

LA CIBERSEGURIDAD QUE MANEJAN LAS INFRAESTRUCTURAS CRÍTICAS
EN COLOMBIA ESPECÍFICAMENTE LAS DEL SECTOR SALUD Y
PROTECCIÓN SOCIAL

JOSÉ DAVID OSORIO ÁLZATE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DOSQUEBRADAS
2024

LA CIBERSEGURIDAD QUE MANEJAN LAS INFRAESTRUCTURAS CRÍTICAS
EN COLOMBIA ESPECÍFICAMENTE LAS DEL SECTOR SALUD Y
PROTECCIÓN SOCIAL

JOSÉ DAVID OSORIO ÁLZATE

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

EDGAR ROBERTO DULCE VILLAREAL
Tutora de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DOSQUEBRADAS
2024

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

CONTENIDO

	Pág.
GLOSARIO.....	12
INTRODUCCIÓN	16
1. DEFINICIÓN DEL PROBLEMA	18
ANTECEDENTES DEL PROBLEMA	18
FORMULACIÓN DEL PROBLEMA.....	19
2. JUSTIFICACIÓN	21
3. OBJETIVOS	22
OBJETIVOS GENERAL	22
OBJETIVOS ESPECÍFICOS	22
4. MARCO REFERENCIAL	23
4.1 MARCO TEÓRICO	23
4.1.1 Ciberseguridad en las infraestructuras críticas del sector salud en Colombia.	23
4.1.2 Ciberataques comunes	26
4.1.2.1 Vulnerabilidades más recurrentes.	26
4.1.3 marco de ciberseguridad de Colombia vs. Europa y América.	27
4.1.4 Buenas prácticas para mejorar la ciberseguridad.....	28
5. MARCO CONCEPTUAL	31
5.1 Vulnerabilidad.....	31
5.2 Infraestructura crítica.	31
5.3 Riesgo.....	31
5.4 Amenaza.	31
5.5 Ciberseguridad.....	31
6. ANTECEDENTES O ESTADO ACTUAL	32
7. MARCO LEGAL.....	34
8. Investigar los ataques que se han venido presentando el del sector salud y protección social en Colombia por medio de artículos, noticias y escritos que se han publicado a lo largo de los últimos 5 años con el fin de determinar cuáles han sido las vulnerabilidades de los sistemas.....	37
8.1 Ataques conocidos en Colombia y el mundo	37
8.1.1 Audifarma.	37
8.1.2 Invima.	37
8.1.3 Instituto Nacional de Cancerología de Colombia.	38
8.1.6 plataforma de salud pública de México.....	38
8.1.10 Sistema de salud pública en Finlandia.	40

9. Examinar los casos que se han presentado en el sector salud y protección social por medio de las lecturas realizadas y comparar cuales han sido las vulnerabilidades más recurrentes para penetrar estos sistemas.	43
9.2.1 Ransomware	43
9.2.2 Phishing.....	43
9.2.3 Ataques de denegación de servicio (DoS).....	43
9.2.4 Backdoor	44
9.2.5 Ataques a dispositivos médicos:	44
9.2.6 Ataques a sistemas de gestión de datos.....	44
Figura 1 grafico ataques más comunes.....	45
10. Comparar los marcos de ciberseguridad que se usan en Colombia respecto a Europa y América, por medio de las leyes que rigen las infraestructuras críticas de cada país o continente, para poder observar cuales son los puntos fuertes o débiles de la seguridad de la información en las IC del sector salud y protección social en Colombia	46
10.3.1 Colombia.....	46
10.3.2 Europa.....	46
10.3.3 América.....	46
Tabla 1 de comparación entre Colombia, Europa y EEUU.....	47
11. Establecer unas buenas prácticas de mejoramiento en la ciberseguridad para el sector salud y protección social priorizando en las vulnerabilidades más comunes que se encuentren a lo largo de la investigación con el fin de determinar los aspectos en que s debe enfocar éste.	62
11.1 Buenas Prácticas para Prevenir Ransomware	62
11.1.1 Mantén tus sistemas actualizados:.....	62
11.1.2 Usa software de seguridad confiable:	62
11.1.3 Realiza copias de seguridad:.....	62
11.1.4 Sé cauteloso con los correos electrónicos:	62
11.1.5 Navega de forma segura:.....	62
11.1.6 Restringe privilegios de usuario:.....	62
11.1.7 Educación en seguridad:	62
11.1.8 Filtrado de contenido web:.....	63
11.1.9 Control de aplicaciones:	63
11.1.10 Monitoreo constante:.....	63
11.2 Buenas Prácticas para Prevenir Phishing.....	63
11.2.1 Educación en Seguridad:.....	63
11.2.2 Verifica la Identidad:.....	63
11.2.3 Mantén el Software Actualizado:	63
11.2.4 Utiliza Autenticación de Dos Factores (2FA):.....	63
11.2.5 No Hagas Clic en Enlaces Sospechosos:.....	63
11.2.6 No Descargues Archivos Adjuntos Desconocidos:.....	63
11.2.7 Cuidado con los Mensajes de Urgencia:	63
11.2.8 Usa Soluciones de Seguridad:.....	63
11.2.9 Reporta Correos de Phishing:	64
11.2.10 Comprueba las Fuentes de Información:.....	64
11.3 Buenas Prácticas para Prevenir Ataques de Denegación de Servicio (DoS)	64

11.3.1 Monitoreo Continuo:	64
11.3.2 Firewalls y Filtros:	64
11.3.3 Balanceo de Carga:	64
11.3.4 Actualizaciones de Software:	64
11.3.5 Ancho de Banda Suficiente:	64
11.3.6 DDoS Mitigation Services:	64
11.3.7 Plan de Respuesta:	64
11.3.8 Educa a tu Personal:	64
11.3.9 Restringe el Acceso:	65
11.3.10 Respuesta Automatizada:	65
11.3.11 Backup de Datos:	65
11.3.12 Distribución de DNS:	65
11.4 Buenas Prácticas para Prevenir Ataques Backdoor	65
11.4.1 Mantén el Software Actualizado:	65
11.4.2 Firewalls y Antivirus:	65
11.4.3 Auditoría de Acceso:	65
11.4.4 Control de Acceso:	65
11.4.5 Seguridad en la Autenticación:	65
11.4.6 Educación en Seguridad:	65
11.4.7 Monitoreo Continuo:	65
11.4.8 Pruebas de Penetración:	66
11.4.9 Seguridad en el Desarrollo:	66
11.4.10 Actualizaciones de Firmware:	66
11.4.11 Política de Respuesta a Incidentes:	66
11.4.12 Evaluación de Terceros:	66
11.5.1 Actualización de Firmware y Software:	66
11.5.2 Aislamiento de Red:	66
11.5.3 Autenticación Fuerte:	66
11.5.4 Auditorías de Seguridad:	66
11.5.5 Control de Acceso Físico:	67
11.5.6 Formación del Personal:	67
11.5.7 Seguridad en la Cadena de Suministro:	67
11.5.8 Gestión de Incidentes:	67
11.5.9 Monitorización Continua:	67
11.5.10 Actualización de Políticas:	67
11.5.11 Colaboración:	67
11.5.12 Cumplimiento Normativo:	67
11.6 Buenas Prácticas para Prevenir Ataques a Sistemas de Gestión de Datos	67
11.6.1 Actualización Regular:	67
11.6.2 Control de Acceso:	68
11.6.3 Encriptación de Datos:	68
11.6.4 Auditorías de Seguridad:	68
11.6.5 Copias de Seguridad:	68
11.6.6 Firewalls y Seguridad Perimetral:	68
11.6.7 Formación del Personal:	68
11.6.8 Política de Contraseñas Fuertes:	68
11.6.9 Monitorización Continua:	68
11.6.10 Gestión de Parches:	68
11.6.11 Control de Dispositivos Extraíbles:	68

11.6.12 Cumplimiento Normativo:	68
12. CONCLUSIONES.....	70
13. RECOMENDACIONES.....	72
BIBLIOGRAFÍA.....	74
ANEXOS.....	79
ANEXO A. LOS CIBERATAQUES A LAS EMPRESAS DE LATINOAMÉRICA Y ESTADOS UNIDOS....	79
ANEXO B. Las empresas que han sufrido ciberataques	80
ANEXO C. Video de sustentación de la monografía para optar por el título de especialista en seguridad informática de la UNAD	81

LISTA DE TABLAS

	Pág.
Tabla 1 de comparación entre Colombia, Europa y EEUU	47

LISTA DE FIGURAS

	Pág.
Figura 1 grafico ataques más comunes	45

LISTA DE CUADROS

Pág.

Cuadro 1 Titulo del cuadro..... **¡Error! Marcador no definido.**

LISTA DE ANEXOS

	Pág.
ANEXO A. LOS CIBERATAQUES A LAS EMPRESAS DE LATINOAMÉRICA Y ESTADOS UNIDOS.....	79
ANEXO B. LAS EMPRESAS QUE HAN SUFRIDO CIBERATAQUES.....	80
ANEXO C. Video de sustentación de la monografía para optar por el título de especialista en seguridad informática de la UNAD	81

GLOSARIO

- **BACKDOORS¹**: Conocido en español como puerta trasera este tipo de ataque entra al sistema por una entrada desconocida para el usuario sin ser detectado, esta es la diferencia que tiene con los troyanos los cuales deja entrar a nuestro sistema camuflados en archivos aparentemente normales
- **BRECHA DIGITAL²**: Es la desigualdad que hay en sistemas informáticos, se puede hablar de la tecnología que se usa en países del primer mundo en diferencia a la que se usa en países del tercer mundo.
- **CIBERATAQUES³**: Es la intención de ingresar a los computadores para adueñarse de los datos o utilizar estos para realizar ataques a otros sistemas.
- **CIBERDELINCUENTES⁴**: Son personas malintencionadas que tienen como objetivo ingresar a los sistemas de otras personas para sustraer información valiosa.
- **HACKER⁵**: No todos los hackers en el mundo cibernético son malintencionados, existen muchos tipos de hackers, así también un hacker puede ser cualquiera con conocimientos de software y hardware, con los cuales puede saltar la seguridad de un sistema.
- **MALWARE⁶**: Es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.
- **RANSOMWARE⁶**: Este ataque bloquea el acceso al sistema y para poder volver a tener acceso a este se debe pagar una suma de dinero al atacante, este ataque fue creado por hackers mal intencionados que tienen gran conocimiento en el área de programación

¹ GÓMEZ, Juan Armando. 2023. ¿Qué es un Backdoor o Puerta Trasera?: 5 consejos para evitarlos. [En línea] 2023. <https://www.deltaprotect.com/blog/backdoor-o-puerta-trasera>.

² MINTIC. Brecha Digital. [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.mintic.gov.co/portal/inicio/5467:Brecha->.

³ UNISYS. S.F. Ciberataques: lo que debe saber. [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.unisys.com/es/glossary/what-is-cyber-attack/>.

⁴ ACKTIB. S.F. Los Ciberdelincuentes: Quiénes son, qué hacen y por qué lo hacen. [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://acktib.com/blog-los-ciberdelincuentes-quienes-son-que-hacen-y-por-que-lo-hacen/>.

⁵ BANCO PICHINCHA. S.F. ¿Qué hacen los hackers y qué tipos existen? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.pichincha.com/blog/que-es-un-hacker>.

⁶ AVAST. S.F. ¿Qué es el malware y cómo protegerse de los ataques? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.avast.com/es-es/c-malware>.

- **RIESGO INFORMÁTICO⁷**: Es el proceso que se lleva a cabo para los activos informáticos en el cual se identifican sus vulnerabilidades y amenazas a las cuales están expuestos
- **SECTOR PRIVADO⁸**: Es lo opuesto al sector público, buscan el lucro con el ejercicio de sus actividades y esta no es controlada por el estado.
- **SEGURIDAD INFORMÁTICA⁹**: Es la que se encarga de resguardar la información que se encuentra en un sistema informático.
- **TECNOLOGÍA¹⁰**: Es el arte de cambiar o cambiar algo que ya existe y convertirlo en algo novedoso mediante un proceso.
- **VULNERABILIDAD¹¹**: Es la falta de seguridad que hay en un sistema la cual puede ser utilizada por una persona malintencionada para penetrar en el sistema y adueñarse de la información.

⁷ MANCUZO, gabriel. 2023. ¿Qué es un riesgo en Ciberseguridad? Definición y tipos. [En línea] 12 de JULIO de 2023. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://ciberseguridadtips.com/que-es-un-riesgo-en-ciberseguridad-definicion-causas/>.

⁸ LÓPEZ, jose francisco. 2019. Sector Privado. [En línea] 17 de MAYO de 2019. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://economipedia.com/definiciones/sector-privado.html>.

⁹ HUBSPOT. 2023. Seguridad informática: qué es, tipos y características. [En línea] 08 de 05 de 2023. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://blog.hubspot.es/website/que-es-seguridad-informatica>.

¹⁰ UNIVERSIDAD NACIONAL DEL LITORAL. S.F. ¿QUÉ ES LA TECNOLOGÍA? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <http://www.unl.edu.ar/ingreso/cursos/cac/21ot/>.

¹¹ SANTANDER. S.F. ¿Qué es una vulnerabilidad informática? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20inform%C3%A1tica%2C%20una%20vulnerabilidad%20es,malintencionada%20para%20compro meter%20su%20seguridad>.

RESUMEN

En la presente monografía se quiere proponer métodos para la solución de problemas que se vienen presentado en las infraestructuras críticas en cuanto a la ciberseguridad ya que muchas empresas no tienen el suficiente conocimiento en cuanto a los peligros que hay en la red y lo fácil que les hacen el camino a los crackers de entrar a los servidores y por ende a la información de la misma si no se cuenta con parámetros mínimos de seguridad, para esto existen normas que rigen la ciberseguridad de las infraestructuras críticas (ICs) las cuales deben tomar en cuenta para tener una buena seguridad de la información, así como también dar capacitaciones a su personal ya que con un acto tan simple como ingresar una USB a un computador de la empresa o abrir un correo sospechoso puede traer grandes problemas a la organización abriendo así una puerta por la que se podría realizar un ataque de los tantos que existen, y así tener acceso total al sistema dejándolo vulnerable a cualquier ciberataque y con esto robando información de la ICS poniendo en riesgo la confidencialidad de los pacientes y usuarios del sistema así como información valiosa de la empresa con la cual pueden perjudicar a la sociedad.

Palabras Claves: Ciberataques, brechas, sector privado, seguridad informática, vulnerabilidad.

ABSTRACT

In this monograph we want to propose methods for solving problems that have been presented in critical infrastructure in terms of cybersecurity as many companies do not have enough knowledge about the dangers that exist in the network and how easy they make the way for crackers to enter the servers and therefore the information of the same if you do not have minimum security parameters, for this there are rules governing the cybersecurity of the CI which must take into account to have a good information security, There are rules governing the cybersecurity of CIs which must be taken into account to have a good information security, as well as provide training to their staff because with an act as simple as entering a USB to a company computer or open a suspicious email can bring big problems to the organization thus opening a door through which you could make an attack of the many that exist, and thus have full access to the system leaving it vulnerable to any cyber-attack and thus stealing information from the ICS putting at risk the confidentiality of patients and system users as well as valuable information of the company with which they can harm society.

Keywords: Cyberattacks, private sector, computer security, breaches, vulnerability.

INTRODUCCIÓN

La seguridad en el sector de la salud se ha convertido en una preocupación crítica en los últimos cinco años debido a la creciente amenaza de ciberdelincuentes que aprovechan las vulnerabilidades en los sistemas de información. Estos ataques no solo buscan robar datos de infraestructuras críticas, sino que también recurren al bloqueo de sistemas para exigir rescates, una práctica cada vez más común entre personas malintencionadas que buscan lucrar a expensas de las debilidades en las redes informáticas de las organizaciones.

Esta monografía se propone explorar en profundidad los métodos empleados por los delincuentes cibernéticos en el sector de la salud en los últimos años. Se analizarán casos concretos en los que estos ataques han tenido éxito, así como las devastadoras consecuencias que han tenido para las organizaciones y los pacientes afectados. Dado que el sector de la salud maneja información altamente sensible y tiene un flujo constante de usuarios, se ha convertido en un objetivo de alto valor para los ciberdelincuentes.

Además de destacar los problemas y desafíos que enfrenta el sector de la salud en cuanto a seguridad cibernética, esta monografía también se centrará en proporcionar información sobre buenas prácticas que pueden ayudar a prevenir estos ataques. Se abordarán estrategias y medidas que las organizaciones de salud pueden implementar para fortalecer su seguridad informática y proteger los datos de los pacientes.

Asimismo, se llevará a cabo una evaluación de la situación de Colombia en términos de seguridad informática en comparación con otros países de América Latina y el mundo. Esto permitirá comprender mejor el estado actual de la ciberseguridad en el país y destacar áreas donde se pueden realizar mejoras.

El entorno digital se ha expandido a un ritmo asombroso en las últimas décadas. La proliferación de dispositivos conectados a Internet, la creciente dependencia de la nube para almacenar datos y la rápida adopción de la inteligencia artificial han transformado la forma en que interactuamos con la tecnología. A medida que la vida cotidiana se ha vuelto cada vez más digital, también lo han hecho las amenazas que se enfrentan en línea.

Los ciberataques pueden tomar muchas formas: desde el robo de datos personales y financieros hasta el secuestro de sistemas informáticos completos para exigir rescates. La ingeniería social, el phishing y el malware son solo algunas de las herramientas en el arsenal de los ciberdelincuentes. Estos ataques pueden tener un costo inmenso, tanto en términos económicos como en la privacidad y la seguridad de las personas.

En un mundo cada vez más interconectado, las infraestructuras críticas, como las redes de energía, los sistemas de agua y las instalaciones de atención médica, también están en la mira de los ciber atacantes. El sabotaje de estos sistemas puede tener consecuencias devastadoras para la sociedad en su conjunto.

1. DEFINICIÓN DEL PROBLEMA

ANTECEDENTES DEL PROBLEMA

En Colombia hay muy poca información sobre la ciberseguridad que se debe tener en el sector salud por esto muchas empresas de este sector se han visto afectadas por los ciberataques de personas malintencionadas

En un estudio que se realizó en el instituto europeo de software de Bulgaria titulado “Hybrid Exercising for Cyber-Resilient Healthcare and Cross-Sector Crisis Response Operability”¹² en el estudio se habla de la cooperación que debe tener la parte tecnológica con la operativa para hacerle un mejor frente a los ciberdelincuentes, y proponen cierto tipo de test que se pueden hacer en las organizaciones para mejorar la ciberseguridad.

El estudio que se realizó y aún sigue en curso llega a la conclusión de que todas las partes de la empresa deben estar articuladas en la lucha contra la ciberdelincuencia ya que muchos aparatos electrónicos no cuentan con ciberseguridad, pero son vulnerables a ataques.

En otro estudio que se encontró referente al caso de esta monografía fue “TIC al servicio de la salud” en este artículo el ingeniero y magister en sistemas Jeimy J. Cano M.¹³ habla de la importancia de la seguridad informática porque el sector salud está involucrando muchos dispositivos tecnológicos para hacer mejor la comunicación de médico-paciente muchas veces sin tener en cuenta la seguridad que se debe tener en la parte de sistemas.

Como conclusión el magister dice que el departamento de sistemas debe estar y trabajar de la mano con los médicos apoyándolos en la ciberseguridad.

Por otro lado, en el informe y resumen del foro económico mundial titulado “Industria de la salud y TI”¹⁴ puede ver como la tecnología cada vez está más de la mano con la salud por lo que se quiere llegar a tratar pacientes ambulatorios con solo ingresar a un sitio web y poner sus síntomas, o ser visto por un médico por video llamada, y

¹² SHARKOV, George et al. Hybrid Exercising for Cyber-Resilient Healthcare and Cross-Sector Crisis Response Operability, » Sofia, 2021.

¹³ CANO, Jeimy Seguridad y Ciberseguridad en los dispositivos médicos [En línea]. - 18 de noviembre de 2018. - [Fecha de consulta: 18 de febrero de 2023]. disponible en: https://www.researchgate.net/publication/329222111_Seguridad_y_Ciberseguridad_en_los_dispositivos_medicos.

¹⁴ GONZÁLEZ RODRÍGUEZ, Javier, et al. Lo humano y lo tecnológico en medicina [En línea] // Lo humano y lo tecnológico en medicina. - 2018 de noviembre de 2018. - [Fecha de consulta: 10 de febrero de 2023]. disponible en: https://www.researchgate.net/publication/329222111_Seguridad_y_Ciberseguridad_en_los_dispositivos_medicos.

así agilizar el sistema de salud reduciendo los costos tanto a la entidad de salud como al paciente.

En conclusión, los aportes tecnológicos que puede dar la tecnología a la salud son inmensos, pero también conlleva una gran responsabilidad en cuanto al tema de seguridad ya que en manos de ciberdelincuentes puede traer consecuencias graves a los usuarios.

En el artículo “Lo humano y lo tecnológico en medicina”¹⁵ habla de lo importante que se ha vuelto la tecnología para la salud, pero dice que en Colombia está muy lejos de llegar a una salud digna ya que para acceder a este tipo de avances tecnológicos se necesita tener una medicina prepagada, en el artículo dan la opinión de diferentes médicos e ingenieros.

Las opiniones concuerdan en que por más mínimo que sea el avance en Colombia en la parte de tecnología siempre va a ir de la mano con la salud ya que con el simple hecho de usar un microscopio o un computador para imprimir una fórmula ya se está usando sistemas y tecnologías.

FORMULACIÓN DEL PROBLEMA

En la actualidad por estudios que ha realizado la empresa Fortinet ¹⁶. y datos que ha revelado la policía nacional de Colombia se ha descubierto que en el 2022 se realizaron 52.000 ataques un promedio de 5000 por mes, esto fue tanto en el sector privado como público, evidenciándose que fue más alta la cifra en el privado, se quiere demostrar con esta monografía en donde están las brechas de seguridad que dieron pie a estos ataques cibernéticos en las infraestructuras críticas analizando los ciberataques más relevantes en Colombia más puntualmente en el sector salud, se conocen ataques como los que se realizaron a el hospital San Jorge de Pereira, la gobernación de Pereira, el ataque a la empresa SANITAS, entre otros.

Se puede tomar como referencia el ataque que se realizó en Sanitas en el 2022 el cual hizo que las citas de los pacientes se retrasaran, y por esto se retrasaron también procedimientos que se le debían realizar a los pacientes, como cirugías, exámenes, entrega de medicamentos, etc.

¹⁵ CANO, Jeimy Industria de la salud y TI [En línea] // Industria de la salud y TI. - 18 de noviembre de 2018. - [Fecha de consulta: 19 de febrero de 2023]. disponible en: https://www.researchgate.net/publication/329222111_Seguridad_y_Ciberseguridad_en_los_dispositivos_medicos.

¹⁶ SOY EMPRENDEDOR Colombia tuvo más de 20 mil millones de intentos de ciberataques en 2022 [En línea]. - 22 de Marzo de 2023. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://soyemprendedor.co/colombia-tuvo-mas-de-20-mil-millones-de-intentos-de-ciberataques-en-2022/9926/>.

El ataque realizado a AUDIFARMA¹⁷. este año fue uno de los más nombrados y que generaron más controversia entre los usuarios, el ciberataque comprometido la página web y la app móvil motivo por el cual el agendamiento de citas y solicitar medicamentos se tuvo que realizar en los puntos físicos de la entidad y atendían a los pacientes por orden de llegada lo cual generó un retraso en las operaciones y la asistencia de los mismos, el ataque fue visible para la seguridad de AUDIFARMA cuando ya se había realizado esto lleva a pensar que no se está manejando una seguridad en tiempo real con monitoreo las 24 horas ya que el atacante pudo ingresar al sistema sin que la empresa detectara anomalías en su sistema, faltaría un mejor escaneo de vulnerabilidades en la ICS.

También se puede mencionar un ataque que sufrió el sector salud de Costa Rica¹⁸. en el cual no se robó información si no que fue dirigido a los aparatos electrónicos como por ejemplo a las máquinas de rayos X las cuales quedaron inservibles generando así un caos en los hospitales y clínicas, los pacientes llegaban y no había máquinas para realizar los procedimientos que necesitaban.

La mayoría de estos ataques se han generado por medio de ransomware o ataques maliciosos los cuales son los más comunes y nocivos para el sector salud.

Pregunta problema:

¿Cuáles son medidas de ciberseguridad que manejan las infraestructuras críticas en Colombia específicamente las del sector salud y protección social mediante la inspección de los ciberataques que han tenido en los últimos 5 años?

¹⁷ PORTAFOLIO Lo que se sabe del ataque cibernético a infraestructura de Audifarma [En línea]. - 24 de enero de 2023. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.portafolio.co/negocios/empresas/audifarma-lo-que-se-sabe-del-ataque-cibernetico-a-la-empresa-577384>.

¹⁸ SWISSINFO El Seguro Social de Costa Rica sufre ciberataque que afecta a hospitales [En línea]. - 31 de mayo de 2022. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: https://www.swissinfo.ch/spa/costa-rica-ciberataque_el-seguro-social-de-costa-rica-sufre-ciberataque-que-afecta-a-hospitales/47637614.

2. JUSTIFICACIÓN

El sector salud en Colombia como empresas prestadoras de servicios tienen a su cargo mucha información sensible de personas, pertenecen al sector salud y de protección social por esta razón son llamadas ICs(infraestructuras críticas), esto significa que si llega a tener un problema en su sistema afectaría a gran parte de la población, es por esto que se quiere realizar una monografía de las brechas, vulnerabilidades que han tenido las IC del sector salud a lo largo del territorio nacional y cuáles han sido los motivos por los cuales han recibido ciberataques, cual es el modo más común en el que han penetrado la seguridad de estos sistemas, también se quiere conocer la evolución de la ciberseguridad de las infraestructuras críticas de Colombia respecto al resto del mundo para así conocer que debilidades y fortalezas tiene la ciberseguridad en Colombia y como ha ido evolucionando a través de los años para estar más preparada para este tipo de ataques, tanto en prevención como en contrarrestarlos.

3. OBJETIVOS

OBJETIVOS GENERAL

Analizar la ciberseguridad que manejan las infraestructuras críticas en Colombia específicamente las del sector salud y protección social mediante la inspección de los ciberataques que han tenido en los últimos 5 años, para así poder llegar a establecer cuáles han sido las vulnerabilidades más comunes que han tenido.

OBJETIVOS ESPECÍFICOS

- Investigar los ataques que se han venido presentando en el sector salud y protección social en Colombia por medio de artículos, noticias y escritos que se han publicado a lo largo de los últimos 5 años con el fin de determinar cuáles han sido las vulnerabilidades de los sistemas.
- Examinar los casos que se han presentado en el sector salud y protección social por medio de las lecturas realizadas y comparar cuáles han sido las vulnerabilidades más recurrentes para penetrar estos sistemas.
- Comparar los marcos de ciberseguridad que se usan en Colombia respecto a Europa y América, por medio de las leyes que rigen las infraestructuras críticas de cada país o continente, para poder observar cuáles son los puntos fuertes o débiles de la seguridad de la información en las IC del sector salud y protección social en Colombia
- Establecer unas buenas prácticas de mejoramiento en la ciberseguridad para el sector salud y protección social priorizando en las vulnerabilidades más comunes que se encuentren a lo largo de la investigación con el fin de determinar los aspectos en que se debe enfocar éste.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Ciberseguridad en las infraestructuras críticas del sector salud en Colombia. La ciberseguridad en Colombia es algo muy importante para las empresas y más aún para las ICS ya que este tipo de empresas presta en su mayoría servicios fundamentales a la sociedad, por este motivo es muy importante tener una buena seguridad en la parte tecnológica e informática para prevenir un ataque, robo o daño en la información de estas empresas, a medida que pasa el tiempo la seguridad se vuelve más efectiva ya que anteriormente se esperaba que sucediera el problema para así encontrar una solución en las partes afectadas, en la actualidad la seguridad se está enfocando en adelantarse a la mayoría de problemas que puedan surgir para así tener unas infraestructuras más seguras, algunas empresas han optado por invertir más en seguridad y algunas de ellas cambiando totalmente el esquema para así mejorar significativamente y estar mucho más protegidos a problemas futuros, cabe destacar que las empresas encargadas a la ciberseguridad se están especializando aún más invirtiendo una gran parte del presupuesto en personal más especializado en este ámbito y se encuentra realizando campañas para formar aún más a sus empleados, en los problemas que más se han enfocado es en mejorar el escaneo en tiempo real para prevenir ataques antes de que sucedan, mejorar las respuestas automáticas de la seguridad si en algún momento no se está pendiente de esta y que sean realmente efectivas que no solo envíen notificaciones si no que contrarresten algún ataque que se realice, protección al usuario final, dar capacitaciones a los empleados de las ICS para educarlos mediante la problemática que se presenta día a día por los diferentes métodos de ataques que realizan los crackers, ya que por medio de estudios la parte más vulnerable de la cadena en un sistema es el humano, y estos aprovechan esta debilidad para sus ciberataques¹⁹.

Las ICS están empezando a realizar ataques monitoreados a sus sistemas para ver sus debilidades y así mejorar las vulnerabilidades que se presentan para estar preparados a ataques futuros, un ejemplo de estos ataques controlados se realizó en Medellín el cual consistió en dejar varias USB alrededor de la empresa con un malware indetectable para el empleado, al terminar la jornada laboral entraron los ingenieros en seguridad informática y encontraron que en 10 de los 100 pc se encontraba el virus comprobando esto que por falta de conocimiento “el ser humano es el eslabón más débil del sistema”(Kevin Mitnic).

¹⁹ LESMES DIAZ, Laura ¿Qué pasa con la ciberseguridad en las plataformas de salud de Colombia? [En línea]. - 24 de enero de 2023. --[Fecha de consulta: 23 de abril de 2023]. disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-las-plataformas-de-salud-de-colombia-736510>.

Desde el 2020 la tecnología se ha hecho mucho más vital en la vida cotidiana como consecuencia de la pandemia del COVID-19, por esta razón los ciberataques han aumentado considerablemente y la mayoría de las ICS no estaban preparadas para tales ataques, llevándose a cabo con éxito muchos de estos, por estas razones muchas empresas están iniciando y consolidando su departamento de sistemas interno, ya que la mayoría de las empresas tercerizaba este departamento por temas de economía pero con el paso del tiempo y el aumento en los ciberataques se han concientizado de que el departamento de tecnología es parte fundamental de una empresa para la seguridad de su información.

Cada que el mundo avanza la tecnología también lo hace a pasos agigantados y lo que se veía como un beneficio para una empresa ahora se ah convierte en una necesidad para esta, pero no solo crece la tecnología si no también los ciberataques y ciberdelincuentes, en los últimos 5 años se han venido presentando varios ataques en el sector salud de Colombia con cifras preocupantes y alarmantes para el país, se han presentado ataques en empresas de este sector como lo son Keralty, Sanitas, Colsanitas²⁰, esta situación es tan trascendental en los servicios que estas empresas prestan virtualmente los cuales fueron inhabilitados y no se pudieron prestar servicios como autorizaciones y agendamiento de citas, también se presentaron casos en que los crackers divulgaron información sensible como información de los pacientes e información fiscal de estas empresas, pero no solo las empresas han sido víctimas de ataques ya que se conoció que la cuenta de Twitter de la ministra de salud también fue hackeada por algunas horas²¹, al igual que se presentó un ataque en la página web de Invima la cual fue deshabilitada por varias semanas esto es algo muy grave debido a que la empresa INVIMA es la más importante del país en cuanto a la vigilancia sanitaria, se han creado rumores tras esta serie de ataques como los que se enfocan en que esto se ha realizado para dañar el prestigio de las personas encargadas de estas empresas pero no ha tenido muchos fundamentos por lo que se ha desestimado, se ha dado más al rumor de que los ciberdelincuentes han realizado esta serie de ataques al sector salud por temas lucrativos y se enfocan en este sector ya que tienen información sensible de muchas personas y pueden cobrar una mejor recompensa, la mayoría de estos ataques se han realizado por medio de ransomware ya que con este tipo de ataques a estas infraestructuras críticas pueden inutilizar los sistemas y pedir recate por ellos bloqueando el acceso y la información que tienen estos sistemas, con estos ataques que se han presentado se ha amenazado las infraestructuras críticas del sector salud pero también ha puesto en peligro la vida de los pacientes, ya que con el retraso en las citas, ordenes o cirugías la salud del paciente se puede ver afectada

²⁰ INTEREMPRESAS Los ciberataques al sector sanitario se multiplican por seis en un año [En línea]. - 23 de marzo de 2023. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://www.interempresas.net/Ciberseguridad/Articulos/471124-Los-ciberataques-al-sector-sanitario-se-multiplican-por-seis-en-un-ano.html>.

²¹ EL COLOMBIANO Hackearon la cuenta de Twitter de la ministra de Salud, Carolina Corcho [En línea]. - 26 de noviembre de 2022. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://www.elcolombiano.com/colombia/hackearon-cuenta-de-twitter-de-la-ministra-de-salud-carolina-corcho-DN19143752>.

por el tiempo que demora en realizar los procedimientos o en la entrega de medicamentos.

El ingeniero Oswaldo Palacios afirma: “Un paciente no debería llegar a un hospital donde no funcionen los equipos de rayos X o algún otro dispositivo que esté conectado a la red informática porque estos fueron hackeados”²² respecto a esta afirmación se llega a la conclusión de lo importante que se han vuelto los sistemas para las empresas de salud ya que lo que es una ventaja para los pacientes como lo pueden ser los equipos de rayos x que al estar conectados a la red pueden consultar más fácilmente los resultados del procedimiento también trae consigo problemas ya que si el sistemas es atacado queda vulnerable la información sensible que este tiene de los pacientes por esto es muy importante una buena seguridad en las ICS y tener bien capacitados a los empleados que manejan este tipo de sistemas para que realicen buenas prácticas y no abran brechas o generen vulnerabilidades en los sistemas que permitan a los ciber atacantes ingresar como se dice vulgarmente no dejar puertas ni ventanas abiertas a la ciberdelincuencia 8.

Como se ha mencionado anteriormente los ataques más usados por los ciberdelincuentes son los ransomware²³ y las ICS han querido poner más atención a este tipo de ataques logrando contener muchos de estos antes de que sean ejecutados por los ciberdelincuentes, por esta razón los crackers han empezado a buscar backdoors en los sistemas para venderlos en la Deep Web ya que son más lucrativos que por ejemplo una tarjeta de crédito la cual se puede conseguir por menos de \$10 dólares y estos backdoors se pueden vender hasta por \$10.000 dólares, otro método muy frecuente que usan para realizar ataques es el phishing, como se cita anteriormente el eslabón más débil de un sistema es el ser humano por esto y por la falta de conocimiento de los empleados que tienen acceso al sistema pueden ser vulnerados fácilmente mediante un mensaje de texto o un correo electrónico en el cual inconscientemente ingresan o abren un link el cual está infectado y le dan acceso total al delincuente para que pueda ingresar a los servidores donde está contenida la información de la empresa de salud dejando vulnerable la información sensible de los pacientes y los dispositivos que estén conectados al sistema.*

²² PRENSARIO Los ciberataques: La enfermedad incurable del sector Salud [En línea]. - Prensario, 7 de abril de 2021. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://prensariotila.com/los-ciberataques-la-enfermedad-incurable-del-sector-salud/>.

²³ RANSOMWARE HELP Ransomware En El Sector Médico: Estadísticas Y Consejos De Seguridad [En línea]. - 2023. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://helpransomware.com/es/ransomware-en-el-sector-medico/>.

4.1.2 Ciberataques comunes. Como solución al objetivo número dos del presente trabajo se determina que el ataque más utilizado por los ciberdelincuentes para penetrar en los sistemas son las backdoors o puertas traseras en las cuales encuentran fácilmente vulnerabilidades²⁴ y los ransomware porque estos delincuentes tienen como objetivo conseguir sumas de dinero a cambio de recuperar la información que secuestraron de la empresa con este tipo de ataque que se llevó a cabo como fue el caso de AUDIFARMA a la cual le estaban pidiendo una suma de dinero y si no se cumplían las demandas se iban a hacer públicas la información sensible de pacientes, usuarios y empleados que los ciberdelincuentes tenían en su poder.

4.1.2.1 Vulnerabilidades más recurrentes. En Colombia, el sector salud ha experimentado una serie de ciberataques en los últimos años. Estos ciberataques han afectado a hospitales, clínicas, laboratorios y otras organizaciones de atención médica. A continuación, se presentan algunas de las vulnerabilidades más recurrentes de ciberataques en el sector salud colombiano:

1. **Falta de actualizaciones de seguridad:** Las organizaciones del sector salud a menudo no actualizan sus sistemas y software con las últimas actualizaciones de seguridad, lo que las hace vulnerables a los ciberataques.
2. **Contraseñas débiles:** Las contraseñas débiles son una de las principales vulnerabilidades en la seguridad cibernética. Muchas organizaciones del sector salud utilizan contraseñas simples y fáciles de adivinar, lo que facilita el acceso no autorizado a los sistemas.
3. **Phishing:** El phishing es una técnica de ingeniería social que involucra el envío de correos electrónicos o mensajes de texto fraudulentos para engañar a las personas para que revelen información confidencial o hagan clic en enlaces maliciosos. Las organizaciones del sector salud son a menudo objetivos de ataques de phishing.
4. **Ransomware:** El ransomware es un tipo de malware que cifra los archivos del sistema de la organización y exige un rescate para desbloquearlos. Los ciberdelincuentes pueden utilizar el ransomware para atacar las organizaciones del sector salud y exigir rescates.
5. **Falta de capacitación en seguridad cibernética:** La falta de capacitación en seguridad cibernética del personal de las organizaciones del sector salud es una vulnerabilidad importante. Los empleados pueden cometer errores de seguridad, como hacer clic en enlaces maliciosos o divulgar información confidencial sin darse cuenta.
6. **Vulnerabilidades de dispositivos médicos:** Los dispositivos médicos, como los monitores de pacientes y los equipos de diagnóstico, a menudo tienen

²⁴ JAIMOVICH, Desirée Los 14 tipos de ciberataques más comunes (y cómo prevenirlos) [En línea]. - 25 de octubre de 2022. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://blog.invgate.com/es/tipos-de-ciberataque>.

vulnerabilidades de seguridad. Los ciberdelincuentes pueden explotar estas vulnerabilidades para acceder a los sistemas de información médica.

Es importante que las organizaciones del sector salud tomen medidas para abordar estas vulnerabilidades y protegerse contra los ciberataques. Esto incluye la implementación de políticas y procedimientos de seguridad sólidos, la capacitación del personal en seguridad cibernética y la realización de evaluaciones de seguridad periódicas.

4.1.3 marco de ciberseguridad de Colombia vs. Europa y América. En cuanto al marco de ciberseguridad, Colombia ha avanzado en los últimos años en la creación de políticas y regulaciones para protegerse contra los ciberataques. Sin embargo, todavía hay diferencias significativas en comparación con Europa y América en términos de madurez del marco de ciberseguridad.

Europa ha liderado el camino en la adopción de marcos de ciberseguridad sólidos y bien definidos²⁵. La Unión Europea (UE) ha establecido un marco legal para la protección de datos personales con el Reglamento General de Protección de Datos (RGPD). Además, la UE ha implementado el Reglamento de Ciberseguridad de la UE, que establece medidas obligatorias para garantizar la seguridad de las redes y los sistemas de información.

En América, Estados Unidos²⁶ ha sido líder en la implementación de marcos de ciberseguridad. La Estrategia Nacional de Ciberseguridad de Estados Unidos establece objetivos específicos y metas para proteger la infraestructura crítica y mejorar la seguridad cibernética. Además, la Ley de Modernización de la Infraestructura del Ciberespacio (CISA) establece un marco de trabajo para proteger la infraestructura crítica de ciberataques.

En Colombia, la Ley de Ciberseguridad establece un marco legal para la protección de las redes y sistemas de información críticos en el país. La ley define la infraestructura crítica como "los recursos, sistemas y servicios esenciales para el funcionamiento de la economía, la sociedad y la vida de las personas, cuya interrupción o degradación puede ocasionar un impacto significativo en la seguridad, estabilidad, salud, bienestar o supervivencia de la población". Además, Colombia cuenta con el Plan Nacional de Ciberseguridad, que tiene como objetivo fortalecer la protección de los sistemas de información del país.

A pesar de estos esfuerzos, aún hay desafíos en el marco de ciberseguridad de Colombia. Por ejemplo, la falta de recursos y de capacitación para las

²⁵ ECS ENISA introduces the European Cybersecurity Skills Framework [En línea]. - 23 de septiembre de 2022. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://ecs-org.eu/enisa-introduces-the-european-cybersecurity-skills-framework/>.

²⁶ CISTERNELLI, eric 7 Cybersecurity Frameworks That Help Reduce Cyber Risk [En línea]. - 31 de marzo de 2023. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk>.

organizaciones en el sector salud puede dificultar la implementación de medidas efectivas de seguridad cibernética. También es importante destacar que las amenazas cibernéticas son globales y en constante evolución, por lo que es necesario un esfuerzo continuo para mantenerse al día en la protección contra los ciberataques.

En resumen, aunque Colombia²⁷ ha avanzado en la implementación de un marco de ciberseguridad, todavía hay diferencias significativas en comparación con Europa y América en términos de madurez del marco de ciberseguridad. Es importante continuar trabajando en la implementación de medidas de seguridad efectivas para protegerse contra los ciberataques y mantenerse al día con las amenazas en constante evolución.

4.1.4 Buenas prácticas para mejorar la ciberseguridad. La ciberseguridad es crucial en el sector de la salud y protección social debido a la naturaleza confidencial de la información que se maneja²⁸. A continuación, se presentan algunas buenas prácticas para mejorar la ciberseguridad en este sector, priorizando las vulnerabilidades más comunes:

Capacitación del personal: La formación en ciberseguridad debe ser una prioridad para todo el personal que trabaje en el sector de la salud y protección social. El personal debe estar al tanto de las mejores prácticas de seguridad y ser consciente de los riesgos asociados a la manipulación y transmisión de información sensible. Se deben proporcionar regularmente cursos de formación en ciberseguridad para garantizar que el personal esté actualizado en cuanto a las últimas amenazas y vulnerabilidades²⁹.

Actualización del software y hardware: El software y el hardware utilizados en el sector de la salud y protección social deben mantenerse actualizados para evitar vulnerabilidades conocidas. Se deben aplicar parches de seguridad y actualizaciones regularmente para corregir las vulnerabilidades conocidas en el software y hardware utilizados.

²⁷ CATRIL OPAZO, Juan Eduardo, et al. NIST cybersecurity framework in south America: Argentina, Brazil, Chile, Colombia, And Uruguay. 2021. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://repositorio.uchile.cl/handle/2250/184569>

²⁸ AGUILERA CRUZ, Roberto. 4 aspectos clave para cuidar la ciberseguridad en las empresas de salud [En línea]. - 4 de agosto de 2022. - [Fecha de consulta: 24 de abril de 2023]. disponible en: https://www.ey.com/es_mx/health-sciences-wellness/ciberseguridad-en-las-empresas-de-salud.

²⁹ LONDOÑO, Ingrid 5 buenas prácticas de ciberseguridad que debes conocer [En línea]. - 28 de octubre de 2020. - [Fecha de consulta: 24 de abril de 2023]. disponible en: https://www.piranirisk.com/es/blog/5-buenas-practicas-de-ciberseguridad-que-debe-conocer?hs_amp=true&utm_term=&utm_campaign=Matriz+de+Riesgos+-+General+-+Julio+2022&utm_source=adwords&utm_medium=ppc&hsa_acc=9508207643&hsa_cam=17802451156&hsa_grp=138377008.

Contraseñas seguras: Las contraseñas deben ser seguras y complejas para evitar accesos no autorizados. El personal debe ser instruido sobre la importancia de utilizar contraseñas fuertes y cambiarlas periódicamente. Además, se deben implementar políticas de contraseñas para garantizar que las contraseñas utilizadas sean lo suficientemente seguras³⁰.

Acceso limitado: El acceso a la información sensible debe ser limitado solo al personal que lo necesite para realizar sus tareas. Se deben implementar políticas de acceso para garantizar que solo el personal autorizado tenga acceso a la información sensible.

Copias de seguridad regulares: Es importante realizar copias de seguridad regulares de la información sensible. Esto asegurará que, en caso de una violación de seguridad, la información sensible no se pierda.

Uso de software antivirus y firewall: El uso de software antivirus y firewall es una buena práctica para proteger los sistemas y redes de las amenazas cibernéticas. Se deben implementar políticas de seguridad para garantizar que todo el software antivirus y el firewall estén actualizados y funcionando correctamente.

Evaluaciones regulares de seguridad: Se deben realizar evaluaciones regulares de seguridad para identificar las vulnerabilidades y amenazas cibernéticas. Estas evaluaciones pueden incluir pruebas de penetración y simulaciones de ataques para identificar debilidades en la seguridad.

Encriptación de datos: La encriptación de datos es una forma efectiva de proteger la información sensible. Se deben utilizar algoritmos de encriptación fuertes para proteger la información en tránsito y en reposo³¹.

Protección de dispositivos móviles: Los dispositivos móviles, como smartphones y tabletas, también deben ser protegidos para evitar violaciones de seguridad. Se deben implementar políticas de seguridad para dispositivos móviles, como la encriptación de datos, la autenticación de usuario y la restricción de aplicaciones no autorizadas.

³⁰ EKRAN 12 Cybersecurity Best Practices & Measures to Prevent Cyber Attacks in 2023 [En línea]. - 15 de marzo de 2023. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://www.ekransystem.com/en/blog/best-cyber-security-practices>.

³¹ KASPERSKY What is Data Encryption? [En línea]. - 2023. [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://www.kaspersky.com/resource-center/definitions/encryption>.

Gestión de vulnerabilidades³²: Se deben implementar políticas y procedimientos para la gestión de vulnerabilidades. Esto incluye la identificación, evaluación y mitigación de vulnerabilidades conocidas en el software y hardware utilizados en el sector de la salud y protección social.

Protección de redes Wi-Fi: Las redes Wi-Fi utilizadas en el sector de la salud y protección social deben ser protegidas para evitar accesos no autorizados. Se deben implementar políticas de seguridad para redes Wi-Fi, como la encriptación de datos y la autenticación de usuario.

Monitoreo de seguridad³³: El monitoreo continuo de la seguridad es importante para detectar cualquier actividad sospechosa en los sistemas y redes. Se deben implementar herramientas de monitoreo de seguridad y establecer políticas y procedimientos para el manejo de alertas de seguridad.

Políticas de seguridad de terceros: Si se utilizan servicios de terceros en el sector de la salud y protección social, se deben establecer políticas de seguridad claras y procesos de evaluación para garantizar que los proveedores de servicios cumplan con los estándares de seguridad necesarios.

Implementación de controles de acceso: Es importante implementar controles de acceso en los sistemas y redes para evitar accesos no autorizados. Los controles de acceso pueden incluir la autenticación de usuario, la asignación de roles y permisos, y la monitorización de actividad de usuario.

Política de respuesta a incidentes: Se debe establecer una política de respuesta a incidentes para garantizar una respuesta rápida y efectiva en caso de una violación de seguridad. Esto puede incluir la notificación de las autoridades pertinentes y la coordinación con expertos en ciberseguridad.

En general, es importante tener una estrategia completa de ciberseguridad para el sector de la salud y protección social que aborde todas las posibles amenazas y vulnerabilidades. La implementación de buenas prácticas de ciberseguridad, combinada con una formación y concienciación adecuadas del personal, puede ayudar a proteger la información sensible y garantizar la seguridad de los sistemas y redes en el sector.

³² FORTRA Gestión de vulnerabilidades: qué es, procesos y buenas prácticas [En línea]. - 27 de julio de 2022. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://www.fortra.com/es/blog/gestion-vulnerabilidades>.

³³ ALFARO, ivan Claves para un monitoreo de ciberseguridad efectivo [En línea]. - 23 de agosto de 2021. - [Fecha de consulta: 24 de abril de 2023]. <https://www.b-secure.co/blog/claves-para-un-monitoreo-de-ciberseguridad-efectivo>.

5. MARCO CONCEPTUAL

5.1 Vulnerabilidad. Una vulnerabilidad en un sistema es la inhabilidad de hacer frente a un problema o ataque que se realice a la red informática de la empresa generando daños o robos de información en los servidores y que la empresa no sepa como contrarrestar estos ataques o daños provocados por el ciberdelincuente.

5.2 Infraestructura crítica. Las infraestructuras críticas son infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Fuente: Ministerio de Defensa

5.3 Riesgo. El riesgo de TI se refiere a la amenaza que representa el mal uso o la falla, intencional o no, de la estructura y el equipo de TI de una empresa, por parte de piratas informáticos, ataques de phishing o incluso robo de datos cometido por los empleados.

5.4 Amenaza. Una amenaza cibernética es una actividad que tiene como objetivo comprometer la seguridad de un sistema o interrumpir el mundo digital en general.

5.5 Ciberseguridad. La ciberseguridad es la práctica de proteger los sistemas críticos y la información confidencial de los ataques digitales. También conocidas como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad tienen como objetivo combatir las amenazas a los sistemas y aplicaciones en red, ya sea que provengan del interior o del exterior de una empresa.

6. ANTECEDENTES O ESTADO ACTUAL

Se puede encontrar muchos artículos relacionados con los ataques que se han venido presentando en el sector salud no solo en Colombia si no en Latinoamérica y el mundo que han venido creciendo desde la pandemia del COVID-19 ya que los procedimientos, citas, etc., se han vuelto más virtuales, por esto el sector salud es uno de los más apetecidos por los ciberdelincuentes, en el artículo “Aumento de ciberataques al sector salud y sus graves consecuencias” escrito por la periodista Iris Montoya Ricaurte³⁴, habla del grave aumento que se ha venido presentando en el ámbito de los ciberataques en el sector salud en el habla de un estudio que realizó la plataforma AKAMAI la cual es una de las plataformas más confiables y conocidas que prestan servicio de nube, en él dice que un ataque a un hospital por ejemplo puede ir desde al desabastecimiento de medicamentos, los retrasos en las citas y hasta la muerte de los pacientes, informa también que antes los ciberataques se centraban en información y en sistemas que no comprometieran la vida humana pero al día de hoy esto ya no es un impedimento para los ciberdelincuentes con tal de lograr su cometido.

Uno de los ataques que mencionan fue a un hospital el cual fue atacado con un Ransomware Hive, y esto genero un daño en los sistemas ocasionando que los procedimientos del hospital se hicieran analógicamente retrasando toda la programación del hospital y generando que no pudieran recibir más pacientes hasta que se normalizara el sistema.

Por otro lado en una entrevista que se le realizó a Hannes Molsen, encargado de la ciberseguridad en la empresa DRAEGER especializada en seguridad informática, la entrevista lleva por título “Conectividad segura y protegida”³⁵, en esta habla de la seguridad que deben tener los hospitales ya que en un sistema extenso es muy difícil tener una buena seguridad, él recomienda que se deben seccionar los sistemas para así poder tener una mejor ciberseguridad en los hospitales y clínicas que ha utilizado este método se ha mejorado la seguridad considerablemente, habla también de la importancia que tienen las sesiones de capacitación que se le brindan a los empleados para mejorar aún más el capital humano enfocándose en temas como el e-mail, las memorias USB, los enlaces, etc.

En la tesis “Cyber Risk Management in the Finnish Healthcare Sector” de Hanne Hellstén para optar por el grado de magister en la universidad de Tampere³⁶, cuenta

³⁴ RICAURTE, Iris Montoya Aumento de ciberataques al sector salud y sus graves consecuencias [En línea] // Aumento de ciberataques al sector salud y sus graves consecuencias. - 20 de FEBRERO de 2023. - [Fecha de consulta: 15 de febrero de 2023]. disponible en: <https://www.ventasdeseguridad.com/2023022023067/noticias/empresas/aumento-de-ciberataques-al-sector-salud-y-sus-graves-consecuencias.html>.

³⁵ DRAEGER Conectividad segura y protegida [En línea] // Conectividad segura y protegida. - 1 de JUNIO de 2020. - [Fecha de consulta: 14 de febrero de 2023]. disponible en: <https://www.draeger.com/Library/Content/safe-and-secure-connectivity-br-PDF-10446-es.pdf>.

³⁶ MOLSEN, Hannes Conectividad segura y protegida [Entrevista]. - 1 de JUNIO de 2020. - [Fecha de consulta: 14 de febrero de 2023].

sobre los riesgos que tiene el sector salud en cuanto a la seguridad de su información, los riesgos cibernéticos surgen del uso de TI y pueden dragar la

honradez, disponibilidad o confidencialidad de servicios o datos, afirma que Los ataques cibernéticos en el sector de la salud han sido impulsados por una variedad de motivos, muchos de los cuales involucran ganancias financieras de una forma u otra.

7. MARCO LEGAL

En Colombia, existen varias leyes y normativas que regulan la seguridad informática, entre las que destacan la Ley 1266 de Habeas Data, que establece los derechos de los titulares de la información y las obligaciones de los responsables de los datos; y la Ley 1273 de 2009, que tipifica los delitos informáticos y establece las sanciones correspondientes.

Además, Colombia cuenta con entidades encargadas de velar por la seguridad informática en el país, como la Agencia Nacional de Seguridad Cibernética (ANSPEC) y el Centro Cibernético Policial (CCP), quienes trabajan en conjunto para garantizar la protección de los sistemas y datos de las empresas y ciudadanos colombianos.

En este punto se va a enumerar las leyes colombianas que coinciden con el tema de ciberseguridad y de la protección de datos y seguridad de la información en Colombia.

- Constitución Política de Colombia Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar". De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
- Decreto 1078 de 2015, Establece las regulaciones para la protección de datos personales en Colombia.
- Decreto 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado"
- Decreto 338 de marzo de 2022, establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital y crea el modelo y las instancias de gobernanza de seguridad digital entre otras disposiciones

- Decreto 620 de 2020: Establece el marco normativo para la protección de la información clasificada.

- Documento CONPES 3854, Política Nacional de Seguridad Digital

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

- Ley 1266 de 2008, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

- Ley 1273 de 2009, Define los delitos informáticos y establece sanciones para las personas que los cometan.

- Ley 128 de 2018, Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.

- Ley 1341 de 2009, Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC.

- Ley 1437 DE 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. (Uso de medios electrónicos Procedimiento Administrativo Electrónico), Artículo 1 de la ley 1755 de 2015.

- Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

- Ley 1672 de 2013, Lineamientos para la Adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos

- Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones

- Ley 527 de 1999, Establece el marco legal para el comercio electrónico en Colombia, incluyendo la autenticación y firma digital.

- Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.

- Ley 603 de 2000, Por la cual se modifica el artículo 47 de la Ley 222 de 1995, Artículo 2. Artículo 2º. Las autoridades tributarias colombianas podrán verificar el estado de cumplimiento de las normas sobre derechos de autor por parte de las sociedades para impedir que, a través de su violación, también se evadan tributos.
- Norma Técnica Colombiana NTC- ISO/IEC Colombiana 27001:2013. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.
- Resolución 2346 de 2007: Regula la seguridad de la información en el sector financiero.

el marco legal en un proyecto de ciberseguridad en Colombia es fundamental para garantizar la protección de los datos y sistemas de información, así como para establecer las sanciones correspondientes en caso de incumplimiento de las normativas.

8. INVESTIGAR LOS ATAQUES QUE SE HAN VENIDO PRESENTANDO EL DEL SECTOR SALUD Y PROTECCIÓN SOCIAL EN COLOMBIA POR MEDIO DE ARTÍCULOS, NOTICIAS Y ESCRITOS QUE SE HAN PUBLICADO A LO LARGO DE LOS ÚLTIMOS 5 AÑOS CON EL FIN DE DETERMINAR CUÁLES HAN SIDO LAS VULNERABILIDADES DE LOS SISTEMAS.

Los ciberataques como se menciona anteriormente en el sector salud colombiano han aumentado desde la contingencia del COVID-19³⁷. y así mismo en toda Latinoamérica y el mundo ya que más empresas usan los sistemas para estar en contacto con sus usuarios en el caso del sector salud es muy fácil encontrar organizaciones que por medio de su página web o de una aplicación se pueda pedir citas, autorizar ordenes o pedir exámenes, etc., unos de los ataques más conocidos y nombrados en este sector han sido:

8.1 ATAQUES CONOCIDOS EN COLOMBIA Y EL MUNDO

Los ciberataques en el sector salud son una preocupación creciente tanto en Colombia como en todo el mundo. Aquí se presentan algunos ejemplos de ciberataques conocidos en el sector salud:

8.1.1 Audifarma. El ataque tuvo lugar el domingo 22 de enero de 2023, el hackeo que los ciberdelincuentes realizaron en Audifarma tuvo comprometidos tanto el sitio web como la app de la empresa en un comunicado emitido por la misma empresa dio a conocer que el ataque que sufrieron fue por medio de un ransomware y la empresa como medida de seguridad deshabilito los servidores tanto virtuales como físicos, quedando así sin atención virtual al usuario son medidas que no se deberían utilizar ya que se retrasan los procedimientos por estos es esencial tener una buena ciberseguridad que monitoree en tiempo real y permita contrarrestar ataques al instante³⁸.

8.1.2 Invima. En el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (INVIMA) se produjo un primer ciberataque en el primer semestre de 2022, específicamente el 6 de febrero, Posteriormente, el Invima fue víctima de otro ciberataque el 3 de octubre de 2022 se atribuye también a un ransomware el instituto estuvo sin servicios unos días creando así un caos por los pagos que debían hacer los usuarios llevando a que la organización tuviera que alargar los

³⁷ MORALES ROJAS, Juan Gilberto Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial [En línea]. - 2022. - [Fecha de consulta: 15 de febrero de 2023]. disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11574/Ataques%20ciberneticos_Trabajo%20grado_Juan%20Morales_v2.pdf?sequence=1&isAllowed=y.

³⁸ AUDIFARMA. Ataque cibernético a infraestructura tecnológica de Audifarma [En línea]. - 23 de enero de 2023. - [Fecha de consulta: 15 de febrero de 2023]. disponible en: <http://audifarmaapp.com/comunicado-general-ciberataque-audifarma/>.

plazos de los pagos estableciendo una inconformidad en los clientes y retrasando los procesos³⁹.

8.1.3 Instituto Nacional de Cancerología de Colombia. Ataque ransomware al Instituto Nacional de Cancerología de Colombia en 2019: En julio de 2019, el Instituto Nacional de Cancerología de Colombia sufrió un ataque de ransomware que afectó sus sistemas de información. Los atacantes exigieron un rescate para desbloquear los sistemas.

8.1.4 Ministerio de salud y protección social de Colombia⁴⁰ En el año 2020, el Ministerio de Salud y Protección Social de Colombia sufrió un ciberataque que afectó sus operaciones. Este ataque cibernético fue un incidente significativo que generó preocupación en el sector de la salud del país. El ataque cibernético fue descrito como un ataque dirigido al Ministerio de Salud y Protección Social de Colombia. Se trató de un incidente de seguridad informática que afectó las operaciones y la infraestructura tecnológica de la entidad.

El ataque cibernético generó preocupación y pudo haber interrumpido las actividades y servicios relacionados con la salud y la protección social en Colombia. Sin embargo, los detalles específicos sobre las consecuencias del ataque no se proporcionan en los resultados de búsqueda.

8.1.5 Costa Rica. En Costa Rica se presentó un ataque a las entidades públicas los cuales constaron de ransomware, defacement a la web que modifica la página web, robaron archivos de correos electrónicos, el gobierno tuvo que pedir ayuda a entidades de ciberseguridad de EEUU, España, Israel al igual que de la empresa Microsoft con esto se puede ver que en Latinoamérica está muy atrasado en seguridad informática ya que son muchos los casos que se han presentado no solo en entidades de salud si no en entidades del gobierno y empresas privadas .

8.1.6 plataforma de salud pública de México. Ataque a la plataforma de salud pública de México en 2021: En enero de 2021, la plataforma de salud pública de México fue atacada por un grupo de hackers que intentaron acceder a información confidencial de los pacientes⁴¹.

³⁹ RICO BARRERA, susana maría El Invima es objeto de nuevo ataque cibernético [En línea]. - 4 de octubre de 2022. - [Fecha de consulta: 15 de febrero de 2023]. disponible en: <https://consultorsalud.com/Invima-objeto-ataque-cibernetico/>.

⁴⁰ BAJONERO, geraldin. Ciberataque a gran escala en Colombia: así es la grave situación que enfrenta el país. [En línea] 13 de 09 de 2023. [Fecha de consulta: 28 de septiembre de 2023]. disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-que-informacion-se-pudieron-haber-robado-en-el-ciberataque-805730>.

⁴¹ AGUIRRE QUEZADA, juan pablo Ciberseguridad, desafío para México y trabajo legislativo [En línea]. - marzo de 2022. - [Fecha de consulta: 28 de febrero de 2023]. disponible en: <http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5551/Cuaderno%20de%20Investigaci%C3%B3n%2087.pdf?sequence=1&isAllowed=y>.

8.1.7 Sistema de salud de Baltimore (EEUU). El ciberataque al Sistema de Salud de Baltimore en 2019 fue un evento significativo que afectó gravemente los sistemas informáticos de la ciudad estadounidense. El ataque ocurrió el 7 de mayo de 2019.

Fue un ataque de ransomware, específicamente utilizando una variante llamada "RobbinHood". El ransomware cifró los archivos de la ciudad y exigió un rescate para desbloquearlos, el ataque paralizó los sistemas informáticos de la ciudad, lo que afectó no solo al Sistema de Salud, sino también a otros servicios esenciales, incluyendo el sistema de gestión de emergencias 911. La ciudad quedó prácticamente inmovilizada durante un tiempo.

Baltimore era susceptible a este tipo de ataque debido a sus prácticas de TI y a la falta de seguridad adecuada en sus sistemas informáticos. Las autoridades de Baltimore se negaron a pagar el rescate exigido por los ciberdelincuentes. En cambio, optaron por reconstruir sus sistemas y restaurar los datos desde copias de seguridad⁴².

8.1.8 Ataque a la Universidad de Miami En junio de 2021, la Universidad de Miami anunció un ataque de ransomware que afectó a su sistema de salud. Accellion, proveedor de servicios de nube a nivel mundial con sede en Silicon Valley, fue objeto de un ciberataque a finales del año anterior, pero se prolongó hasta principios de 2021. Las entidades públicas y privadas afectadas entre ellas universidad de miami todavía están lidiando con los efectos en de cierta manera.

8.1.9 Ataque a LabCorp Labor, una de las mayores empresas de pruebas médicas de los Estados Unidos, sufrió un ataque de ransomware que afectó sus sistemas y operaciones. Laboratory Corporation of America Holdings o LabCorp tiene 60.000 empleados en todo el mundo, participa en ensayos clínicos en casi 100 países y procesa aproximadamente 2,5 millones de pruebas por semana. Esto significa que LabCorp gestiona y almacena datos altamente confidenciales relacionados con la salud de millones de personas. Como puedes imaginar, cuando la empresa anunció que había detectado "actividad sospechosa" en su red informática, las reacciones no fueron precisamente positivas. La gente está realmente asustada por la información sobre su salud. Resulta que no tenían mucho de qué preocuparse. La noticia llegó el lunes cuando la compañía presentó un 8-K ante la Comisión de Bolsa y Valores. El documento no dice mucho, aparte de que, durante el fin de semana, algunas computadoras y servidores de LabCorp se comportaron de manera inusual. Aunque la presentación sugirió que el equipo de TI de la empresa no tenía idea del problema al que se enfrentaban en ese momento, muchos sistemas se cerraron para evitar daños reales.

⁴² MARTÍNEZ, ana. El peligro de conectarlo todo: una ciudad lleva un mes «hackeada» por un peligroso «ransomware». [En línea] 10 de 06 de 2020. [Fecha de consulta: 28 de septiembre de 2023]. disponible en: https://www.abc.es/tecnologia/redes/abci-baltimore-ciudad-lleva-hackeada-peligroso-ransomware-robbinhood-201906070334_noticia.html.

8.1.10 Sistema de salud pública en Finlandia. Ataque al sistema de salud pública de Finlandia en 2020: En diciembre de 2020, se descubrió que el sistema de salud pública de Finlandia había sido objeto de un ciberataque masivo. Los atacantes accedieron a información confidencial de los pacientes y a datos de salud⁴³.

8.1.11 Ataque al Hospital Universitario Düsseldorf Un ataque de ransomware paralizó las operaciones del hospital y, lamentablemente, resultó en la muerte de un paciente cuando tuvo que ser redirigido a otro centro médico debido a la incapacidad del hospital para proporcionar atención de emergencia.

8.1.12 Ataque a Centene Corporation En enero de 2020, la aseguradora de salud Centene Corporation anunció que un disco duro con datos médicos de pacientes desapareció, lo que podría haber sido un ciberataque.

8.1.13 Ataque a WannaCry Este ataque de ransomware se propagó globalmente, afectando a hospitales y sistemas de salud en varios países. Los sistemas de atención médica en el Reino Unido, en particular, se vieron gravemente afectados.

8.1.14 Ataque al Sistema de Salud de Irlanda En mayo de 2021, el Sistema de Salud de Irlanda fue víctima de un ciberataque importante que afectó sus servicios médicos.

8.1.15 Ataque al Sistema de Salud de Nueva Zelanda En agosto de 2021, el Sistema de Salud de Nueva Zelanda fue blanco de un ciberataque que afectó sus operaciones.

Tomando en cuenta los ataques anteriores y para culminar con el objetivo número uno de la monografía podemos encontrar que las siguientes vulnerabilidades son las más comunes y recurrentes en los sistemas del sector salud:

- Ransomware⁴⁴: El ransomware es un tipo de malware que cifra los archivos del sistema y exige un rescate para restaurarlos. Los ciberdelincuentes pueden utilizar el ransomware para cifrar los registros médicos de los pacientes o los sistemas de información de los hospitales y exigir un rescate para desbloquearlos.

⁴³ BUSINESS WORLD Philippine healthcare among most vulnerable to attacks — Kaspersky [En línea]. - 23 de septiembre de 2022. - [Fecha de consulta: 28 de febrero de 2023]. disponible <https://www.bworldonline.com/top-stories/2022/09/23/476285/philippine-healthcare-among-most-vulnerable-to-attacks-kaspersky/>.

⁴⁴ AVAST. ¿Qué es el malware y cómo protegerse de los ataques? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.avast.com/es-es/c-malware>.

- Vulnerabilidades en el Factor Humano: El factor humano es una de las principales fuentes de vulnerabilidades en el sector de la salud. Los errores humanos, como la falta de conciencia sobre la ciberseguridad y el descuido en el manejo de contraseñas, pueden exponer sistemas a amenazas.
- Tráfico Malicioso a la Red: La infiltración de tráfico malicioso a las redes de atención médica es una amenaza constante. Los atacantes pueden intentar acceder a información confidencial o interrumpir servicios críticos.
- Phishing⁴⁵: El phishing es una táctica común utilizada para engañar a los usuarios y obtener acceso a sistemas de salud. Los correos electrónicos falsos y los sitios web fraudulentos son herramientas comunes en ataques de phishing.
- Sistemas Operativos Vulnerables: Los sistemas operativos obsoletos o sin parches representan un alto riesgo en el sector de la salud. Estas vulnerabilidades pueden ser explotadas por atacantes para acceder a datos críticos.
- Vulnerabilidades en Redes de Proveedores de Atención Médica⁴⁶: Las redes de proveedores de atención médica a menudo tienen vulnerabilidades persistentes, lo que las hace objetivos atractivos para los ciberataques.
- Aumento de Ciberataques⁴⁷: El sector de la salud ha experimentado un aumento significativo en los ciberataques en los últimos años, con un 74% más de ataques registrados.

En conclusión, el sector salud es un objetivo importante para los ciberdelincuentes, y hay numerosos casos de ciberataques en Colombia y en todo el mundo que han afectado a organizaciones de salud y a los datos de sus pacientes. Estos ataques pueden tener graves consecuencias para la seguridad y privacidad de la información de los pacientes, así como para la continuidad de los servicios de salud. Por lo tanto, es importante que las organizaciones de salud tomen medidas adecuadas para proteger sus sistemas y datos, incluyendo la implementación de medidas de seguridad cibernética y la educación y concientización de los empleados sobre la importancia de la seguridad de la información. Además, es fundamental que las

⁴⁵ AVAST. ¿Qué es el malware y cómo protegerse de los ataques? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.avast.com/es-es/c-malware>.

⁴⁶ INISEG. Ciberseguridad sanitaria al descubierto: vulnerabilidades y tendencias [En línea] – 26 de mayo de 2020 - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.iniseg.es/blog/ciberseguridad/ciberseguridad-sanitaria-al-descubierto-vulnerabilidades-y-tendencias/>.

⁴⁷ ACHC. Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad [En línea] – febrero de 2024 - [Fecha de consulta: 25 de marzo de 2024]. disponible en: <https://revistahospitalaria.org/enportada/ciberseguridad-en-el-sector-salud-un-compromiso-moral-legal-y-de-sostenibilidad/#:~:text=Asimismo%2C%20seg%C3%BAAn%20el%20Cyber%20Security,incidentes%20de%20todas%20las%20industrias.>

organizaciones estén preparadas para responder a un posible ciberataque y tengan un plan de contingencia en caso de que ocurra.

9. EXAMINAR LOS CASOS QUE SE HAN PRESENTADO EN EL SECTOR SALUD Y PROTECCIÓN SOCIAL POR MEDIO DE LAS LECTURAS REALIZADAS Y COMPARAR CUALES HAN SIDO LAS VULNERABILIDADES MÁS RECURRENTES PARA PENETRAR ESTOS SISTEMAS.

Como solución al objetivo número dos del presente trabajo se determina que el ataque más utilizado por los ciberdelincuentes para penetrar en los sistemas son las backdoors o puertas traseras en las cuales encuentran fácilmente vulnerabilidades y los ransomware porque estos delincuentes tienen como objetivo conseguir sumas de dinero a cambio de recuperar la información que secuestraron de la empresa con este tipo de ataque que se llevó a cabo como fue el caso de AUDIFARMA a la cual le estaban pidiendo una suma de dinero y si no se cumplían las demandas se iban a hacer públicas la información sensible de pacientes, usuarios y empleados que los ciberdelincuentes tenían en su poder.

El sector salud es uno de los sectores más vulnerables a los ciberataques debido a la gran cantidad de información confidencial y sensible que se maneja en este sector. A continuación, se presentan algunos de los ciberataques comunes que pueden afectar al sector salud:

9.2.1 Ransomware⁴⁸: El ransomware es un tipo de malware que cifra los archivos del sistema y exige un rescate para restaurarlos. Los ciberdelincuentes pueden utilizar el ransomware para cifrar los registros médicos de los pacientes o los sistemas de información de los hospitales y exigir un rescate para desbloquearlos.

9.2.2 Phishing⁴⁶: El phishing es una técnica que utilizan los ciberdelincuentes para engañar a los usuarios y conseguir información confidencial, como nombres de usuario y contraseñas. En el sector salud, los ciberdelincuentes pueden enviar correos electrónicos falsos que parecen provenir de organizaciones legítimas, como hospitales o proveedores de seguros médicos, para obtener información confidencial.

9.2.3 Ataques de denegación de servicio (DoS)⁴⁶: Los ataques de denegación de servicio (DoS) consisten en inundar un servidor o una red con tráfico malintencionado para hacer que el sistema se vuelva inaccesible. Los ciberdelincuentes pueden utilizar este tipo de ataque para inutilizar los sistemas de información de los hospitales y hacer que los pacientes no puedan recibir atención médica.

⁴⁸ AVAST. ¿Qué es el malware y cómo protegerse de los ataques? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.avast.com/es-es/c-malware>.

9.2.4 Backdoor⁴⁹: Un backdoor (puerta trasera) es un método oculto y no autorizado para acceder a un sistema informático, aplicación o dispositivo sin pasar por los procedimientos de autenticación y seguridad habituales. Esencialmente, un backdoor es una vulnerabilidad intencional o no intencional que permite a un usuario remoto o malintencionado acceder a un sistema o red sin la necesidad de identificación o autenticación.

9.2.5 Ataques a dispositivos médicos⁵⁰: Los dispositivos médicos, como los marcapasos y los monitores de signos vitales, pueden ser hackeados y controlados de forma remota por los ciberdelincuentes. Esto puede poner en peligro la vida de los pacientes y comprometer la seguridad del hospital.

9.2.6 Ataques a sistemas de gestión de datos⁵¹: Los sistemas de gestión de datos, como los sistemas de información de pacientes y los sistemas de gestión de registros médicos electrónicos, pueden ser atacados por los ciberdelincuentes para acceder a información confidencial. Los datos de los pacientes pueden ser robados o alterados, lo que puede poner en peligro su seguridad y su privacidad.

Estos son algunos de los ciberataques más comunes que pueden afectar al sector salud. Es importante que las organizaciones del sector salud implementen medidas de seguridad robustas para proteger sus sistemas y datos sensibles.

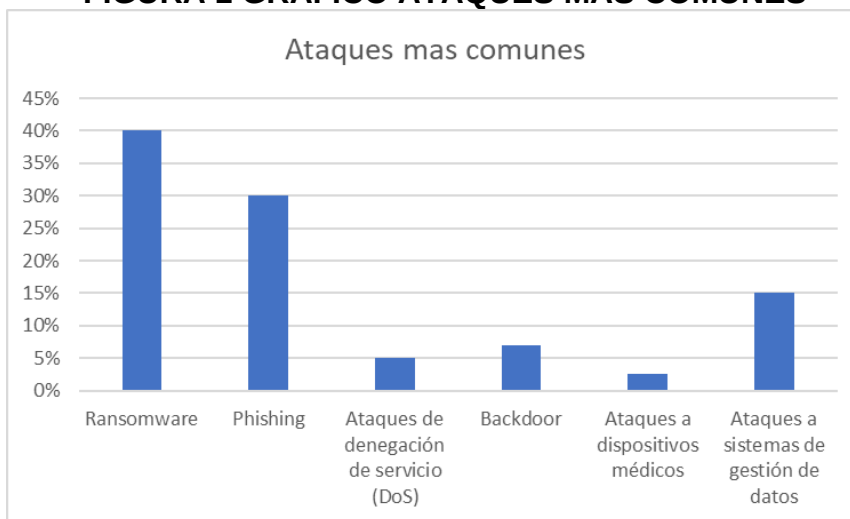
A continuación, se presenta un gráfico que muestra una pequeña estadística derivada de la investigación realizada en cada ataque investigado en el sector salud.

⁴⁹ GÓMEZ, Juan Armando. 2023. ¿Qué es un Backdoor o Puerta Trasera?: 5 consejos para evitarlos. [En línea] 2023. <https://www.deltaprotect.com/blog/backdoor-o-puerta-trasera>.

⁵⁰ UNIVERSIDAD VERACRUZANA. 2019. Noti_infosegura: ¿Cuáles son las principales motivaciones de ataque a dispositivos médicos? [En línea] 29 de 09 de 2019. [Citado el: 21 de 09 de 2023.] https://www.uv.mx/infosegura/general/noti_ataques-3/.

⁵¹ Geekflare Editorial. 2023. Las amenazas más peligrosas para las bases de datos y cómo prevenirlas. [En línea] 14 de 09 de 2023. [Citado el: 21 de 09 de 2023.] <https://geekflare.com/es/database-threats-and-prevention-tools/>.

FIGURA 1 GRAFICO ATAQUES MÁS COMUNES



Nota. La imagen nos muestra un gráfico de los ciberataques más comunes en el sector salud. Tomado de. El autor

10. COMPARAR LOS MARCOS DE CIBERSEGURIDAD QUE SE USAN EN COLOMBIA RESPECTO A EUROPA Y AMÉRICA, POR MEDIO DE LAS LEYES QUE RIGEN LAS INFRAESTRUCTURAS CRÍTICAS DE CADA PAÍS O CONTINENTE, PARA PODER OBSERVAR CUALES SON LOS PUNTOS FUERTES O DÉBILES DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS IC DEL SECTOR SALUD Y PROTECCIÓN SOCIAL EN COLOMBIA

En términos generales, los marcos de ciberseguridad en Colombia, Europa y América comparten varios aspectos comunes, pero también hay algunas diferencias importantes en cuanto a las leyes y regulaciones que rigen la protección de las infraestructuras críticas (IC) y la seguridad de la información en el sector de la salud y protección social.

10.3.1 Colombia. En Colombia, la Ley 2033 de 2020 establece los criterios para la identificación y protección de las infraestructuras críticas y establece las obligaciones de los operadores críticos en cuanto a la seguridad de la información y la gestión de riesgos. Esta ley se enfoca en la protección de las infraestructuras críticas en sectores como energía, comunicaciones, transporte, servicios financieros, entre otros, pero no especifica aspectos de ciberseguridad en el sector de la salud y protección social⁵².

10.3.2 Europa. En Europa, la Directiva de Seguridad de las Redes y Sistemas de Información (NIS, por sus siglas en inglés) establece un marco de ciberseguridad para las infraestructuras críticas de los estados miembros de la Unión Europea. La NIS exige que los proveedores de servicios esenciales y los operadores de infraestructuras críticas tomen medidas adecuadas para gestionar los riesgos de seguridad cibernética y notifiquen los incidentes de ciberseguridad a las autoridades competentes. En el sector de la salud y protección social, la NIS se aplica a los proveedores de servicios sanitarios y farmacéuticos, y también a los proveedores de servicios sociales esenciales, tales como hogares de ancianos y servicios de atención domiciliaria⁵³.

10.3.3 América. En América, en los Estados Unidos existe la Ley de Protección de la Infraestructura Crítica de la Nación (CIPA, por sus siglas en inglés), que establece un marco para la protección de las infraestructuras críticas en los sectores público y privado, incluyendo el sector de la salud y protección social. La CIPA exige que

⁵² OCHGROUP ¿Cuáles son los marcos de referencia para la seguridad de la información (ciberseguridad)? [En línea]. - 16 de febrero de 2023. - [Fecha de consulta: 28 de febrero de 2023]. - disponible en: <https://www.ochgroup.co/cuales-son-los-marcos-de-referencia-para-la-seguridad-de-la-informacion-ciberseguridad/>.

⁵³ COMISION EUROPEA El marco de certificación de la ciberseguridad de la UE [En línea]. - 7 de junio de 2022. - [Fecha de consulta: 28 de febrero de 2023]. - disponible en: <https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-certification-framework>.

los proveedores de servicios críticos adopten medidas de seguridad apropiadas y notifiquen los incidentes de ciberseguridad a las autoridades competentes⁵⁴.

A continuación, se muestra una tabla en la cual se comparan los puntos fuertes y débiles, así como las mejoras que debe tomar cada país o continente para sus marcos de ciberseguridad:

TABLA 1 DE COMPARACIÓN ENTRE COLOMBIA, EUROPA Y EEUU

PAÍS	PUNTOS FUERTES	PUNTOS DÉBILES	MEJORAS
COLOMBIA	Legislación y Regulación: Colombia ha avanzado en la creación de leyes y regulaciones relacionadas con la ciberseguridad. El Decreto Único 1078 es un ejemplo de la normativa que establece pautas para la seguridad de la información. Participación en Iniciativas Globales: Colombia ha	Brecha en la Implementación: A pesar de los avances en la legislación, la implementación efectiva de medidas de ciberseguridad en las empresas y organizaciones aún enfrenta desafíos. Muchas empresas carecen de la infraestructura y los recursos necesarios. Falta de Recursos Humanos Especializados: Colombia enfrenta	Capacitación y Educación Continua: Colombia debe invertir en la formación y capacitación de profesionales en ciberseguridad. Esto incluye la promoción de programas académicos especializados y la formación continua para mantenerse al día con las últimas tendencias y amenazas cibernéticas. Coordinación Interinstitucional: Es fundamental mejorar la coordinación entre

⁵⁴ COMISION FEDERAL DEL COMERCIO Marco de ciberseguridad del NIST [En línea]. - 2023. - [Fecha de consulta: 28 de febrero de 2023]. disponible en: <https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist>.

	participado en iniciativas globales de ciberseguridad y ha trabajado en colaboración con organismos internacionales para fortalecer su postura en este campo. Creación de Conciencia: Se han llevado a cabo campañas de concienciación sobre ciberseguridad para educar a la población y las empresas sobre las amenazas cibernéticas y las mejores prácticas. Colaboración Público-Privada: Existe una colaboración	una escasez de profesionales altamente capacitados en ciberseguridad, lo que dificulta la protección efectiva contra las amenazas cibernéticas. Amenazas Emergentes: Las amenazas cibernéticas evolucionan constantemente, y Colombia debe estar preparada para enfrentar nuevas y avanzadas formas de ataques. Coordinación Interinstitucional: Aunque ha habido avances, la coordinación entre diversas instituciones gubernamentales y	las diferentes instituciones gubernamentales y privadas involucradas en ciberseguridad. Una mayor colaboración permitirá una respuesta más efectiva ante incidentes cibernéticos y una estrategia integral. Protección de Infraestructura Crítica: Colombia debe priorizar la protección de su infraestructura crítica, como sistemas de energía, agua, transporte y salud, contra ciberataques. Esto requiere estándares de seguridad más altos y una vigilancia constante.
--	---	--	---

	creciente entre el gobierno y el sector privado en Colombia para abordar los desafíos de ciberseguridad de manera conjunta.	privadas en Colombia puede ser un desafío en la lucha contra las amenazas cibernéticas.	Políticas y Regulaciones Actualizadas: El marco legal y regulatorio de ciberseguridad debe mantenerse actualizado para abordar las amenazas en constante evolución. Se deben establecer regulaciones claras y efectivas para empresas y organizaciones. Concienciación Pública: Promover la concienciación sobre ciberseguridad entre la población es esencial. Campañas educativas pueden ayudar a reducir el riesgo de caer en trampas cibernéticas y mejorar la higiene digital.
--	--	--	---

			Inversión en Tecnologías de Seguridad: El gobierno y las empresas deben invertir en tecnologías de seguridad avanzadas, como sistemas de detección de intrusiones y análisis de amenazas, para identificar y mitigar riesgos de manera proactiva. Respuesta a Incidentes Mejorada: Desarrollar un plan de respuesta a incidentes sólido y efectivo es esencial. Esto garantizará una reacción rápida y coordinada cuando ocurran ciberataques. Colaboración Internacional: Colombia debe seguir colaborando a nivel
--	--	--	---

			internacional en la lucha contra el cibercrimen y la ciberseguridad. Esto incluye la cooperación con organismos internacionales y otros países para abordar amenazas cibernéticas transfronterizas. Evaluación de Riesgos Continua: Realizar evaluaciones periódicas de riesgos cibernéticos ayudará a identificar nuevas amenazas y vulnerabilidades, permitiendo una acción preventiva. Promoción de la Ciberseguridad en las Empresas: Fomentar que las empresas implementen medidas de ciberseguridad sólidas es esencial. Esto podría
--	--	--	---

			incluir incentivos para la adopción de mejores prácticas de seguridad.
Observaciones	Colombia ha avanzado en el desarrollo de su marco de ciberseguridad, pero aún enfrenta desafíos, especialmente en la implementación efectiva y la capacitación de recursos humanos especializados. La ciberseguridad es un campo en constante evolución, y Colombia debe seguir fortaleciendo sus capacidades para protegerse contra las amenazas cibernéticas en curso y emergentes.		
PAÍS	PUNTOS FUERTES	PUNTOS DÉBILES	MEJORAS
EEUU	Amplia Adopción: El NIST Cybersecurity Framework ha sido ampliamente adoptado tanto en el sector público como en el privado en Estados Unidos. Esto ha contribuido a la estandarización de prácticas de ciberseguridad en todo el país.	No Obligatorio: Aunque ampliamente adoptado, el marco no es obligatorio por ley. Las organizaciones pueden optar por no implementarlo, lo que limita su alcance y efectividad. Necesidad de Recursos: Implementar el NIST Framework requiere	Coordinación Interinstitucional Reforzada: Mejorar la coordinación entre agencias gubernamentales, sectores público y privado, y organismos de aplicación de la ley para una respuesta más eficiente a incidentes cibernéticos. Actualización de Regulaciones:

	Flexibilidad y Adaptabilidad: El marco es flexible y se puede adaptar a diversas organizaciones y sectores. Esto permite a las empresas personalizar sus enfoques de ciberseguridad según sus necesidades y riesgos específicos. Enfoque Basado en Riesgos: El NIST Framework se basa en la evaluación de riesgos, lo que significa que las organizaciones pueden priorizar sus esfuerzos de ciberseguridad en función de las amenazas y	recursos considerables, tanto en términos de tiempo como de inversión. Las pequeñas empresas pueden encontrarlo desafiante. Evolución Continua: Dado que la ciberseguridad es un campo en constante evolución, el marco debe actualizarse regularmente para mantenerse al día con las amenazas emergentes. Enfoque Nacional: Aunque es sólido a nivel nacional, puede no ser tan relevante para organizaciones con operaciones internacionales, ya que no aborda	Mantener las regulaciones de ciberseguridad actualizadas para abordar nuevas amenazas y tecnologías emergentes, promoviendo la adopción de mejores prácticas en todas las industrias. Mayor Inversión en Investigación y Desarrollo: Destinar más recursos a la investigación y desarrollo en ciberseguridad para impulsar la innovación y mantenerse a la vanguardia de las tecnologías de defensa cibernética. Fortalecimiento de la Educación en Ciberseguridad: Fomentar programas
--	--	---	---

	vulnerabilidades más relevantes. Colaboración Público-Privada: Fomenta la colaboración entre el gobierno y el sector privado para abordar las amenazas cibernéticas de manera conjunta.	adecuadamente las cuestiones de ciberseguridad a nivel global.	educativos que preparen a profesionales altamente calificados en ciberseguridad y ciber inteligencia. Mayor Concienciación Pública: Lanzar campañas de concienciación pública para educar a los ciudadanos sobre las amenazas cibernéticas y promover prácticas de seguridad en línea. Protección de Infraestructura Crítica: Priorizar la protección de infraestructuras críticas, como energía, agua y sistemas de salud, con medidas de seguridad avanzadas. Colaboración Internacional Reforzada: Fortalecer
--	--	---	---

			la cooperación internacional en la lucha contra el cibercrimen y las amenazas cibernéticas transnacionales. Evaluación de Riesgos Continua: Realizar evaluaciones periódicas de riesgos cibernéticos para identificar nuevas amenazas y vulnerabilidades. Mayor Inversión en Ciber resiliencia: Fomentar la adopción de estrategias de ciber resiliencia que permitan a las organizaciones recuperarse rápidamente de los ciberataques. Desarrollo de Estrategias Nacionales de
--	--	--	--

			Ciberseguridad: Definir estrategias nacionales de ciberseguridad claras y orientadas a objetivos para guiar los esfuerzos de protección cibernética del país. Inversión en Capacidades Ofensivas y Defensivas: Desarrollar capacidades tanto ofensivas como defensivas para disuadir a los adversarios cibernéticos y defender las redes nacionales.
Observaciones	el Marco de Ciberseguridad del NIST tiene numerosos puntos fuertes que lo han convertido en un estándar líder en Estados Unidos. Sin embargo, también presenta desafíos, como su falta de obligatoriedad y la necesidad de adaptación continua a un entorno cibernético cambiante.		

CONTINENTE	PUNTOS FUERTES	PUNTOS DÉBILES	MEJORAS
EUROPA	Regulación Avanzada: Europa cuenta con regulaciones avanzadas en ciberseguridad, como el Reglamento General de Protección de Datos (GDPR) y la Directiva NIS, que establecen altos estándares de seguridad y privacidad. Cooperación Internacional: La Unión Europea (UE) promueve la cooperación internacional en ciberseguridad a través de agencias como ENISA y participa	Brecha en Capacidades: A pesar de los avances, Europa aún enfrenta una brecha en la disponibilidad de profesionales de ciberseguridad altamente calificados. Amenazas Cibernéticas en Evolución: Las amenazas cibernéticas están en constante evolución, lo que requiere una adaptación continua de las medidas de seguridad. Ciberseguridad: Existe una desigualdad en la madurez de ciberseguridad entre	Coordinación Transfronteriza: Europa debe mejorar la coordinación entre los países miembros para abordar amenazas cibernéticas transfronterizas de manera más efectiva. Esto incluye compartir información sobre incidentes y colaborar en la respuesta. Estandarización: Establecer estándares comunes de ciberseguridad en toda la UE para garantizar que todas las organizaciones cumplan con un nivel mínimo de seguridad cibernética. Formación Continua: Fomentar la formación y capacitación continua

	activamente en foros globales de ciberseguridad. Inversión en Investigación: Europa invierte en investigación y desarrollo en ciberseguridad, fomentando la innovación y el avance tecnológico en este campo. Ecosistema de Empresas de Ciberseguridad: Europa alberga un creciente ecosistema de empresas de ciberseguridad que ofrecen soluciones avanzadas para la protección de datos y sistemas.	los países de la UE, con algunos más avanzados que otros. Dependencia de Tecnología Extranjera: Europa depende en gran medida de tecnología y soluciones de ciberseguridad extranjeras, lo que plantea preocupaciones sobre la soberanía tecnológica. Amenazas Geopolíticas: Europa está sujeta a amenazas cibernéticas relacionadas con tensiones geopolíticas, lo que puede poner en riesgo la seguridad cibernética.	en ciberseguridad para profesionales y ciudadanos, lo que ayudará a cerrar la brecha de habilidades y aumentar la concienciación sobre ciberseguridad. Programas Educativos: Integrar la educación en ciberseguridad en los programas escolares desde edades tempranas para cultivar una cultura de ciberseguridad desde la juventud. Investigación e Innovación: Aumentar la inversión en investigación y desarrollo en ciberseguridad para promover la innovación y el desarrollo de
--	--	--	---

	Enfoque en la Educación Cibernética: Se promueve la educación y concienciación en ciberseguridad, formando a profesionales altamente capacitados en este campo.		tecnologías avanzadas de ciberseguridad. Planes de Continuidad: Fomentar la implementación de planes de continuidad de negocio y recuperación ante desastres que aborden los aspectos cibernéticos, garantizando la capacidad de recuperación frente a ataques. Alianzas Estratégicas: Fomentar la colaboración entre el sector público y privado para compartir información, mejores prácticas y recursos en tiempo real. Adaptación a Amenazas
--	---	--	---

			Emergentes: Mantener el marco regulatorio actualizado y flexible para adaptarse a las amenazas cibernéticas en constante evolución. Concienciación Pública: Realizar campañas de concienciación pública sobre ciberseguridad para empoderar a los ciudadanos a proteger sus datos y dispositivos. En resumen, Europa ha tomado medidas significativas en ciberseguridad, pero es crucial seguir mejorando la coordinación, la capacitación, la inversión en investigación y la cooperación público-privada para fortalecer aún más el marco de ciberseguridad y
--	--	--	---

			proteger a la región de amenazas cibernéticas en constante evolución.
Observaciones	Europa ha logrado avances significativos en ciberseguridad con regulaciones sólidas y colaboración internacional, pero aún enfrenta desafíos relacionados con la capacitación de profesionales y la evolución de las amenazas cibernéticas. La ciberseguridad continúa siendo una prioridad en la agenda europea.		

En cuanto a los puntos fuertes y débiles de la seguridad de la información en las IC del sector salud y protección social en Colombia, es importante destacar que Colombia está en proceso de fortalecer su marco regulatorio y normativo en ciberseguridad, por lo que se espera que se puedan implementar medidas de seguridad más efectivas en el futuro. No obstante, la falta de una ley específica que regule la seguridad de la información en el sector salud y protección social puede ser considerado un punto débil. Además, es importante destacar que, en Colombia, al igual que en otros países de la región, se han reportado incidentes de ciberseguridad en el sector salud, lo que evidencia la necesidad de implementar medidas más efectivas de protección de la información y la infraestructura crítica en este sector.

11. ESTABLECER UNAS BUENAS PRÁCTICAS DE MEJORAMIENTO EN LA CIBERSEGURIDAD PARA EL SECTOR SALUD Y PROTECCIÓN SOCIAL PRIORIZANDO EN LAS VULNERABILIDADES MÁS COMUNES QUE SE ENCUENTREN A LO LARGO DE LA INVESTIGACIÓN CON EL FIN DE DETERMINAR LOS ASPECTOS EN QUE SE DEBE ENFOCAR ÉSTE.

11.1 BUENAS PRÁCTICAS PARA PREVENIR RANSOMWARE⁵⁵

El ransomware es una amenaza cibernética grave, pero puedes tomar medidas para prevenirlo:

11.1.1 Mantén tus sistemas actualizados: Actualiza regularmente tu sistema operativo y software de seguridad. Las actualizaciones a menudo corrigen vulnerabilidades que los ciberdelincuentes podrían aprovechar.

11.1.2 Usa software de seguridad confiable: Instala y mantén actualizado un software antivirus y antimalware de calidad. Esto ayudará a detectar y bloquear amenazas antes de que causen daño.

11.1.3 Realiza copias de seguridad: Haz copias de seguridad regulares de tus datos importantes. Almacenar copias fuera de línea o en la nube puede ser útil si tus archivos se cifran.

11.1.4 Sé cauteloso con los correos electrónicos: Evita abrir correos electrónicos sospechosos o hacer clic en enlaces o archivos adjuntos desconocidos. El phishing es una forma común de distribuir ransomware.

11.1.5 Navega de forma segura: Utiliza navegadores seguros y evita sitios web no confiables. Algunos ransomware se distribuyen a través de sitios web maliciosos o descargas.

11.1.6 Restringe privilegios de usuario: No otorgues a los usuarios más acceso del necesario. Limita los derechos de administrador para reducir el impacto de un ataque.

11.1.7 Educación en seguridad: Capacita a tus empleados sobre la seguridad cibernética y el reconocimiento de amenazas. La concienciación es clave para evitar ataques.

⁵⁵ CLOUDFLARE Cómo prevenir los ataques de ransomware [En línea]. - [Fecha de consulta: 06 de 06 de 2024.]- disponible en: <https://www.cloudflare.com/es-es/learning/security/ransomware/how-to-prevent-ransomware/#:~:text=C%C3%B3mo%20prevenir%20los%20ataques%20de,ransomware%20acaben%20con%20una%20red..>

11.1.8 Filtrado de contenido web: Utiliza sistemas de filtrado de contenido web para bloquear el acceso a sitios web maliciosos conocidos.

11.1.9 Control de aplicaciones: Implementa políticas de control de aplicaciones para evitar la ejecución de software no autorizado.

11.1.10 Monitoreo constante: Supervisa activamente tus sistemas en busca de comportamientos inusuales que puedan indicar un ataque.

11.2 BUENAS PRÁCTICAS PARA PREVENIR PHISHING⁵⁶

El phishing es una amenaza cibernética común, pero puedes protegerte y prevenirlo siguiendo estas buenas prácticas:

11.2.1 Educación en Seguridad: Capacita a tus empleados y a ti mismo sobre cómo reconocer correos electrónicos y mensajes sospechosos. La concienciación es fundamental.

11.2.2 Verifica la Identidad: Antes de proporcionar información confidencial, verifica la identidad del remitente. Comprueba la dirección de correo electrónico y el dominio de la página web.

11.2.3 Mantén el Software Actualizado: Actualiza regularmente tu software de seguridad y sistema operativo para estar protegido contra las últimas amenazas.

11.2.4 Utiliza Autenticación de Dos Factores (2FA): Habilita la 2FA en tus cuentas en línea para añadir una capa adicional de seguridad.

11.2.5 No Hagas Clic en Enlaces Sospechosos: Evita hacer clic en enlaces de correos electrónicos no solicitados o sospechosos. En su lugar, visita el sitio web oficial directamente.

11.2.6 No Descargues Archivos Adjuntos Desconocidos: Los archivos adjuntos pueden contener malware. Descarga solo archivos de fuentes de confianza.

11.2.7 Cuidado con los Mensajes de Urgencia: Los estafadores a menudo crean una sensación de urgencia. Mantén la calma y verifica la autenticidad del mensaje.

11.2.8 Usa Soluciones de Seguridad: Emplea soluciones de seguridad, como filtros de correo electrónico y software antivirus, que puedan detectar y bloquear correos de phishing.

⁵⁶ HSIEH, Jerry 10 consejos prácticos para que los empleados prevengan los ataques de phishing [En línea]. - SPLASHTOP. - [Fecha de consulta: 06 de 06 de 2024.] - <https://www.splashtop.com/es/blog/10-tips-employees-prevent-phishing>.

11.2.9 Reporta Correos de Phishing: Si recibes un correo de phishing, repórtalo a tu equipo de seguridad de TI o al proveedor de correo electrónico.

11.2.10 Comprueba las Fuentes de Información: Verifica la autenticidad de las fuentes de noticias y sitios web antes de proporcionar información personal.

11.3 BUENAS PRÁCTICAS PARA PREVENIR ATAQUES DE DENEGACIÓN DE SERVICIO (DOS)⁵⁷

Los ataques de Denegación de Servicio (DoS) pueden paralizar tus servicios en línea. Aquí hay buenas prácticas para prevenirlos:

11.3.1 Monitoreo Continuo: Establece sistemas de monitoreo para detectar patrones de tráfico inusuales y posibles ataques DoS.

11.3.2 Firewalls y Filtros: Utiliza firewalls y filtros de red para bloquear tráfico malicioso y limitar el acceso no autorizado.

11.3.3 Balanceo de Carga: Implementa balanceo de carga para distribuir el tráfico de manera uniforme y evitar la sobrecarga de servidores.

11.3.4 Actualizaciones de Software: Mantén todo el software, incluyendo sistemas operativos y aplicaciones, actualizado con parches de seguridad.

11.3.5 Ancho de Banda Suficiente: Asegúrate de tener suficiente ancho de banda para manejar picos inesperados de tráfico.

11.3.6 DDoS Mitigation Services: Considera la posibilidad de contratar servicios de mitigación DDoS de terceros que puedan filtrar el tráfico malicioso antes de que llegue a tu red.

11.3.7 Plan de Respuesta: Desarrolla un plan de respuesta a incidentes para actuar rápidamente en caso de un ataque DoS.

11.3.8 Educa a tu Personal: Capacita a tu equipo para reconocer signos de un ataque DoS y cómo responder adecuadamente.

⁵⁷ INCIBE Medidas de prevención contra ataques de denegación de servicio [En línea]. - 07 de 09 de 2019. - [Fecha de consulta: 06 de 06 de 2024.] - disponible en <https://www.incibe.es/empresas/blog/medidas-prevencion-ataques-denegacion-servicio>.

11.3.9 Restringe el Acceso: Limita el acceso a servicios críticos solo a usuarios autorizados.

11.3.10 Respuesta Automatizada: Utiliza soluciones de respuesta automática que puedan mitigar automáticamente los ataques DoS.

11.3.11 Backup de Datos: Realiza copias de seguridad regulares de tus datos para protegerlos de la pérdida en caso de un ataque exitoso.

11.3.12 Distribución de DNS: Utiliza servidores DNS distribuidos para evitar que un ataque DoS afecte tu resolución de nombres.

11.4 BUENAS PRÁCTICAS PARA PREVENIR ATAQUES BACKDOOR⁵⁸

Los ataques backdoor son una seria amenaza para la seguridad cibernética. Aquí te presento algunas buenas prácticas para prevenirlos:

11.4.1 Mantén el Software Actualizado: Mantén todos tus sistemas operativos, aplicaciones y software actualizados con los últimos parches de seguridad para cerrar posibles vulnerabilidades utilizadas para instalar backdoors.

11.4.2 Firewalls y Antivirus: Utiliza firewalls y software antivirus confiables para detectar y bloquear amenazas antes de que lleguen a tu sistema.

11.4.3 Auditoría de Acceso: Realiza auditorías regulares para rastrear actividades sospechosas en tu red y sistemas. Identifica y elimina cualquier acceso no autorizado.

11.4.4 Control de Acceso: Implementa políticas de control de acceso para limitar quién puede acceder a sistemas y datos críticos.

11.4.5 Seguridad en la Autenticación: Utiliza autenticación fuerte, como contraseñas complejas y autenticación de dos factores, para proteger el acceso a cuentas y sistemas.

11.4.6 Educación en Seguridad: Capacita a tus empleados sobre prácticas de seguridad cibernética, incluyendo cómo reconocer posibles ataques de phishing que podrían llevar a la instalación de backdoors.

11.4.7 Monitoreo Continuo: Establece sistemas de monitoreo de seguridad que puedan detectar comportamientos anómalos y alertar sobre posibles amenazas.

⁵⁸ JOVANOVIĆ ana What Is a Backdoor & How to Prevent Backdoor Attacks [En línea]. - 05 de 06 de 2024. -[fecha de consulta 06 de 06 de 2024.] - disponible en: <https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/>.

11.4.8 Pruebas de Penetración: Realiza pruebas de penetración regulares para identificar y corregir posibles vulnerabilidades antes de que los atacantes las exploten.

11.4.9 Seguridad en el Desarrollo: Si desarrollas software, sigue prácticas seguras de codificación y realiza revisiones de seguridad.

11.4.10 Actualizaciones de Firmware: Actualiza el firmware de tus dispositivos y routers para protegerlos de posibles vulnerabilidades que los atacantes podrían aprovechar para instalar backdoors.

11.4.11 Política de Respuesta a Incidentes: Prepara una política de respuesta a incidentes para actuar eficazmente en caso de un ataque. Esto incluye la identificación, mitigación y eliminación de backdoors.

11.4.12 Evaluación de Terceros: Si trabajas con proveedores externos, asegúrate de que sigan buenas prácticas de seguridad cibernética para evitar la introducción de backdoors en tu entorno.

11.5 Buenas Prácticas para Prevenir Ataques a Dispositivos Médicos⁵⁹

La seguridad de los dispositivos médicos es crucial para proteger la integridad de los pacientes y garantizar la continuidad de los servicios de atención médica. Aquí hay algunas buenas prácticas para prevenir ataques a dispositivos médicos:

11.5.1 Actualización de Firmware y Software: Mantén actualizados los firmware y software de tus dispositivos médicos para incluir las últimas correcciones de seguridad. Esto es fundamental para cerrar posibles vulnerabilidades.

11.5.2 Aislamiento de Red: Separa los dispositivos médicos de la red principal o utiliza redes virtuales privadas (VPN) para reducir el riesgo de acceso no autorizado.

11.5.3 Autenticación Fuerte: Implementa autenticación de usuarios y contraseñas robustas en los dispositivos médicos para evitar el acceso no autorizado.

11.5.4 Auditorías de Seguridad: Realiza auditorías periódicas de seguridad en tus dispositivos médicos para identificar y abordar posibles vulnerabilidades.

⁵⁹ CROTHALL How to Protect Medical Devices From Cyberattacks [En línea]. - [Fecha de consulta: 06 de 06 de 2024.] - <https://www.crothall.com/blog/how-to-protect-medical-devices-from-cyberattacks/>.

11.5.5 Control de Acceso Físico: Limita el acceso físico a los dispositivos médicos solo al personal autorizado.

11.5.6 Formación del Personal: Capacita al personal médico y técnico en prácticas seguras de ciberseguridad y cómo reconocer posibles amenazas.

11.5.7 Seguridad en la Cadena de Suministro: Verifica la seguridad de los dispositivos médicos desde la cadena de suministro hasta la implementación para evitar dispositivos comprometidos.

11.5.8 Gestión de Incidentes: Desarrolla un plan de respuesta a incidentes que incluya medidas específicas para tratar los ataques a dispositivos médicos.

11.5.9 Monitorización Continua: Establece sistemas de monitorización continua para detectar comportamientos inusuales en los dispositivos médicos que podrían indicar un ataque.

11.5.10 Actualización de Políticas: Revise y actualiza regularmente las políticas de seguridad de dispositivos médicos para mantenerse al día con las amenazas emergentes.

11.5.11 Colaboración: Colabora con fabricantes, proveedores de atención médica y reguladores para compartir información sobre amenazas y mejores prácticas.

11.5.12 Cumplimiento Normativo: Asegúrate de cumplir con los requisitos normativos específicos para dispositivos médicos, como HIPAA en los Estados Unidos.

11.6 BUENAS PRÁCTICAS PARA PREVENIR ATAQUES A SISTEMAS DE GESTIÓN DE DATOS⁶⁰

La seguridad de los sistemas de gestión de datos es esencial para proteger la confidencialidad, integridad y disponibilidad de la información crítica de una organización. Aquí están algunas buenas prácticas para prevenir ataques a estos sistemas:

11.6.1 Actualización Regular: Mantén todos los sistemas y software de gestión de datos actualizados con las últimas correcciones de seguridad para proteger contra vulnerabilidades conocidas.

⁶⁰ ESCUELA EUROPEA DE EXCELENCIA 10 mejores prácticas de ciberseguridad para las organizaciones [En línea]. - 18 de 11 de 2020. - [Fecha de consulta: 06 de 06 de 2024.] - disponible en: <https://www.escolaeuropeaexcelencia.com/2020/11/10-mejores-practicas-de-ciberseguridad-para-las-organizaciones/>.

11.6.2 Control de Acceso: Implementa una rigurosa gestión de acceso, asegurando que solo el personal autorizado tenga acceso a datos sensibles. Utiliza autenticación de dos factores cuando sea posible.

11.6.3 Encriptación de Datos: Utiliza encriptación para proteger los datos tanto en reposo como en tránsito. Esto garantiza que los datos sean ilegibles para cualquier persona no autorizada.

11.6.4 Auditorías de Seguridad: Realiza auditorías de seguridad periódicas para identificar y abordar posibles debilidades en los sistemas de gestión de datos.

11.6.5 Copias de Seguridad: Implementa un plan de copias de seguridad regulares y pruebas de recuperación de desastres para garantizar la disponibilidad de los datos en caso de un ataque.

11.6.6 Firewalls y Seguridad Perimetral: Configura firewalls y otras medidas de seguridad perimetral para proteger los sistemas de gestión de datos contra ataques externos.

11.6.7 Formación del Personal: Proporciona formación en ciberseguridad a los empleados para que estén al tanto de las mejores prácticas y de cómo reconocer posibles amenazas.

11.6.8 Política de Contraseñas Fuertes: Implementa políticas de contraseñas sólidas que requieran contraseñas complejas y cambios regulares.

11.6.9 Monitorización Continua: Establece sistemas de monitorización para detectar actividad inusual o sospechosa en tiempo real.

11.6.10 Gestión de Parches: Gestiona y aplica de manera proactiva parches de seguridad en todos los sistemas y software.

11.6.11 Control de Dispositivos Extraíbles: Limita o prohíbe el uso de dispositivos de almacenamiento extraíbles no autorizados en sistemas de gestión de datos críticos.

11.6.12 Cumplimiento Normativo: Asegúrate de cumplir con las regulaciones de protección de datos relevantes, como el RGPD en la Unión Europea.

En conclusión, el sector salud debe tomar medidas proactivas para proteger la información y datos sensibles de sus pacientes contra los ciberataques. Al implementar buenas prácticas de seguridad cibernética, como la concientización y capacitación del personal, el fortalecimiento de la seguridad de la red, la protección de datos, las pruebas de penetración, el respaldo y recuperación de datos, y la colaboración con las autoridades de ciberseguridad, el sector salud puede reducir

los riesgos de ciberataques y proteger la privacidad y confidencialidad de los datos de sus pacientes. Al hacerlo, el sector salud puede mantener la confianza de sus pacientes y brindar atención médica segura y de calidad en un entorno digital cada vez más complejo.

12. CONCLUSIONES

El actual trabajo identificó las diferentes metodologías de ciberataques más usuales que se han dado entre el 2018 al 2023 en Colombia, la importancia de estar al tanto las metodologías que manejan los ciberdelincuentes que perturban a el pueblo colombiano, ya que, recurrentemente estos ciberataques se han transformado en un dolor de cabeza para la comunidad. Los colombianos no están preparados para este tipo de ciberataques por falta de comprensión, esta investigación se brinda teniendo en cuenta los artículos y escritos, así como entrevistas que han realizado los medios y personas familiarizadas con estos ataques que trabajan en este ámbito, ya que, la mayoría de las personas que trabajan en el sector salud se conectan a internet y manipulan sus redes, pero, no tienen en cuenta las instrucciones para una buena práctica de los sistemas poniendo así en riesgo el sistema de la empresa dándole vía libre a los delincuentes cibernéticos.

La seguridad informática es un tema crítico en la actualidad debido al creciente número de ciberataques que afectan a empresas, organizaciones y usuarios finales. Es esencial que las empresas y organizaciones implementen medidas de seguridad adecuadas para proteger sus sistemas y datos confidenciales, y que los usuarios finales tomen medidas para proteger sus dispositivos y redes domésticas. Algunas de las medidas de seguridad que se pueden implementar incluyen el uso de contraseñas seguras y la autenticación multifactorial, la instalación de software de seguridad y actualizaciones de seguridad regulares, la implementación de políticas de acceso y permisos de usuario, y la educación de los empleados y usuarios finales sobre los riesgos y las mejores prácticas de seguridad. Además, es importante tener en cuenta que los ciberataques no solo pueden afectar a los sistemas informáticos y los datos confidenciales, sino también a los dispositivos médicos, los sistemas de control industrial y otros sistemas críticos que pueden tener un impacto directo en la seguridad y la vida de las personas.

En resumen, la seguridad informática es un tema crítico que afecta a todas las industrias y a la sociedad en general. Es esencial que se tomen medidas para proteger los sistemas y los datos confidenciales, y que se eduque a los empleados y usuarios finales sobre los riesgos y las mejores prácticas de seguridad para prevenir los ciberataques.

los marcos de ciberseguridad en Colombia, Europa y América tienen similitudes en cuanto a la protección de las infraestructuras críticas y la seguridad de la

información, pero también existen diferencias importantes en cuanto a las leyes y regulaciones que rigen en cada región. En Colombia, la Ley 2033 de 2020 establece los criterios para la identificación y protección de las infraestructuras críticas, pero no se enfoca específicamente en el sector de la salud y protección social. Mientras que en Europa y los Estados Unidos, existen leyes específicas que regulan la protección de las infraestructuras críticas en este sector. En cuanto a los puntos fuertes y débiles de la seguridad de la información en las IC del sector salud y protección social en Colombia, se destaca la necesidad de implementar medidas más efectivas de protección de la información y la infraestructura crítica en este sector, teniendo en cuenta que se han reportado incidentes de ciberseguridad. En general, se puede concluir que la ciberseguridad es un tema prioritario a nivel global, y que cada vez más países están adoptando marcos regulatorios y normativos para proteger sus infraestructuras críticas y garantizar la seguridad de la información. Es importante que se continúe avanzando en esta materia, y que se promueva la colaboración y el intercambio de experiencias entre países para mejorar la protección frente a las amenazas cibernéticas.

el sector salud debe estar altamente comprometido en garantizar la seguridad de los datos y la información de sus pacientes ante los constantes riesgos de ciberataques. La implementación de buenas prácticas como la concientización y capacitación del personal, el mantenimiento y fortalecimiento de la seguridad de la red, la protección de datos, las pruebas de penetración, el respaldo y recuperación de datos y la colaboración y coordinación con las autoridades de ciberseguridad son esenciales para prevenir y mitigar los riesgos de ciberataques. Al aplicar estas buenas prácticas, el sector salud puede proteger la privacidad y confidencialidad de los datos de sus pacientes y mantener la confianza en su capacidad para brindar atención médica segura y de calidad.

13.RECOMENDACIONES

Tras un exhaustivo análisis de la literatura especializada y los datos recopilados durante los últimos cinco años, se ha identificado un patrón alarmante de vulnerabilidades en el sector salud y protección social en Colombia. estas vulnerabilidades abarcan desde fallos en la infraestructura tecnológica hasta deficiencias en los protocolos de seguridad informática.

la comparación de casos en el sector ha revelado vulnerabilidades recurrentes, como la falta de actualizaciones de software y la deficiente capacitación del personal en ciberseguridad. estas debilidades son explotadas repetidamente por los actores malintencionados, comprometiendo la integridad de los sistemas de salud y protección social.

al contrastar los marcos de ciberseguridad entre Colombia, Europa y América, se ha observado una brecha significativa en la implementación y cumplimiento de normativas. mientras que Europa muestra una regulación más robusta, Colombia carece de medidas efectivas para proteger sus infraestructuras críticas en el sector de la salud.

en vista de estos hallazgos, se recomienda implementar medidas urgentes de mejoramiento en la ciberseguridad del sector salud y protección social en Colombia. esto incluye la actualización constante de sistemas, la capacitación continua del personal y la adopción de estándares internacionales de seguridad informática.

mantener los dispositivos actualizados: es fundamental instalar regularmente las actualizaciones de software y firmware en los dispositivos, ya que estas suelen incluir parches de seguridad que protegen contra vulnerabilidades conocidas.

utilizar una red privada virtual (vpn): emplear una vpn al conectarse a internet añade una capa adicional de seguridad al cifrar la conexión y ocultar la dirección ip, lo que dificulta que los hackers rastreen las actividades en línea o accedan a datos sensibles.

ser prudente con los correos electrónicos y enlaces sospechosos: evitar abrir correos electrónicos de remitentes desconocidos o enlaces que parezcan sospechosos, ya que pueden ser phishing, malware o ataques de ingeniería social diseñados para robar datos personales o infectar dispositivos.

En respuesta a las crecientes amenazas de ciberseguridad, se han desarrollado diversas estrategias para mitigar riesgos y proteger los sistemas críticos en el sector de salud y protección social en Colombia. La implementación de políticas de acceso restringido y la utilización de contraseñas seguras y dinámicas son fundamentales para evitar accesos no autorizados y asegurar la integridad de la información.

Además, se destaca la importancia de realizar copias de seguridad regulares y garantizar el borrado seguro de la información cuando ya no sea necesaria. Estas medidas aseguran que los datos puedan recuperarse en caso de un incidente y que la información sensible no quede expuesta a posibles brechas de seguridad.

La formación continua del personal en ciberseguridad es otro pilar esencial. La capacitación en el reconocimiento de intentos de phishing, la correcta gestión de contraseñas y el uso seguro del correo electrónico puede reducir significativamente el riesgo de ataques exitosos. Este enfoque proactivo fomenta una cultura de seguridad dentro de las organizaciones.

Finalmente, la adopción de tecnologías de seguridad avanzadas, como la autenticación de dos factores y el uso de redes privadas virtuales (VPN), proporciona capas adicionales de protección. Estas herramientas dificultan que los atacantes puedan acceder a los sistemas y datos sensibles, reforzando así la seguridad general de las infraestructuras críticas.

BIBLIOGRAFÍA

ACKTIB. Los Ciberdelincuentes: Quiénes son, qué hacen y por qué lo hacen. [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://acktib.com/blog-los-ciberdelincuentes-quienes-son-que-hacen-y-por-que-lo-hacen/>.

AGUILERA CRUZ, Roberto. 4 aspectos clave para cuidar la ciberseguridad en las empresas de salud [En línea]. - 4 de agosto de 2022. - [Fecha de consulta: 24 de abril de 2023]. disponible en: https://www.ey.com/es_mx/health-sciences-wellness/ciberseguridad-en-las-empresas-de-salud.

AGUIRRE QUEZADA, Juan Pablo. Ciberseguridad, desafío para México y trabajo legislativo [En línea]. - marzo de 2022. - [Fecha de consulta: 28 de febrero de 2023]. disponible en: <http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5551/Cuaderno%20de%20Investigaci%C3%B3n%2087.pdf?sequence=1&isAllowed=y>.

ALFARO, Ivan. Claves para un monitoreo de ciberseguridad efectivo [En línea]. - 23 de agosto de 2021. - [Fecha de consulta: 24 de abril de 2023]. <https://www.b-secure.co/blog/claves-para-un-monitoreo-de-ciberseguridad-efectivo>.

AUDIFARMA. Ataque cibernético a infraestructura tecnológica de Audifarma [En línea]. - 23 de enero de 2023. - [Fecha de consulta: 15 de febrero de 2023]. disponible en: <http://audifarmaapp.com/comunicado-general-ciberataque-audifarma/>.

AVAST. ¿Qué es el malware y cómo protegerse de los ataques? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.avast.com/es-es/c-malware>.

BANCO PICHINCHA. ¿Qué hacen los hackers y qué tipos existen? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.pichincha.com/blog/que-es-un-hacker>.

BUSINESS WORLD. Philippine healthcare among most vulnerable to attacks — Kaspersky [En línea]. - 23 de septiembre de 2022. - [Fecha de consulta: 28 de febrero de 2023]. disponible <https://www.bworldonline.com/top-stories/2022/09/23/476285/philippine-healthcare-among-most-vulnerable-to-attacks-kaspersky/>.

CANO, Jeimy. Industria de la salud y TI [En línea] // Industria de la salud y TI. - 18 de noviembre de 2018. - [Fecha de consulta: 19 de febrero de 2023]. disponible en:

https://www.researchgate.net/publication/329222111_Seguridad_y_Ciberseguridad_en_los_dispositivos_medicos.

CANO, Jeimy Seguridad y Ciberseguridad en los dispositivos médicos [En línea]. - 18 de noviembre de 2018. - [Fecha de consulta: 18 de febrero de 2023]. disponible en:

https://www.researchgate.net/publication/329222111_Seguridad_y_Ciberseguridad_en_los_dispositivos_medicos.

CATRIL OPAZO, Juan Eduardo, et al. NIST cybersecurity framework in south America: Argentina, Brazil, Chile, Colombia, And Uruguay. 2021. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://repositorio.uchile.cl/handle/2250/184569>

CIBERNOS GRUPO La ciberseguridad es cosa de todos: buenas prácticas para empleados [En línea]. – 2023. - [Fecha de consulta: 28 de febrero de 2023]. disponible en: <https://www.grupocibernos.com/blog/ciberseguridad-buenas-practicas-empleados>.

CISTERNELLI, eric 7 Cybersecurity Frameworks That Help Reduce Cyber Risk [En línea]. - 31 de marzo de 2023. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk>.

COMISIÓN EUROPEA El marco de certificación de la ciberseguridad de la UE [En línea]. - 7 de junio de 2022. - [Fecha de consulta: 28 de febrero de 2023]. - disponible en: <https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-certification-framework>.

COMISIÓN FEDERAL DEL COMERCIO Marco de ciberseguridad del NIST [En línea]. - 2023. - [Fecha de consulta: 28 de febrero de 2023]. disponible en: <https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist>.

DRAEGER Conectividad segura y protegida [En línea] // Conectividad segura y protegida. - 1 de JUNIO de 2020. - [Fecha de consulta: 14 de febrero de 2023]. disponible en: <https://www.draeger.com/Library/Content/safe-and-secure-connectivity-br-PDF-10446-es.pdf>.

ECS ENISA introduces the European Cybersecurity Skills Framework [En línea]. - 23 de septiembre de 2022. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://ecs-org.eu/enisa-introduces-the-european-cybersecurity-skills-framework/>.

EKRAN 12 Cybersecurity Best Practices & Measures to Prevent Cyber Attacks in 2023 [En línea]. - 15 de marzo de 2023. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://www.ekransystem.com/en/blog/best-cyber-security-practices>.

EL COLOMBIANO Hackearon la cuenta de Twitter de la ministra de Salud, Carolina Corcho [En línea]. - 26 de noviembre de 2022. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://www.elcolombiano.com/colombia/hackearon-cuenta-de-twitter-de-la-ministra-de-salud-carolina-corcho-DN19143752>.

FORTRA Gestión de vulnerabilidades: qué es, procesos y buenas prácticas [En línea]. - 27 de julio de 2022. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://www.fortra.com/es/blog/gestion-vulnerabilidades>.

GÓMEZ, Juan Armando. 2023. ¿Qué es un Backdoor o Puerta Trasera?: 5 consejos para evitarlos. [En línea] 2023. <https://www.deltaprotect.com/blog/backdoor-o-puerta-trasera>.

GONZÁLEZ RODRÍGUEZ, Javier, et al. Lo humano y lo tecnológico en medicina [En línea] // Lo humano y lo tecnológico en medicina. - 2018 de noviembre de 2018. - [Fecha de consulta: 10 de febrero de 2023]. disponible en: https://www.researchgate.net/publication/329222111_Seguridad_y_Ciberseguridad_en_los_dispositivos_medicos.

HUBSPOT. Seguridad informática: qué es, tipos y características. [En línea] 08 de 05 de 2023. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://blog.hubspot.es/website/que-es-seguridad-informatica>.

INTEREMPRESAS Los ciberataques al sector sanitario se multiplican por seis en un año [En línea]. - 23 de marzo de 2023. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://www.interempresas.net/Ciberseguridad/Articulos/471124-Los-ciberataques-al-sector-sanitario-se-multiplican-por-seis-en-un-ano.html>.

JAIMOVICH, Desirée Los 14 tipos de ciberataques más comunes (y cómo prevenirlos) [En línea]. - 25 de octubre de 2022. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://blog.invgate.com/es/tipos-de-ciberataque>.

KASPERSKY What is Data Encryption? [En línea]. - 2023. [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://www.kaspersky.com/resource-center/definitions/encryption>.

LESMES DIAZ, Laura ¿Qué pasa con la ciberseguridad en las plataformas de salud de Colombia? [En línea]. - 24 de enero de 2023. --[Fecha de consulta: 23 de abril de 2023]. disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-las-plataformas-de-salud-de-colombia-736510>.

LONDOÑO, Íngrid 5 buenas prácticas de ciberseguridad que debes conocer [En línea]. - 28 de octubre de 2020. - [Fecha de consulta: 24 de abril de 2023]. disponible en: <https://www.piranirisk.com/es/blog/5-buenas-practicas-de-ciberseguridad-que>

[debe-conocer?hs_amp=true&utm_term=&utm_campaign=Matriz+de+Riesgos+-+General+-+Julio+2022&utm_source=adwords&utm_medium=ppc&hsa_acc=9508207643&hsa_cam=17802451156&hsa_grp=138377008](https://economy.com.co/debe-conocer?hs_amp=true&utm_term=&utm_campaign=Matriz+de+Riesgos+-+General+-+Julio+2022&utm_source=adwords&utm_medium=ppc&hsa_acc=9508207643&hsa_cam=17802451156&hsa_grp=138377008).

LÓPEZ, José francisco. Sector Privado. [En línea] 17 de MAYO de 2019. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://economipedia.com/definiciones/sector-privado.html>.

MANCUZO, gabriel. ¿Qué es un riesgo en Ciberseguridad? Definición y tipos. [En línea] 12 de JULIO de 2023. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://ciberseguridadtips.com/que-es-un-riesgo-en-ciberseguridad-definicion-causas/>.

MINTIC. Brecha Digital. [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.mintic.gov.co/portal/inicio/5467:Brecha->.

MOLSEN, Hannes Conectividad segura y protegida [Entrevista]. - 1 de JUNIO de 2020. - [Fecha de consulta: 14 de febrero de 2023].

MORALES ROJAS, juan gilberto Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial [En línea]. - 2022. -[Fecha de consulta: 15 de febrero de 2023].disponible en: [http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11574/Ataques%20ciberneticos Trabajo%20grado Juan%20Morales v2.pdf?sequence=1&isAllowed=y](http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11574/Ataques%20ciberneticos%20Trabajo%20grado%20Juan%20Morales_v2.pdf?sequence=1&isAllowed=y).

OCHGROUP ¿Cuáles son los marcos de referencia para la seguridad de la información (ciberseguridad)? [En línea]. - 16 de febrero de 2023. - [Fecha de consulta: 28 de febrero de 2023]. - disponible en: <https://www.ochgroup.co/cuales-son-los-marcos-de-referencia-para-la-seguridad-de-la-informacion-ciberseguridad/>.

PORTAFOLIO Lo que se sabe del ataque cibernético a infraestructura de Audifarma [En línea]. - 24 de enero de 2023. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.portafolio.co/negocios/empresas/audifarma-lo-que-se-sabe-del-ataque-cibernetico-a-la-empresa-577384>.

PRENSARIO Los ciberataques: La enfermedad incurable del sector Salud [En línea]. - Prensario, 7 de abril de 2021. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://prensariotila.com/los-ciberataques-la-enfermedad-incurable-del-sector-salud/>.

RAMOS sergio Los ciberataques al sector salud amenazan incluso la vida de los pacientes [En línea]. - 23 de febrero de 2023. - [Fecha de consulta: 28 de febrero de 2023].

2023]. disponible en: <https://socialgeek.co/noticias/los-ciberataques-al-sector-salud-amenazan-incluso-la-vida-de-los-pacientes/>.

RANSOMWARE HELP Ransomware En El Sector Médico: Estadísticas Y Consejos De Seguridad [En línea]. - 2023. - [Fecha de consulta: 23 de abril de 2023]. disponible en: <https://helpransomware.com/es/ransomware-en-el-sector-medico/>.

RICAURTE, Iris Montoya Aumento de ciberataques al sector salud y sus graves consecuencias [En línea] // Aumento de ciberataques al sector salud y sus graves consecuencias. - 20 de FEBRERO de 2023. - [Fecha de consulta: 15 de febrero de 2023]. disponible en: <https://www.ventasdeseguridad.com/2023022023067/noticias/empresas/aumento-de-ciberataques-al-sector-salud-y-sus-graves-consecuencias.html>.

RICO BARRERA, susana maría El Invima es objeto de nuevo ataque cibernético [En línea]. - 4 de octubre de 2022. - [Fecha de consulta: 15 de febrero de 2023]. disponible en: <https://consultorsalud.com/invima-objeto-ataque-cibernetico/>.

SANTANDER. ¿Qué es una vulnerabilidad informática? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20inform%C3%A1tica%2C%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad>.

SHARKOV, George et al. Hybrid Exercising for Cyber-Resilient Healthcare and Cross-Sector Crisis Response Operability, » Sofia, 2021.

SOY EMPRENDEDOR Colombia tuvo más de 20 mil millones de intentos de ciberataques en 2022 [En línea]. - 22 de marzo de 2023. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://soyempreendedor.co/colombia-tuvo-mas-de-20-mil-millones-de-intentos-de-ciberataques-en-2022/9926/>.

SWISSINFO El Seguro Social de Costa Rica sufre ciberataque que afecta a hospitales [En línea]. - 31 de mayo de 2022. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: https://www.swissinfo.ch/spa/costa-rica-ciberataque_el-seguro-social-de-costa-rica-sufre-ciberataque-que-afecta-a-hospitales/47637614.

UNISYS. Ciberataques: lo que debe saber. [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <https://www.unisys.com/es/glossary/what-is-cyber-attack/>.

UNIVERSIDAD NACIONAL DEL LITORAL. ¿QUÉ ES LA TECNOLOGÍA? [En línea] S.F. - [Fecha de consulta: 25 de marzo de 2023]. disponible en: <http://www.unl.edu.ar/ingreso/cursos/cac/21ot/>.

ANEXOS

ANEXO A. LOS CIBERATAQUES A LAS EMPRESAS DE LATINOAMÉRICA Y ESTADOS UNIDOS⁶¹

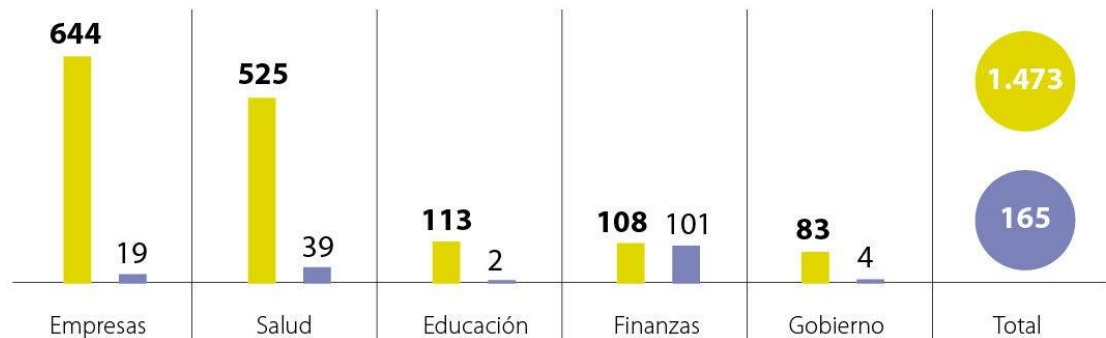
LOS CIBERATAQUES A LAS EMPRESAS EN AMÉRICA LATINA Y ESTADOS UNIDOS

¿CÓMO INGRESÓ EL ATACANTE?



LOS SECTORES IMPACTADOS

■ Número de brechas ■ Datos expuestos (en millones de registros)



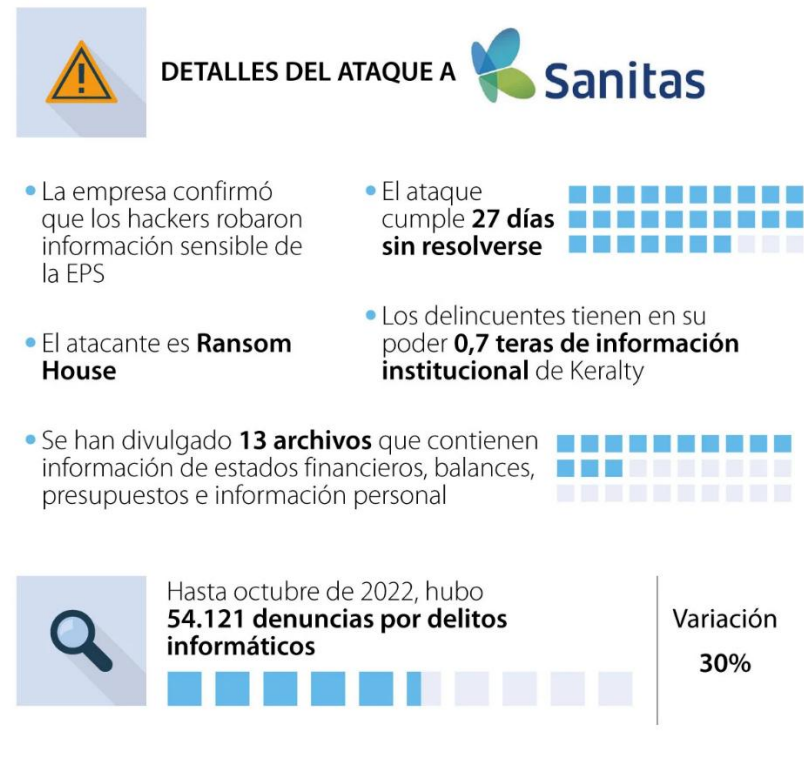
Fuente: 2020 Compromise Flashcard Gráfico: LR-GR

⁶¹ Fuente: LA REPUBLICA ¿Cuánto les ha costado a las empresas latinoamericanas los ciberataques? [En línea]. - 2023. - [Fecha de consulta: 8 de mayo de 2023]. disponible en: <https://mc.net.co/cuanto-les-ha-costado-a-las-empresas-latinoamericanas-los-ciberataques%E2%80%8B/>.

ANEXO B. LAS EMPRESAS QUE HAN SUFRIDO CIBERATAQUES⁶²

LAS EMPRESAS QUE HAN SUFRIDO CIBERATAQUES

Empresa	Fecha	Afectación
	12/diciembre/2022	Afectación del Data Center alterno e implicó un contagio en 25% de la infraestructura
	16/diciembre/2022	Afectó los servicios prepago de energía y agua
	28/noviembre/2022	Imposibilitó que los usuarios pudieran acceder a las citas programadas y medicamentos certificados



Fuente: Centro Cibernético de la Policía Nacional, Cámara Colombiana de Comercio y Telecomunicaciones, Fortinet, NCS, Sonda LR / Gráfico: LR-AL

⁶² Fuente: LA REPUBLICA EPM, Sanitas y AFINIA continúan en jaque por ataque cibernético contra sus sistemas [En línea]. - 22 de diciembre de 2022. - [Fecha de consulta: 8 de mayo de 2023]. disponible en: <https://www.larepublica.co/empresas/epm-sanitas-y-afinia-continuan-en-jaque-por-ataque-cibernetico-contra-sus-sistemas-3513721>.

**ANEXO C. VIDEO DE SUSTENTACIÓN DE LA MONOGRAFÍA PARA
OPTAR POR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD
INFORMÁTICA DE LA UNAD**

<https://youtu.be/Rm9Y48RKWBM>