DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Asignatura

Fundamentos de ciberseguridad

1.1. Introducción

Profesor

Juan Ignacio Iturbe A.

Juan Ignacio Iturbe Araya

Académico, DIINF - USACH

Mail: juan.iturbe@usach.cl

Twitter: @jiturbe

Linkedin: http://cl.linkedin.com/in/juaniturbe

Objetivos de aprendizaje

- OA1: Definir el concepto de ciberseguridad
- OA2: Motivar la importancia de la ciberseguridad en una organización.
- OA3: Explicar los desafíos de la ciberseguridad
- OA4: Reconocer los objetivos de la ciberseguridad.

¿Qué es la ciberseguridad?

- “La ciberseguridad es la colección de herramientas, políticas, conceptos de seguridad, medidas de seguridad, pautas, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, aseguramiento y tecnologías que se utilizan para proteger el entorno y la organización del ciberespacio y los activos de los usuarios”.

Stallings, William. Effective Cybersecurity . Pearson Education.

Estudio de Microsoft revela que dos de cada cinco empresas ha sufrido un ciberataque en Chile

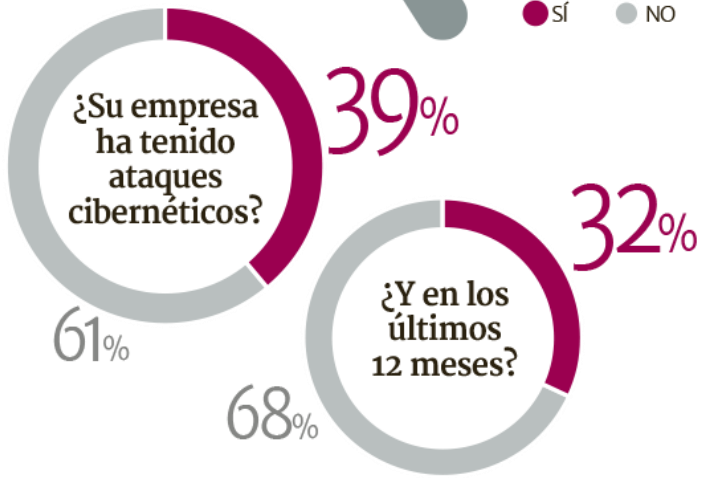
Microsoft dio a conocer los resultados del estudio "Ciberseguridad en las empresas chilenas", que entre las conclusiones arrojó que los principales ataques que sufren las firmas de cualquier tamaño en Chile, son de pérdida temporal de acceso a archivos, sitios web eliminados y programas o sistemas corruptos.

El estudio de carácter cuantitativo, consideró encuestas telefónicas a encargados de ciberseguridad de 202 empresas micro (35), pequeñas (93), medianas (61) y grandes (13) en Chile.

52% dice que la seguridad informática es una prioridad en su empresa

58% cree que Chile es un target/objetivo para los piratas informáticos

Ataques cibernéticos



68% dice que un ataque cibernético afecta la imagen y reputación corporativa

49% de las empresas declara ser muy vulnerable o algo vulnerable

44% de las empresas ha invertido en ciberseguridad en los últimos 12 meses

61% instaló un software de seguridad como medida frente a ciberataques

¿Qué tipo de ataques cibernéticos ha tenido su empresa? %

FUENTE: "CIBERSEGURIDAD EN LAS EMPRESAS CHILENAS", MICROSOFT, 2019.

Tres principales temores en Ciberseguridad

- Fuga de información (71%)
- Continuidad operacional (67%)
- Protección contra phishing, ransomware y amenazas avanzadas (66%)

Ciberseguridad en las empresas chilenas (Microsoft,

https://www.trendtic.cl/2019/05/ciberataques-en-chile-4-de-cada-10-empresas-reconocen-haber-sido-victima/

Ciberseguridad en Chile

US$ 129M

7% crecimiento año a año en 2017

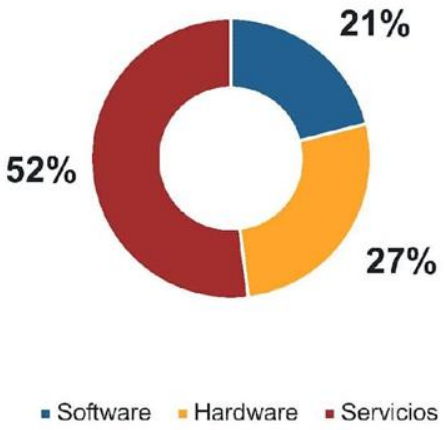
83% de los entrevistados invierte el **20%** o menos del total de TI en ciberseguridad

39% de los entrevistados aumentó su presupuesto de ciberseguridad en 2017

22% de los entrevistados está considerando el **outsourcing** de servicios administrados de ciberseguridad

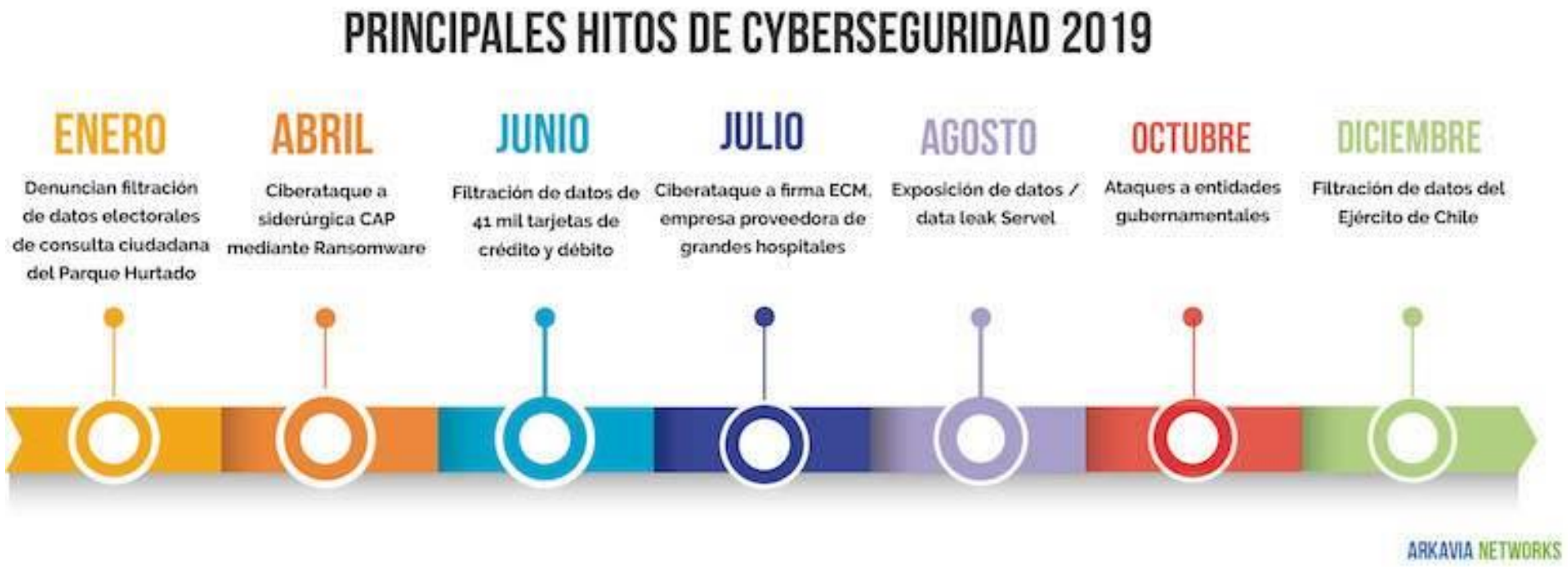
30% de los entrevistados no comunica sus políticas de ciberseguridad

Inversión en soluciones de ciberseguridad



Fuente: IDC Latin America Cybersecurity Report 2017 / IDC Latin America Security Solutions 2016

Eventos 2019



https://www.eleconomistaamerica.cl/telecomunicacion-tecnologia-cl/noticias/10272597/12/19/Ciberseguridad-hitos-2019-y-desafios-2020.html

Hitos 2020

14 Enero 2020	Microsoft pone fin al soporte para las versiones de sistemas operativos Windows 7 y Windows Server 2008.
17 Febrero 2020	Se evidencia campaña "Fox-Kitten" cuyo objetivo era la explotación de vulnerabilidades de VPN.
Marzo 2020	Llega el teletrabajo a Chile, forzado por la pandemia.
30 Marzo 2020	Fuerte explotación de vulnerabilidades de plataforma de videollamadas: Zoom.
Abril 2020	Incremento de ataques de ransomware dirigidos a hospitales y entidades educacionales.
31 Mayo 2020	Anonymuous inicia campañas de hacktivismo y ataques a entidades gubernamentales y de seguridad de Estados Unidos, motivadas por la muerte de George Floyd.
Junio 2020	Se evidencian campañas de explotación de vulnerabilidades de exim. • Actualmente, a nivel mundial existen alrededor de 271.500 activos vulnerables asociados al CVE-2019-10149 • Se debe hacer hincapié en que es una vulnerabilidad parcheada hace más de 1 año
16 Julio 2020	Twitter sufre el mayor hackeo de su historia.
Agosto 2020	Incremento de ataques tipo DDoS dirigidos a entidades financieras, de turismo y comercio electrónico
12 Septiembre 2020	Un ciberataque provoca la muerte de un paciente en una clínica en Alemania.
28 Septiembre 2020	Filtración código Windows XP.
9 Diciembre 2020	FireEye comunica haber sido víctima de un acceso no autorizado a un conjunto de sus herramientas.
13 Diciembre 2020	SolarWinds reconoce infección de malware en cadena de suministro de su plataforma.

https://www.entel.cl/corporaciones/notas/pdf/Informe-Ciberseguridad-2020.pdf

Hitos 2021

El phishing es el principal vector de acceso para amenazas más sofisticadas como el **ransomware.**

Los cibercriminales continúan aprovechando **las brechas en el trabajo remoto para acceder a las redes corporativas.**

Más de **7 mil millones**

de intentos de ciberataques en América Latina y el Caribe

Chile

410 millones

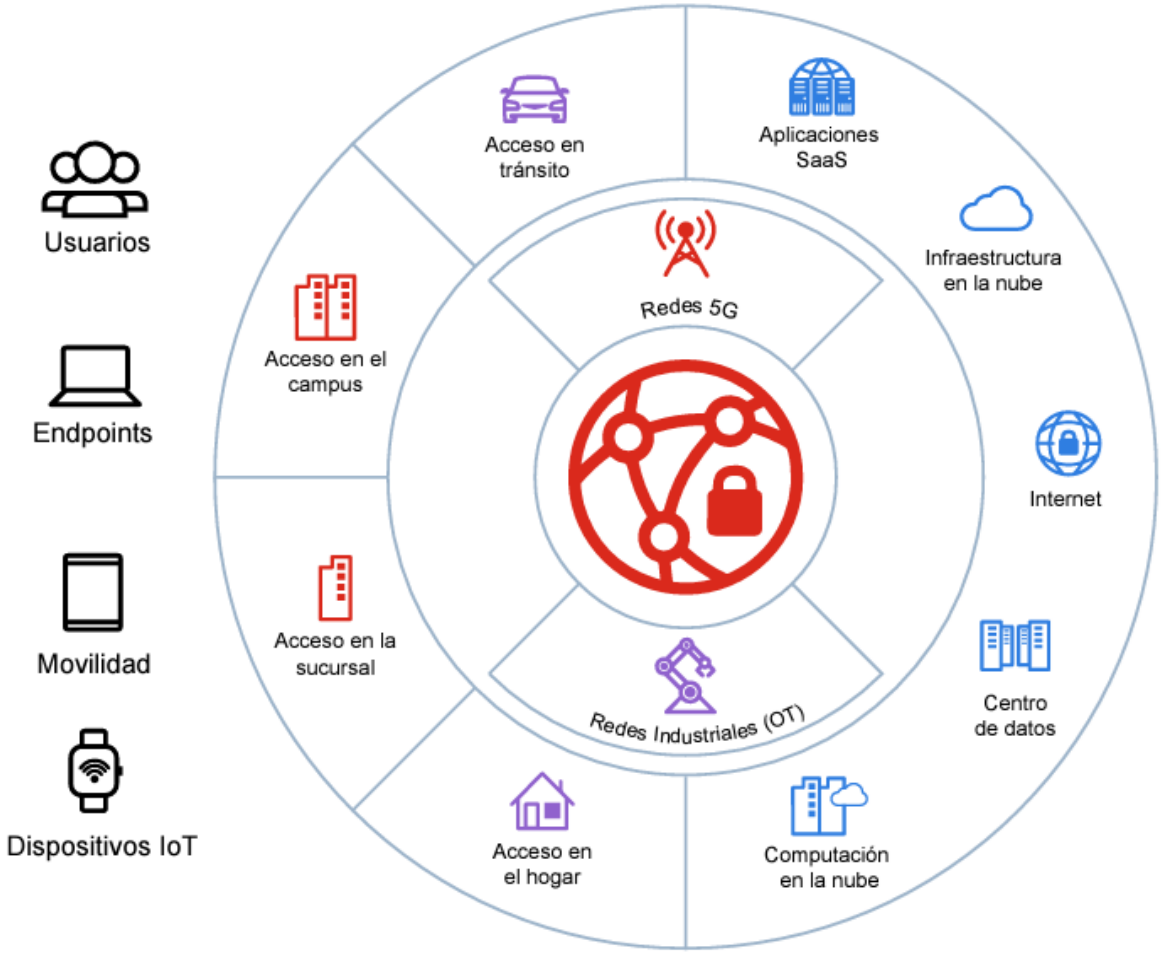
de intentos de ciberataques

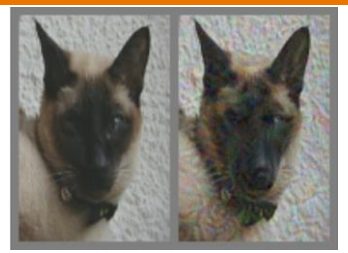
Malware basado en la web:

incremento en la **utilización de redes sociales** para difundir publicidad y sitios web engañosos. Los **usuarios comprometidos** comparten mensajes con contenido malicioso a sus **contactos desde sus perfiles de redes sociales,** sin tener conocimiento de ello.

https://www.csirt.gob.cl/noticias/chile-recibe-410-millones-de-intentos-de-ciberataques-en-el-primer-trimestre-de-2021/

Superficie digital cada vez más amplia





Lo que viene…


5G

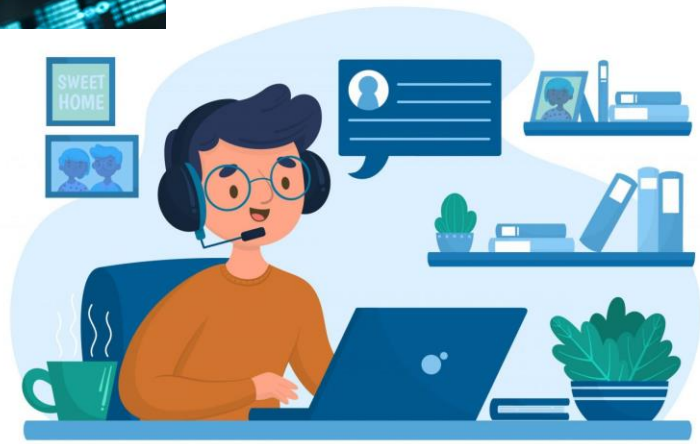

Digite su usuario
y contraseña


CUÍDATE DE LA
SUPLANTACIÓN
de identidad


XBOX
LANZA
SE
LANZA
XBOX 360


Transformación Digital
IoT
Machine Learning
Cloud Computing
Big Data
@rosanarosas17


Datos Personales
Descargar


SWEET
HOME

Desafíos de la ciberseguridad

- Escala y complejidad del ciberespacio.
- Naturalezas de las amenazas.
- Necesidades de uso versus implementación de seguridad.
- Dificultades estimando costos y beneficios.

Actividad en clase

Desarrollar un DFD sobre el intercambio de información al realizar una compra en una página web. Ej. En mercado libre

(10 minutos) Identifique individualmente:

- Los componentes del ciberespacio que participan en esta compra.
- Posibles amenazas sobre el proceso.
- Requerimientos funcionales y requerimientos de seguridad del proceso
- El costo de la materialización de las amenazas sobre el proceso.
- El costo de la implementación de requerimientos de seguridad que impidan o reduzcan el riesgo de materialización de las amenazas.

(10 minutos) En grupos discuta sus resultados y llegue a un consenso.

Actividad formativa 1: Resumen y amenazas 2021 y Tendencias 2022

- Informe de ciberseguridad 2022, Entel.
- Responda en el foro asociado:
  - Identifique los conceptos que desconozca y busque el significado de 5 de estos.
  - ¿Cuáles son los problemas relacionados con ciberseguridad más relevantes que tienen las empresas del informe?
  - ¿Qué es un DDoS?
  - ¿Qué es el CVE?
  - ¿Cómo han afectado los ciberataques al desarrollo de nueva legislación en Chile?
  - ¿Cuáles son las amenazas más relevantes que aparecen en el informe? ¿Por qué?
  - ¿Cómo estás me pueden afectar? ¿De qué forma?
  - ¿Qué es lo que más le llamó la atención del informe?

Recursos bibliográficos

- Stallings, William. Effective Cybersecurity . Pearson Education.
- https://www.ciberseguridad.gob.cl/
- Biblioteca digital USACH – AENOR
- ISO/IEC 27K
- https://www.incibe.es/