Primer Workshop Internacional de Informática Médica - Salud Digital

TEMA 1: Seguridad de la Información en la Salud digital.

Ministerio de Telecomunicaciones y de la Sociedad de la Información

República del Ecuador

Gobierno del Encuentro | Juntos lo logramos

DATOS A TENER EN CUENTA

Durante 2020, **la salud fue la séptima industria más atacada globalmente**, recibiendo **el 6,6% de todos los ataques** de las diez principales. En comparación con 2019, había ocupado el décimo lugar y recibido el 3% de los ataques.

- **Filtraciones de datos, debido al nivel de sensibilidad de la información que se maneja**
- **Pacientes:** exposición de nuestra información privada y que cualquiera pueda acceder a **datos como enfermedades y los tratamientos** a los que fuimos sometidos

- La razón principal de los ciberatacantes radica en el dinero, dado que una **historia clínica puede oscilar entre USD 200 y 2000 en un mercado negro**
- Aumento de ataques predominando el **ransomware**, en organizaciones de atención médica
- **Registros médicos** de pacientes tiene un alto valor en el mercado negro

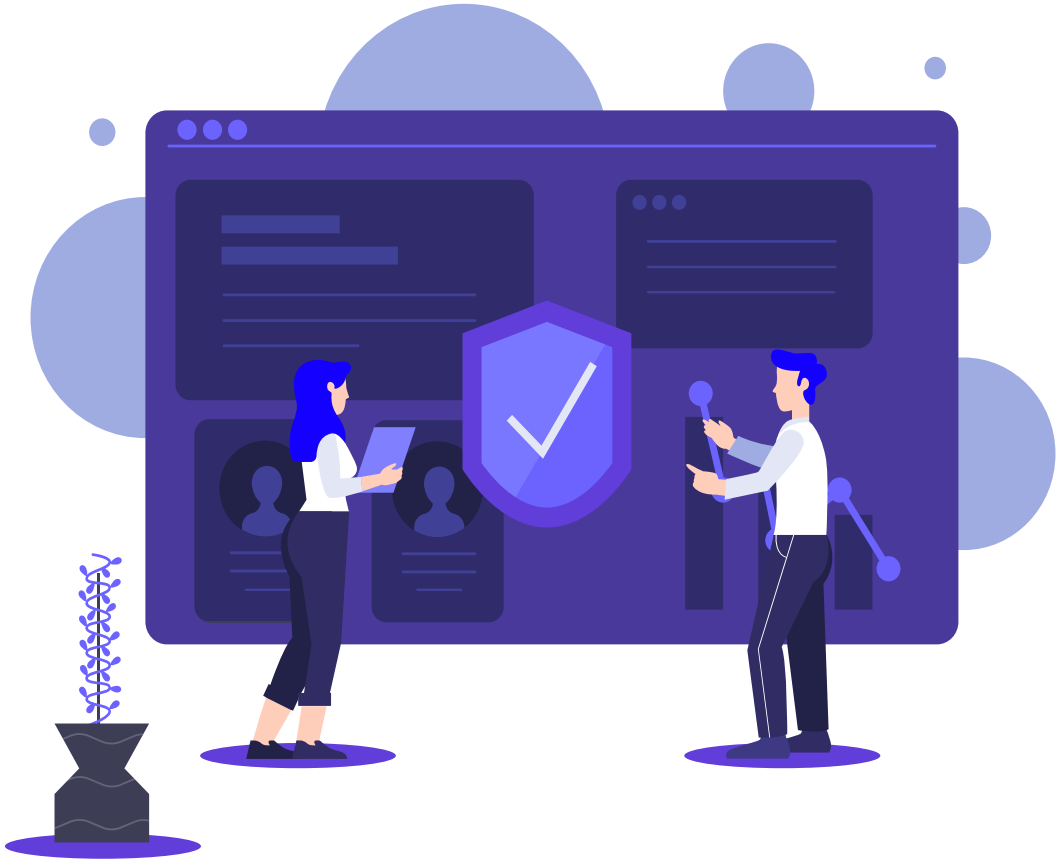
¿QUÉ ES SALUD DIGITAL?

Es la incorporación del uso de las tecnologías de información en los servicios, procesos de atención y asistencia sanitaria que se ofrece a los ciudadanos. (Fuente: OMS).

La Salud Digital permite una mayor conexión entre los profesionales de la salud y pacientes mejorando el bienestar y la calidad de vida.

CONCEPTUALIZACIÓN DE LA SALUD DIGITAL

¿Cómo protegemos y aseguramos la Salud Digital?



Procesos administrativos

Integración de sistemas de información con la dinámica de la administración de la salud

Aseguramiento de la información

Prácticas de seguridad y control de la información personal de los pacientes en la gestión de la administración de la salud.

Procedimientos médicos

Ejercicio de las prácticas médicas propias de la dinámica de la atención del paciente.

Ciberseguridad en equipos médicos

Prácticas de gestión de riesgos y resiliencia digital tanto de la infraestructura como de los dispositivos médicos.

SEGURIDAD DE LA INFORMACIÓN

- Conjunto de políticas, controles y procesos que permiten *proteger* la información de las amenazas, con el fin de asegurar la continuidad de las operaciones.

Procesos

INFORMACIÓN

Tecnología
Equipos

Personas

PANANORAMA DE AMENAZAS INFORMATICAS EN EL SECTOR

2020 EEUU

Organización sanitaria en Illinois, (Champaign Urbana Public Health District) sufrió un ataque de ransomware
Empleados no podían acceder a los archivos del sistema. La información electrónica de salud del paciente la tenían en la nube, por lo que el ataque fue mitigado.

2020 INGLATERRA /ABC INTERNACIONAL

Cibercriminales contra la salud: oleada de hospitales colapsados por secuestros virtuales en plena pandemia.

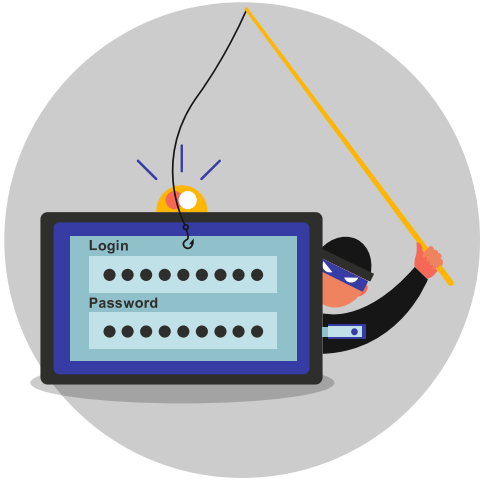
2019 AUSTRALIA

Un ataque de ransomware comprometió los sistemas informáticos de varios hospitales servicios de salud en el país. (se perdió acceso al historial clínico de los pacientes).

PRINCIPALES AMENAZAS A ESTE SECTOR

Dispositivos y aplicaciones médicas vulnerables

Aplicaciones médicas que funcionan en sistemas operativos desactualizados y no compatibles, e incluso APPs desarrolladas hace mucho tiempo y sin soporte.



Violación de datos de phi/ehr

Atacantes que apuntan a robar información confidencial de salud (PHI) y registros electrónicos de salud (EHR) de pacientes.

Robo de propiedad intelectual

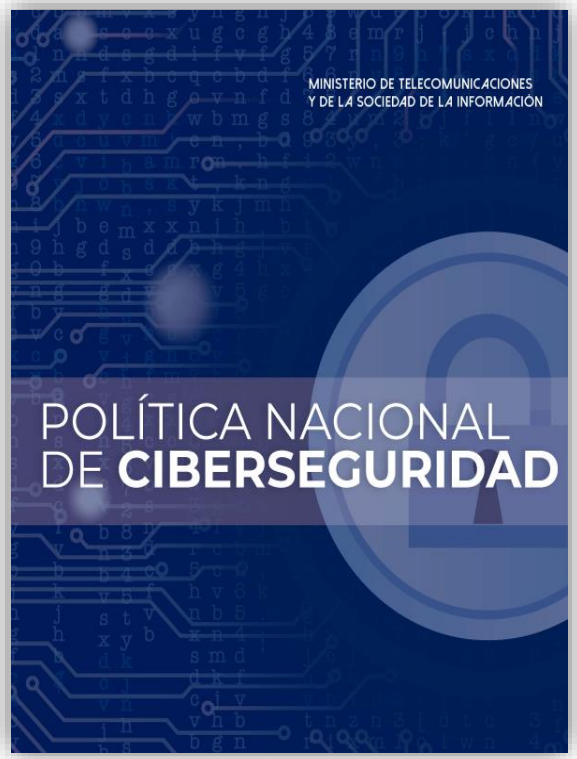
Los ciberdelincuentes, suelen dirigir su ataque a propiedad intelectual relacionada con dispositivos médicos, fórmulas en desarrollo, vacunas, entre otros.

Fuente: REPORTE DELOITTE "Escenario de amenazas en la industria de Salud y Ciencias de la Vida"

NORMATIVA LEGAL EN EL ECUADOR

- La Constitución del Estado, en su Art. 66, numeral 19 "**La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley**"
- El Art. 7 de la Ley Orgánica de Salud, "historia clínica única redactada en términos precisos, comprensibles y completos; **así como la confidencialidad respecto de la información en ella contenida…**"
- El Art. 4 de la Ley de Derechos y Amparo al Paciente, "Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, **tenga el carácter de confidencial**"
- El Art. 6 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, "**El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial.**"

Acuerdo Ministerial
N° 006-2021 Política de Ciberseguridad



Ley de Protección de Datos Personales

DATOS PERSONALES SENSIBLES

Incluye:

- Salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria que revelen información sobre su estado de salud.
- Estado de discapacidad de los titulares.

PILAR II Sistemas de información y Gestión de Incidentes

- Protección de los sistemas que permiten el procesamiento de los datos en todo nivel…

  …Fundamental la atención a incidentes informáticos que afecten a estos sistemas impactando en la **confidencialidad, integridad y disponibilidad de los datos** y la entrega y calidad de los servicios.

POLITICA DE CIBERSEGURIDAD

PILAR III Protección de la infraestructura crítica digital y servicios esenciales

…Construir las condiciones necesarias de robustez y resiliencia para garantizar el normal funcionamiento de las infraestructuras críticas digitales.

La economía, **salud pública**, sistemas electorales, seguridad, el funcionamiento del Estado y del sector privado, pueden verse vulnerados directamente, impactando el bienestar de la ciudadanía en general.

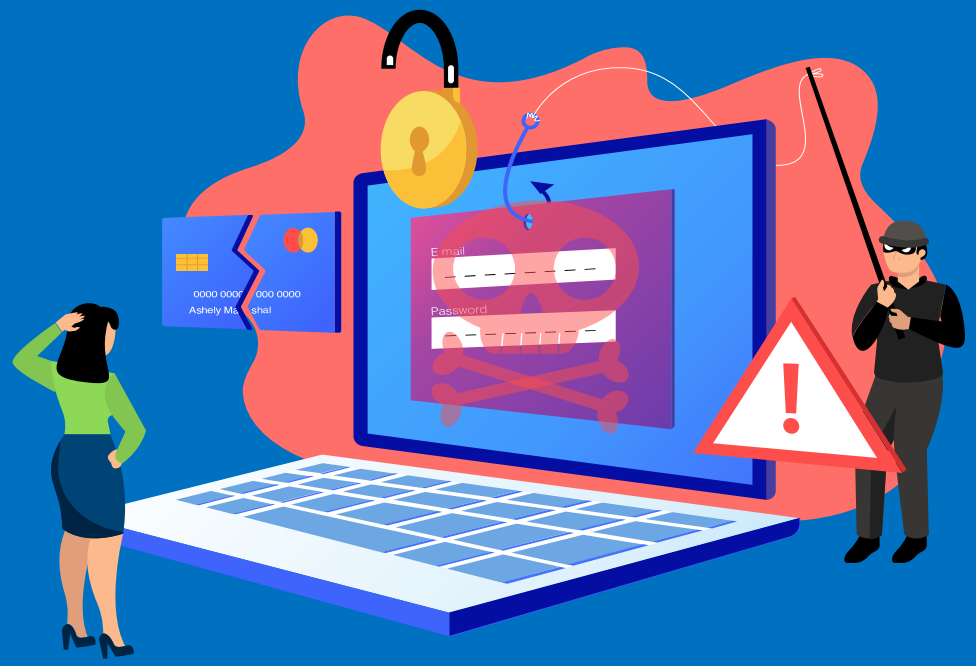
RIESGOS DE NO INVERTIR EN CIBERSEGURIDAD EN EL SECTOR SALUD

SUSTRACCIÓN DE IDENTIDAD

Sustracción de identidad de los médicos e información clínica de los pacientes

VENTA INDISCRIMINADA DE INFORMACIÓN

Extorsión, bloqueo al acceso, incluso muerte del paciente por no ejecutar intervenciones críticas por causa de ataques cibernéticos.



FILTRACIÓN DE INFORMACIÓN

Filtración de información clínica en contrabando, estafas y falsificaciones manipulando la sensibilidad de la gente.

ACCESOS INDEBIDOS

Acceso a datos privados de pacientes, infraestructuras tecnológicas débiles e inseguras

RECOMENDACIONES

1. Fomentar el uso del chip de la cédula electrónica para incorporar los componentes e-health como un mecanismo de confianza y seguridad de la información en los servicios que presta el sector salud.

2. La historia clínica digital debe Incorporar mecanismos de seguridad de la información para proteger la información (ej. Cifrado de información).

3. Implementar herramientas de ciberseguridad para salvaguardar la integridad de la información de los sistemas informáticos.

RECOMENDACIONES

4 Implementar la interoperabilidad entre toda la red pública integral de salud (RPIS) y la privada aplicando controles de transporte seguro de información.

5 Incluir en la Estrategia Integral de salud la prevención proactiva de riesgos cibernéticos garantizando en todo momento la confidencialidad, integridad y disponibilidad de los datos de los pacientes.

6 Aumentar la apropiación y concientización en el sector de la salud, sobre los retos y riesgos de seguridad propios de una práctica médica digital.
Generar conciencia tanto en médicos como en pacientes de lo grave que puede resultar una exposición de sus datos o el bloqueo a los mismos.

GRACIAS

Ministerio de Telecomunicaciones y de la Sociedad de la Información

República del Ecuador

Gobierno del Encuentro | Juntos lo logramos