

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

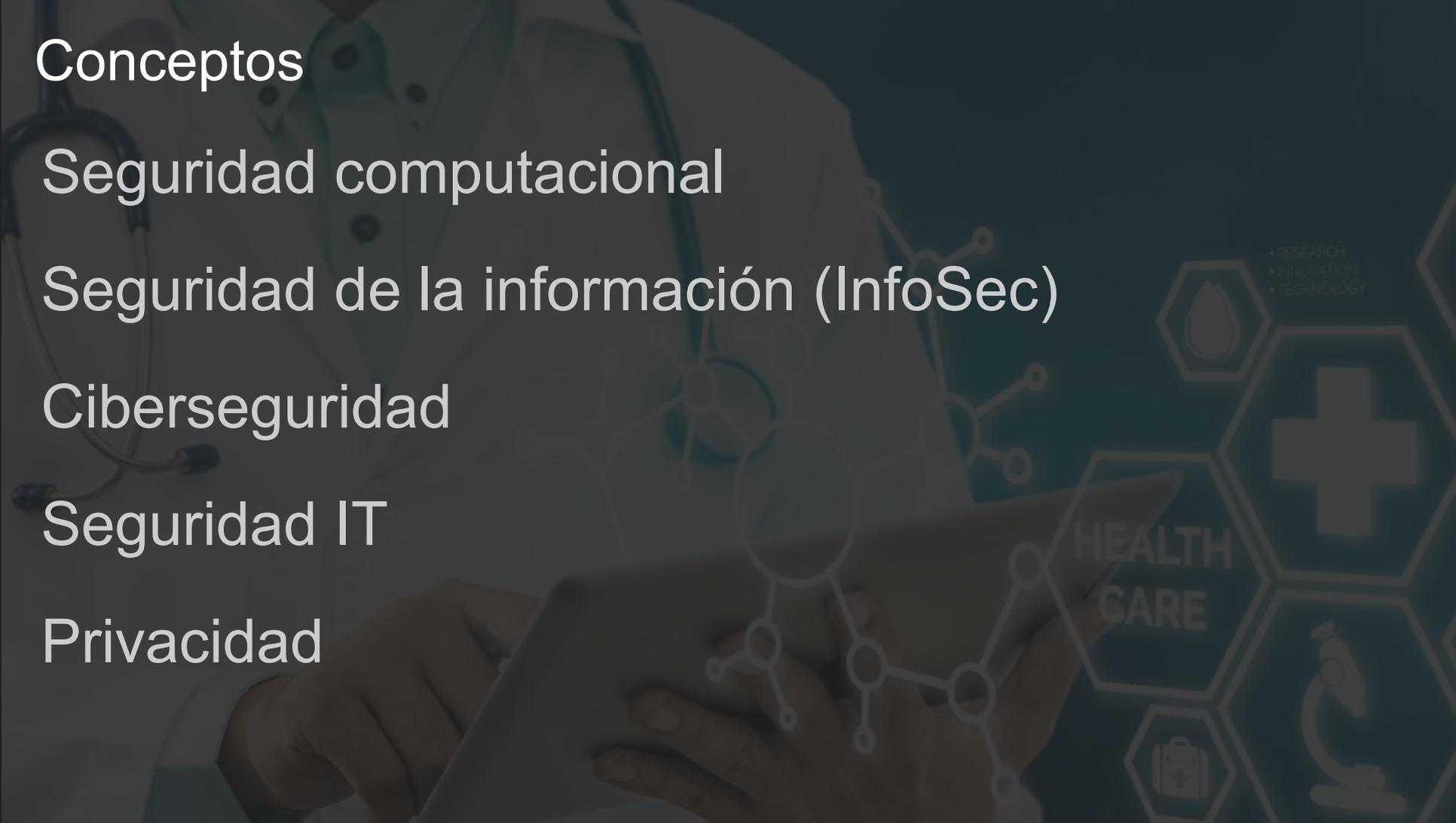


• RESEARCH
• INNOVATION
• TECHNOLOGY

HEALTH
CARE

> 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

• RESEARCH
• INNOVATION
• TECHNOLOGY

Seguridad IT vs Infosec

Firewalls

Antivirus

Escanners 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

Gestión de vulns
Era protección

2000

Security information
and event
management (SIEM)

Sistemas de detección
de intrusión (IDS)

Arquitectura de capas

Gestión de Amenazas
Era Detección

2010

Endpoint Detection and
Response (EDR)

Identity and Access
Management (IdAM)

Gestión de riesgos
Era Respuesta

Evolución de la seguridad: Ofensivo

1990

Virus

Worms

Redes abiertas

Configs Inseguras

2000

Script Kiddies

Ataques desde cliente

Escanners

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

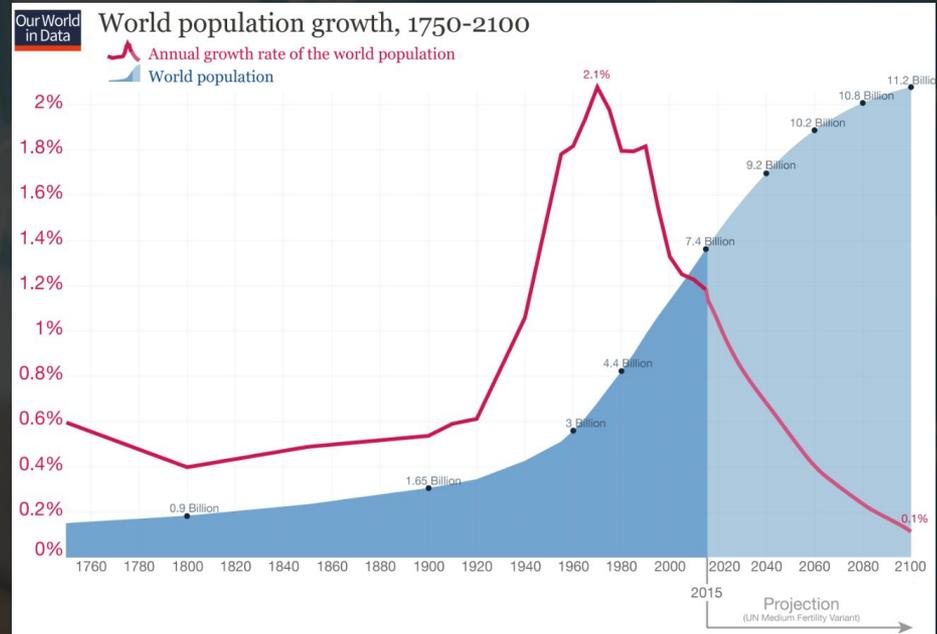
Presiones internas del negocio

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)”

• RESEARCH
• INNOVATION
• TECHNOLOGY

HEALTH
CARE

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)

PROYECTO SIDRA
SISTEMA DE INFORMACIÓN DE LA RED ASISTENCIAL

RED P SALUD

USUARIO: ENRIQUE QUINTANA

DEPENDENCIA: HOSPITAL PADRE HURTADO

TIEMPO RESTANTE DE SESIÓN 14:5

Inicio IC Especialidades Médicas Telemedicina

Listado IC para resolver

Gastroenterología Nefrología

Desde 02/04/2018 Hasta 25/04/2018

Busque por RUT Buscar Filtro por Edad 40-50 años

No Gestionadas GES No Ges Todas

Priorizadas para agenda Alta Media Baja Todas

Priorizadas resueltas Pertinentes No Pertinentes Toc

Fecha IC	Origen	Folio	Rut Paciente	Edad	Motivo Solicitud
19/04/2018	CENTRO DE SALUD FAMILIAR PABLO DE RONHA	7438856	12077888-8	40 Años	Control de Especialidad
24/04/2018	CENTRO DE SALUD FAMILIAR LA GRANJA SUR	121807	12088812-8	50 Años	(N18) INSUFICIENCIA RENAL CRONICA

Selección Exportar

• RESEARCH
• INNOVATION
• TECHNOLOGY

HEALTH
CARE



Solo la semana pasada

• Follo Interno	121572	• Follo Siges	: 0
• Fecha Interconsulta	19/04/2018	• Establecimiento de Origen	: CENTRO DE SALUD FAMILIAR LA GRANJA SUR
• Rut Paciente	XXXXXXXX	• Nombre Paciente	: Luisa Gonzalez Olave
• Fecha Nacimiento	05/02/1943	• Edad	: 75 Años
• Direccion	alfredo valenzuela #10160	• Comuna	: LA GRANJA
• Especialidad origen	Medicina Familiar	• Especialidad Destino	: Nefrologia
• Motivo Solicitud	(N200) CALCULO DEL RINON		
• Sospecha Diagnostica	(N200) CALCULO DEL RINON		
• Fundamento Diagnostico	PACIENTE DE 75 AÑOS CON ANTC DE HTA EN TTD CON AMLODIPINO 5MG 1, LOSARTAN 50MG 1, AAS 100MG 1, HIDROCLOROTIAZIDA 50MG 1, QUIEN PRESENTA DE LARGA DATA DOLOR LUMBAR TIPO COLICO INCAPACITANTE. SE REALIZA ECOTOMOGRAFIA RENAL 19/04/18 QUE REPORTA LITIASIS RENAL BILATERAL. PACIENTE ACTUALMENTE CON 1 COLICO RENAL CADA 2 SEMANAS EN TRATAMIENTO CON ANTIESPASMODICOS SOS. SE DERIVA PARA VALORACION Y CONDUCTA		
• Exámenes realizados			
• Rut Profesional	25841145-5		

Proteger  Ver

 Chat disponible para interconsulta

Subir Archivo



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 medicamento 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).

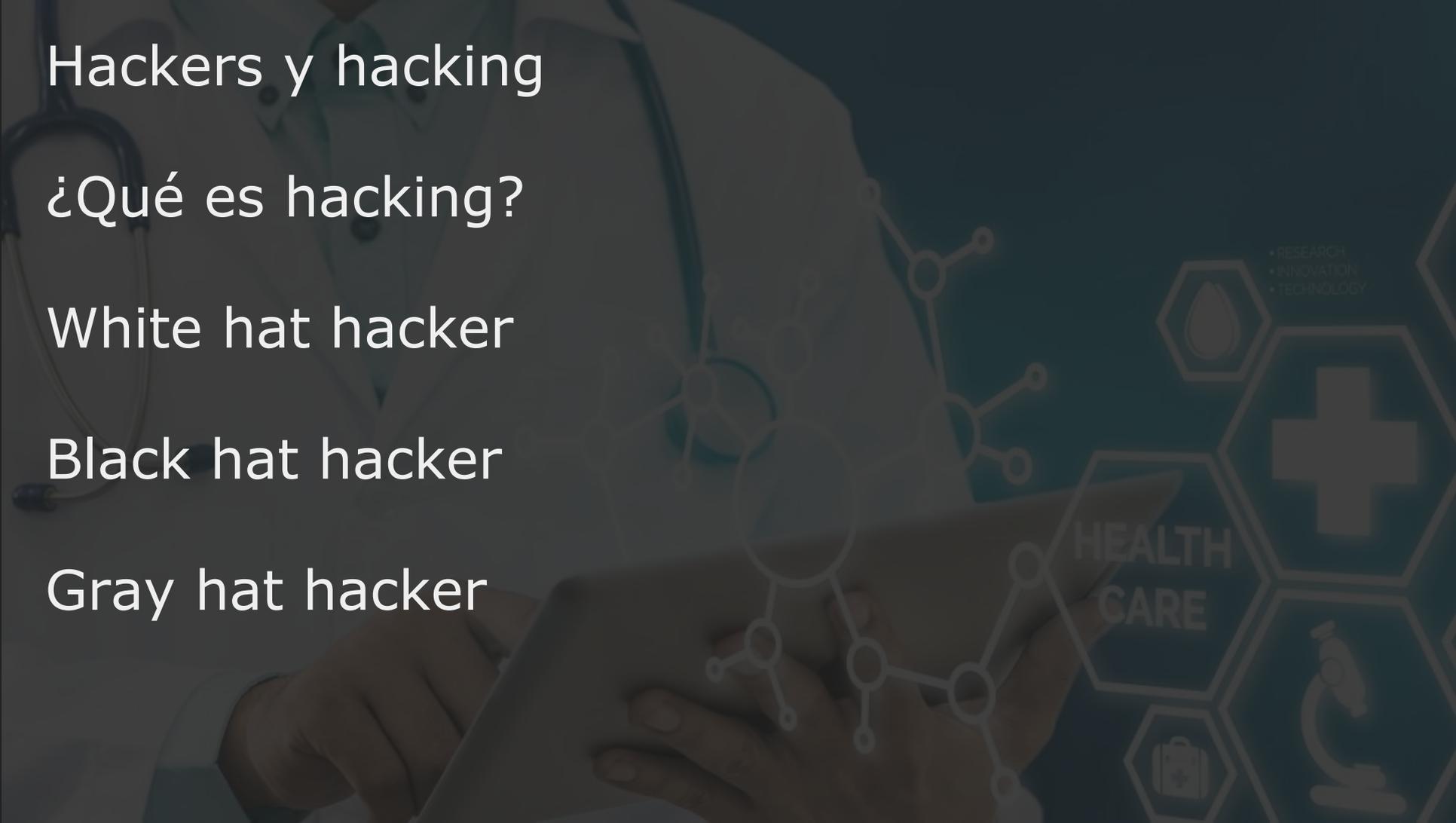


Caso de estudio: Resultado

“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](#)

- RESEARCH
- INNOVATION
- TECHNOLOGY

HEALTH
CARE



Phishing

¿Qué es phishing?



- RESEARCH
- INNOVATION
- TECHNOLOGY

HEALTH
CARE

Ransomware

¿Qué es ransomware?

[Wannacry](#)

• RESEARCH
• INNOVATION
• TECHNOLOGY

HEALTH
CARE

¿Qué tan fácil es hackear?

- RESEARCH
- INNOVATION
- TECHNOLOGY

HEALTH
CARE

Caso hospital Italiano

Shodan

Carestream | Cerca paziente (7249)

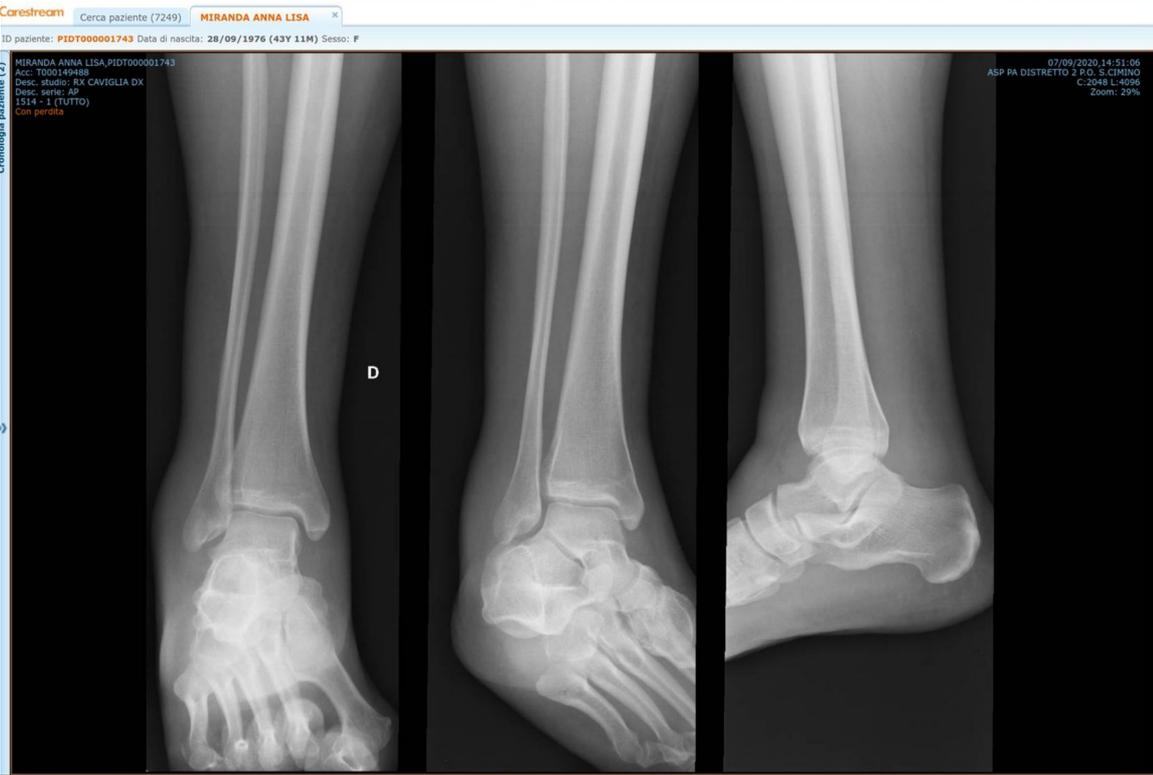
Ricerca libera | Ultima visualizzazione

Cerca paziente: anna

Filtra per: Data - Tutto | Posizione paziente - Tutto | Studi con - Tutto | Stato - Tutto | Modalità - Tutto | Medio corrente

Nome paziente	ID paziente	Data di nascita	Sexo	Esame più recente del paziente
MICELL, ANNA MARIA	PIDT700013287	30/03/1944 (78Y 5M)	F	08/09/2020 09:16 CR POLSO T000149509
MIRANDA, ANNA LISA	PIDT700001743	28/09/1976 (43Y 11M)	F	07/09/2020 14:52 CR CAVIGLIA T000149488
MAZZE, ANNA	4948	08/10/1946 (73Y 10M)	F	07/09/2020 12:30 US I000213761
LO PRESTI, ANNA	50596	22/10/1972 (47Y 10M)	F	07/09/2020 11:07 MG BREAST U000046233
GIANGRANDE, ANNA	PIDP00020622	29/08/1974 (46Y)	F	07/09/2020 09:17 CR CHEST P000049232
GUARNEGLI, ANNA MARIA	PIDC000073017	14/04/1954 (66Y 4M)	F	07/09/2020 01:39 DX CHEST I000213729
FERRANTE, ANNA	PIDB000015402	30/05/1962 (58Y 3M)	F	06/09/2020 16:08 DX HIP I000213711
IMBURGIA, ANNA	PIDT700015871	17/11/1988 (31Y 9M)	F	06/09/2020 12:53 US T000149467
FIGARELLA, ANNA	PIDC000020978	10/02/1952 (68Y 6M)	F	06/09/2020 09:56 DX ABDOMEN C000059548
PAPPALARDO, ANNA MARIA	101504	07/05/1964 (56Y 3M)	F	04/09/2020 16:41 US R000169588
MORANA, ANNA MARIA	PIDB000050474	22/10/1963 (56Y 10M)	F	04/09/2020 14:00 US T000149406
MODICA, ANNA	PIDC000072940	20/08/1932 (88Y)	F	04/09/2020 12:30 CT I000213565
CURFUSI, ANNA MARIA	PIDC000011554	22/08/1948 (72Y)	F	04/09/2020 12:27 DX CHEST C000049599
PROFETA, ANNA	PIDB000009702	27/01/1954 (66Y 7M)	F	04/09/2020 11:41 DX CHEST I000213558
LO RE, ANNA MARIA	PIDC000041866	28/08/1958 (62Y)	F	04/09/2020 11:07 CR CHEST B000249374
BLANDA, ANNA MARIA MARIA	PIDU000006149	17/09/1947 (72Y 11M)	F	04/09/2020 10:46 MG BREAST U000046214
MALTEPEO, ANNA	PIDT700007689	04/01/1958 (62Y 8M)	F	04/09/2020 10:36 CR COSTE T000149397
FUNDARO, ANNA MARIA	PIDB000079559	10/01/1950 (70Y 7M)	M	04/09/2020 10:08 CR WRIST B000169554
IMBRIERONE, ANNA SANTA	159312	10/11/1959 (60Y 9M)	F	04/09/2020 09:11 CR CHEST B000169546
GRADO, ANNA MARIA	PIDB000019709	01/01/1953 (67Y 8M)	F	04/09/2020 09:09 DX HIP I000213570
LA COLLA, ANNA	PIDB0000058424	21/07/1930 (90Y 1M)	F	03/09/2020 12:11 CR PELVIS R000169504
SCHIMMENTI, ANNA	PIDB000041006	24/12/1949 (70Y 8M)	F	03/09/2020 11:08 US R000169490
GARGANO, ANNA	PIDB000001683	07/02/1970 (50Y 6M)	F	03/09/2020 09:54 CR T SPINE B0002149227
PIZZIMENTI, ANNA	PIDC000072957	14/04/1968 (52Y 4M)	F	02/09/2020 22:01 DX SPINE I000213475
SCIRE, ANNA IMMACOLATA	PIDB000021288	30/09/1959 (60Y 10M)	F	02/09/2020 10:33 CR HAND B000249132
LUPARELLO, ANNA	PIDT7000014663	17/11/1946 (73Y 9M)	F	01/09/2020 22:00 CR THORACE T000149242
ROBPELLI, ANNA	PIDB000080212	10/08/1928 (92Y)	F	01/09/2020 11:02 US R000169371
SCAVUZZO, ANNA	PIDT700011518	08/10/1939 (80Y 10M)	F	01/09/2020 10:31 US P000069094
GOVERNALI, ANNA MARIA	PIDC000007737	01/05/1954 (66Y 3M)	F	31/08/2020 20:02 CT C000059424
PASSARELLO, ANNA MARIA	PIDP000004245	27/07/1937 (83Y 1M)	F	31/08/2020 12:33 CT CHEST P000069065
FIGARELLA, ANNA CONCETTA CONCETTA	19237	07/12/1940 (79Y 8M)	F	31/08/2020 12:30 DX CHEST V000049621
BERGOLINO, ANNA	PIDT000054856	22/07/1931 (89Y 1M)	F	31/08/2020 10:48 CT T000149180
VIGOLA, ANNA	PIDC000116647	10/06/1952 (68Y 2M)	F	31/08/2020 09:31 DX HIP I000213287
DI TRAPANI, ANNA ANNA	33478	07/07/1976 (44Y 1M)	F	31/08/2020 08:57 DX LEG I000213284
BORDONARO, ANNA	4489	29/08/1958 (62Y)	F	31/08/2020 08:37 CR HAND B000248914
CAMMARATA, ANNA LISA	PIDV000015163	16/06/1975 (45Y 2M)	F	30/08/2020 04:53 CT I000213238
SENATORE, ANNA	PIDT7000015908	25/09/1947 (72Y 11M)	F	29/08/2020 17:14 CR GINOCCHIO T000149120
FRAGOSTINO, ANNA	BRU000007813	03/07/1961 (59Y 1M)	F	29/08/2020 15:26 CT I000213200

Caso hospital Italiano



- RESEARCH
- INNOVATION
- TECHNOLOGY

HEALTH
CARE

Caso hospital Italiano

Problema de reportar

Uso de PEC

Formulario

• RESEARCH
• INNOVATION
• TECHNOLOGY

Sep 20, 2020, 9:41 AM ✓

Gentile utente, come indicato sul sito e nel messaggio precedente, per contattarci all'indirizzo csirt@alfacert.gov.it occorre utilizzare una PEC (Posta Elettronica Certificata), mentre l'email da cui sta provando a inviare il messaggio non lo è. Questo il motivo dell'errore. Cordiali saluti.

Sep 20, 2020, 10:24 AM

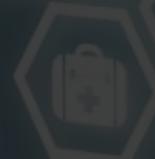
Non sapevo della PEC. Invierò le informazioni qui. Non sono italiano e non ho voglia di pagare per la posta elettronica

Sep 20, 2020, 3:31 PM ✓

Charla

- RESEARCH
- INNOVATION
- TECHNOLOGY

HEALTH
CARE



Cursos recomendados MOOC (RITx)

[Network Security](#)

[Cybersecurity Risk Management](#)

[Cybersecurity Fundamentals](#)

[Computer Forensics](#)

• RESEARCH
• INNOVATION
• TECHNOLOGY

HEALTH
CARE

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.