INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

DIPLOMATURA UNIVERSITARIA EN GERENCIAMIENTO DE LA CIBERDEFENSA

NOVIEMBRE DE 2023

TRABAJO FINAL INTEGRADOR

"CIBERSEGURIDAD EN LA INDUSTRIA DE LA SALUD".

INTEGRANTES: **TC Marcelo Alberto GARCÍA**

TC Diego PARIENTE

SP Andrea Silvana SIBILA

RESUMEN DEL PROYECTO

El presente trabajo final integrador aborda la problemática de la ciberseguridad en la industria de la salud. Dentro de la presente investigación se han abordado tanto las instituciones públicas como privadas. El abordaje ha sido exploratorio y se realizó con una visión holística del tema. Se ha investigado en fuentes públicas sobre instituciones médicas dentro y fuera del país. Se ha propuesto abordar qué factores han de ser importantes a la hora de aumentar la resiliencia de los sistemas informatizados dentro de las instituciones sanitarias frente a los ciberataques.

“CIBERSEGURIDAD EN LA INDUSTRIA DE LA SALUD”

Ciberseguridad en la Industria de la Salud: Examinar la ciberseguridad en el sector de la salud, que es especialmente importante debido a la sensibilidad de la información médica. investigar casos de ataques a hospitales y clínicas y cómo se pueden prevenir.

En el presente trabajo final integrador se abordará la ciberseguridad en la industria de la salud y la problemática que conlleva en la misma el manejo de información confidencial, como son los datos de los pacientes y sus respectivas historias clínicas digitales. Normalmente las instituciones de salud, emplean a compañías externas a su organización para la informatización de las historias clínicas de sus pacientes, no obstante, esto no las exime de la responsabilidad primaria que tienen en la protección de los datos personales de sus pacientes. Dichas instituciones suelen ser un objetivo tentador para las operaciones cibernéticas de la delincuencia.

Debemos tener especialmente presente que la protección de la información es uno de los pilares en todo sistema informático, que debe asegurar su confidencialidad, si integridad y su disponibilidad. Todo ello comienza con la protección tanto de las redes como de sus dispositivos informáticos (ya sean de conmutación y/ o ruteo, es decir networking; o de sistemas y/ o servicios), que son finalmente los puntos más vulnerados en este ámbito tan particular. Sea por descuidos, falta de conciencia por parte del personal o simplemente porque no tienen las habilidades requeridas para realizar un buen uso de los medios informáticos.

Por ello, el tema de la ciberseguridad en la sanidad ha sido ampliamente debatido en especial después de la pandemia, con los ataques de ransomware a hospitales o la filtración de los datos de historiales de pacientes revendidos en la web oscura. Otro ejemplo son incursiones cibernéticas en la cadena de frío para comprometer el transporte de vacunas, esto se considera un problema real.

JUSTIFICACIÓN

Por sus características particulares, la sanidad ha sido y seguirá siendo objetivo codiciado por los ciberdelincuentes. Por lo tanto, su protección debe ser una prioridad. Para ello hay que preguntarse, ¿están protegidas sus infraestructuras informáticas? ¿cómo se lleva a cabo la concientización y/ o capacitación del personal con respecto al tema? ¿cómo incrementar los recursos que ayuden a proteger las redes informáticas de las instituciones sanitarias?

Para cumplimentar las normativas y/o políticas de seguridad vigente, nos planteamos las siguientes interrogantes: ¿existen normativas y/o políticas que den soporte al cumplimiento en cuanto a la ciberseguridad de los sistemas informatizados? ¿o sólo es una recomendación del estado del arte? En caso de existir hay ¿algún organismo oficial que las regule y certifique su control?, o queda librada al leal saber y entender de las partes?

Capacitación y concientización de los usuarios del quinto dominio, como se lleva a cabo: de acuerdo a las siguientes interrogantes: ¿las instituciones de la salud capacitan a los usuarios de sus redes (médicos, técnicos de la salud y enfermeras, personal administrativo)? ¿existe un control sobre esto?, es decir ¿hay un plan que contribuya a su implementación?

Protección de la infraestructura crítica, manejaremos las siguientes interrogantes: ¿los efectores de salud, invierten seriamente en los servicios que están afectados a la seguridad en de la información?

Ley de protección de datos personales, este es un punto importante ya que la ley 25.326 "…*instituye un mecanismo de protección de los datos personales, que incluye los datos sensibles y de salud; así también estableció principios de licitud de tratamiento de datos personales en general, que resultan aplicables a los datos relativos a la salud*", menciona esto en uno de sus párrafos. Es importante tener en cuenta cuando aplicamos software para el uso de datos que son sensibles, como los de las historias clínicas de los pacientes. Entonces, como interrogante: ¿las instituciones sanitarias, protegen con profesionalismo los datos personales de sus pacientes?

La formación del personal, entre los niveles mencionados es el más inmediato sobre el que hay que intervenir. Se puede señalar aquí como punto de inflexión, los usuarios que están conectados de manera virtual, son una bisagra en esta seguridad que se menciona, si se está preparado o no para llevar adelante un teletrabajo, entonces ¿qué tipo de seguridad se proporciona? Ello redundará en pos de salvaguardar la información en el momento y formas oportunas. Cabe mencionar que para ello existen diversos controles de seguridad que se pueden aplicar teniendo en cuenta su entorno específico de riesgo de seguridad de la información.

PLANTEAMIENTO DEL PROBLEMA

Elección del tema: “CIBERSEGURIDAD EN LA INDUSTRIA DE LA SALUD”

a) **Problema detectado**: Examinar la ciberseguridad en el sector de la salud, que es especialmente importante debido a la sensibilidad de la información médica. Investigar casos de ataques a hospitales y clínicas y cómo se pueden prevenir.
b) **Formulación del problema**: ¿La información se encuentra resguardada y cumple con las medidas de seguridad para su contención y la aplicación de la fórmula CID (Confidencialidad – Integridad y Disponibilidad)? ¿Como se procede a su resguardo? ¿Se aplican método de backups? ¿Tienen plan de contingencia? ¿Está restringido el acceso a la seguridad física de la información?

Debido al inherente peligro asociado al acceso de los recursos físicos por parte de personal autorizado y no autorizado, la seguridad física es un componente básico del plan de seguridad total del hospital. Por ello es necesario escribir las medidas y contramedidas relacionadas a la protección física de los recursos de información sensibles e identificar riesgos asociados a las facilidades, datos, medios, equipamientos y sistemas.

HIPÓTESIS O SOLUCIÓN PROPUESTA

“La implementación de las normativas y del estado del arte vigente en el empleo del 5to dominio favorecen la resiliencia a los ciberataques.”

OBJETIVOS A SER ALCANZADOS PARA SUSTENTAR LA HIPÓTESIS

- ✓ Explorar cuáles son los riesgos a los que se enfrentan las instituciones sanitarias en el 5to dominio.
- ✓ Describir los problemas detectados en el ámbito de la salud y que se relacionen con su accionar en el ciberespacio.
- ✓ Analizar el empleo de activos humanos y recursos materiales en la protección del espacio cibernético de las instituciones sanitarias.
- ✓ Desarrollar propuestas que aumenten la resiliencia de las tareas y actividades propias de la industria de la sanidad en el espacio cibernético.

MARCO TEÓRICO PRELIMINAR

Los ataques informáticos son una amenaza tanto para gobiernos, como para organizaciones públicas o privadas y para la ciudadanía. Conjuntamente los desafíos se ven agravados por la falta de expertos en la materia y se estima que no se cuenta con la cantidad suficiente de graduados para cubrir el incremento de los puestos en ciberseguridad a nivel mundial.[1]

1 Sánchez, C. (08 de febrero de 2019).

En el mundo hiperconectado, la ciberseguridad se ha convertido en un tema central. Podría pensarse que el conflicto bélico en Europa es algo lejano, sin embargo, ya se sabe que empezó a través de ciberataques mucho antes que la primera detonación en el territorio. La seguridad informática es un tema complejo per se, por ello le dedicamos la sección central y particularmente, para entender cómo se ve afectado el campo de la salud, en el que se manejan datos tan sensibles.[2]

Esto ha sido observado por los expertos cada vez con más frecuencia en el siglo XXI, por caso este grupo de investigación encontró citas de expertos que se referían a la guerra entre Rusia y Ucrania y cómo se habían incrementado los ciberataques entre ambos, incluso antes de que se produjeran ataques con fuegos cinéticos. "Esta guerra se planificó de forma cibernética porque hay reportes desde hace 5 años atrás de Microsoft y otras operadoras de seguridad que advertían que Rusia estaba introduciendo malware (software malicioso) en empresas, bancos y dependencias oficiales de Ucrania"[3], expuso Jorge Severino quien tiene formación en sistemas, una maestría en seguridad CCAT y realizó certificaciones internacionales en administración y seguridad de bases de datos en Oracle, Microsoft e IBM, implementación de las normativas y del estado del arte vigente en el empleo del quinto dominio que favorecen la resiliencia a los ciberataques.

- ✓ Normas ISO 27002
- ✓ CIS Controls, versión 8.
- ✓ Ley 2563 "Protección de Datos Personales".

Marco Norma ISO27002

Haciendo uso de las normas que componen la serie ISO 27000 se pone un enfoque en la 27001 la cual indica cómo se puede implementar un sistema de gestión de seguridad de la información en conjunto con otras normas. Asimismo, la ISO 27002 es una guía de buenas prácticas que describe los objetivos de controles y controles recomendados en cuanto a la seguridad de la información. Involucrando a todos los dominios con sus correspondientes objetivos de controles.

En cuanto a las técnicas de seguridad en sistemas de gestión de la información, cuyos puntos a observar y analizar son:

- Identificar los activos dentro del alcance del SGSI (Sistema de Gestión de Seguridad de la Información) y los propietarios de estos activos.
- Identificar las amenazas a estos activos.
- Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.
- Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.

Marco Controles CIS (Center for Internet Security)

Se definen controles, esto es para poder obtener un conjunto de acciones priorizadas que colectivamente forman mejores prácticas de defensa, que mitigan los ataques más comunes contra sistemas y redes.
Los controles CIS son desarrollados por una comunidad de expertos en TI, que aplican como

2 LUNA, Daniel (2022)

3 Severino, J (2022).

experiencia de primera mano cómo defensores cibernéticos para crear éstas mejores prácticas de seguridad aceptadas globalmente y su declaración de misión profesa que su función es ayudar a las personas, empresas y los gobiernos a protegerse contra amenazas cibernéticas generalizadas.

Asimismo, las actividades que imparten los controles CIS, no son solo una lista de buenas prácticas sino un conjunto de acciones priorizadas y altamente focalizadas que tienen una red de soporte comunitario para hacerlas implementables, utilizables, escalables y compatibles con todos los requerimientos de seguridad gubernamental o industrial.

Los mencionados controles son:

- Inventario y control de activos (hardware).
- Inventario y control de activos (software).
- Protección de datos.
- Configuración segura de activos y software empresarial.
- Gestión de cuentas.
- Gestión de control de accesos.
- Gestión continua de vulnerabilidades.
- Gestión de registros de auditorías.
- Protecciones de correo electrónico y navegador web.
- Defensa contra malware.
- Recuperación de datos.
- Gestión de infraestructura de red.
- Supervisión y defensa de la red.
- Capacitación en habilidades y conciencia de seguridad.
- Gestión de proveedores de servicios.
- Seguridad de software de aplicación.
- Gestión de respuesta a incidentes.
- Pruebas de penetración.

Ley 2563 - Protección de Datos Personales

"*Corresponde analizar el objeto protegido por la norma y los principios rectores que rigen la materia. En primer lugar, la ley 25.326, tiene como objetivo la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, tercer párrafo de la Constitución Nacional (art.1º).*"

METODOLOGÍAS Y TÉCNICAS UTILIZADAS PARA SUSTENTAR/ CONSTRASTAR LA HIPÓTESIS

En esta investigación el enfoque empleado ha sido cualitativo. El grupo ha obtenido una visión general del comportamiento de las instituciones sanitarias en el ciberespacio mediante la recopilación de información pública en los medios de comunicación y a través de entrevistas a profesionales de la salud en su interrelación con el mismo en el desarrollo de sus actividades profesionales habituales.

Las principales detectadas son:

Inicialmente se ha efectuado una investigación exploratoria en el ámbito público para recabar información de las capacitaciones ofrecidas a los agentes sanitarios del estado. Sólo se encontraron CUATRO (4) capacitaciones, todas ellas de carácter virtual, a saber:

- ✓ Seguridad de la información: Uso seguro de las tecnologías de la información y las comunicaciones (TIC). Introducción al concepto de infraestructura críticas.
- ✓ Curso virtual orientado a concientizar sobre la protección de la información y a elevar el nivel de seguridad de los organismos a partir de promover prácticas responsables y de buen uso de las herramientas informáticas de uso habitual en el ámbito laboral. A estos fines nos adentramos en conceptos fundamentales de la seguridad de la información, seguridad de las contraseñas a ser utilizadas por el usuario y desarrollamos el concepto de "phishing", entre otros.
- ✓ Uso seguro de las tecnologías de la información y las comunicaciones (TIC)
- ✓ Curso virtual complementario del curso "Seguridad de la Información – Conceptos Fundamentales". Esta propuesta educativa está orientada a promover la toma de conciencia en relación con los riesgos que acarrea el uso de las TIC, Tecnologías de la Información y Comunicación; a partir del reconocimiento de ciertas amenazas habituales y de la generación de estrategias para la prevención de posibles fallas de seguridad, focalizándonos en las Redes Sociales, la Ingeniería Social y desarrollamos el concepto de "Malware", entre otros.

1) Nuevos desafíos para la seguridad:

Curso virtual complementario de los cursos "Seguridad de la Información – Conceptos Fundamentales" y "Uso seguro de las tecnologías de la información y las comunicaciones (TIC)". En el mismo, nos enfocamos en los dispositivos móviles, los riesgos de la conocida "computación en la nube" y las medidas de seguridad posibles para hacer de ella un uso efectivo y útil.

Curso virtual enfocado en las amenazas a las infraestructuras críticas las cuales responden a diversos motivos, tanto accidentales como intencionales. Hablamos de incidentes provocados por malas prácticas, catástrofes, atentados o guerras, por ejemplo. En los últimos años se ha agregado a la lista un componente que aumenta considerablemente el riesgo sobre la seguridad de las infraestructuras críticas: las redes de computadoras. Por ello, nos enfocamos en un análisis de las infraestructuras criticas posibles, una revisión de la situación mundial en la materia y en recomendaciones y "buenas prácticas" o "lecciones aprendidas" aplicables.
Esta oferta académica se encuentra vinculada a la página de la Subsecretaría de Ciberdefensa del Ministerio de Defensa, pero cuando efectuamos una investigación exploratoria por el sitio del Ministerio de Salud se ha encontrado el siguiente hallazgo:

- Formación y capacitación de Talento Humano, caso práctico:

Desarrollo y actualización de las competencias de las y los trabajadores de salud para el ejercicio profesional de calidad.
Y luego de efectuar dicha exploración en el listado de cursos y capacitaciones no se pudo hallar ninguna oferta académica que brinde capacitación para los agentes estatales usuarios del ciberespacio en el ámbito específico de sus competencias.

En tanto dentro de la actividad privada en forma exploratoria se ha encontrado la oferta académica de CUATRO (4) Jornadas de Informática en Salud brindadas por el Departamento de Informática del Hospital Italiano.

Ver el siguiente link:
https://www1.hospitalitaliano.org.ar/landing/innova-salud-digital/sites/default/files/2022-09/11_Innova CiberseguridadHospitalItaliano.pdf

El Hospital Italiano de Buenos Aires (HIBA) es un hospital de alta complejidad acreditado en nivel 7 de HIMSS (Healthcare Information and Management Systems Society), que es el mayor nivel de digitalización que puede obtener una institución de salud y se concede cuando se ha logrado un entorno de registros médicos completamente electrónico.
"En el modelo del homeworking el perímetro de seguridad no se puede controlar con el paradigma de hace algunos años, por eso hay que reforzar la cultura del usuario en la prevención. Por ejemplo, que actualice los parches de seguridad, que tenga antivirus y en el caso del Hospital Italiano nuestras conexiones son a través de una VPN (red privada virtual por sus siglas en inglés) que es un túnel seguro", evaluó. Al mismo tiempo, sostuvo que "los que están más preparados son los entes de gobierno y las entidades bancarias, además de los hospitales porque el bien más importante con el que cuentan es la información". "Las organizaciones de salud estamos expuestas como cualquier organización y según datos a nivel mundial los focos más atacados son el ciberterrorismo, las unidades financieras y luego las unidades de salud", aportó Assale.[4]
La empresa Microsoft publicó en marzo pasado un estudio que vaticina que para el año 2025 habrá 3,5 millones de puestos vacantes en el área de ciberseguridad en todo el mundo. Esto implica un incremento del 350 por ciento en un período de ocho años. Ante el crecimiento de la demanda de graduados en seguridad informática ¿se puede considerar a la ciberseguridad el trabajo del futuro? "Existe un área de vacancia en ciberseguridad ya que es transversal a todas las industrias, por eso desde una Pyme hasta una multinacional necesita un área de seguridad informática; al margen de aquellas que tienen regulaciones estrictas como los sistemas bancarios que están regulados por el Banco Central o los hospitales regidos por las leyes de protección de datos personales", explicó Jorge Eterovic [5]

Durante el abordaje de esta investigación hemos visto que se resignifica la importancia de la ciberseguridad a través de algunas iniciativas públicas como las capacitaciones en ofrecidas a través de la plataforma del INAP (Instituto Nacional de Administración Pública) y otras privadas como las ofrecidas por el HIBA (Hospital Italiano de Buenos Aires). No obstante, lo señalado los ciberataques se incrementaron y alcanzaron una eficacia mayor. Incluso aquellas instituciones sanitarias como el Hospital Italiano que contaban previamente con toda una estructura propia encargada de la gestión de la ciberseguridad, han sido víctimas de ciberataques exitosos que exhiben una muestra real de la vulnerabilidad a la que se encuentran expuestas y debería modular nuestra percepción de la seguridad en la que nos encontramos.
A lo largo de la investigación hemos recopilado información de ciberataques exitosos a instituciones de la salud tanto públicas como privadas, en países en vías de desarrollo y en

4 ASSALE (2022)

5 ETEROVIC, Jorge (2022)

países desarrollados también. Sólo por citar algunos de los casos recopilados tenemos a los siguientes:

- El hackeo al hospital más grande de Neuquén: cómo es la investigación y quién estaría detrás. (JUN-2023)

La noticia de que el Hospital Castro Rendón, el más grande de Neuquén había sido víctima de un hackeo que terminó con la filtración de más de 100 mil pacientes impactó en la órbita institucional del sistema provincial. Sobre todo, tras conocerse que la maniobra se perpetró para vendar datos en la web.

https://www.rionegro.com.ar/sociedad/hackeo-al-hospital-mas-grande-de-neuquen-asi-es-la-investigacion-y-quien-seria-el-responsable-2955426/

- Un virus informático afecta el sistema de PAMI: aseguran que es un ciberataque.

Otra de las notificaciones que les llegaron a los empleados de la obra social de los jubilados indicaba lo siguiente: "Por cuestiones de seguridad informática, 1 se reporta caída total de sistemas en el país; 2 es necesario que apaguen todas las computadoras; 3 atendemos con protocolo".

Todas estas acciones fueron parte del plan de contingencia que se desarrolló en los sistemas de PAMI, que afectó la atención en todas las oficinas del país y la realización de trámites virtuales.

El problema afecta la atención de jubilados en todo el país. Afirman que el ciberataque “ha sido mitigado”. (AGO 2023)

https://www.perfil.com/noticias/cordoba/un-virus-informatico-afecta-el-sistema-de-pami-es-un-problema-grave.phtml

- A nivel local, el Hospital Italiano, ubicado en la Ciudad de Buenos Aires, sufrió una filtración de 21 GB de información interna.

Una nueva filtración afectó a una entidad de salud en Argentina.

El grupo de ransomware Knight (ex Cyclops), publicó un primer lote de información con 21 GB de datos de un usuario privilegiado del Hospital Italiano.

A diferencia de la enorme cantidad de filtraciones de datos que hubo durante los últimos años en Argentina -con OSDE a la cabeza en lo que refiere a salud-, en este caso, afortunadamente, no hay datos de pacientes.

https://medium.com/@juanbrodersen/filtran-datos-del-hospital-italiano-breach-en-okta-arrastra-a-1password-y-cuatro-d%C3%ADas-para-6046de97b662

https://www.reddit.com/r/argentina/comments/17if6i7/filtran_datos_del_hospital_italiano/?rdt=54551

- Hackeo a OSDE: suben archivos robados con historias clínicas e información de afiliados, políticos y famosos

Ciberdelincuentes de Lockbit publicaron en la dark web casi 140 GB sustraídos a la prepaga a fines de junio.

https://www.clarin.com/tecnologia/hackeo-osde-subieron-archivos-robados-informacion-afiliados-politicos-famosos-historias-clinicas_0_Z2OM4JEnR4.html

- Un ataque hacker afectó a hospitales y servicios de atención médica en cinco estados de EEUU

El "incidente de información de seguridad" provocó el cierre de salas de emergencias y desvíos de ambulancias. Expertos investigan la extensión del problema en California, Texas, Connecticut, Rhode Island y Pensilvania

https://www.infobae.com/estados-unidos/2023/08/05/un-ataque-hacker-afecto-a-hospitales-y-servicios-de-atencion-medica-en-cinco-estados-de-eeuu/

- Un hospital hackeado y la muerte de un bebé: ¿el primer fallecimiento por un caso de ransomware?

Una madre de Alabama presentó una demanda por muerte por negligencia contra un hospital de Mobile, alegando que no haber revelado que había sufrido un ciberataque provocó la muerte de su bebé nueve meses después.

La madre ha estado peleando con el hospital durante casi dos años mientras la instalación busca proteger los registros involucrados en el incidente, según los registros judiciales

.https://www.al.com/news/2021/10/alabama-mom-claims-baby-died-because-of-undisclosed-cyberattack-fights-for-hospital-records.html

https://www.infobae.com/america/eeuu/2021/09/30/un-hospital-hackeado-y-la-muerte-de-un-bebe-el-primer-fallecimiento-por-un-caso-de-ransomware/

En esta investigación se ha expuesto como se ha incrementado la propagación de los ciberataques y que los mismos no constituyen hechos aislados, sino por lo contrario un fenómeno (ya sea en el marco de la delincuencia o en el accionar de actores estatales en el empleo de fuegos no cinéticos) en franca expansión. Así mismo se ha expuesto la escasa concientización de los usuarios del ciberespacio, que a su vez se ve retroalimentada por una limitada oferta en materia de capacitación y una nula obligatoriedad en la realización de la misma quedando en manos del agente estatal y/ o privado la voluntad de aplicar a la misma.

También se ha expuesto el marco normativo, cuyo cumplimiento y la estricta observancia del estado del arte en materia de diseño de implementaciones atendiendo a la seguridad

informática incrementaría notablemente la seguridad en el empleo del ciberespacio. Es decir que la estricta observancia de lo señalado anteriormente, indudablemente contribuiría a favorecer la resiliencia a los ciberataques de las infraestructuras informáticas en el ámbito de la salud.

No obstante, como ha sido expresado es el usuario de las misma el eslabón más débil de esta cadena de seguridad. Y es allí, donde se debe incrementar el esfuerzo de las instituciones en la capacitación de los mismos.

CONCLUSIONES:

Es menester dotar a los profesionales de la salud de los conocimientos necesarios para que puedan transitar la transformación digital favoreciendo el incremento de las ventajas aportadas y disminuyendo los riesgos inherentes a este nuevo espacio de desarrollo de las actividades de la humanidad.

Pero, el abordaje que se debe realizar no debe ser específico, sino integral. Es decir que el mismo debe poseer una concepción holística de la problemática en cuestión y como tal debe proveer una respuesta integral para satisfacer soluciones exitosas. Tal modelo debe ser capaz de integrar en el mismo tres grandes fuentes y/o dominios, a saber: personas, procesos y tecnologías. Sólo a través de este enfoque sistémico podremos asegurar el empleo del quinto dominio y negar la afectación del mismo por parte de ciberdelincuentes o ciber atacantes. Es decir, estaremos en condiciones de asegurar la confidencialidad, integridad y disponibilidad de la información que en este dominio procesemos. Dentro de la infraestructura crítica de un país, su sistema sanitario cobra importancia destacada. Como lo hemos mencionado anteriormente, y ha sido documentado en numerosa información pública, las instituciones sanitarias no se encuentran a salvo de los ciberataques y ningún esfuerzo para incrementar la seguridad informática puede ser considerado como excesivo. Aún más, esto cobra vital importancia toda vez que las instituciones sanitarias manipulan un gran volumen de información confidencial, dado que las mismas han comenzado a implementar la historia clínica digital de cada uno de sus pacientes. Y ante la eventualidad de un ciber ataque que pudiera comprometer la confidencialidad de esta información, dicha institución sería judicialmente responsable por no proteger satisfactoriamente a la misma. Es más, sería pasible de ser sentada en el banquillo de los acusados y tener que demostrar que ha hecho todo lo materialmente posible.

Es por todo lo dicho anteriormente que se ha establecido como modelo exitoso el establecido con la concepción de seguridad de extremo a extremo por diseño. Esto sumado a un monitoreo constante de la red, el establecimiento y cumplimiento de una política de archivos de respaldo de la información y a un programa de capacitaciones dentro de la organización ha permitido proteger a la infraestructura crítica de dicho centro asistencial. Entendiendo por tal a la información empleada y no solo a los dispositivos de red y procesamiento de la misma.

REFERENCIAS INICIALES Y BIBLIOGRAFÍA PRELIMINAR

- https://salud.gob.ar/dels/printpdf/99#:~:text=En%20la%20Rep%C3%BAblica%20Argentina%20se,datos%20relativos%20a%20la%20salud.
- https://e-legis-ar.msal.gov.ar/htdocs/legisalud/migration/html/14402.html
- https://www.cisecurity.org/controls

ANEXOS

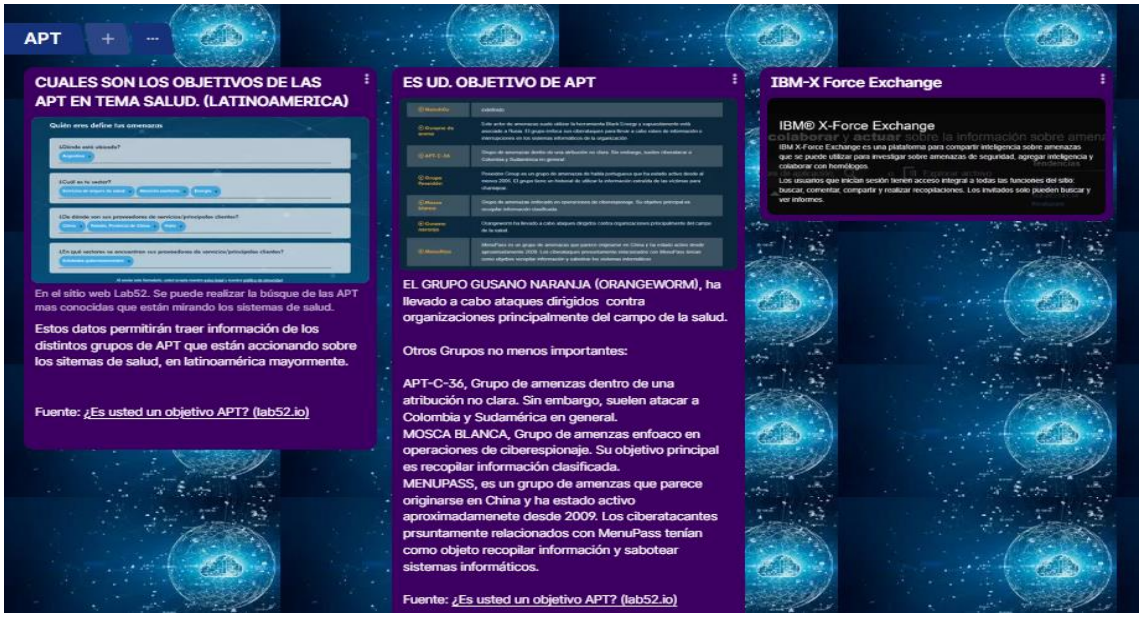
ANEXO 1 – Noticias de interés del problema planteado. Algunos artículos de diarios que muestran las distintas vulnerabilidades y sus consecuentes ataques a los sistemas informáticos en el área de Salud.

Ver el siguiente link.:

- https://padlet.com/mediumdecisionunited/diplomatura-en-gesti-n-de-la-ciberdefensa-qzqtz9no558h6f20

ANEXO 2 - Búsqueda de los distintos tipos de APT que podrían causar daño a las distintas empresas de salud y que están persistiendo en América Latina.

- https://lab52.io/
- https://exchange.xforce.ibmcloud.com/
- https://padlet.com/mediumdecisionunited/diplomatura-en-gesti-n-de-la-ciberdefensa-qzqtz9no558h6f20


APT
CUALES SON LOS OBJETIVOS DE LAS APT EN TEMA SALUD. (LATINOAMERICA)
En el sitio web Lab52. Se puede realizar la búsque de las APT mas conocidas que están mirando los sistemas de salud.
Estos datos permitirán traer información de los distintos grupos de APT que están accionando sobre los sitemas de salud, en latinoamérica mayormente.
Fuente: ¿Es usted un objetivo APT? (lab52.io)
ES UD. OBJETIVO DE APT
EL GRUPO GUSANO NARANJA (ORANGEWORM), ha llevado a cabo ataques dirigidos contra organizaciones principalmente del campo de la salud.
Otros Grupos no menos importantes:
APT-C-36, Grupo de amenzas dentro de una atribución no clara. Sin embargo, suelen atacar a Colombia y Sudamérica en general.
MOSCA BLANCA, Grupo de amenzas enfoaco en operaciones de ciberespionaje. Su objetivo principal es recopilar información clasificada.
MENUPASS, es un grupo de amenzas que parece originarse en China y ha estado activo aproximadamenete desde 2009. Los ciberatacantes prsuntamente relacionados con MenuPass tenían como objeto recopilar información y sabotear sistemas informáticos.
Fuente: ¿Es usted un objetivo APT? (lab52.io)
IBM-X Force Exchange
IBM® X-Force Exchange
IBM X-Force Exchange es una plataforma para compartir inteligencia sobre amenazas que se puede utilizar para investigar sobre amenazas de seguridad, agregar inteligencia y colaborar con homólogos.
Los usuarios que inician sesión tienen acceso integral a todas las funciones del sitio: buscar, comentar, compartir y realizar recopilaciones. Los invitados solo pueden buscar y ver informes.

IBM® X-Force Exchange
IBM X-Force Exchange es una plataforma para compartir inteligencia sobre amenazas que se puede utilizar para investigar sobre amenazas de seguridad, agregar inteligencia y colaborar con homólogos.
Los usuarios que inician sesión tienen acceso integral a todas las funciones del sitio: buscar, comentar, compartir y realizar recopilaciones. Los invitados solo pueden buscar y ver informes.

C.V. DEL EJECUTOR DEL TRABAJO FINAL

- TC Marcelo Alberto **GARCÍA**

  Ingeniero Electrónico

  Especialista en Planeamiento Estratégico para Acción Militar Conjunta

  Especialista en Planeamiento Estratégico

- TC Diego Alejandro **PARIENTE**

  Licenciado en Administración

  Especialista en Planeamiento Estratégico para Acción Militar Conjunta

  Oficial de Estado Mayor Conjunto

- SP Andrea Silvana **SIBILA**

  Licenciada en Gestión Educativa

  Especialista en Educación y TIC

  Profesora de Informática

  https://www.blogger.com/blog/post/edit/preview/2405399828710765000/2821842870844214809