Magister en Informática Médica

Seguridad de la información {en Salud}

Philippe Delteil

24 de Octubre

> whoami

Ing. Civil Cs. Computación

3 años en SSMSO

Jefe Depto. Seguridad e innovación

Info-sec / Seguridad / Salud

Cohorte Mauco Molina (PUC)

Instructor de Workshops en Defcon

Bug Bounty hunter

> Temas clase

- Definiciones y conceptos sobre seguridad
- Legislación
- Caso de estudio
- Hackers y hacking
- BioHacking Village CTF
- Ransomware
- Caso de hospital Italiano
- Charla 'Relatos macabros de un hacker en salud pública'

Conceptos

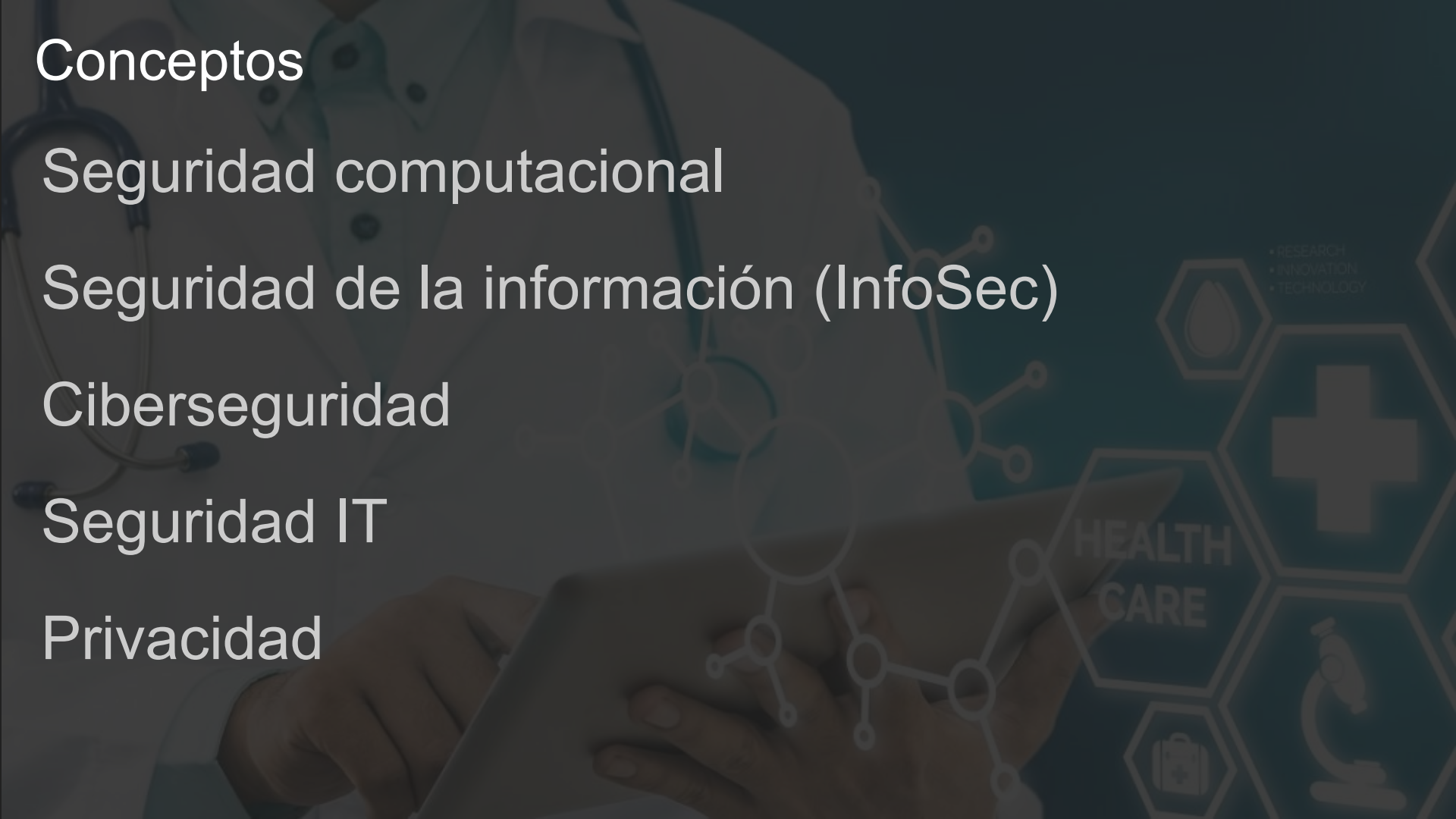
Seguridad computacional

Seguridad de la información (InfoSec)

Ciberseguridad

Seguridad IT

Privacidad



Seguridad computacional

Medidas y controles que aseguran:

- Confidentiality (C) – acceso autorizado
- Integrity (I) – Modificación y destrucción
- Availability (A) – acceso y uso confiable permanente

Aplicable a:

Servidores, computadores, notebooks, tablets y celulares.

Dispositivos de red, routers, switches, etc.

Sistemas operativos, software y firmware.

Seguridad de la información (InfoSec)

International Standards Organization (ISO) (2014) lo define como:

"Preservación de la confidencialidad, integridad y disponibilidad (CIA) de la información"

Además, de otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucrados ".

Ciberseguridad

Muchos simplemente definen la ciberseguridad como un subconjunto de InfoSec, ya que se refiere a la "Información en el Ciberespacio".

Pero..

¿Qué es el ciberespacio?

¿Qué son los activos en el ciberespacio?

¿Qué pasa con los activos no basados en información en el ciberespacio?

¿En qué se diferencia de seguridad computacional y la InfoSec?

Ciberseguridad - Ciberespacio

“Conjunto de sistemas de información interconectados que dependen del tiempo y de los seres humanos que interactúan con estos sistemas”.

- Ottis y Lorents (2010)

Es un ecosistema dinámico, evolutivo, virtual, conectado y multinivel de infraestructura física, software, regulaciones, procesos e interacciones influenciado por una creciente población de contribuyentes.

Ciberseguridad - Activos en el ciberespacio

Información en sí misma

Infraestructura de la información

Internet, software integrado, firmware, protocolos de comunicación, etc.

Activos sin información

Infraestructura crítica: red de energía, suministro de agua, salud pública, transporte, telecomunicaciones, finanzas servicios, etc.

Internet de las cosas

Vehículos / Dispositivos médicos / etc

Seguridad IT vs Infosec

Firewalls

Antivirus

Escaners de vulnerabilidades

Penetration Testing

Detección de intrusos (IDS)

Análisis forense

Control de accesos Seguridad redes

Encriptación

Orientado a la Tecnología/Técnico

Propiedad intelectual

Cumplimiento regulatorio

Integridad financiera/del negocio

Espionaje industrial

Privacidad de la info.

Gobernacion/Crisis Management

Business Continuity

Risk analysis

Orientado al Negocio

Otros conceptos

Activo: Objeto valioso para la institución

Vulnerabilidad: Cualquier debilidad de un activo.

Amenazas, atacantes, adversarios: Potencial de un actor con motivos de ejecutar cierta vulnerabilidad.

Actor: Persona, organización, gobierno.

Motivación: Publicidad, financiera, política, religiosa.

Riesgo: Vulnerabilidad expuesta a un activo (potencialmente) afectado por una amenaza.

Controles/Mitigación: Acciones para reducir el riesgo.

Riesgo

¿Pero, qué es el riesgo?

Riesgos

Cont. negocio
Pérdida $
Privacidad
Reputación
Confianza

Sanciones legales

Crecimiento

Pérdida de vidas

=

Amenazas

E. enojados

E. deshonestos

Criminales

Gobiernos

Terroristas

Competencia
Hackers

Naturaleza

+

Vulnerabilidades

Errores software
Procesos errados
Controles inefectivos
Fallas de hardware
Cambios del negocio
Sistemas legados
Plan de continuidad errado
Errores humanos!

+

Activos

Servidores

Computadores

Celulares

Redes inf.

Software

Datos/información

Infraestructura física

Evolución de la seguridad: Defensa

1990

Anti-Virus

Firewalls

Security guidelines

2000

Security information and event management (SIEM)

Sistemas de detección de intrusión (IDS)

Arquitectura de capas

2010

Endpoint Detection and Response (EDR)

Identity and Access Management (IdAM)

Gestión de vulns
Era protección

Gestión de Amenazas
Era Detección

Gestión de riesgos
Era Respuesta

Evolución de la seguridad: Ofensivo

1990

Virus
Worms
Redes abiertas
Configs Inseguras

2000

Script Kiddies
Ataques desde cliente
Escaners automatizados
Demasiados logs/alertas

2010

APTs
DDoS
Botnets
Phishing
Ransomware

Aumenta frecuencia - Sofisticación - Herramientas
Disminuye Barrera técnica

Desafíos actuales y futuros

Más dispositivos en internet

Más usuarios

Mayor capacidad de ataque

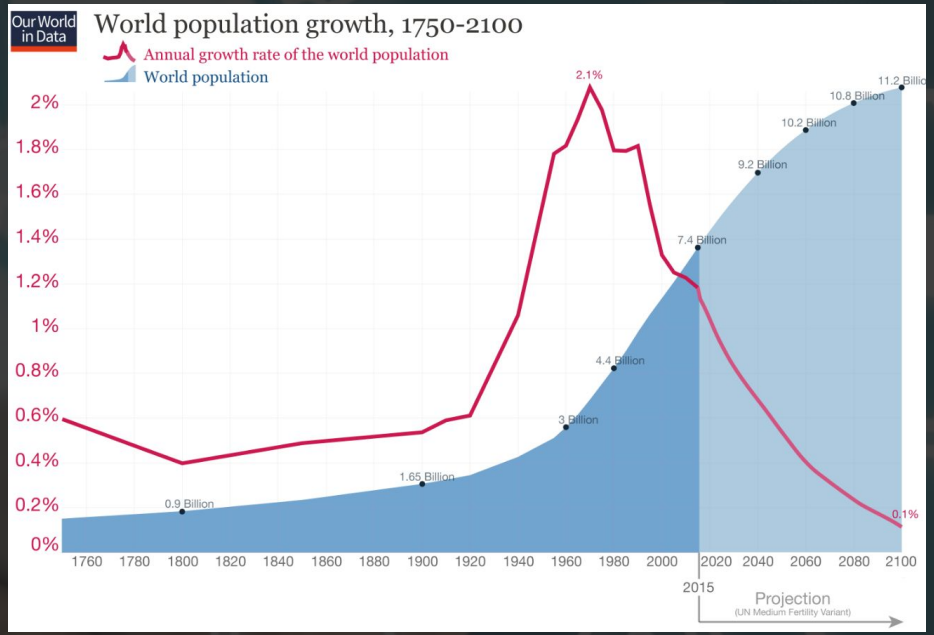
Presiones internas del negocio

Rigidez

Presupuesto

Talento!

Humanos!!



Ley 19.628 Protección de datos de carácter personal

Diferencia entre datos personales y datos sensibles.

“Relación o cercanía que tengan con el ámbito más íntimo de la persona (dato sensible), o más privado, pero no por ello no importante y no digno de protección (dato personal)”

- Tesis “El dato sensible. Su tratamiento en Chile y en el derecho comparado. (2008)”

Ley 19.628 Protección de datos de carácter personal

- Promulgación ‘99.
- Derecho de privacidad en constituciones de la región.
- Declaración de DDHH también lo incluyen
- Protección de datos personales y derecho a la vida privada e intimidad.
- Habeas Data permite la cancelación, bloqueo y gratuidad en todas aquellas operaciones ligadas al tratamiento de datos.
- Chile entra OCDE el 2010. Se insta a mejorar la ley.

Ley 19.628 - Artículo 2° - Definiciones

Almacenamiento de datos, conservación o custodia de datos en un registro o banco de datos.

Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

Dato estadístico, el dato que, no puede ser asociado a un titular identificado o identificable.

Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables

Ley 19.628 - Artículo 2° - Definiciones

Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Ley 19.628 - Artículo 2° - Definiciones

Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

Artículo 10.- No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Ley 19.628 - Problemas

No contempla requisitos básicos:

Seguridad

Sanciones (prop. a daño ocasionado)

Control a través de un ente especializado y autónomo. Se actúa ya ocurrido el daño y no como un mecanismo de protección preventiva

Intercambio de información ha cambiado

Ley 19.628 - Directrices de la OCDE - 8 principios

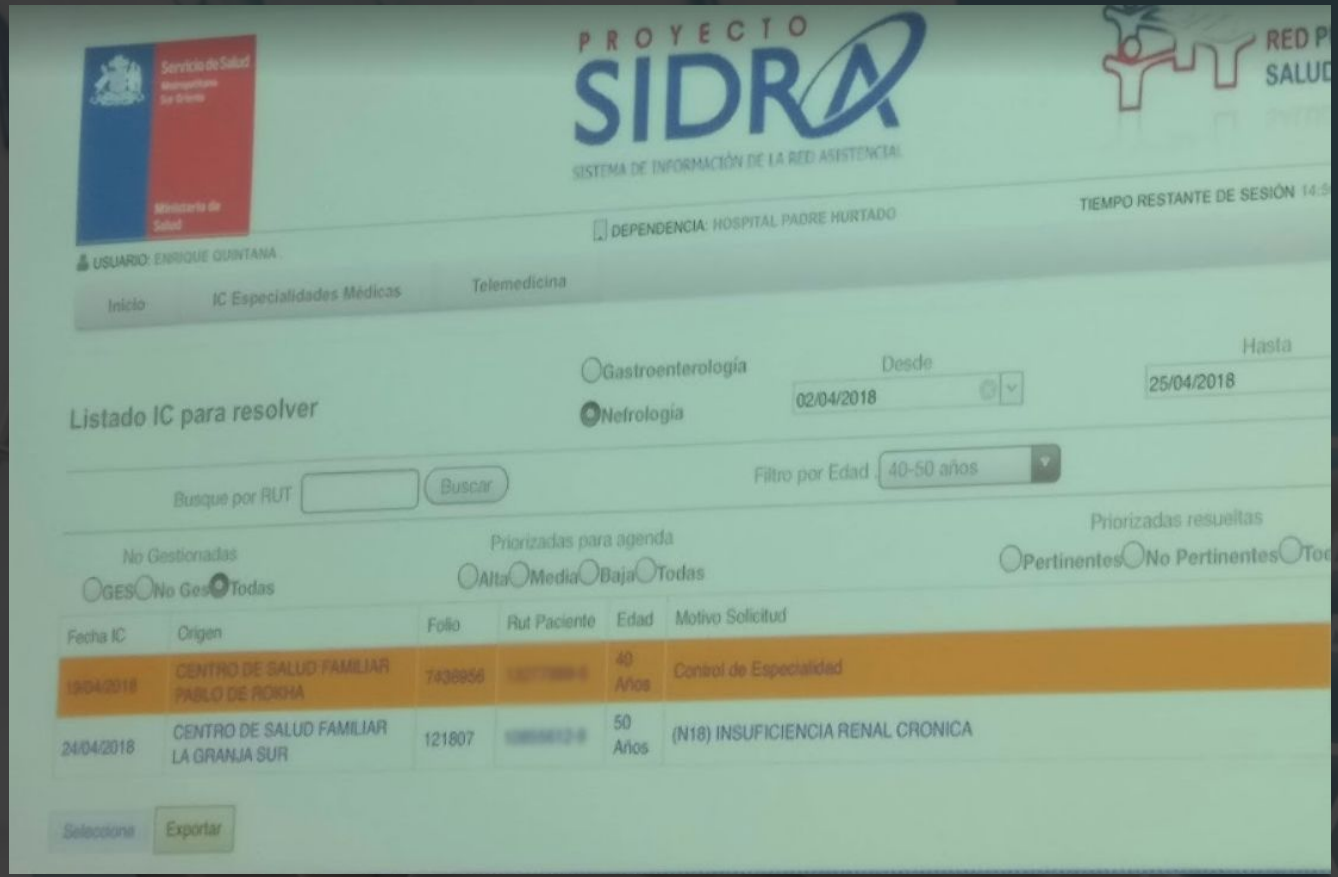
5. **Salvaguardia de la Seguridad**. Control y seguridad, capaces de proteger los datos de la pérdida, acceso no autorizado, destrucción o mal uso, modificación o divulgación.

6. **Principio de Transparencia.** Evolución, prácticas y políticas relativas a datos personales.

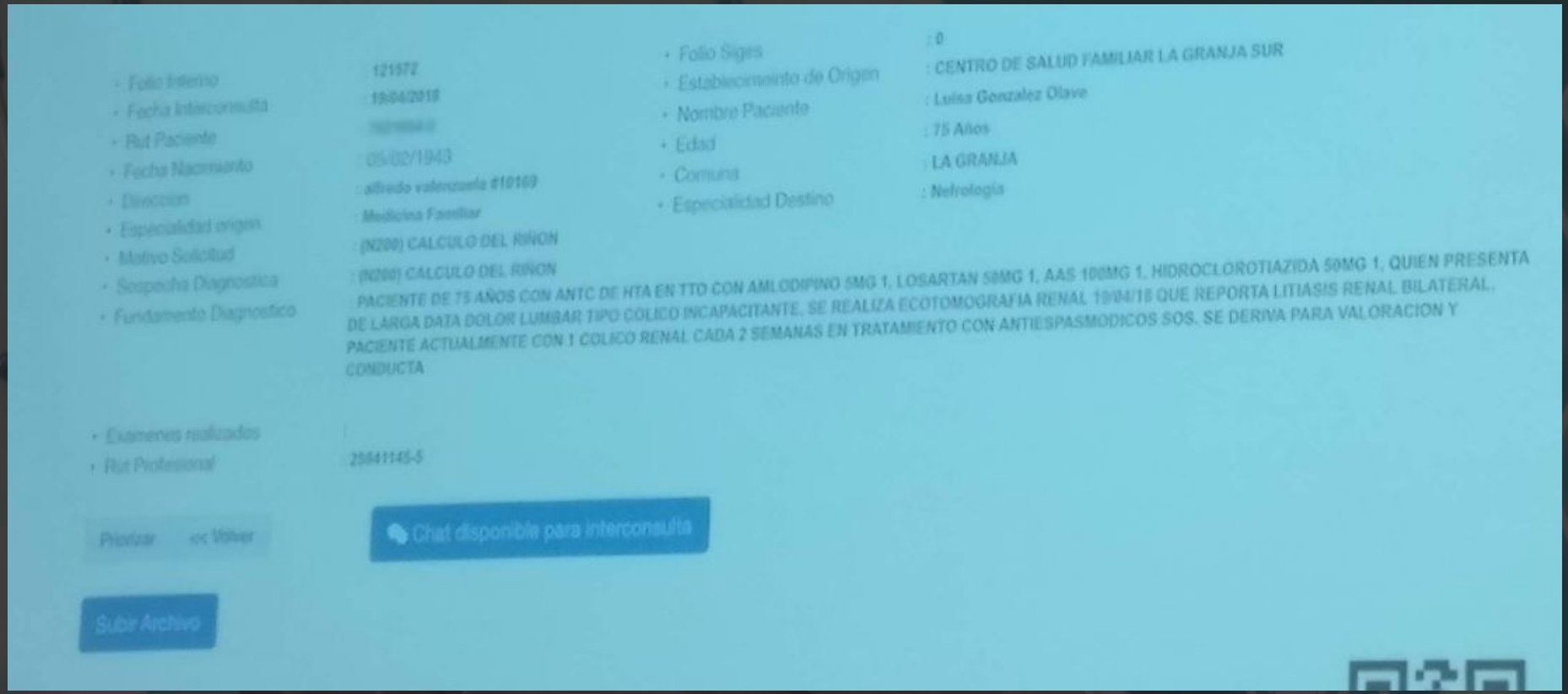
7. **Participación Individual**. Derecho a que el controlador de datos confirmen que poseen datos sobre su persona, y que le comuniquen estos datos en un tiempo, forma y precios razonables.

8. **Ppo. de responsabilidad.** Responsabilidad de cumplir con las medidas que hagan efectivos los principios mencionados con

Solo la semana pasada (2018)



Solo la semana pasada



Caso de estudio: Presentación

- Afiliada a Isapre Banmédica
- Funcionario publico
- Unidad de Víctimas y Testigos Ministerio Público
- 2009. Diagnóstico de depresión mayor severa (9% población)
- Acogida al GES (ex AUGE)
- Compra médicamento Cruz Verde
- Dependiente indicó que no cubrían otros medicamentos

Caso de estudio: Acciones

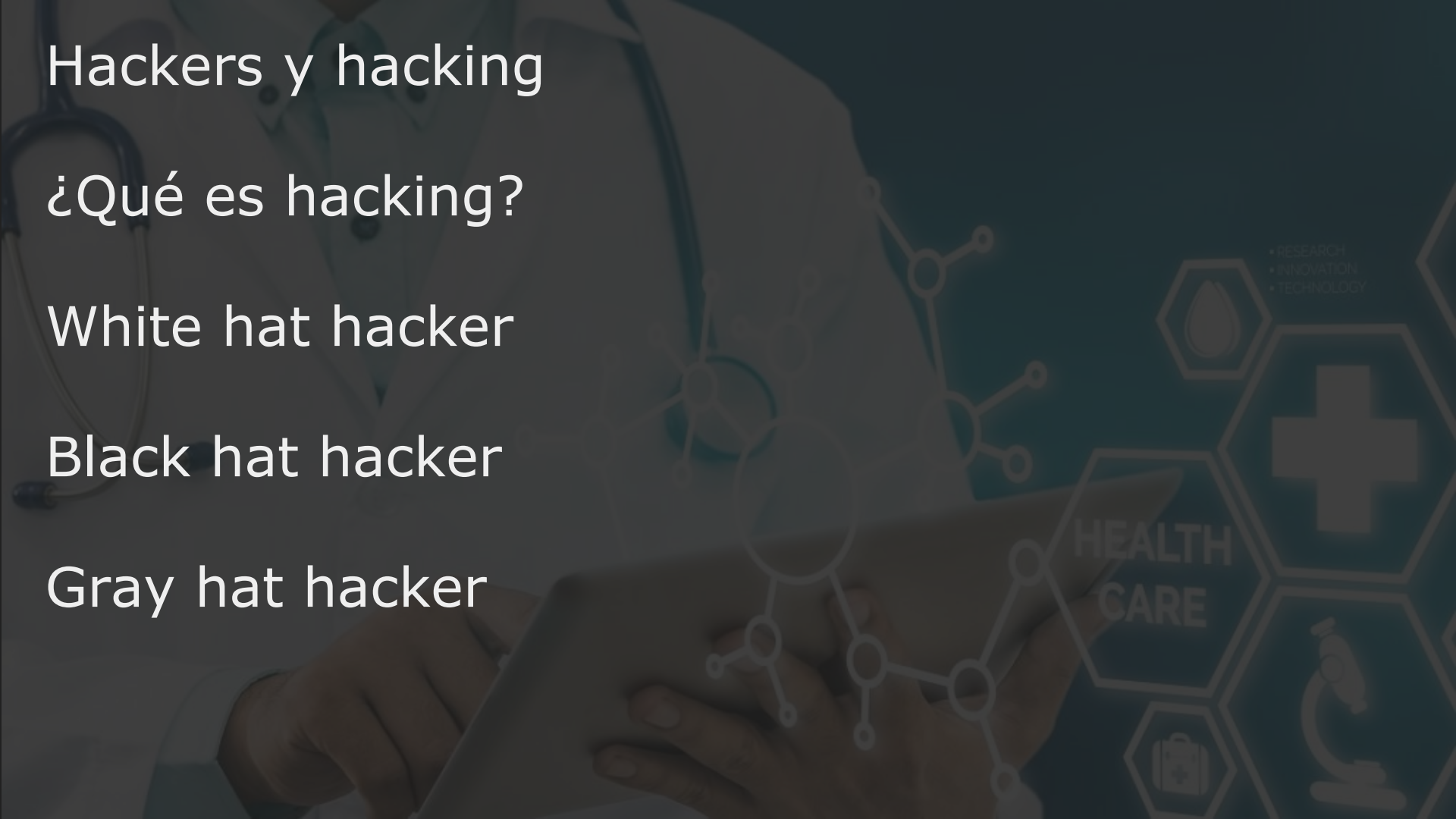
- Reclamo Adm. en Super. de Salud
- Eliminación inmediata diagnóstico en Farmacia
- Recurso de Protección, infracción art. 19 N°4 de Constitución.
- Corte de apelaciones Declara extemporáneo. Suprema confirma sentencia.
- Art. 2° g) Ley 19.628. Concepto de datos sensibles .
- Art. 10° Ley 19.628.
- Art. 19 No. 4 de la Constitución. (D° al respeto y protección a la vida privada y honra de la persona y su familia).

Caso de estudio: Resultado

“Por no arbitrar mecanismos suficientes para cumplir con la obligación de cautelar el derecho a la privacidad de la información transmitida a la Farmacia, irregularidad que transgrede lo dispuesto en el artículo N°5 de la Ley 19.628 sobre Protección de Datos de Carácter Personal”

Multa final de 30 UF ~760mil

Serie de circulares con instrucciones de uso de los datos sensibles



Hackers y hacking

¿Qué es hacking?

White hat hacker

Black hat hacker

Gray hat hacker

Bio hacking Village

Enlace

Phishing

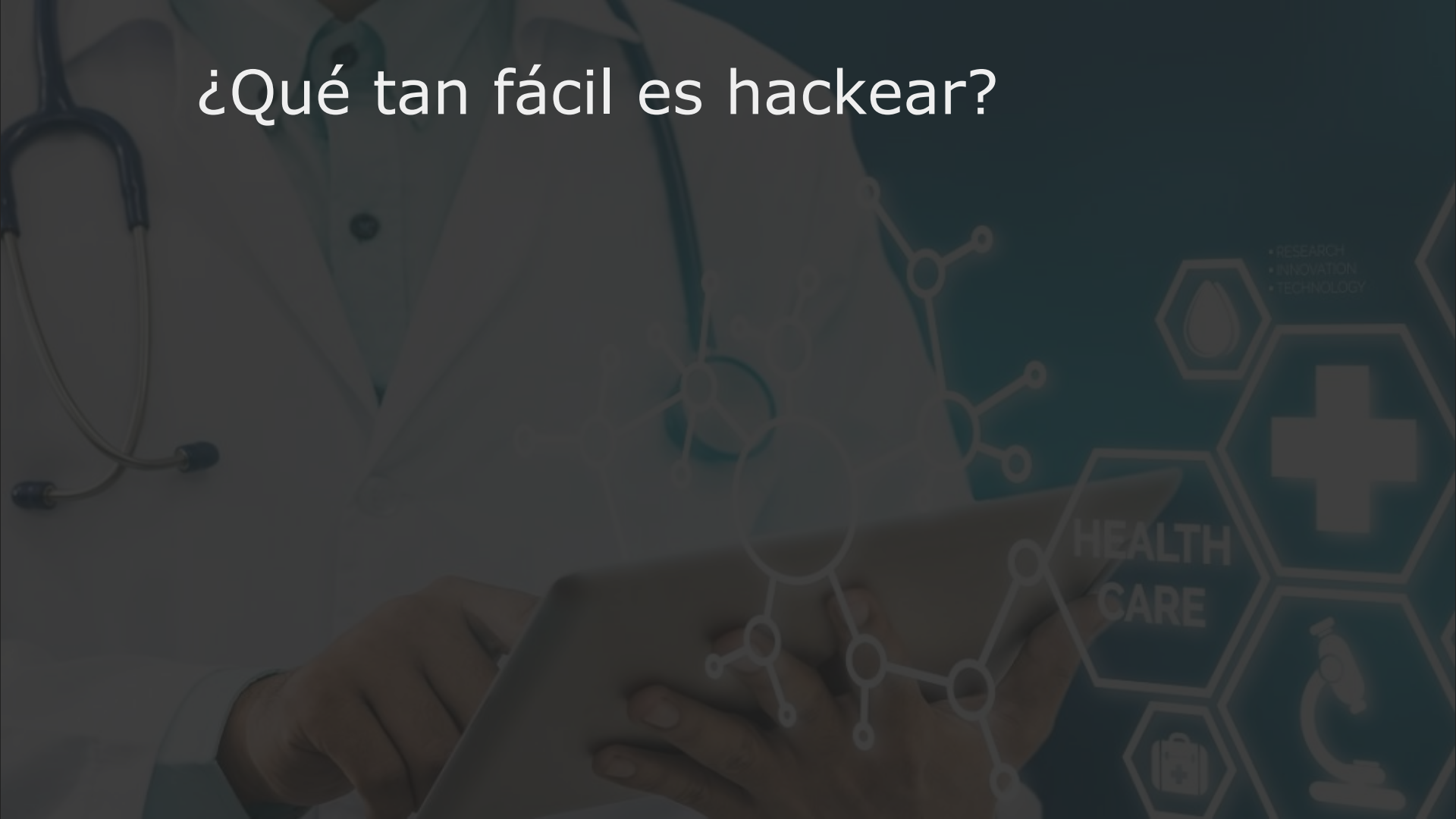
¿Qué es phishing?

Ransomware

¿Qué es ransomware?

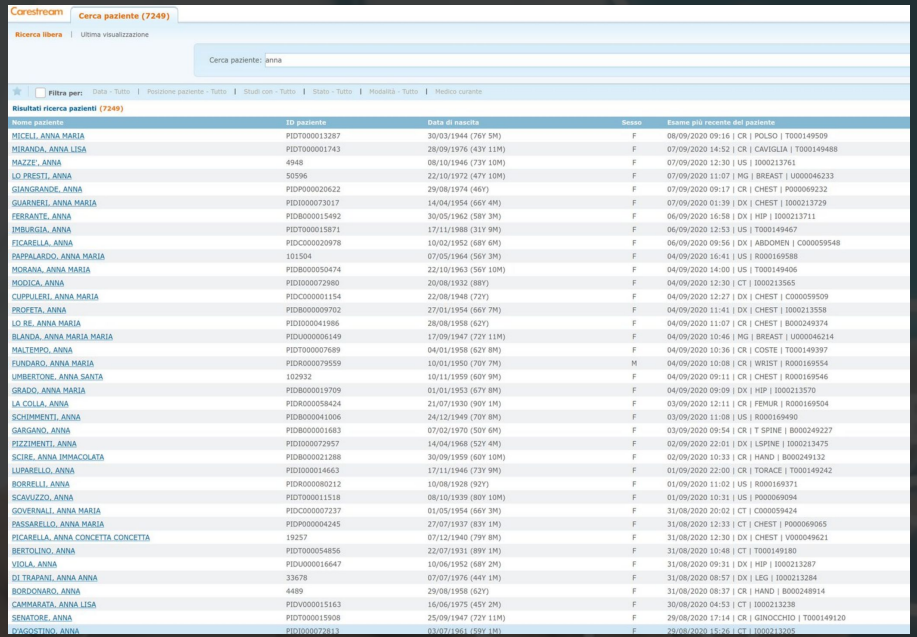
[Wannacry]

¿Qué tan fácil es hackear?

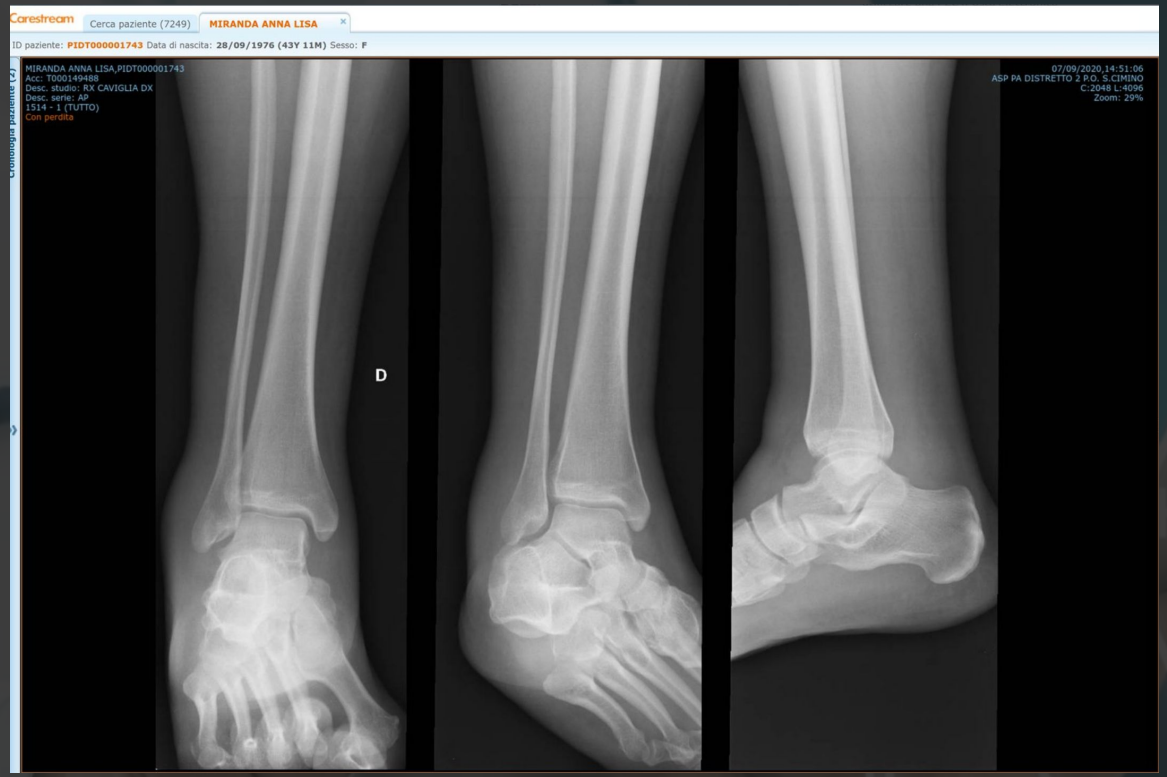


Caso hospital Italiano

Shodan



Caso hospital Italiano



Caso hospital Italiano

Problema de reportar

Uso de PEC

Formulario

Charla

Cursos recomendados MOOC (RITx)

Network Security

Cybersecurity Risk Management

Cybersecurity Fundamentals

Computer Forensics

Enlaces/Referencias

Ransomware

Sobre ley 19.628 “ESTADO SITUACIONAL DE LA PROTECCIÓN DE DATOS PERSONALES EN CHILE, REGULACIÓN JURÍDICA Y ALCANCES”. TESIS MAGÍSTER EN GESTIÓN Y POLÍTICAS PÚBLICAS. TANIA BARRERA Q.