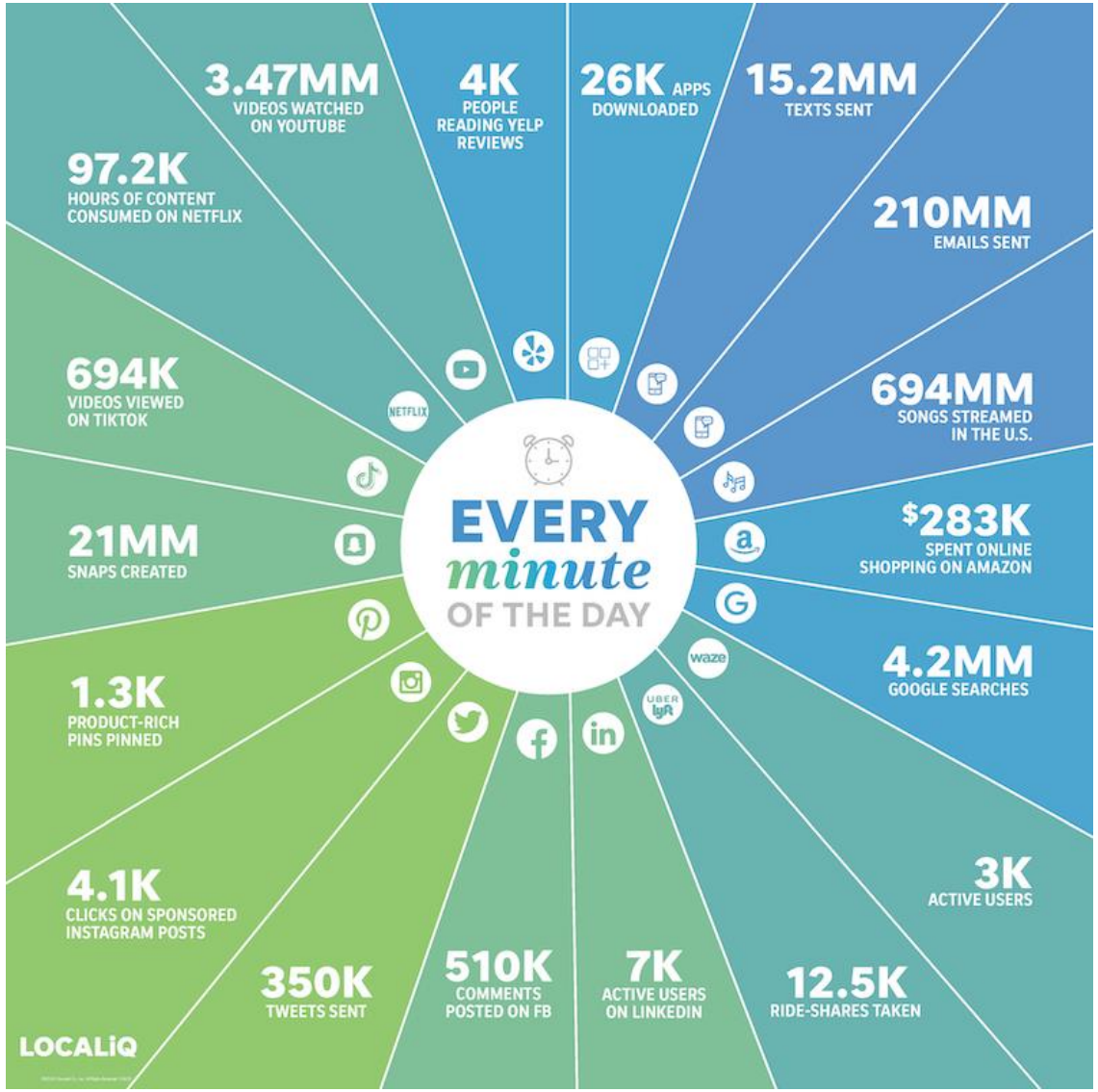
CIBERSEGURIDAD DÍA A DÍA

POR ERICK IRIARTE AHON @COYOTEGRIS

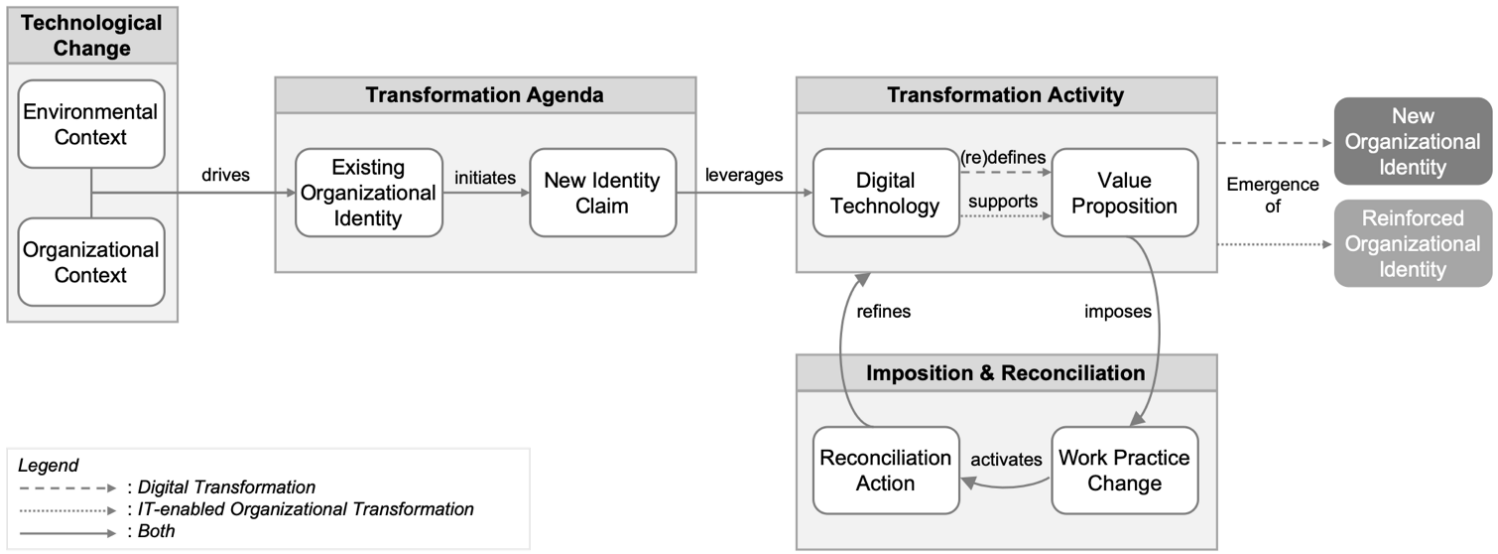
PASOS PREVIOS

UN MINUTO...



ADOPCIÓN DE TECNOLOGÍAS

UNPACKING THE DIFFERENCE BETWEEN DIGITAL TRANSFORMATION AND IT-ENABLED ORGANIZATIONAL TRANSFORMATION (WESSEL ET AL)



Covid-19 and Remote Work Cause Major Shifts in Cybersecurity

Malicious Actors Take Advantage of Global Pandemic and Other Significant Events

IoT attacks

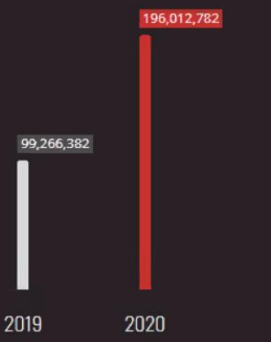
Cybercriminals also took notice of the increased reliance of organizations and employees on the internet of things (IoT). This should be a major concern since home networks and devices could be abused by attackers to gain access to the corporate networks they're connected to. Routers are particularly vulnerable, especially since security at an employee's home is not as tight as at an enterprise workplace.

15.5%
of routers were possibly victimized.

5.1%
of routers were possibly compromised.

In 2020, we saw an uptick in the total number of inbound attack events, which was more than triple the 2019 tally, and in the total number of outbound attack events, which nearly doubled from 2019.

A comparison of the detection counts of possible inbound attacks in 2019 and 2020



A comparison of the detection counts of possible outbound attacks in 2019 and 2020

Fuente: TrendMicro

CIBERSEGURIDAD: ALGUNAS SITUACIONES

Se calcula que hay un ataque informático en el mundo cada 39 segundos: ONU

Las Naciones Unidas aseguran que se ha aumentado la criminalidad cibernética en la pandemia.

Publicado **hace 6 días** on **22/05/2020**
Por **Forbes Staff**

EFE.- El cibercrimen se ha disparado durante la pandemia del coronavirus, con un aumento del 600 % en el número de correos electrónicos maliciosos y con repetidos ataques contra organizaciones sanitarias y de investigación médica, advirtió este viernes Naciones Unidas.

Patrick W 🙈🙉🙊
@TAGACAT

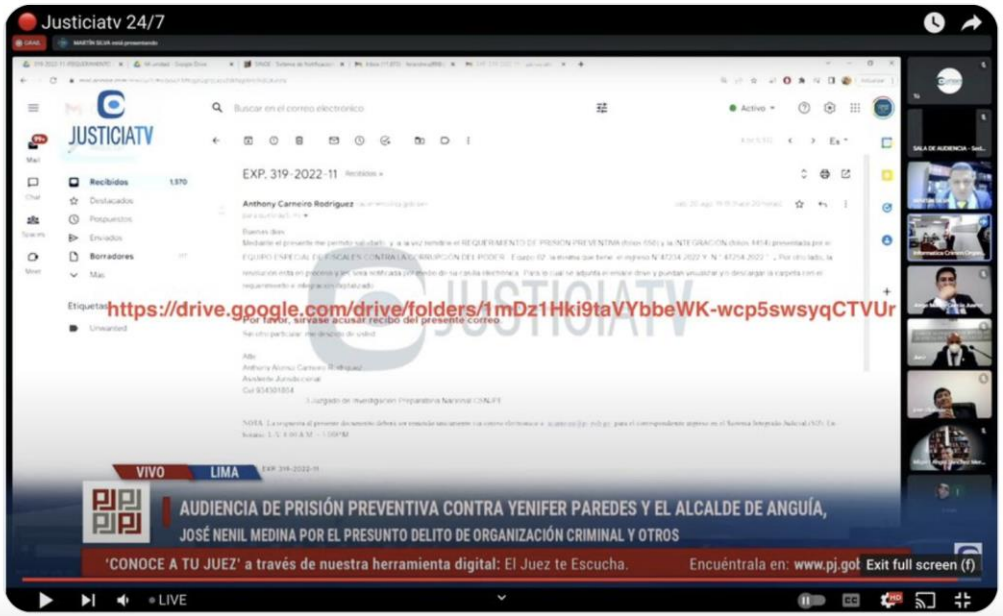
Acá pueden revisar todos los archivos de:

"Audiencia de Prisión Preventiva contra #YeniferParedes y el alcalde de Anguía, (...) por el presunto delito de Organización Criminal y otros"

Esto según pantallazo compartido por la defensa:

drive.google.com/drive/folders/...

Translate Tweet



forbes.pe/negocios/2022-09-16/uber-investiga-incidente-de-ciberseguridad-tras-reporte-de-hackeo/

Forbes PERÚ

NEGOCIOS

Uber investiga "incidente de ciberseguridad" tras reporte de hackeo

Un hacker se apoderó de la cuenta de un empleado en la aplicación de Slack y la utilizó para enviar un mensaje a trabajadores de Uber.

Publicado hace 3 semanason Septiembre 16, 2022
Por **Forbes Staff**

Foto: Getty Images.

Uber Technologies Inc reportó que investiga un incidente de ciberseguridad, después de que medios informaron que su red sufrió un hackeo y la compañía tuvo que cerrar varios sistemas internos de comunicación e ingeniería.

Un pirata informático comprometió la cuenta de un empleado en la aplicación de mensajería laboral Slack y la utilizó para enviar un mensaje a los trabajadores de Uber anunciando que la empresa había sufrido una violación a la seguridad de sus datos, según un reporte del *New York Times* del jueves que citó a un portavoz de Uber.

Leer también: Uber encenderá los motores de sus primeros taxis eléctricos en Perú

Al parecer, el pirata informático pudo acceder posteriormente a otros sistemas internos, publicando una foto explícita en una página de información interna para los

csirt.gob.cl/noticias/conti-costa-rica-y-peru/

CSIRT

Quiénes somos | Acerca de Ciberseguridad | Preguntas Frecuentes | Decretos de Ciberseguridad | Eventos | English

Alerta de Seguridad Cibernética | Ataques del ransomware Conti en Costa Rica y Perú

Pueden descargar esta información en formato PDF aquí: 10CND22-00067-01 Comunicado Ransomware Conti 11.05.2022.

ALERTA DE SEGURIDAD CIBERNÉTICA

El CSIRT de Gobierno hace un llamado a todas las instituciones del Estado a estar alertas y tomar las medidas de precaución necesarias ante el grupo de ransomware ruso Conti. Esto, debido a los ataques informáticos que afectaron a las instituciones públicas de Perú y Costa Rica en las últimas semanas.

Antecedentes de los ciberataques

En abril de 2022, el gobierno de Costa Rica confirmó haber sido víctima del ransomware Conti, el cual afectó, en su mayoría, al Ministerio de Hacienda y a entidades como la Junta Administrativa del Servicio Eléctrico de la provincia de Cartago (Jasec), el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones; el Ministerio de Trabajo y Seguridad Social; al Instituto Meteorológico Nacional (IMN), a Radiográfica Costarricense (Racsa) y la Caja Costarricense del Seguro Social (CCSS). Debido a esta situación, el gobierno se vio obligado a deshabilitar varios servicios informáticos y a declarar Estado de Emergencia Nacional desde el 8 de mayo.

Poco tiempo después, a principios de mayo, el mismo grupo ruso informó a través de un blog en la dark web que la Dirección General de Inteligencia de Perú había sido atacada por Conti. En esta ocasión, los delincuentes aseguran haber accedido a la red del organismo y haber realizado copias de información sensible, accediendo así infraestructura crítica, incluida las redes de agua y electricidad.

Sobre el ransomware Conti

Conti se considera una variante de modelo de ransomware como servicio (RaaS), es muy destructiva y funciona bajo la modalidad de doble extorsión, poniendo en riesgo la información y la reputación de la entidad afectada. Según la investigación de Cybereason, "Conti no sólo encripta los archivos en el host infectado, sino que también se propaga a través de SMB y encripta archivos en diferentes hosts, lo que podría comprometer el toda la red. La rutina de encriptación rápida tarda solo unos segundos o minutos, debido al uso de subprocesos múltiples, lo que también hace que sea muy difícil detenerla una vez que se inicia la rutina de encriptación".

Al igual que la mayoría de los ataques de ransomware, Conti logra acceder a las redes de las instituciones por distintos medios:

- Campañas de phishing, donde adjuntan documentos maliciosos en formato Word o envían enlaces. En ambos casos buscan que la persona descargue un malware como TrickBot o aplicaciones legítimas.

- Buscan explotar vulnerabilidades.

- Ataques sobre equipos con el servicio de RDP expuesto a Internet.

Recomendaciones

Ante el impacto que han tenido los países afectados por el ransomware Conti, el CSIRT de Gobierno solicita a las instituciones del Estado tomar las medidas de mitigación necesarias. Para ello, entregamos las siguientes recomendaciones:

Tweets de @CSIRTGOB

CSIRT GO... @CSIR... · 8h

Como CSIRT de Gobierno (#CSIRTGob) les advertimos de un sitio fraudulento que suplanta el login de #Microsoft. Más información aquí: csirt.gob.cl/alertas/8ffr22...

Para más alertas y vulnerabilidades ingresa a csirt.gob.cl #ciberseguridad @SubseInterior

Las consecuencias del hackeo de Guacamaya en Chile: un general del Ejército renunció y la titular de Defensa compareció ante legisladores

Latinus | septiembre 30, 2022

Foto: AP

AP.- Un general del **Ejército de Chile renunció** el 22 de septiembre a la jefatura del **Estado Mayor Conjunto de las Fuerzas Armadas**, tras un hackeo masivo de correos, informó en su momento la titular del Ministerio de Defensa Nacional, **Maya Fernández**.

La renuncia del general **Guillermo Paiva**, se concretará hoy, 30 de septiembre, y sucedió luego de que se conociera que el **grupo de hackers llamado "Guacamaya"** pirateó miles de correos electrónicos.

elpais.com/mexico/2022-10-01/lopez-obrador-antepone-sus-problemas-de-salud-a-las-fallas-en-politica-de-ciberseguridad.html

EL PAÍS México

HACKEO MASIVO SEDENA >

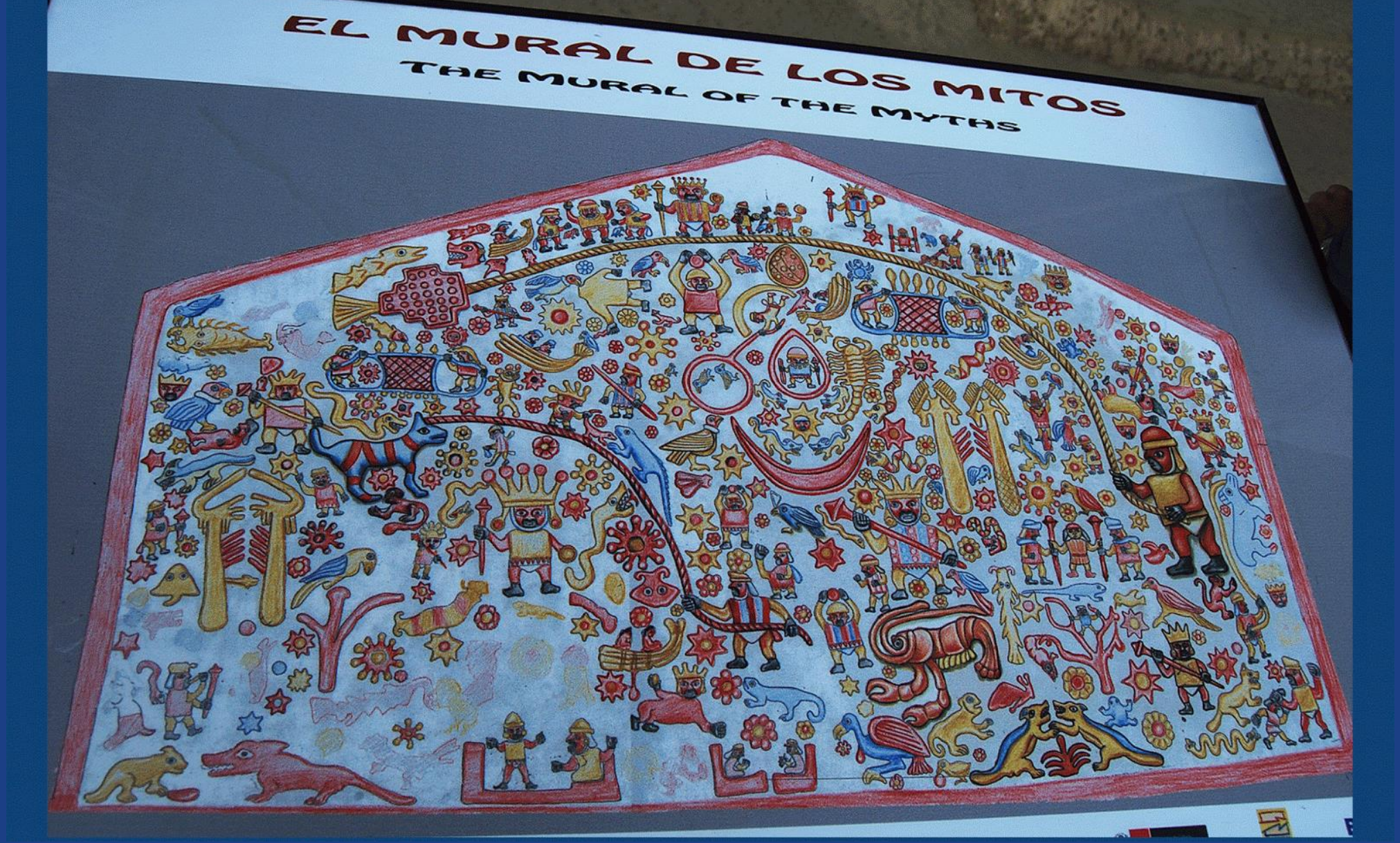
El ciberataque al Ejército revela las fallas en la política de ciberseguridad de México

Los especialistas exponen un enorme agujero en la protección de los asuntos de Estado más delicados

El presidente Andrés Manuel López Obrador, durante la rueda de prensa de la mañana del 30 de septiembre en Palacio Nacional en la que reconoció este viernes que el Ejército padeció un hackeo.
SÁSHENKA GUTIÉRREZ (EFE)

"Es cierto, hubo un ataque cibernético, así le llaman, al robo de información y mediante esos mecanismos modernos extraen archivos, es gente muy especializada, no cualquiera, no sé si en México haya especialistas en este ramo de la cibernética [...] Tengo entendido de que este mismo grupo ya ha hecho lo mismo en otros países, creo que en Colombia, en Chile, por eso pienso que es algo que se maneja desde el extranjero, que no es de México"

CIBERSEGURIDAD: REPENSANDO NUESTRO ENTORNO



www.clarin.com/sociedad/robot-mato-hombre-Alemania_0_1386461528.html

El caso generó además una insólita situación en las redes sociales. Una de las primeras en informar sobre el accidente fatal fue Sarah O'Connor, periodista del diario Financial Times, de Inglaterra. "Un robot mató a un trabajador en una planta de VW en Alemania", escribió en Twitter. Y, de inmediato, empezaron a retuitearla miles de usuarios. ¿La razón? El nombre de la reportera es muy similar a Sarah Connor, el de la protagonista de la película Terminator. "Sos nuestra única esperanza ahora. La resistencia te apoya completamente como nuestra líder", le escribió el usuario @fakejourno. "Terminator está cerca, corre Sarah, corre!!!", le advirtió @coyotegris.

Sarah O'Connor 1 jul
@sarahoconnor_
A robot has killed a worker in a VW plant in Germany
ft.com/fastft/353721

FakeJourno Seguir
@FakeJourno
@sarahoconnor_ You are our only hope now. Resistance fully supports you as our leader.
12:15 - 1 jul 2015
293 407

Sarah O'Connor 1 jul
@sarahoconnor_
A robot has killed a worker in a VW plant in Germany
ft.com/fastft/353721

Erick Iriarte Ahon Seguir
@coyotegris
.@sarahoconnor_ skynet is close, run Sarah, ruN!!!
17:57 - 1 jul 2015

lo más visto

Sociedad

01 **Se cayó el "puente" del glaciar Perito Moreno**
02 **Infografía interactiva: el antes y después del rompimiento del glaciar**
03 **Un joven de 20 años, el único sobreviviente del accidente de la avioneta**
04 **La carta de despedida de una joven que es ejemplo de fortaleza y alegría de vivir**
05 **El glaciar Perito Moreno completó su ruptura cuando nadie lo veía**

Los videos más vistos

SEGURIDAD DE LA INFORMACIÓN ¿PARA QUÉ?

Premisa: La información es un activo de las organizaciones.

Premisa: La información y su gestión dan una ventaja competitiva frente a otros actores del mercado.

Premisa: Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

SEGURIDAD DE LA INFORMACIÓN ¿PARA QUÉ?

Premisa: La inversión en **Prevención** es menor que el gasto el **Resolución de Problemas**.

Premisa: El diseño de los sistemas de información no fue diseñado frente a retos de la Sociedad de la Información.

Premisa: El control de la información es frágil, siendo que una vez difundida es difícil su gestión.

Premisa: La gestión en elementos técnicos, diseños de seguridad se ha realizado desde la perspectiva técnica, dejandose de lado el factor humano y la perspectiva jurídica.

EVALUACIÓN DE RIESGOS DE SEGURIDAD

Premisa: El análisis de riesgos tiene que tener una relación directa entre las consecuencias del fallo de seguridad con la inversión económica en la creación de los controles requeridos. [Amenazas Reales vs. Amenazas Ficticias / Pérdidas Reales vs. Pérdidas Potenciales vs. Posibles Pérdidas].

Premisa: La evaluación se debe realizar constantemente, no es una acción no planificada. De manera especial se debe considerar para una evaluación "especial": cambios organizacionales, cambio en la técnica, cambio del "norte" del negocio.

EVALUACIÓN DE RIESGOS DE SEGURIDAD

Premisa: Deberían realizarse estas revisiones con distintos niveles de detalle dependiendo de los resultados de las evaluaciones previas y de los umbrales de riesgo que la gerencia está dispuesta a aceptar. Se suelen realizar las evaluaciones de riesgo primero a alto nivel, como un medio de priorizar recursos en áreas de alto riesgo, y después en un nivel más detallado para enfocar riesgos específicos.

¿QUÉ CONTROLES? ¿CUÁNTO INVIERTO?

La inversión en controles de seguridad tiene que estar pensada directamente en el tamaño y diseño de la organización, no todos los controles le son aplicables a todas las organizaciones.

La inversión económica en controles tiene que estar guiada por la necesidad real de la organización, así como en los reales peligros, y no tiene que sobredimensionarse en base a la "última tecnología".

LAS FILTRACIONES

¿QUIÉN?

ACTOR EXTERNO

EXTRACCIÓN
EXPOSICIÓN
FILTRACIÓN A PROVEEDOR
INTERMEDIO

ACTOR INTERNO

FILTRACIÓN
EXTRACCIÓN
¿COMPENSACIÓN?

DATOS PERSONALES

GENERALES
SENSIBLES (EN ESPECIAL FINANCIEROS)

DATOS CORPORATIVOS

INFORMACIÓN ESTRATÉGICA
INFORMACIÓN ACUMULADA

EN LA COMPAÑÍA

SHAREHOLDERS

EN EL ECOSISTEMA

STAKEHOLDERS

EN LOS USUARIOS

EN LA COMPETENCIA

CORTO VS LARGO PLAZO

DECLARACIÓN DE BRECHA

¿OBLIGATORIO?
¿COSTO/ BENEFICIO?

DIRECTIVA DE SEGURIDAD DE PROTECCIÓN DE DATOS

OFICIAL DE SEGURIDAD

ACTIVOS CRÍTICOS NACIONALES
¿SANCIÓN?

VALORIZACIÓN CORPORATIVA

USUARIOS

Y EL DÍA DESPUÉS DE MAÑANA...

- Reputación Corporativa
- Políticas de Gestión
- Continuidad del Negocio
- Responsabilidad Legal
- Impacto sobre usuarios
- Impacto sobre el ecosistema
- Volver a punto 0
- Cultura de ciberseguridad y de protección de datos

¿Y LOS DIRECTORIOS?

CONTACTO@EBIZLATIN.COM + 51 1 518 3360