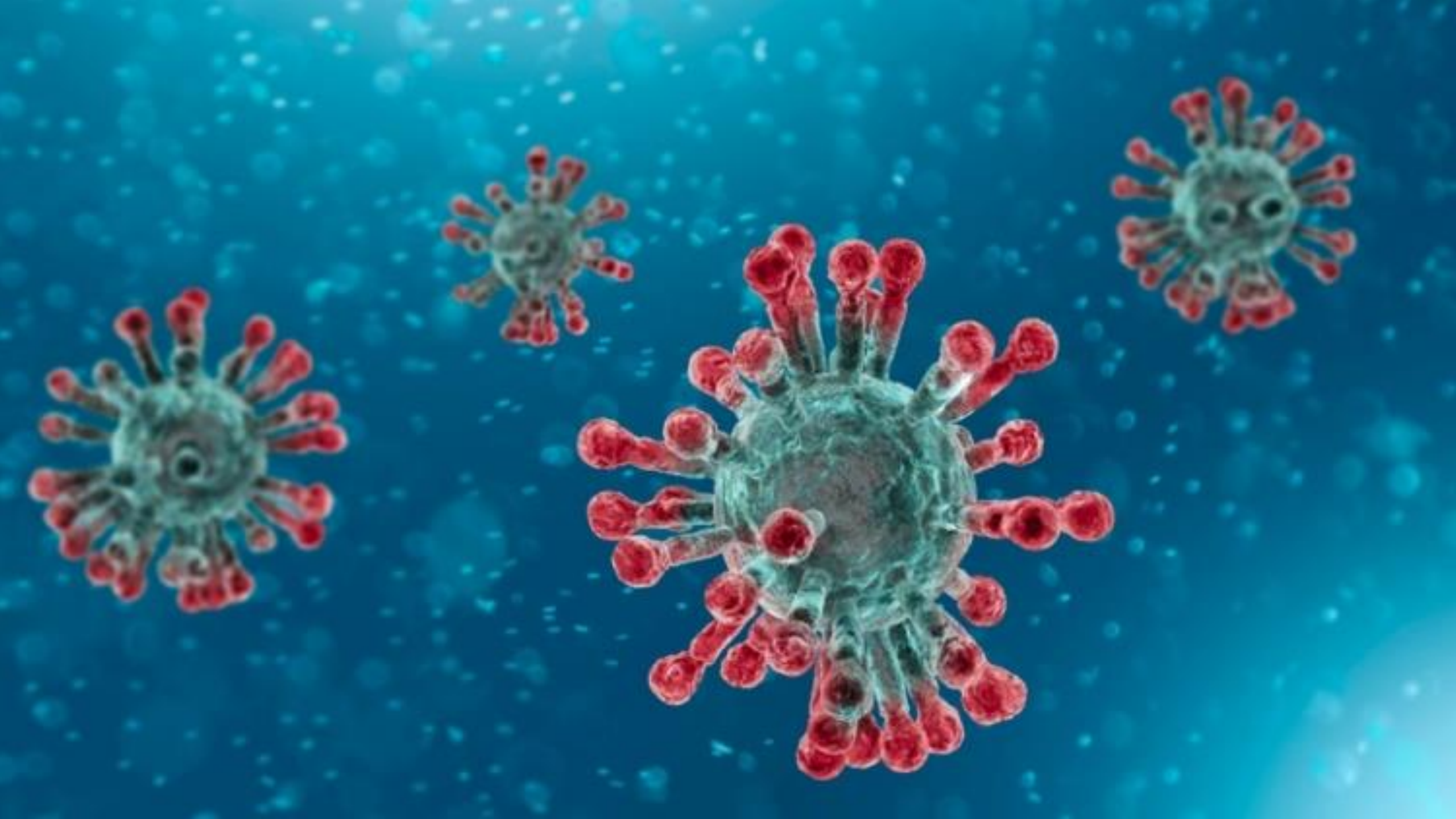


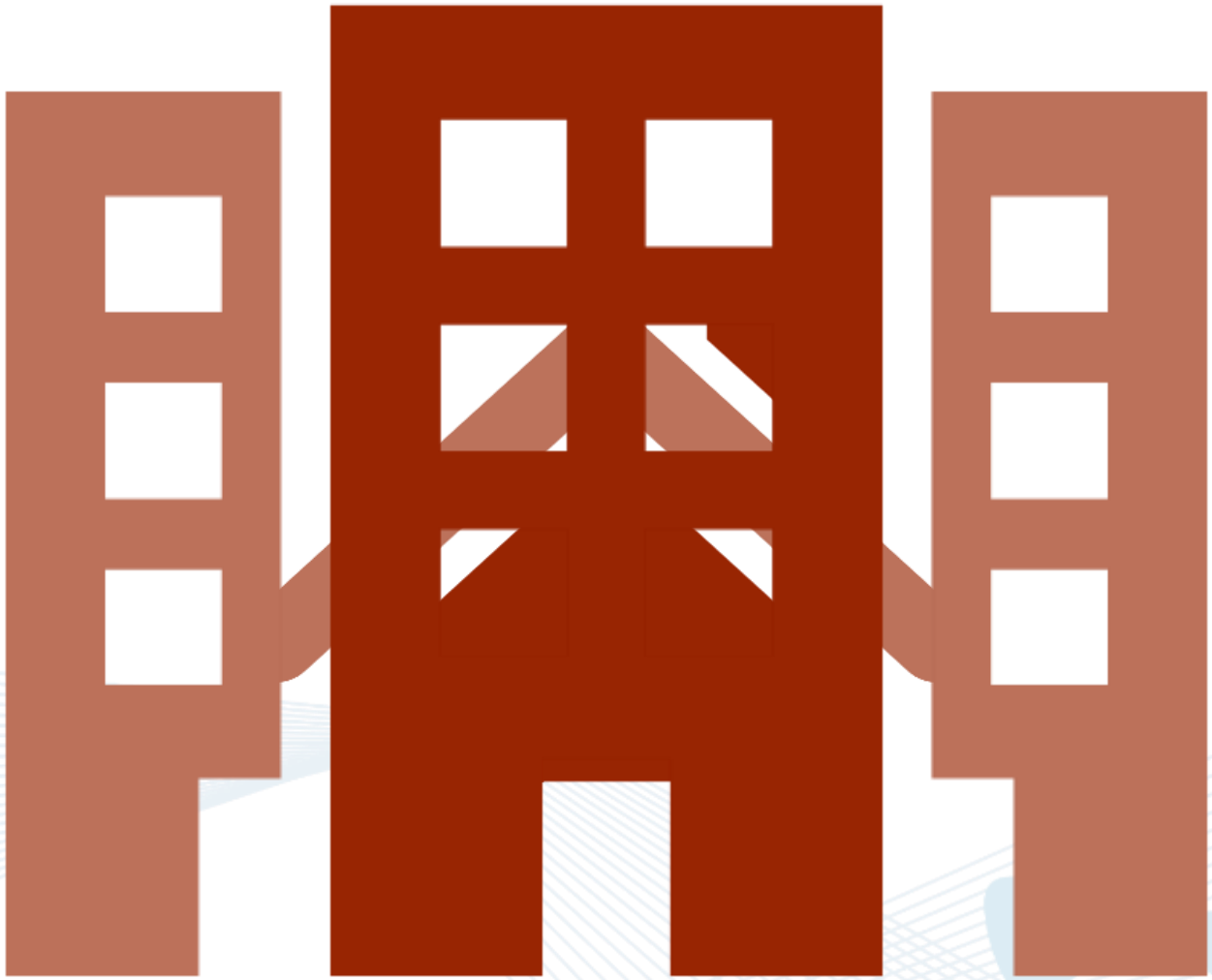



El Riesgo está creciendo mucho



El **impacto** crece con la dependencia de la tecnología
La **probabilidad** crece con la conectividad
El **riesgo** es producto de ambas





TyN MAGAZINE

Colombia es cada vez más vulnerable ante las fake news y el fraude

By Staff - 12/03/2020 0

weliv

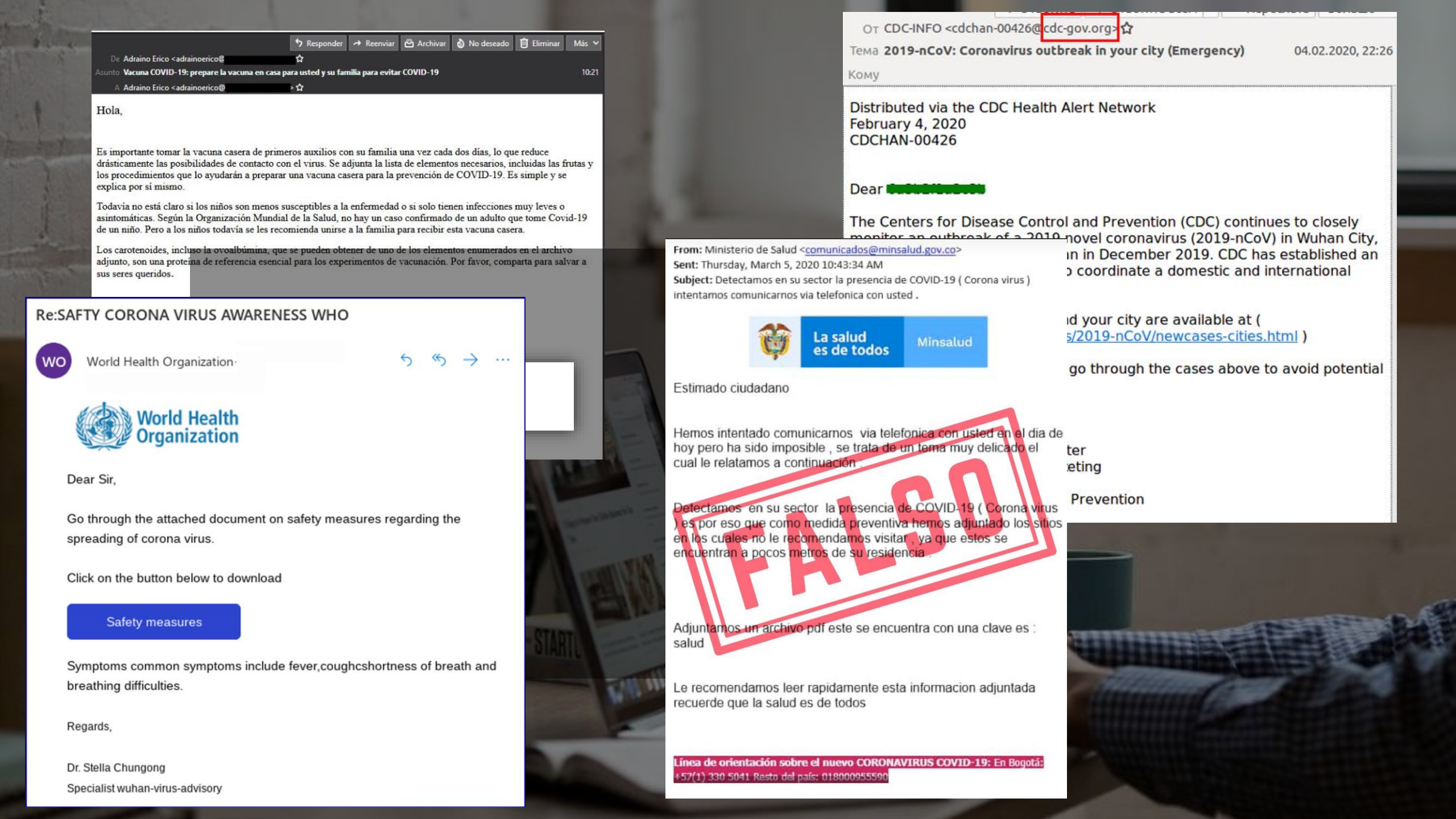
Crecen las campañas de malware que intentan aprovechar el temor provocado por el COVID-19

cen las campañas de phishing y de distribución de malware que se aprovechan de la preocupación por

EL TIEMPO

El teletrabajo puede abrir puertas a ciberataques

Los colaboradores son el 'eslabón más débil'. Expertos recomiendan estrategias de trabajo remoto.



Responder | Reenviar | Archivar | No deseado | Eliminar | Más

De Adraino Erico <adrainoerico@[redacted]>

Asunto **Vacuna COVID-19: prepare la vacuna en casa para usted y su familia para evitar COVID-19** 10:21

A Adraino Erico <adrainoerico@[redacted]>

Hola,

Es importante tomar la vacuna casera de primeros auxilios con su familia una vez cada dos días, lo que reduce drásticamente las posibilidades de contacto con el virus. Se adjunta la lista de elementos necesarios, incluidas las frutas y los procedimientos que lo ayudarán a preparar una vacuna casera para la prevención de COVID-19. Es simple y se explica por sí mismo.

Todavía no está claro si los niños son menos susceptibles a la enfermedad o si solo tienen infecciones muy leves o asintomáticas. Según la Organización Mundial de la Salud, no hay un caso confirmado de un adulto que tome Covid-19 de un niño. Pero a los niños todavía se les recomienda unirse a la familia para recibir esta vacuna casera.

Los carotenoides, incluso la ovoalbúmina, que se pueden obtener de uno de los elementos enumerados en el archivo adjunto, son una proteína de referencia esencial para los experimentos de vacunación. Por favor, comparta para salvar a sus seres queridos.

Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization

World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong

Specialist wuhan-virus-advisory

От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely
monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City,
n in December 2019. CDC has established an
o coordinate a domestic and international

d your city are available at (
s/2019-nCoV/newcases-cities.html)

go through the cases above to avoid potential

ter
eting

Prevention

From: Ministerio de Salud <comunicados@minsalud.gov.co>
Sent: Thursday, March 5, 2020 10:43:34 AM
Subject: Detectamos en su sector la presencia de COVID-19 (Corona virus)
intentamos comunicarnos via telefonica con usted .

La salud es de todos | Minsalud

Estimado ciudadano

Hemos intentado comunicarnos via telefonica con usted en el dia de hoy pero ha sido imposible , se trata de un tema muy delicado el cual le relatamos a continuación .

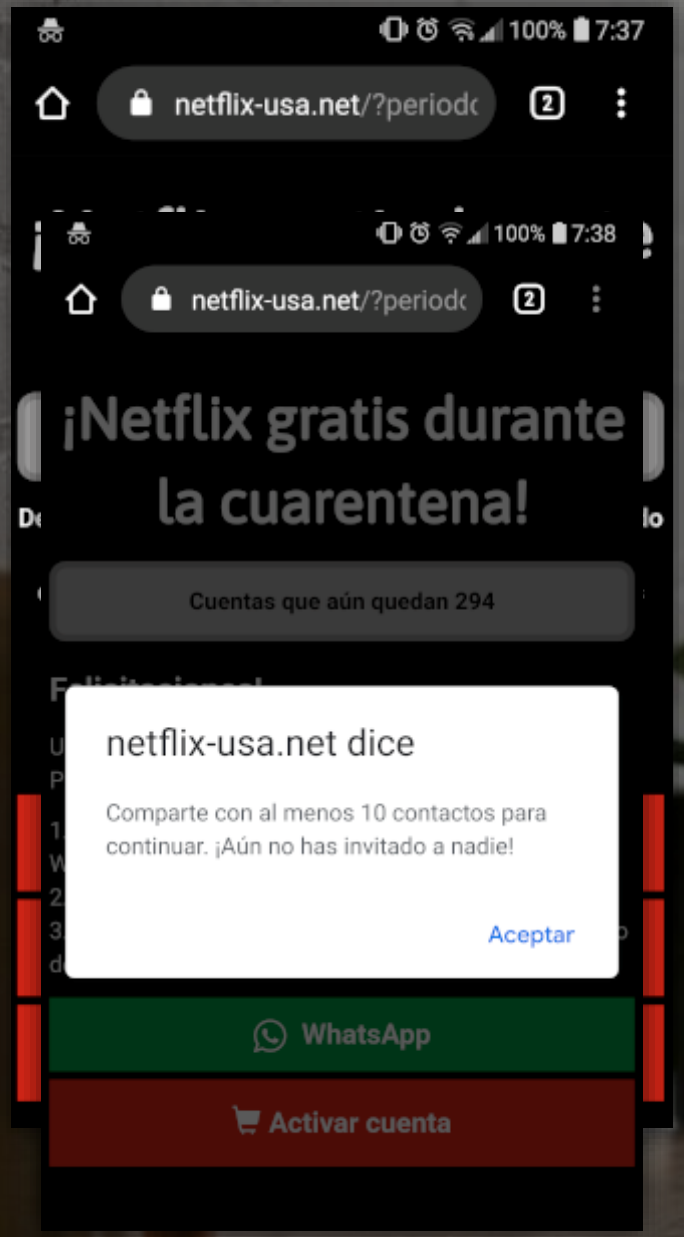
Detectamos en su sector la presencia de COVID-19 (Corona virus) es por eso que como medida preventiva hemos adjuntado los sitios en los cuales no le recomendamos visitar , ya que estos se encuentran a pocos metros de su residencia .

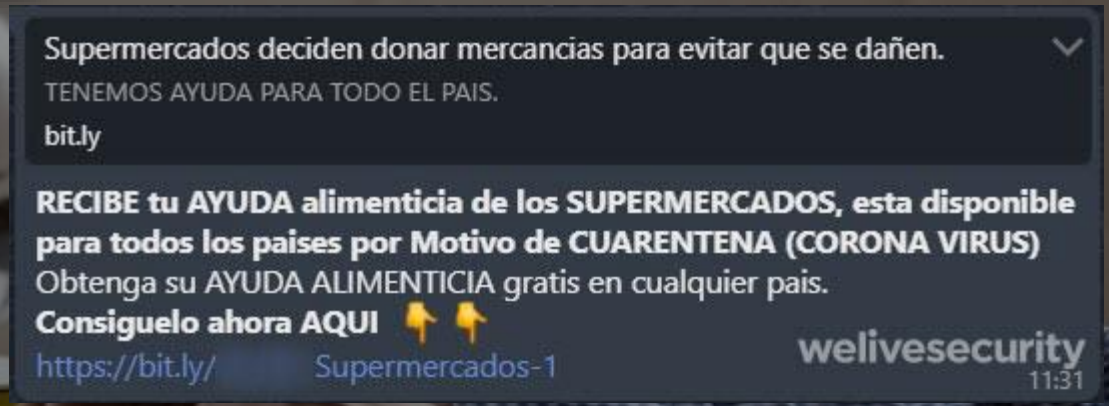
FALSO

Adjuntamos un archivo pdf este se encuentra con una clave es : salud

Le recomendamos leer rapidamente esta informacion adjuntada recuerde que la salud es de todos

Línea de orientación sobre el nuevo CORONAVIRUS COVID-19: En Bogotá: +57(1) 330 5041 Resto del país: 018000955590

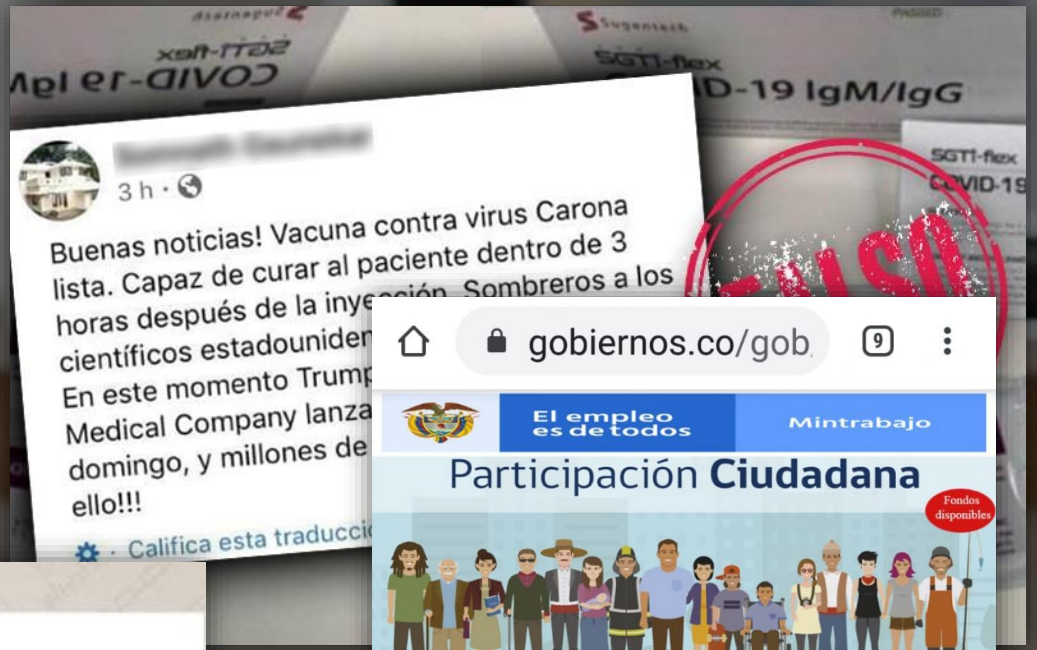


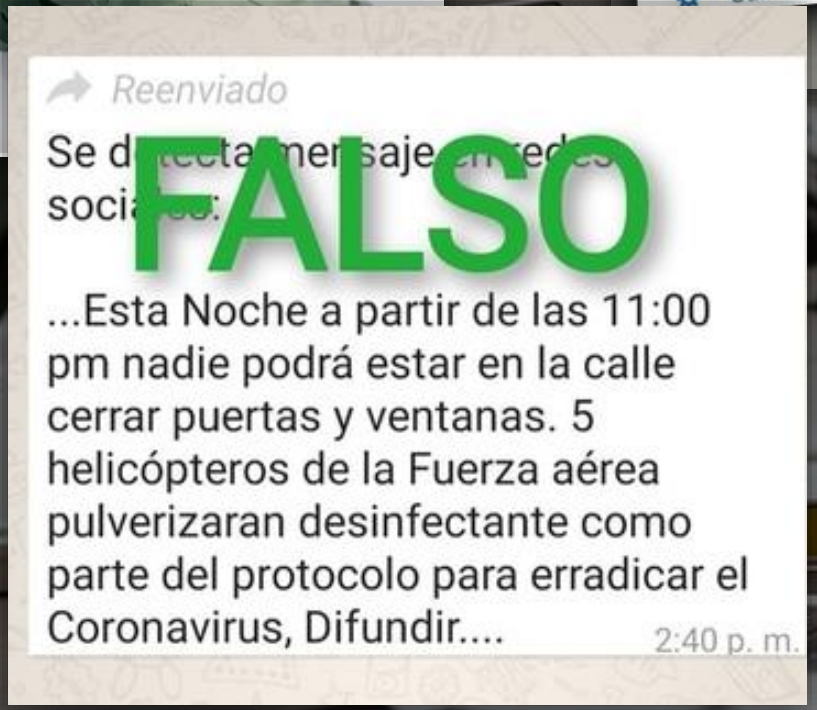


Nuevas costumbres y necesidades

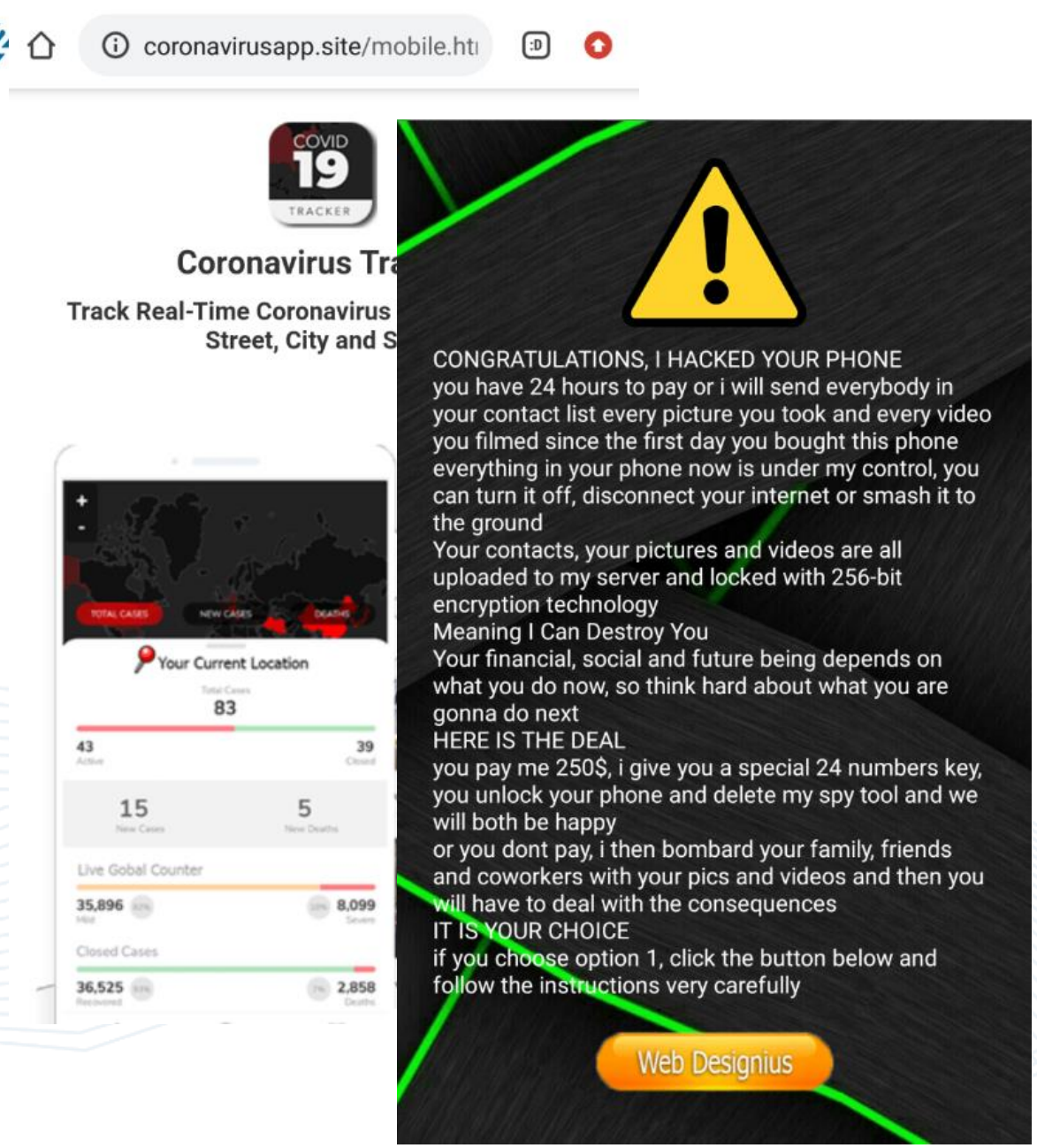
Fake news


Traffic CARACAS
@traffiCARACAS
via @RSTV_anfitrion: Medicos caen mientras operan al coronavirus. La transmisión es inmediata.
1:12


3 h ·
Buenas noticias! Vacuna contra virus Carona
lista. Capaz de curar al paciente dentro de 3
horas después de la inye
científicos estadounide
En este momento Trump
Medical Company lanza
domingo, y millones de
ello!!!
· Califica esta traducci
SGTI-flex
D-19 IgM/IgG
FALSO


Reenviado
FALSO
...Esta Noche a partir de las 11:00 pm nadie podrá estar en la calle cerrar puertas y ventanas. 5 helicópteros de la Fuerza aérea pulverizaran desinfectante como parte del protocolo para erradicar el Coronavirus, Difundir....
2:40 p. m.


gobiernos.co/gob
El empleo es de todos
Mintrabajo
Participación Ciudadana
Fondos disponibles
Personas activas 2532
Ministerio de Trabajo de Colombia
Aquellos que trabajaron entre 1984 y 2019 tienen el derecho de retirar $7.000.000 del Fondo de Riesgos Laborales (gob). Verifique si su nombre figura en la lista de aquellos que tienen derecho a retirar estos fondos. En caso de que deba retirar los fondos, DEBERA PERMITIR LAS NOTIFICACIONES.

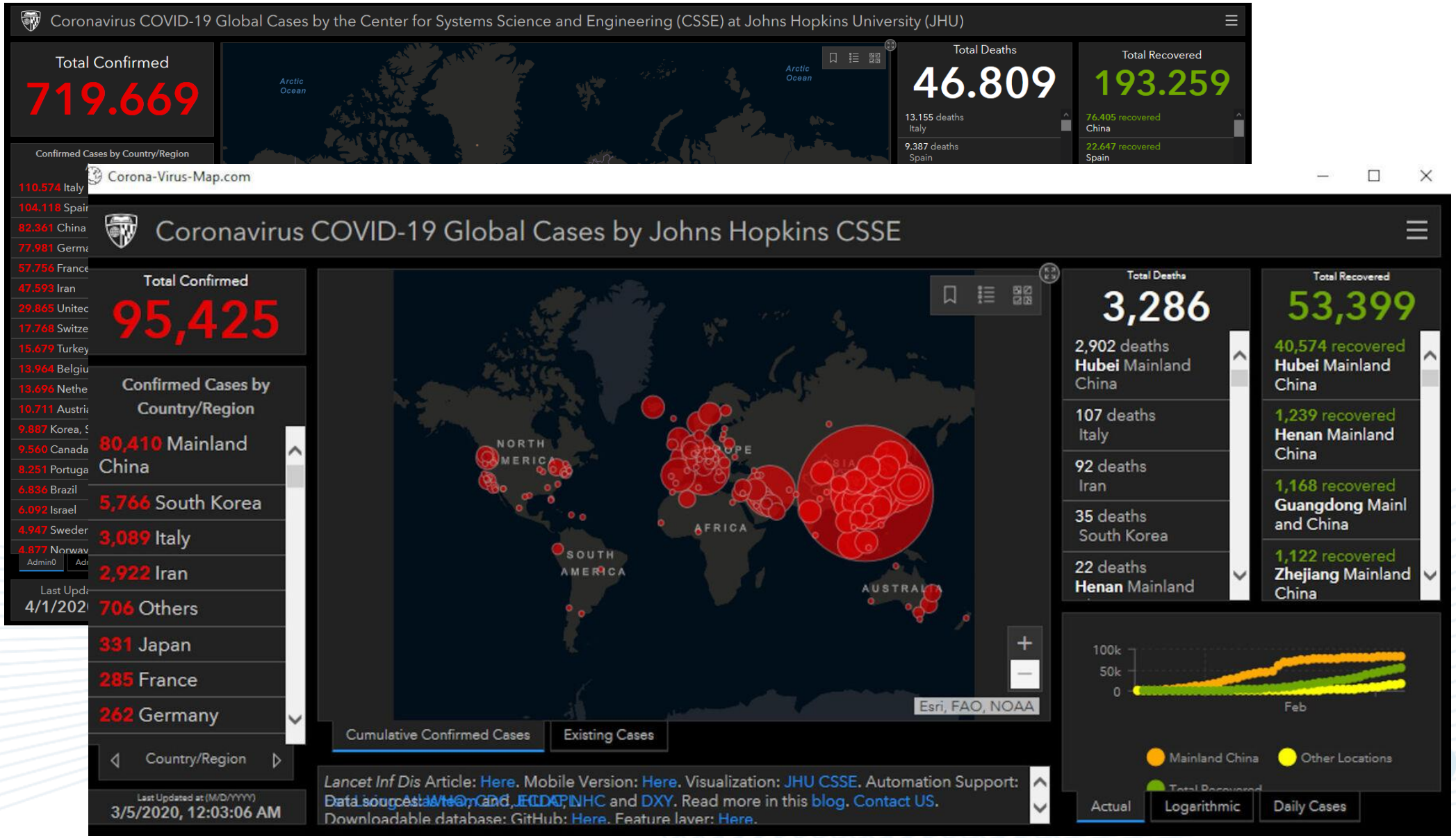


Promete control de toda la información sobre el COVID-19

Lo que **realmente** aporta es un **ransomware** que solicita el pago nada más instalarse.

Promete consejos para prevenir la infección por COVID-19.

Lo que **realmente** aporta es una copia del **troyano bancario Cerberus** que roba credenciales de acceso a sistemas de pago Online.


Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)
Total Confirmed
719.669
Total Deaths
46.809
13.155 deaths Italy
9.387 deaths Spain
Total Recovered
193.259
76.405 recovered China
22.647 recovered Spain
Confirmed Cases by Country/Region
110.574 Italy
104.118 Spain
82.361 China
77.981 Germa
57.756 France
47.593 Iran
29.865 Unitec
17.768 Switze
15.679 Turkey
13.964 Belgiu
13.696 Nethe
10.711 Austria
9.887 Korea, S
9.560 Canada
8.251 Portuga
6.836 Brazil
6.092 Israel
4.947 Sweden
4.877 Norway
Admin0
Last Upda
4/1/202
Corona-Virus-Map.com
Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE
Total Confirmed
95,425
Confirmed Cases by Country/Region
80,410 Mainland China
5,766 South Korea
3,089 Italy
2,922 Iran
706 Others
331 Japan
285 France
262 Germany
Country/Region
Last Updated at (M/D/YYYY)
3/5/2020, 12:03:06 AM
NORTH AMERICA
AFRICA
SOUTH AMERICA
Esri, FAO, NOAA
Cumulative Confirmed Cases
Existing Cases
Lancet Inf Dis Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support:
Data sources: WHO, CDC, ECDC, NHC and DXY. Read more in this blog. Contact US.
Downloadable database: GitHub: Here. Feature layer: Here.
Total Deaths
3,286
2,902 deaths Hubei Mainland China
107 deaths Italy
92 deaths Iran
35 deaths South Korea
22 deaths Henan Mainland
Total Recovered
53,399
40,574 recovered Hubei Mainland China
1,239 recovered Henan Mainland China
1,168 recovered Guangdong Mainland China
1,122 recovered Zhejiang Mainland China
100k
50k
0
Feb
Mainland China
Other Locations
Actual
Logarithmic
Daily Cases

- Equipo y antivirus actualizado
- Higiene digital / Desconfianza digital / Hábitos
- Confirma las fuentes de la información que lees
- Busca siempre la información en organismos verificados y oficiales
- Comprueba los remitentes de los correos electrónicos y no sigas enlaces
- No compartas información dudosa sin verificarla antes
- Si es demasiado bueno para ser verdad, no es verdad

- No descargues aplicaciones fuera de las tiendas oficiales
- Utiliza webs para comprobar direcciones sospechosas como virustotal.com
- Comprueba los permisos de las apps antes de instalarlas.
- Instala un antivirus también en tu móvil
- Reporta los incidentes lo antes posible

9
/ 76

Community Score

9 engines detected this URL

http://corona-virus-map.com/

corona-virus-map.com

502
Status

text/html
Content Type

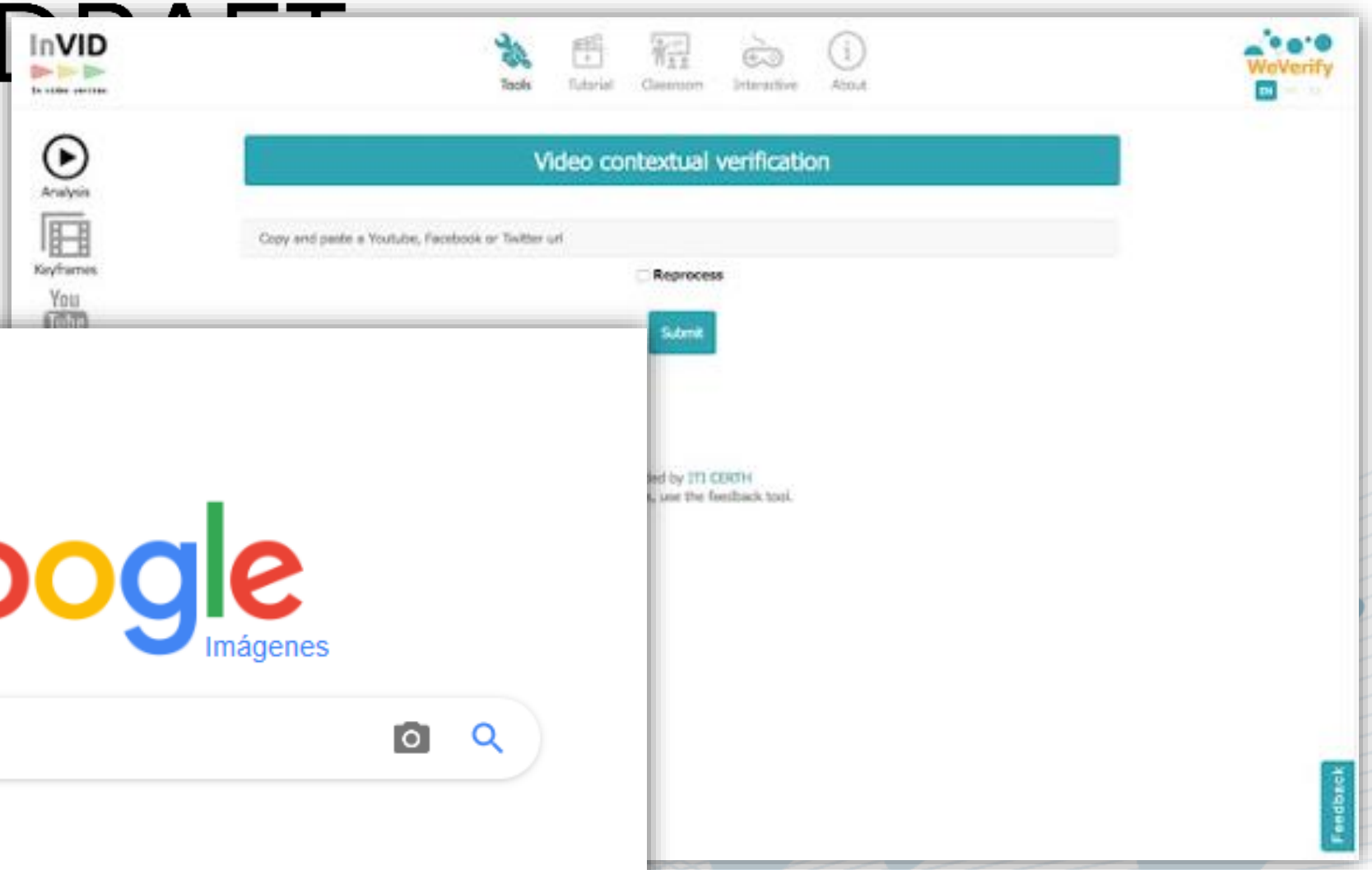
2020-04-02 03:39:09 UTC
8 hours ago

DETECTION | DETAILS | COMMUNITY 10+

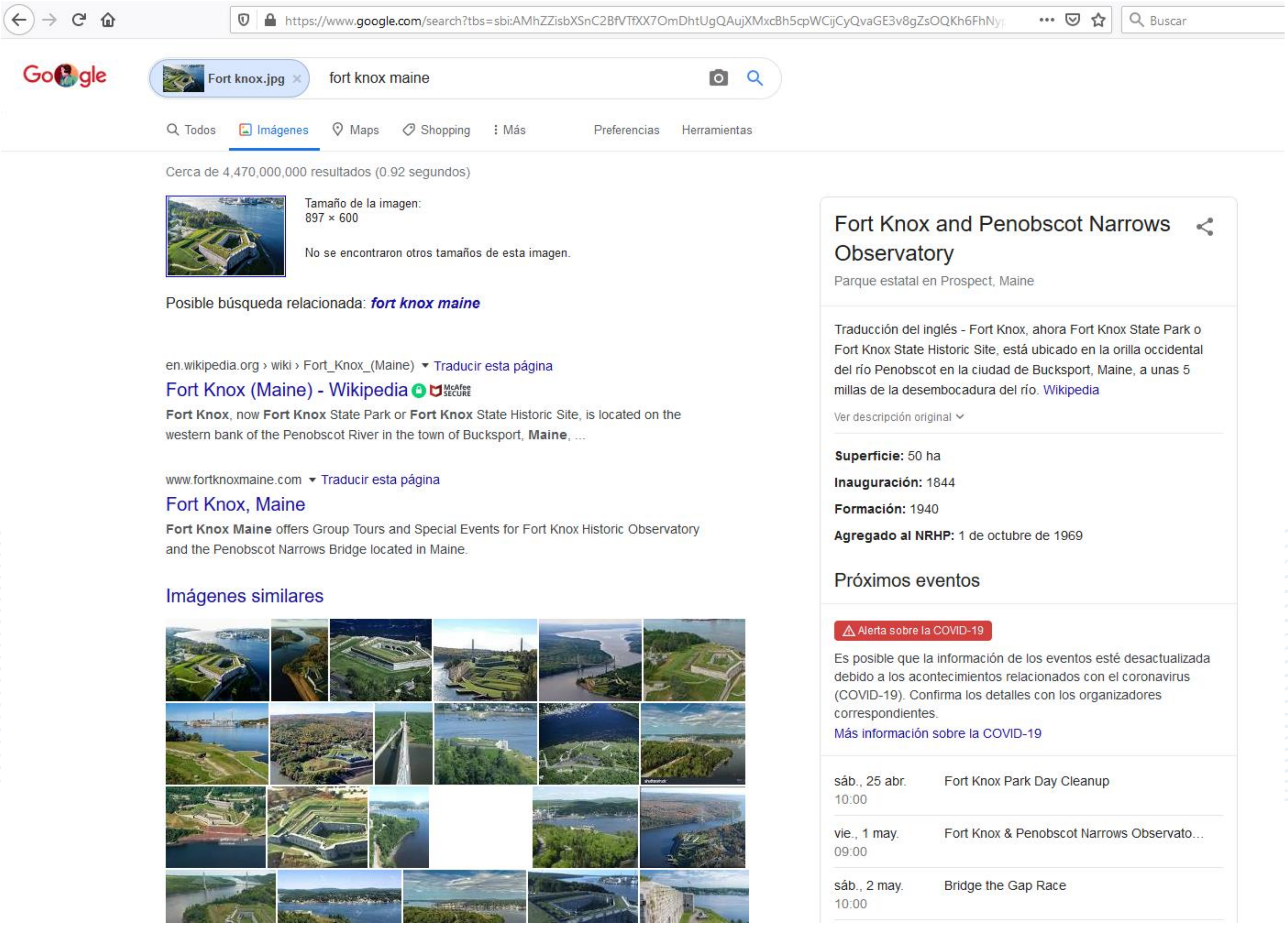
CLEAN MX	Malicious	CRDF	Malicious
CyRadar	Malicious	DNS8	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	Kaspersky	Malware
Sophos AV	Malicious	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
Avira (no cloud)	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	BitDefender	Clean
BlockList	Clean	Blueliv	Clean
Botvrij.eu	Clean	Cisco Talos IP Blacklist	Clean
CyberCrime	Clean	Cyren	Clean
desenmascara.me	Clean	Dr.Web	Clean
EmergingThreats	Clean	Emsisoft	Clean
EonScope	Clean	Feodo Tracker	Clean

FIRST DRAFT


COLOMBIACHECK
- No coma cuento -


InVID
Tools
Tutorial
Classroom
Interactive
About
WeVerify
Video contextual verification
Analysis
Keyframes
Copy and paste a Youtube, Facebook or Twitter url
Reprocess
Submit
Feedback

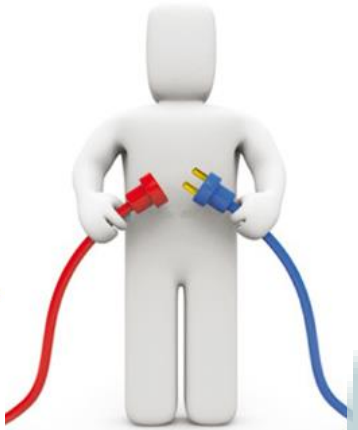

Google
Imágenes


https://www.google.com/search?tbs=sbi:AMhZZisbXSnC2BfVTfXX7OmDhtUgQAujXMxcBh5cpWCijCyQvaGE3v8gZsOQKh6FhNy
Buscar
Fort knox.jpg
fort knox maine
Todos
Imágenes
Maps
Shopping
Más
Preferencias
Herramientas
Cerca de 4,470,000,000 resultados (0.92 segundos)
Tamaño de la imagen:
897 × 600
No se encontraron otros tamaños de esta imagen.
Posible búsqueda relacionada: fort knox maine
en.wikipedia.org › wiki › Fort_Knox_(Maine) ▾ Traducir esta página
Fort Knox (Maine) - Wikipedia
Fort Knox, now Fort Knox State Park or Fort Knox State Historic Site, is located on the western bank of the Penobscot River in the town of Bucksport, Maine, ...
www.fortknoxmaine.com ▾ Traducir esta página
Fort Knox, Maine
Fort Knox Maine offers Group Tours and Special Events for Fort Knox Historic Observatory and the Penobscot Narrows Bridge located in Maine.
Imágenes similares
Fort Knox and Penobscot Narrows Observatory
Parque estatal en Prospect, Maine
Traducción del inglés - Fort Knox, ahora Fort Knox State Park o Fort Knox State Historic Site, está ubicado en la orilla occidental del río Penobscot en la ciudad de Bucksport, Maine, a unas 5 millas de la desembocadura del río. Wikipedia
Ver descripción original
Superficie: 50 ha
Inauguración: 1844
Formación: 1940
Agregado al NRHP: 1 de octubre de 1969
Próximos eventos
Alerta sobre la COVID-19
Es posible que la información de los eventos esté desactualizada debido a los acontecimientos relacionados con el coronavirus (COVID-19). Confirma los detalles con los organizadores correspondientes.
Más información sobre la COVID-19
sáb., 25 abr. 10:00 Fort Knox Park Day Cleanup
vie., 1 may. 09:00 Fort Knox & Penobscot Narrows Observato...
sáb., 2 may. 10:00 Bridge the Gap Race

¿Y en el mundo OT?

Los Sistemas de Control Industrial también se han visto afectados


KARL BENSCHEIDT



- Revisa la visibilidad desde el exterior del perímetro de tus sistemas OT
- Identifica y parchea las vulnerabilidades en tus accesos remotos
- Verifica que no hay puertos expuestos que no deberían estarlo
- Implementa procedimientos de gestión segura de las conexiones remotas
- Monitoriza las conexiones a través del perímetro de las redes OT para identificar actividades sospechosas

Técnico de Comunicaciones y Seguridad en [redacted]

[redacted] · 29 contactos ·

Información de contacto

[redacted]

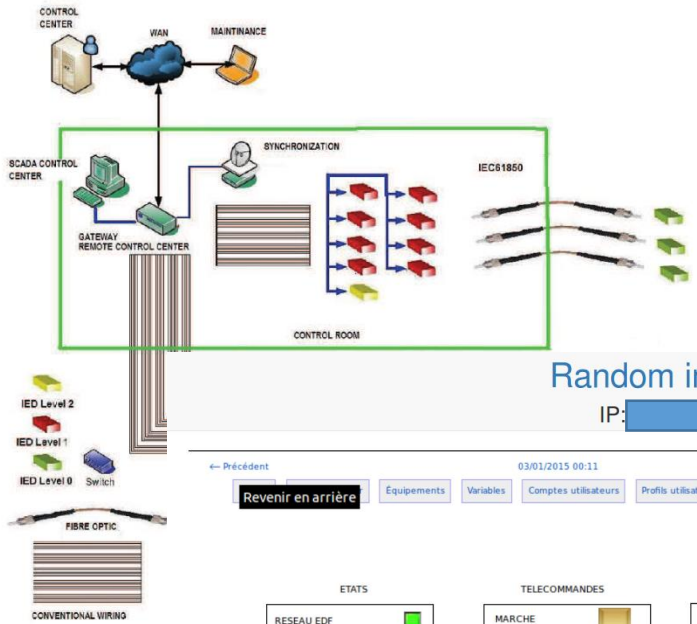
4 años y 10 meses

Técnico de Explotación de Datos [redacted]
ene. de 2019 – actualidad · 8 meses
Madrid

Gestión y mantenimiento de las comunicaciones de los servicios críticos de [redacted]
(Mercado Eléctrico y GAS):
- Despacho de Generación MIOE/MOE [redacted] zado Eléctrico)
- Centrales hidráulicas, térmicas y de ciclo combinado.
- Despacho del GAS (CAU & SAU).
- COR Eléctrico.
- Despacho [redacted] (Despacho de Operación Centralizado Eólico).
- CCI (Control Integrado de Instalaciones Hidráulicas).

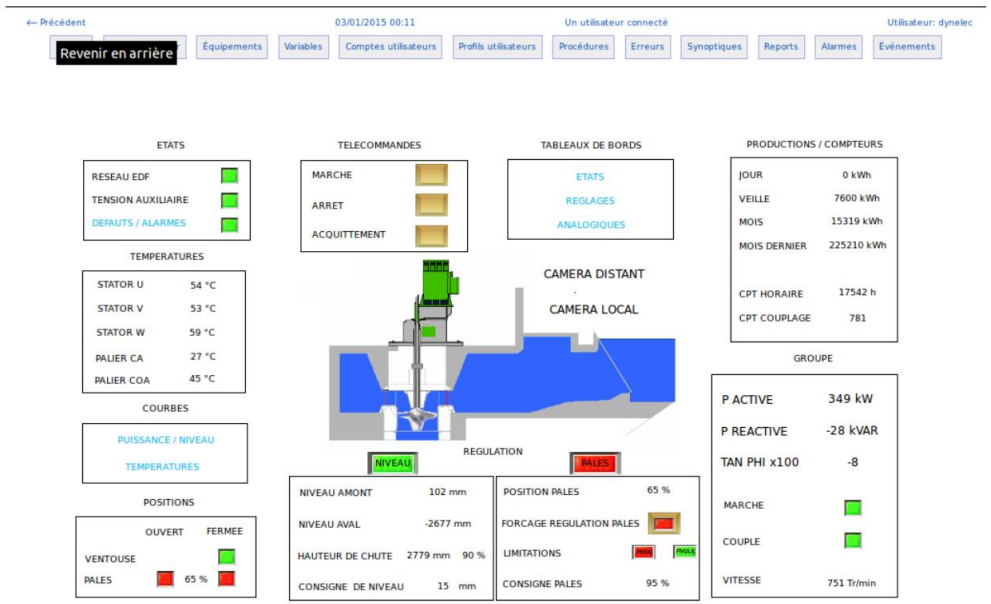
Funciones:
- Configuración y mantenimiento de la red.
- Tratamiento técnico de las averías de la red de datos.
- Coordinación de operadores y mantenedores.
- Asesoramiento y apoyo técnico de infraestructuras y servicios críticos.
- Realización de informes, análisis de impactos de intervenciones y de dimensionamiento de la red de datos.
- Gestión de intervenciones planificadas y gestión de cambios según modelo ITIL.
- Validación de documentación proveniente de proyectos de Desarrollo de Red.
- Documentación y asignación de recursos de red.
- Conocimientos relativos a interconexión de la red de GNF con los diferentes proveedores de servicio
(Transmisión PDH/SDH, M2M, Satelital, MPLS, VPLS, Carrier Ethernet, ADSL, RDSI).
- Análisis y modificación de políticas de seguridad en firewalls (Palo Alto, Juniper, Checkpoint y ASA).
- Gestión de Radius Steelbelted & PULSE Juniper.
- Configuración equipos Cisco Routing & switching (ISR, ASR, Nexus, Catalyst, ACS Radius e ISE).
- Gestión de balanceadores F5 Big IP y Radware.
- Administración de red con Infoblox IB-2000 (IPAM, DNS y DHCP)
- Gestión de peticiones e intervenciones con Remedy F1 ITSM y PPM. Ver menos

LinkedIn



Random image

IP: [redacted]



- **Huella digital: Revisa la información disponible sobre tus sistemas OT y cómo podría utilizarse con fines maliciosos**
- **No des detalles sobre la tecnología que utilizas**
- **Desconfía**

TECHNOLOGY AND IIOT

Aluminum Producer Hydro Says Cyber Attack Hit Operations

Aluminum supplier switching to manual production processes

Bloomberg

MAR 19, 2019

EKANS Ransomware and ICS Operations

Feb 3, 2020 | Blog, Industry News

Upon discovery and investigation, Dragos identified a relationship between EKANS and ransomware called MEGACORTEX, which also contained some ICS-specific characteristics. The identification of industrial process targeting within the ransomware described in this report is unique and represents the first known ICS-specific ransomware variants.

- Del mismo que en una red corporativa, cifrando equipos con arquitecturas de PC/servidor como estaciones de operación, servidores de tiempo real, históricos, etc., impidiendo la efectiva supervisión de la operación del sistema.

- Cifrando equipos en sistemas de proceso específico, inhabilitando actividades esenciales para la operación (básculas, expedición, control de almacenes, etc.)

- De formas específicamente dirigidas a detener procesos en ejecución en estaciones de operación o servidores que el malware reconoce como específicamente industriales.

- En versiones potencialmente más destructivas, interactuando con los controladores para detener la operación de PLC, actuadores o instrumentación.

- **Analiza el riesgo de un ransomware en tus sistemas de producción**
- **Adapta tus planes de continuidad**
- **Evalúa el posible impacto en caso de materializarse esta amenaza**
- **Concienciа a tus empleados**


92966/9764320 4548GFJ
92866/9135228 2167BBV
93566/9135234 8801DTG
911669135216 7801HJX
Yealink
Detallitos de clientes
agradecidos

MUCHAS GRACIAS

Enrique Fenollosa

Gerente General Sudamérica

enrique.fenollosa@s2grupo.com