CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS
RECTORÍA VIRTUAL

ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS

ANÁLISIS DE LA SEGURIDAD DE LA INFORMACIÓN ORGANIZACIÓN PRIVADA IPS MEDELLÍN 2024

Modalidad: Monografía

Autor(s)
CARLOS ALBERTO JIMÉNEZ MARÍN

Director
LUIS ALBERTO CÁRDENAS OTAYA
Maestría en Dirección y Administración de Empresas

MEDELLÍN, COLOMBIA
AGOSTO, 2024

Agradecimientos

Quiero expresar mi más sincero agradecimiento a mi esposa e hijos, quienes me apoyaron incondicionalmente durante este camino hacia mi crecimiento profesional mediante la especialización en gerencia de proyectos. Su comprensión y paciencia fueron fundamentales para que a pesar de mis otras ocupaciones a nivel laboral y familiar pudiera dedicar el tiempo y esfuerzo necesarios a este proyecto. A mis padres, quienes siempre me inculcaron el valor del esfuerzo y la educación, les debo gran parte de este logro. A mi hermana y sobrinos, gracias por su aliento constante y por creer en mis capacidades.

Extiendo mi gratitud al resto de mi familia y de personas allegadas que conocieron de mi incursión en esta carrera, y que con sus palabras de ánimo y apoyo hicieron que este trayecto fuera más llevadero. Hoy puedo decir con orgullo que he alcanzado un objetivo que sinceramente alguna vez consideré como lejano. Gracias a la perseverancia y la resiliencia, he sabido enfrentar y superar los desafíos, demostrando que siempre es posible alcanzar las metas trazadas cuando se trabaja con dedicación y constancia. Este logro es mío y de todos ustedes que estuvieron a mi lado. Gracias por estar conmigo en cada paso de este recorrido y por hacer posible que se cumpliera este sueño.

Resumen

Esta monografía analiza la seguridad de la información en una Institución Prestadora de Servicios de Salud (IPS) en Medellín, cuyo enfoque es la atención a víctimas de violencia sexual y maltrato infantil. La investigación se centra en la evaluación de la infraestructura tecnológica, las políticas de seguridad implementadas y la capacitación del personal en ciberseguridad, con el fin de detectar vulnerabilidades y proponer soluciones efectivas para mejorar la protección de datos confidenciales.

En primer lugar, se introduce el problema de la seguridad de la información en el sector salud, destacando su importancia crítica en un contexto global de creciente ciberataques. La IPS objeto de estudio afronta grandes desafíos debido a la ausencia de políticas internas de seguridad y una marcada dependencia de las políticas externas proporcionadas por los proveedores de servicios mediante aplicaciones en la nube. También, se identifica una inexistencia de capacitación en ciberseguridad del personal, lo que aumenta el riesgo de exposición a amenazas informáticas.

Posteriormente, se lleva a cabo una evaluación del contexto espacial y físico en el que presta sus servicios la IPS, ubicada en un área urbana de Medellín. Identificación de la ausencia de políticas formales de seguridad y la escasa formación del personal. Además, se exploran diversas perspectivas teóricas que permiten comprender mejor la problemática.

El análisis de los resultados obtenidos revela la ausencia de políticas de seguridad de la información dentro de la IPS y una dependencia de las políticas del proveedor externo de historias clínicas. Esta situación deja a la IPS vulnerable a riesgos significativos. La infraestructura tecnológica también presenta deficiencias, como la escasa implementación de medidas de protección (antivirus, firewalls) y la falta de procedimientos para la generación de copias de seguridad. Estos hallazgos destacan la necesidad urgente de implementar un plan integral de seguridad de la información y de mejorar la capacitación en ciberseguridad.

Finalmente, esta monografía presenta un marco de referencia valioso no solo para la IPS, sino también para otras instituciones del sector salud que afronten desafíos similares en materia de seguridad de la información. La propuesta de un plan integral de capacitación y la implementación de políticas de seguridad son la clave para mitigar riesgos y la protección de la

información crítica en un entorno digital cada vez más complejo. La investigación subraya la importancia de una gestión proactiva para fortalecer la seguridad de la información en la organización y garantizar la continuidad operativa en un entorno globalizado.

Palabras clave: ciberseguridad, políticas, infraestructura, capacitación, vulnerabilidades.

Índice

Lista de Figuras

Capítulo 1. Introducción

Actualmente, la seguridad la información es un desafío crucial para las organizaciones del sector salud a nivel mundial. Rápidamente avanza la tecnología y la su vez la implementación de herramientas digitales que han transformado la manera en que se gestionan los datos, aumentando la necesidad de robustecer las medidas de protección para evitar la fuga de información y mitigar los riesgos cibernéticos. Este estudio se enfoca en una IPS privada en Medellín, especializada en la atención a víctimas de violencia sexual y maltrato infantil, que enfrenta desafíos significativos en la seguridad de la información.

De acuerdo con La Organización Panamericana de Salud (OPS), ente regional de la Organización Mundial de la Salud (OMS), ha categorizado a la seguridad de la información como "uno de los ocho principios rectores de la transformación digital del sector de la salud". A su vez, el Banco Mundial recomienda adoptar una serie de medidas para mejorar la resiliencia del sector salud ante ciberataques, entre las que menciona el liderazgo de los Ministerios de Salud y de las autoridades sub nacionales, de manera que propongan legislaciones y regulaciones que promuevan prácticas de ciberseguridad en el sector, tanto respecto a los pacientes, trabajadores, proveedores y operadores de la industria; y la consonancia entre la implementación de medidas de ciberseguridad en salud y los llamados Principios de Desarrollo Digital, específicamente el diseño de usuario, el uso de estándares abiertos, el open data y open source, así como la colaboración internacional (Jarufe Bader, Biblioteca del Congreso Nacional de Chile, 2023).

De acuerdo con (Academia Novasoft, 2023) El auge de conexiones a redes sin seguridad, estaciones de trabajo remotas y la falta de comprensión de esquemas de seguridad tanto por parte de administradores como de empleados, se traduce en un problema crítico. Este problema expone la información a vulnerabilidades que amenazan la confidencialidad de la información propia de la empresa, como la de empleados, proveedores, aliados y de sus usuarios.

La adopción de la tecnología ha impulsado un cambio radical en el sector de la salud en los últimos años. La digitalización de datos y la migración hacia la nube han desencadenado avances de gran envergadura en la atención médica, la investigación y la gestión de la información. No obstante, en paralelo a estas innovaciones, emergen inquietudes relacionadas

con la seguridad y la privacidad de los datos sensibles de los pacientes (Prensario TI Latin America, 2023).

La problemática de la seguridad de la información en esta IPS se presenta en la falta de una infraestructura apropiada, la ausencia de políticas de seguridad efectivas y la falta de capacitación del personal. Estos aspectos combinados generan un ambiente proclive a vulnerabilidades que pueden ser explotadas mediante ciberataques, dejando en riesgo la confidencialidad, integridad y disponibilidad de los datos privados de los pacientes y empleados.

El propósito de este estudio es analizar la efectividad de la infraestructura actual de seguridad de la información, evaluar las políticas implementadas y proponer un plan integral de capacitación para el personal. La relevancia de este estudio radica en su potencial para mejorar las prácticas de ciberseguridad en la IPS, garantizando una mejor protección de los datos y contribuyendo al bienestar de los pacientes y la eficiencia operativa de la organización.

La investigación se enmarca en un contexto global donde la seguridad de la información en el sector salud es una prioridad. Organizaciones como la Organización Mundial de la Salud (OMS) y el Banco Mundial han enfatizado en la importancia de acoger medidas de ciberseguridad en el sector salud para proteger la información de los pacientes y asegurar la continuidad operativa de las instituciones (Jarufe Bader, Biblioteca del Congreso Nacional de Chile, 2023).

En este sentido, este estudio no solo tiene implicaciones locales, sino que también aporta al entendimiento y mejora de las prácticas de ciberseguridad en el sector salud a nivel global.

Además, la implementación de un plan de mejora de ciberseguridad en la IPS de Medellín puede servir como modelo para otras instituciones de salud que enfrentan desafíos similares. La extrapolación de los hallazgos y recomendaciones de este estudio puede guiar a otras organizaciones en la identificación y mitigación de sus propias vulnerabilidades, creando una red de entidades mejor preparadas para enfrentar las amenazas cibernéticas. Así, la mejora de la seguridad de la información no solo beneficiará a la IPS en cuestión, sino que también fortalecerá el sector salud en su totalidad, promoviendo prácticas seguras y resilientes frente a los crecientes desafíos cibernéticos.

La investigación se propone abordar problemas específicos de la IPS privada en Medellín y también contribuir al desarrollo de estrategias y políticas aplicadas a nivel global, mejorando la ciberseguridad en el sector salud y protegiendo a pacientes en todo el mundo. La colaboración y el intercambio de conocimientos en este ámbito son fundamentales para construir un futuro donde la información sanitaria esté adecuadamente protegida contra las amenazas digitales.

También es importante tener en cuenta que de acuerdo con (Cervera García & Goussens, 2024) El sector sanitario es particularmente susceptible a ataques cibernéticos debido a varias razones intrínsecas. La información de salud y los datos sanitarios son extremadamente valiosos para los ciberdelincuentes ya que pueden ser utilizados para el robo de identidad, fraudes médicos o incluso extorsión, tanto a las empresas proveedoras como a los pacientes.

En este contexto, un enfoque integral que abarque políticas, infraestructura y capacitación del personal se presenta como una solución viable. Este enfoque tiene como objetivo superar los desafíos en la seguridad de la información en la IPS privada.

En la organización IPS para víctimas de maltrato, violencias sexuales y/o con afectaciones en su salud mental, ubicada en Medellín, Colombia, se identifica una problemática de alto impacto en relación con la seguridad de la información. Pese a contar con un equipo de 42 profesionales de la salud, compuesta por psicólogos, pediatras, neuropsicólogos, toxicólogos, psiquiatras, trabajadores sociales y auxiliares, a quienes se les ha asignado equipos portátiles para llevar a cabo sus actividades, la corporación carece de una infraestructura de Tecnologías de la Información (TI) especializada.

La ausencia de un área de TI compromete la capacidad de la corporación para establecer y aplicar políticas de seguridad de la información. Este vacío se refleja en la falta de seguridad tanto a nivel de hardware como de software en los equipos asignados, lo que expone la información sensible contenida en las historias clínicas y las claves de acceso a correos electrónicos, entre otros datos confidenciales.

Adicionalmente, se identifica la falta de capacitación de los empleados en cuanto al manejo seguro de la información. El escaso conocimiento específico en este ámbito aumenta el riesgo de posibles brechas de seguridad y pérdida de datos sensibles.

En resumen, la IPS privada enfrenta un desafío integral en la seguridad de la información, abarcando desde la carencia de políticas y medidas de seguridad tecnológicas hasta la necesidad urgente de capacitación para el personal. Esta problemática compromete la integridad, confidencialidad y disponibilidad de los datos manejados por la institución y puede tener implicaciones serias en la calidad de los servicios prestados y la confianza de los usuarios.

Objetivos

Objetivo General

Analizar la efectividad de la infraestructura de la seguridad de la información en la organización privada IPS, enfocada en políticas, medidas tecnológicas y capacitación del personal, con el propósito de que los datos sensibles estén seguros y se cumpla la confidencialidad, seguridad y disponibilidad de la información, dentro del contexto específico de la organización.

Objetivos Específicos

Identificar las políticas existentes relacionadas con la seguridad de la información en la organización privada IPS.

Evaluar la infraestructura tecnológica actual de la organización privada IPS, incluyendo sistemas de seguridad, software antivirus, firewalls y procedimientos de copia de seguridad, para la determinación su nivel de efectividad y su capacidad para protección de la confidencialidad y disponibilidad de la información.

Proponer un plan integral de capacitación para el personal de la organización privada IPS, abordando aspectos clave de seguridad informativa, como el manejo seguro de contraseñas, la identificación de amenazas cibernéticas y los procedimientos de respuesta ante incidentes, para mejorar la conciencia y competencia del personal en ciberseguridad.

Antecedentes

En el contexto de la IPS privada en Medellín, se han identificado dos problemas fundamentales que comprometen la seguridad de la organización: infraestructura deficiente y la ausencia de políticas de seguridad efectivas. Estos aspectos, sumados a la inexistente capacitación del personal en ciberseguridad, incrementan significativamente el riesgo de incidentes de seguridad. La necesidad de abordar estas debilidades es urgente, dado que la literatura reciente subraya la importancia de adoptar un enfoque integral que combine políticas de seguridad, una infraestructura tecnológica robusta y una capacitación continua para mitigar los riesgos cibernéticos.

Estudios recientes acrecientan esta perspectiva, evidenciando que la falta de formación en ciberseguridad es un factor crucial que aporta a la vulnerabilidad de las organizaciones frente a ciberataques. Por lo tanto, implementar un plan integral de capacitación se erige como una medida esencial para mejorar la conciencia y competencia del personal, con el objetivo de salvaguardar la información sensible que se maneja en la IPS.

En uno de esos estudios recientes el autor dice que:

La ciberdelincuencia en el sector salud es una creciente amenaza en la era digital. Con la informatización de registros médicos y la telemedicina en aumento, los ataques cibernéticos pueden tener consecuencias devastadoras. La filtración de datos sensibles o el secuestro de sistemas pueden comprometer la privacidad de los pacientes y poner en peligro la atención médica. Para contrarrestar esta amenaza, se requieren medidas de ciberseguridad sólidas como medida protectora (Cervera García & Goussens, 2024).

El origen de esta problemática y un contexto reciente puede evidenciar que la adopción gradual de nuevas tecnologías de la información ha transformado las actividades y procesos en las organizaciones, generando brechas de seguridad no contempladas. Esto incrementa el riesgo en las operaciones y el control de procesos, haciendo imperativa la utilización de marcos de protección adecuados para alcanzar los objetivos estratégicos organizacionales (Zevallos, 2019).

La implementación de sistemas de gestión de seguridad de la información (SGSI) basados en la norma ISO/IEC 27001 es fundamental para asegurar la integridad, confidencialidad y

disponibilidad de la información. Esta norma proporciona una base común para la elaboración de reglas y un método eficaz de gestión de la seguridad (Revista Innovación y Software, 2023).

Según la Organización Panamericana de la Salud (OPS), ha hecho suyos y adaptado ocho principios que reflejaran los imperativos de la transformación digital del sector de la salud, la evolución de los sistemas de información para la salud y uno de esos principios hace referencia a la seguridad de la información diciendo que, es también imperativo proteger la información de salud sensible y, por consiguiente, es necesario colaborar y crear en conjunto mecanismos para preservar la confidencialidad y la seguridad de la información personal en el entorno de salud pública digital y, simultáneamente, promover el acceso y la transparencia en la información y el conocimiento (Organización Panamericana de la Salud, 2021).

En el comercio electrónico, la seguridad de la información es crucial porque los clientes piden hasta el pago y envío. Esto requiere técnicas específicas para asegurar que no haya filtraciones de datos que puedan perjudicar a los clientes (Revista Innovación y Software, 2023).

Dentro de la literatura especializada, se destacan modelos de gestión de riesgos de seguridad de la información que han evolucionado para incluir metodologías combinadas, como HAZOP y SWIFT. Estas metodologías se basan en la experiencia profesional y la evidencia literaria para enfocarse en riesgos específicos, permitiendo evaluaciones tanto cualitativas como cuantitativas de los riesgos (Zevallos, 2019). Al comparar estos enfoques con la problemática de la IPS, se evidencia que la falta de educación y conciencia sobre la seguridad de la información es una barrera significativa para la protección efectiva de los activos informativos. Esto subraya la necesidad urgente de programas de capacitación y sensibilización dentro de las organizaciones (Zevallos, 2019).

Por ello, implementar un plan integral de capacitación en la IPS es clave para concienciar al personal sobre la importancia de proteger los datos sensibles y establecer políticas de seguridad de la información robustas que protejan la confidencialidad e integridad de los datos. Este plan debe abarcar formación en manejo seguro de contraseñas, identificación de amenazas cibernéticas, y procedimientos de respuesta ante incidentes. A través de una adecuada capacitación y la implementación de políticas sólidas, se podrá mejorar la competencia del

personal en ciberseguridad y garantizar una protección efectiva de la información dentro de la organización.

Otras investigaciones resaltan la importancia crítica de los sistemas de seguridad de la información en las organizaciones del sector salud, donde la protección de los datos es fundamental para asegurar la confidencialidad, integridad y disponibilidad de la información. En Colombia, la implementación de estos sistemas se regula mediante normativas como el Decreto 1008 de 2018 y la Política de Gobierno Digital, que establecen un marco sólido para la gestión de la seguridad informativa en las entidades públicas. Estas normativas están alineadas con estándares internacionales, como la ISO 27001, que ofrece directrices claras sobre la gestión de la seguridad de la información (Llanos Cardona, López, & Mejía Lobo, 2023). La adopción de estas normas no solo responde a un mandato legal, sino que también es una necesidad estratégica para enfrentar los crecientes y complejos riesgos cibernéticos que amenazan la integridad de los sistemas de información en las organizaciones de salud.

En consecuencia, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en las instituciones de salud es innegable, ya que estas manejan un gran volumen de datos sensibles, como historias clínicas, que requieren protección contra accesos no autorizados y otras amenazas. A pesar de los esfuerzos por cumplir con los estándares establecidos, muchas organizaciones aún se encuentran en etapas iniciales de implementación, exponiéndose a vulnerabilidades críticas. Un diagnóstico reciente en una institución hospitalaria reveló un nivel de cumplimiento significativamente bajo, lo que evidencia la necesidad de fortalecer los controles existentes y avanzar hacia la plena implementación de las medidas de seguridad requeridas (Carvajal, Cardona, & Valencia, 2019).

La coyuntura actual, exacerbada por la pandemia y el aumento de la telemedicina, ha incrementado los riesgos de ciberataques, especialmente en un entorno donde la gestión digital de la información médica se ha vuelto la norma. Este contexto subraya la relevancia de establecer medidas rigurosas para proteger la información y evitar su uso indebido o malintencionado (Gutiérrez García, Barrantes Centurión, & Sánchez Silva, 2020).

El análisis de la seguridad de la información en el sector salud entre 2010 y 2021 muestra que la adopción de estándares internacionales ha sido una respuesta efectiva a las crecientes

amenazas de ciberseguridad. Los sistemas de información no solo mejoran la eficiencia en la gestión de historiales clínicos, sino que también juegan un papel crucial en la protección de datos sensibles contra accesos no autorizados y pérdida de información. Estos sistemas, cuando se implementan correctamente, permiten una mayor precisión y fiabilidad en la documentación médica, esencial para la continuidad y calidad del cuidado al paciente. Sin embargo, la revisión de literatura también revela que, a pesar de los avances, todavía existen brechas significativas en la implementación de medidas de seguridad adecuadas, lo que pone de manifiesto la necesidad de continuar fortaleciendo las políticas de seguridad y la capacitación del personal en el manejo de información sensible en el sector salud (Preciado Rodríguez, Valles Coral, & Lévano Rodríguez, 2021).

Finalmente, en un mundo donde el uso de internet es cada vez más prevalente en las actividades cotidianas, es crucial reestructurar la educación en ciberseguridad para proteger a los usuarios de amenazas cada vez más sofisticadas. La prevalencia de técnicas de ataque, como el phishing y el uso de troyanos, subraya la vulnerabilidad de los usuarios frente a ciberdelincuentes que buscan robar información sensible. Tradicionalmente, se ha enseñado a los usuarios a identificar señales de alerta en las URL o sitios web, pero con el avance de la tecnología y la ingeniería social, estas medidas ya no son suficientes (Vilchez Villegas, 2022).

En este sentido, la ciberseguridad organizacional, combinada con la auditoría forense, se presenta como un pilar esencial para garantizar la resiliencia y competitividad de las organizaciones en un entorno globalizado que evoluciona rápidamente. Este enfoque no solo protege los activos de información, sino que también asegura que las organizaciones puedan tomar decisiones informadas a nivel estratégico, táctico y operativo, protegiéndose contra el fraude, la corrupción y otros delitos informáticos que podrían impactar su continuidad y posición en el mercado (Caamaño Fernández & Gil Herrera, 2020).

Capítulo 2. Evaluación

Introducción

Como propósito de este capítulo, se establece el proporcionar una evaluación global de la situación actual de la IPS "Creciendo con Cariño" en relación con la seguridad de la información, partiendo de un análisis contextual y teórico. La seguridad de la información es un aspecto crítico en el sector de la salud, ya que las organizaciones del sector manejan informaciones sensibles que requiere de una protección estricta para evitar accesos no autorizados, pérdidas o variación. Este capítulo se enfoca en la investigación general que busca entender y mejorar la gestión de la seguridad de la información en la IPS, abordando tanto los desafíos presentes como las oportunidades para fortalecer la protección de los datos.

El análisis inicia con la descripción del contexto espacial y físico de la IPS, situada en Medellín, Colombia, una ciudad que se ha afirmado como un centro urbano dinámico y con una infraestructura desarrollada. La ubicación de la IPS en un área urbana como el barrio Conquistadores, caracterizado por su desarrollo y accesibilidad, influye directamente en las operaciones de la organización. La densidad poblacional, la disponibilidad de servicios y la infraestructura local condicionan el entorno operativo de la IPS y cómo se aborda la seguridad de la información.

Después, el capítulo se centra en una evaluación exhaustiva de la situación en estudio, explorando los problemas específicos de la IPS en materia de seguridad de la información. La carencia de políticas formales propias, la dependencia de proveedores externos para la gestión de historias clínicas en la nube, y los incidentes de seguridad como el robo de dispositivos que podrían contener datos sensibles, son algunos de los puntos críticos que se detallarán. Estos problemas no solo reflejan vulnerabilidades existentes, sino que también subrayan la necesidad de una intervención estructurada que aborde estos desafíos de manera efectiva y sostenible.

El análisis también incluye una discusión de las perspectivas teóricas que pueden aplicarse para abordar los problemas identificados. Diferentes teorías y enfoques, como la gestión del riesgo, la seguridad informática y la cultura organizacional, se examinarán para comprender cómo estas perspectivas pueden contribuir para mejorar la seguridad de la

información en la IPS. Este enfoque teórico es fundamental para desarrollar estrategias que no solo aborden las necesidades actuales, sino que también anticipen y mitiguen futuros riesgos.

Finalmente, el capítulo presenta varias opciones de abordaje que podrían implementarse en la IPS en pro de mejorar la seguridad de la información. Estas incluyen la creación de políticas internas de seguridad, la adopción de soluciones tecnológicas avanzadas, la capacitación del personal y la realización de auditorías de seguridad regulares. Estas opciones no solo buscan resolver los problemas actuales, sino también establecer una base sólida para la mejora continua de la seguridad en la organización.

En conjunto, este capítulo pretende dar una visión clara y detallada de la situación actual en la IPS Creciendo con Cariño, y de las posibles soluciones para mejorar la gestión de la seguridad de la información. Al aplicarlo, se pretende ofrecer una guía que permita a la organización tomar decisiones informadas y estratégicas para proteger de manera efectiva los datos sensibles que maneja, asegurando así la confianza y la seguridad de sus operaciones en el futuro.

Contexto Espacial y Físico

La IPS Creciendo con Cariño se encuentra ubicada en Medellín, específicamente en la sede del barrio Conquistadores en la carrera 65 D # 34 21. Medellín es una ciudad conocida por su rápido desarrollo urbano y su posición como centro económico y cultural de Colombia. Con una población aproximada de 2.5 millones de habitantes, se caracteriza por su infraestructura moderna y un alto nivel de acceso a servicios de salud y educación.

La ubicación de la IPS en el barrio Conquistadores, una de las zonas más desarrolladas de la ciudad, le proporciona ciertas ventajas, como el acceso a una infraestructura bien establecida y la proximidad a otros servicios médicos y comerciales. Sin embargo, también presenta desafíos, como la necesidad de adaptarse a un entorno urbano en constante cambio, donde la densidad poblacional y el tráfico pueden afectar la accesibilidad y la seguridad.

Desde el punto de vista económico, Medellín es una de las ciudades más dinámicas de Colombia, con una economía diversificada que incluye sectores como la manufactura, los servicios financieros, el comercio y, cada vez más, la tecnología y la innovación. Este entorno económico genera un contexto favorable para el crecimiento de organizaciones como la IPS

Creciendo con Cariño, que pueden beneficiarse de la disponibilidad de recursos y de un mercado en crecimiento.

No obstante, el crecimiento económico también implica una mayor competencia y la necesidad de que las organizaciones se adapten rápidamente a las nuevas demandas del mercado. En el caso de la IPS, debe prepararse para enfrentar desafíos relacionados con la seguridad de la información, en especial en un entorno donde la digitalización y el uso de tecnologías de la información están aumentando.

En resumen, el contexto espacial y físico de la IPS Creciendo con Cariño en Medellín ofrece oportunidades y desafíos. La IPS debe aprovechar su ubicación estratégica y el entorno económico favorable, mientras se prepara para abordar los riesgos asociados con el crecimiento y la complejidad del entorno urbano.

Situación Objeto de Estudio

La situación actual de la IPS Creciendo con Cariño en relación con la seguridad de la información revela una serie de desafíos importantes que deben ser abordados para asegurar la protección adecuada de los datos sensibles. A partir de las entrevistas y el análisis de la infraestructura de la organización, se identificaron varios problemas específicos que afectan la seguridad de la información.

Uno de los principales problemas es la ausencia de políticas formales de seguridad de la información. La gerente general de la IPS reconoció que no existen políticas propias en este ámbito, y que la organización depende en gran medida de las políticas del proveedor externo de historias clínicas en la nube. Esta dependencia expone a la IPS a riesgos significativos, ya que cualquier falla o brecha en la seguridad del proveedor podría tener consecuencias graves para la protección de la información de los pacientes.

Además, se identificaron incidentes de seguridad relacionados con el robo de computadoras, lo que genera preocupación sobre la posible exposición de datos sensibles. Aunque no se ha confirmado la pérdida de información, estos incidentes subrayan la necesidad de fortalecer las medidas de seguridad física y digital en la organización.

Otro factor clave que afecta la situación es la falta de capacitación y concienciación del personal en temas de seguridad de la información. La falta de formación adecuada puede

resultar en prácticas inseguras y aumentar la vulnerabilidad de la organización ante amenazas cibernéticas. Es clave que la IPS invierta en la educación y capacitación de su personal para fomentar una cultura de seguridad que abarque todos los niveles de la organización.

Por último, la evaluación de la infraestructura tecnológica de la IPS revela que, aunque se usan plataformas en la nube para gestionar historias clínicas, no hay un sistema integral de seguridad de la información que abarque los aspectos de la operación. Esto incluye la protección de otros tipos de datos sensibles, como la información financiera y administrativa, que también deben ser protegidos de manera adecuada.

En conjunto, estos elementos describen una situación en la que la seguridad de la información en la IPS Creciendo con Cariño está comprometida, y donde es necesario implementar medidas correctivas y preventivas para mejorar la protección de los datos y reducir los riesgos asociados.

Perspectivas de Abordaje

Para abordar la problemática de seguridad de la información en la IPS Creciendo con Cariño, es esencial considerar varias perspectivas teóricas que pueden ayudar a comprender y solucionar los desafíos identificados.

Una de las teorías más relevantes en este contexto es la teoría de la gestión del riesgo, que se centra en la identificación, evaluación y mitigación de riesgos en la organización. Esta teoría es útil para entender cómo los riesgos asociados con la seguridad de la información pueden gestionarse eficazmente mediante la implementación de políticas, procedimientos y controles adecuados.

Otra perspectiva teórica importante es la teoría de la seguridad informática, que se enfoca en la protección de los sistemas de información contra amenazas internas y externas. Esta teoría abarca áreas como la criptografía, la seguridad en redes, y la gestión de incidentes de seguridad, proporcionando un marco conceptual para desarrollar soluciones técnicas que protejan los datos sensibles en la IPS.

La teoría de la cultura organizacional es crucial en este contexto, ya que la seguridad de la información depende solo de las medidas técnicas y de la actitud y comportamiento del personal. Inculcar una cultura de seguridad, donde todos los empleados estén comprometidos

con la protección de la información, es clave para reducir las vulnerabilidades y garantizar la eficacia de las políticas de seguridad.

La integración de estas perspectivas teóricas en el análisis de la situación permite desarrollar un enfoque holístico para abordar los desafíos de seguridad en la IPS Creciendo con Cariño. Esto incluye no solo la implementación de soluciones técnicas, sino también la gestión del riesgo y el fortalecimiento de la cultura organizacional.

Opciones de Abordaje

Con base en el análisis previo, se proponen diferentes opciones de abordaje para mejorar la seguridad de la información en la IPS Creciendo con Cariño.

Como primera medida, se recomienda el desarrollo e implementación de políticas internas de seguridad de la información que cubran todos los aspectos de la operación de la IPS. Las políticas deben ser diseñadas basándose en las mejores prácticas internacionales, como las normas ISO/IEC 27001, y deben incluir procedimientos claros para la gestión de riesgos, la protección de datos sensibles, y la respuesta a incidentes de seguridad.

Otra opción es la implementación de soluciones tecnológicas avanzadas, como sistemas de gestión de seguridad de la información (SGSI), que permitan monitorear y proteger de manera continua todos los sistemas y datos de la organización. Esto incluye la encriptación de datos, la autenticación multifactorial, y el uso de firewalls y antivirus de última tecnología.

Además, se propone la diseñar un programa de capacitación y concienciación para el personal, con enfoque en la seguridad de la información. Este programa debe incluir talleres y cursos regulares que eduquen a los empleados sobre las mejores prácticas de seguridad, la identificación de amenazas, y las acciones a tomar en caso de un incidente.

Por último, se sugiere realizar auditorías regulares de seguridad, tanto internas como externas, para evaluar la eficacia de las políticas y soluciones implementadas, y para identificar áreas de mejora continua. Estas auditorías permitirían a la IPS mantenerse al día con las nuevas amenazas y adaptar sus estrategias de seguridad en consecuencia.

Conclusión del Capítulo

En este capítulo, se evaluó la situación actual de la IPS Creciendo con Cariño en relación con la seguridad de la información. Se ha identificado una dependencia excesiva en las políticas de proveedores externos y la falta de políticas internas específicas, lo que representa una vulnerabilidad significativa. Esta situación se agudiza por la insuficiente gestión de incidentes de seguridad, como el robo de dispositivos que contienen información sensible, lo que subraya la necesidad urgente de desarrollar e implementar políticas internas de seguridad de la información.

El análisis del contexto espacial y físico ha revelado que, aunque la IPS en un entorno urbano bien desarrollado ofrece ventajas, también presenta desafíos particulares a considerar en el diseño de estrategias de seguridad. Las características demográficas y económicas de la zona influyen directamente en la efectividad de las medidas de protección de datos, lo que resalta la importancia de adaptar las soluciones a las condiciones locales.

En cuanto a las perspectivas teóricas, la adopción de enfoques basados en la gestión del riesgo y la seguridad informática se ha identificado como crucial para fortalecer la protección de la información. Estas teorías proporcionan un marco sólido para la evaluación y mitigación de riesgos, permitiendo a la IPS desarrollar una cultura organizacional que priorice la seguridad de los datos.

Finalmente, se han propuesto diversas opciones de abordaje, incluyendo la implementación de políticas internas, la adopción de tecnologías avanzadas y la capacitación continua del personal. Estas estrategias no solo abordan las debilidades actuales, sino que también preparan a la organización para enfrentar desafíos futuros de manera más eficaz.

Este análisis establece las bases para el próximo capítulo, donde se examinarán los resultados de la implementación de estas recomendaciones y su impacto en la seguridad de la información, con el objetivo de verificar la efectividad de las estrategias adoptadas y continuar mejorando las capacidades de la organización.

Capítulo 3. Resultados

El primer objetivo de la investigación se centró en identificar las políticas existentes relacionadas con la seguridad de la información dentro de la IPS. Se realizó un cuestionario a 42 empleados de la organización, obteniendo una participación total. Este alto nivel de participación es un indicador del interés significativo por parte del personal en la evaluación de la situación actual de la seguridad de la información. La totalidad de las respuestas proporciona una visión detallada y representativa de las percepciones y conocimientos existentes sobre este tema crítico.

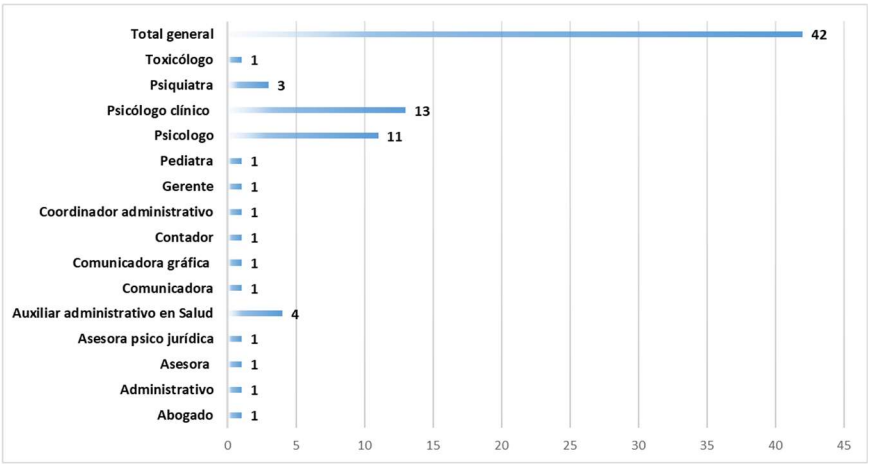


Figura 1. Muestra IPS.

Nota: *Esta figura representa la cantidad de profesionales que participaron en el cuestionario y sus roles en la organización.*

Durante la entrevista con la gerente general de la organización privada IPS, se reveló un hallazgo crucial que subraya una de las principales áreas de mejora dentro de la empresa: la ausencia de políticas formales de seguridad de la información. Este descubrimiento es alarmante, especialmente en un contexto donde la protección de datos sensibles es vital para el funcionamiento seguro y eficiente de cualquier institución, particularmente en el sector salud. La gerente, al reconocer la gravedad de esta omisión, expresó un claro interés en la implementación urgente de tales políticas, afirmando que la protección adecuada de la información es una prioridad no solo para cumplir con las normativas vigentes, sino también para salvaguardar la integridad y confidencialidad de los datos que maneja la organización (Jiménez Marín, 2024).

El hecho de que la gerente general admitiera no conocer política formal de seguridad de la información en la empresa pone en evidencia un vacío significativo en la estrategia de seguridad organizacional. Esta falta de conocimiento y estructura formal en torno a la seguridad de la información expone a la organización a posibles brechas de seguridad y refleja un posible desinterés o falta de prioridad en la implementación de prácticas robustas de protección de datos hasta la entrevista. La inexistencia de políticas claras y estructuradas es un indicador de que la organización ha operado bajo un marco de protección mínimo, confiando en que la falta de incidentes graves hasta la fecha es suficiente para mantener la seguridad.

La falta de políticas formales fue confirmada por la declaración de la gerente al discutir la infraestructura de seguridad de la información. Según sus palabras:

"Nuestras historias clínicas deben estar custodiadas y protegidas según la normativa. En cuanto a la política de seguridad de la información, solo contamos con la política de nuestro proveedor de historia clínica en la nube, que protege exclusivamente las historias clínicas. Actualmente, no tenemos una política propia para la seguridad de la información. Con el crecimiento continuo de nuestra organización, reconocemos la necesidad de implementar políticas de seguridad de la información" (Jiménez Marín, 2024).

De esta declaración se derivan varios hallazgos clave:

Dependencia de políticas externas: La organización confía en las políticas de seguridad del proveedor externo de historias clínicas, lo que significa que la seguridad de la información depende de la eficacia y cumplimiento de estas políticas por parte del proveedor.

Ausencia de políticas internas: La organización carece de políticas internas específicas para la seguridad de la información, lo que deja expuesta a la organización a riesgos que no son cubiertos por el proveedor externo.

Protección limitada a historias clínicas: La política vigente solo protege las historias clínicas, lo que resulta insuficiente para garantizar la seguridad de otros tipos de información sensible.

Reconocimiento de necesidades futuras: La gerente identifica la necesidad de desarrollar e implementar políticas de seguridad de la información, lo que es un paso positivo hacia la mejora de la seguridad organizacional.

Crecimiento y seguridad: La correlación entre el crecimiento de la organización y la necesidad de políticas de seguridad sugiere que el aumento en la cantidad de datos y complejidad de operaciones hace imperativa la adopción de medidas de seguridad más robustas.

Además de los problemas estructurales relacionados con la falta de políticas, la entrevista reveló una división significativa entre los empleados en cuanto a su conocimiento sobre las políticas de seguridad de la información. Este hecho es preocupante, ya que la comprensión común y unificada de las políticas de seguridad es importante para su efectividad. Algunos empleados afirmaron conocer estas políticas, lo que indica que podría haber una falta de comunicación interna o malentendidos sobre lo que realmente existe o está implementado. Por otro lado, aquellos empleados que negaron conocer políticas de seguridad reflejan una desconexión entre la administración y el personal operativo. Este desconocimiento o la mala interpretación de las políticas puede dar lugar a comportamientos que pongan en riesgo la seguridad de la organización, como el uso inadecuado de sistemas o la falta de adherencia a las mejores prácticas de seguridad.

En resumen, la falta de políticas formales de seguridad de la información en la organización IPS representa un riesgo considerable que debe ser abordado con urgencia. La dependencia de políticas externas, la ausencia de protección integral para todos los tipos de datos y la falta de conocimiento uniforme entre los empleados son áreas críticas que requieren atención inmediata. El reconocimiento de la necesidad de políticas de seguridad por parte de la alta gerencia es positivo, pero se necesita una acción para desarrollar e implementar un marco de seguridad robusto adaptado al crecimiento de la organización y proteger adecuadamente los datos sensibles que maneja. La capacitación del personal y la mejora de la comunicación interna serán elementos clave en este proceso, garantizando que todos los empleados comprendan y se adhieran a las nuevas políticas para fortalecer la seguridad organizacional.

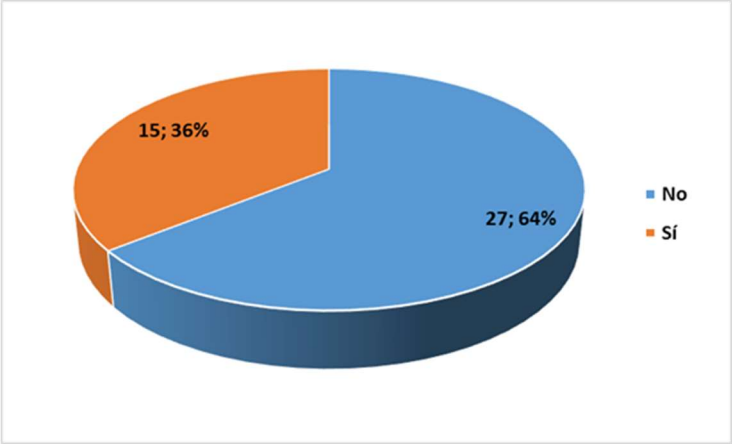


Figura 2. Conocimiento de políticas de seguridad de la información.

Nota: *Esta figura representa la cantidad de profesionales que participaron en el cuestionario y sus roles en la organización.*

El segundo objetivo de la investigación se centró en evaluar la infraestructura tecnológica y los mecanismos de seguridad existentes en la IPS. Este análisis se hizo con una combinación de entrevistas, cuestionarios, revisión documental y observación directa, lo que permitió una visión amplia y detallada de las capacidades y deficiencias actuales en la protección de la información.

Deficiencias en el control y gestión de la protección de datos:

El análisis reveló que la organización carece de políticas de seguridad de la información y de mecanismos adecuados para controlar el acceso de los empleados a los datos sensibles. Esta falta de control expone a la organización a riesgos significativos, ya que no existen lineamientos claros sobre quién puede acceder a qué tipo de información y bajo qué circunstancias.

Desconocimiento de soluciones antivirus:

La mayoría de los empleados no están informados sobre la existencia de soluciones antivirus para proteger la información que procesan, lo que indica una brecha significativa en la comunicación y gestión de las medidas de seguridad. Este desconocimiento podría derivar en prácticas inseguras que comprometan la integridad y confidencialidad de los datos.

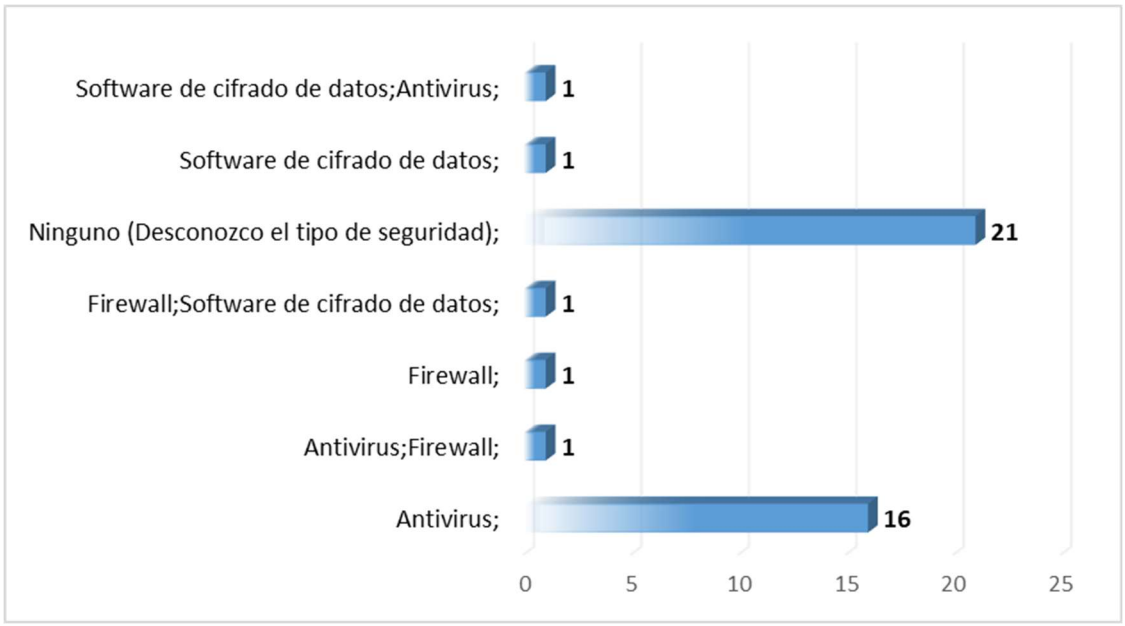


Figura 3. Conocimiento sobre medidas de protección como Antivirus y Firewall.

Nota: *Esta figura representa el nivel de conocimiento de los empleados sobre las medidas de protección de la información, como antivirus, cifrado y firewall.*

Falta de cobertura en la protección de dispositivos:

Se constató que la organización posee una licencia de antivirus válida solo para 10 equipos, dejando al resto de los dispositivos desprotegidos. Además, se evidenció la ausencia de un firewall y software de cifrado de datos, lo que incrementa aún más la vulnerabilidad de la organización ante posibles ataques o fugas de información.

Inconsistencia en la realización de copias de seguridad:

Otro hallazgo crítico fue la inconsistencia en la realización de copias de seguridad. La mayoría de los empleados desconocen si se llevan a cabo copias de seguridad y, entre aquellos que sí lo saben, las respuestas varían en cuanto a la frecuencia con la que se realizan, lo que sugiere una falta de procedimientos documentados y efectivos.

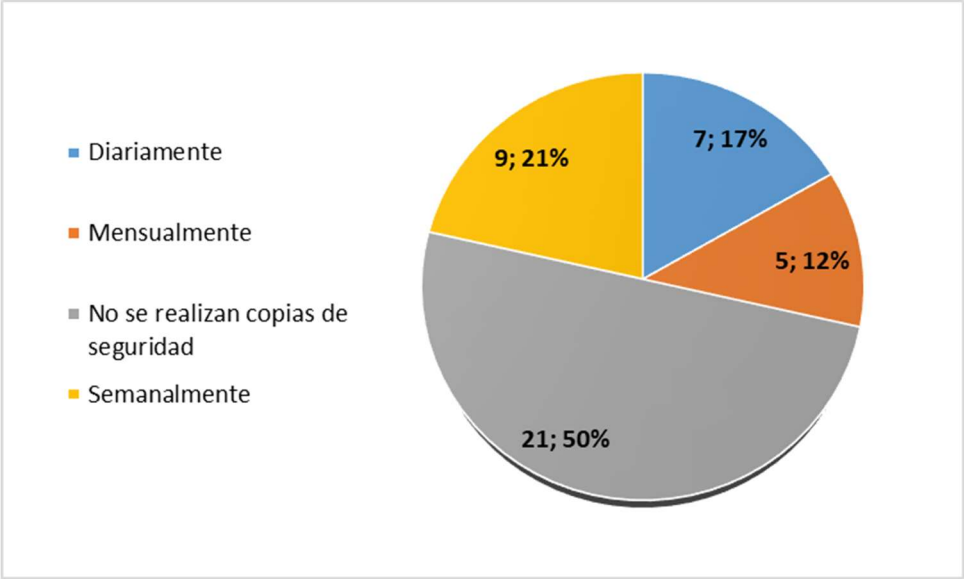


Figura 4. Frecuencia en la realización de copias de seguridad

Nota: *Esta figura identifica si la organización realiza copias de seguridad de los datos y la frecuencia con que se efectúan.*

La mayoría de los empleados no están informados sobre las prácticas de seguridad ni sobre la existencia de medidas de protección, lo que indica una brecha en la comunicación y en la capacitación. Además, la falta de documentación sobre la realización de copias de seguridad y la variabilidad en las respuestas de los empleados acerca de su frecuencia evidencia la falta de procedimientos establecidos y efectivos para la protección de datos.

Este análisis revela una serie de deficiencias significativas en la protección de la confidencialidad y disponibilidad de la información. La ausencia de políticas de seguridad de la información, junto con la falta de soluciones antivirus efectivas, firewall y software de cifrado, denota una gestión deficiente en la protección de datos. Estos hallazgos subrayan la urgencia de implementar mejoras sustanciales en la infraestructura tecnológica y los procesos de seguridad de la organización.

El tercer objetivo de la investigación se orientó a proponer un plan integral de capacitación en ciberseguridad, con el fin de fortalecer las competencias del personal en la protección de la información y responder eficazmente ante posibles amenazas cibernéticas.

El análisis del cuestionario reveló una necesidad significativa de capacitación en seguridad de la información. La mayoría de los encuestados subrayó la importancia de implementar medidas de seguridad, políticas adecuadas y el uso de contraseñas seguras. Esta necesidad se ve reflejada en la falta de conocimientos y habilidades básicas en ciberseguridad entre el personal, lo que podría comprometer seriamente la seguridad de la organización.

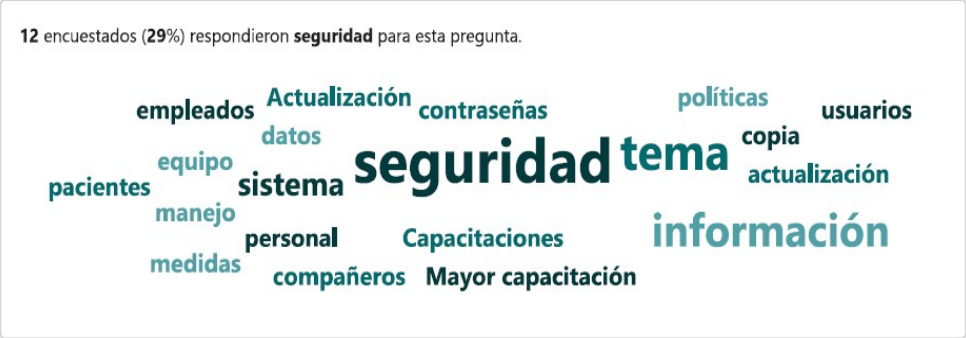


Figura 5. Necesidades de mejora en seguridad de la información.

Nota: *Esta figura refleja las necesidades de mejora en seguridad de la información identificadas por los empleados de la IPS.*

Hallazgos de la entrevista con la gerente general:

La entrevista con la gerente general reveló varios puntos clave que deben ser abordados por la organización:

Como primera medida, la entrevista revela la ausencia de políticas de seguridad de la información propias en la organización. La gerente general admite que solo se dependen de las políticas del proveedor del software de historia clínica en la nube, con lo cual se deja una brecha significativa en la protección integral de la información confidencial. Además, se evidencia que el software de seguridad se usa algo limitado, dado que se usan antivirus básicos y software estándar como Office, sin herramientas específicas y avanzadas de ciberseguridad. La dependencia exclusiva en las políticas del proveedor de la nube puede ser insuficiente para proteger todos los tipos de datos manejados.

La respuesta sobre el uso de software de seguridad revela una dependencia limitada a herramientas básicas, como el antivirus convencional y las plataformas en la nube vinculadas a la gestión de la salud. Esta situación destaca una posible falta de diversificación en las soluciones de seguridad, lo cual podría dejar expuestos ciertos aspectos críticos de la organización. Aunque el uso de plataformas en la nube puede ofrecer niveles de seguridad integrados, es fundamental contar con herramientas adicionales que protejan otros frentes, como el cifrado de datos y la monitorización de actividades sospechosas dentro del sistema.

En cuanto a los incidentes de seguridad, la percepción de seguridad dentro de la organización parece estar influenciada por la ausencia de eventos catastróficos, aunque sí se han registrado robos de computadoras. Estos incidentes generan inquietudes sobre la posibilidad de que se haya comprometido información, especialmente si los usuarios estaban activos en el momento del robo. La falta de pruebas concluyentes sobre la sustracción de datos refleja una brecha en los mecanismos de detección y respuesta ante incidentes, sugiriendo que la organización carece de procesos robustos para rastrear y mitigar posibles fugas de información tras un robo.

La ausencia de incidentes de seguridad mayores podría generar una falsa sensación de seguridad entre los empleados, haciendo que las medidas preventivas no se consideren una prioridad. La experiencia de robos de equipos, aunque sin evidencia de pérdida de información, debería ser suficiente para mejorar la seguridad, como el uso de herramientas para gestionar dispositivos robados y la formación del personal en la identificación y reporte de amenazas potenciales.

Adicionalmente, la necesidad de capacitar a todo el personal es evidente para fortalecer la postura de seguridad de la organización. La capacitación debe ir más allá de la formación básica en el uso de herramientas como el antivirus y la nube, abordando aspectos críticos como la gestión segura de contraseñas, la identificación de señales de actividad maliciosa y el protocolo de respuesta ante incidentes. Una estrategia de capacitación integral no solo mejorará la competencia en ciberseguridad del personal, sino que también contribuirá a crear una cultura organizacional consciente de la importancia de proteger la información sensible.

Este hallazgo se enlaza con la falta de capacitación en ciberseguridad en el equipo de profesionales, incluida la gerente, no se ha formado en este ámbito, y la capacitación existente se enfoca en usar la plataforma del proveedor de la nube, no en prácticas de ciberseguridad. También, la organización ha experimentado robos de computadoras, generando preocupaciones sobre posibles brechas de información. Aunque no se ha confirmado el robo de información, estos incidentes resaltan la necesidad de políticas y medidas de seguridad más robustas.

La gerente también expresa su interés en implementar políticas de seguridad de la información en busca de proteger mejor los datos de la organización, reconociendo la creciente necesidad de políticas a medida que la organización crece. Con base en estos hallazgos, se propone un plan integral de capacitación para el personal, que aborde aspectos importantes de seguridad de la información.

Como primera medida se propone una evaluación y creación del plan integral de seguridad de la Información y para ello se deben tener en cuenta los siguientes aspectos:

Identificación de la infraestructura tecnológica y políticas: esta investigación hasta el momento ha permitido identificar la infraestructura tecnológica y las políticas de seguridad de la información en la organización privada IPS. Mediante del análisis de datos recopilados, se ha evidenciado una dependencia significativa de políticas de seguridad externas, principalmente las implementadas por los proveedores de servicios en la nube, lo cual genera una protección limitada que solo se centra en las historias clínicas dejando brechas por cubrir en otros aspectos.

Evaluación más profunda de la infraestructura: para complementar este apartado, es necesario realizar una evaluación de los componentes de la infraestructura tecnológica. Que incluye no solo la revisión del hardware y software utilizados, sino también la evaluación de la configuración y gestión de estos sistemas. se debe prestar especialmente atención a los siguientes aspectos:

Protección de datos sensibles: evaluar cómo se asegura la confidencialidad, integridad y disponibilidad de los datos en la IPS, más allá de las historias clínicas. Esto incluye revisión de los sistemas de cifrado de datos, el control de acceso y la autenticación de usuarios.

Mecanismos de respaldo de datos: es necesario analizar cómo se maneja el respaldo de datos, su periodicidad, y la seguridad de las copias de respaldo. La falta de un sistema de respaldo robusto puede poner en riesgo la continuidad operativa de la IPS.

Gestión de incidentes de seguridad: evaluar cómo se gestionan los incidentes de seguridad, incluyendo la detección, respuesta y recuperación. Es importante que la IPS tenga un plan de respuesta a incidentes claramente definido y que este sea difundido a todo el personal.

Una vez finalizada la evaluación propuesta anteriormente, será necesario implementar un plan integral de capacitación que aborde las carencias identificadas. Este plan debe ser exhaustivo, abarcando desde la concientización básica hasta la capacitación técnica avanzada para el equipo de TI.

A continuación, se detallan los elementos del plan de capacitación:

Concientizar a los colaboradores sobre la seguridad de la información: como objetivo se establece sensibilizar a todo el personal acerca de la importancia de la seguridad de la información y los riesgos asociados al manejo inadecuado de los datos, en su contenido se pueden abarcar programas de formación continua que incluyan temas como phishing, malware, ingeniería social, y mejores prácticas para el manejo seguro de la información.

En cuanto a la capacitación técnica para el equipo de TI, se establece como objetivo, mejorar las habilidades técnicas del equipo de TI en la gestión y configuración de herramientas de seguridad, en su contenido se tendría principalmente la formación específica sobre la instalación, configuración y gestión de firewalls, sistemas de detección de intrusiones, y políticas de seguridad en entornos en la nube.

Simulacros de ciberataques y respuesta a incidentes, como objetivo se establece preparar al personal para afrontar de manera efectiva los incidentes de seguridad y en su contenido, se podrán realizar de ejercicios de tipo simulacro para identificar debilidades en la infraestructura y en la preparación del equipo. Desarrollo de un plan de respuesta a incidentes, que incluya roles y responsabilidades claras para la contención y recuperación.

Uso seguro y eficiente de herramientas tecnológicas: su objetivo es garantizar que el personal utilice de manera segura y eficiente las herramientas tecnológicas con las que cuenta la IPS y su contenido abarcaría las buenas prácticas para el uso de plataformas en la nube, configuraciones de seguridad y mantenimiento, y el seguimiento periódico de la seguridad de las aplicaciones y herramientas utilizadas.

Dicho plan de capacitación incluiría sesiones acerca del manejo seguro de contraseñas, concientizando al personal la importancia de crear y mantener contraseñas seguras, mediante herramientas de gestión de contraseñas y aplicando con base en políticas el cambio periódico de contraseñas.

Finalmente, se garantizará el uso seguro y eficiente de las herramientas tecnológicas tanto de hardware como de software, impartiendo también buenas prácticas para el uso de plataformas en la nube, configuraciones de seguridad y mantenimiento, y el seguimiento periódico de la seguridad de las plataformas utilizadas. El plan de capacitación integral pretende elevar la conciencia y competencia en ciberseguridad del personal de la IPS.

La implementación del plan propuesto permitirá a mitigar los riesgos asociados a la falta de políticas y medidas de seguridad actuales, promoviendo una cultura organizacional enfocada en la protección de la información. A medida que la organización crece, la capacitación continua y la evaluación periódica de las prácticas de seguridad serán clave para sostener un entorno seguro y confiable. En conclusión, el análisis realizado en este capítulo subraya la necesidad de una intervención integral en la seguridad de la información dentro de la IPS. La falta de políticas internas, el uso limitado de herramientas de seguridad y el desconocimiento del personal sobre las medidas de seguridad actuales representan riesgos significativos que deben ser abordados en un corto plazo.

Capítulo 4. Conclusiones

La infraestructura tecnológica de la organización privada IPS, tal como se evidenció en el estudio, presenta ciertos desafíos que comprometen la seguridad de la información. Aunque la organización tiene sistemas básicos de seguridad, como software antivirus, no sería suficiente para proteger adecuadamente la información sensible y confidencial. La falta de actualizaciones regulares de estos sistemas representa un riesgo significativo, ya que deja a la infraestructura

vulnerable a nuevas amenazas cibernéticas que emergen continuamente. Las actualizaciones son importantes para garantizar que los sistemas puedan detectar, mitigar y neutralizar las amenazas más recientes, y la falta de un proceso sistemático para realizarlas pone en riesgo la disponibilidad, integridad y confidencialidad de la información.

Los procedimientos de copia de seguridad no se realizan de manera sistemática. La copia de seguridad es un componente crítico en cualquier estrategia de seguridad de la información en una organización, ya que garantiza que los datos puedan recuperarse en caso de pérdida, daño o ataques cibernéticos. Sin una copia de seguridad periódica y segura, la IPS se expone al riesgo de perder información sensible, lo que podría tener consecuencias negativas para su operación y reputación de cara a sus pacientes y a la misma competencia. Esta deficiencia en los procedimientos de seguridad resalta la necesidad de una revisión completa de la infraestructura tecnológica, con el objetivo de implementar mejoras que fortalezcan la seguridad y aseguren la continuidad operativa de la organización.

Otro hallazgo crítico del análisis es la implementación inconsistente de las políticas de seguridad de la información dentro de la organización. Si bien, la organización ha establecido ciertas políticas para proteger la información, estas no se aplican de manera uniforme en toda la IPS. Esta falta de consistencia en la implementación genera brechas significativas en la seguridad de la información, ya que algunos de los profesionales pudieran no estar siguiendo los procedimientos adecuados, lo que aumenta la vulnerabilidad a incidentes de seguridad.

La familiaridad de los empleados con las políticas de seguridad es otro aspecto preocupante. Según el estudio, no todos los empleados están al tanto de las políticas de seguridad existentes, lo que sugiere una deficiencia en la comunicación interna y en la formación continua en esta área. La seguridad de la información es una responsabilidad compartida que requiere que todos los profesionales y colaboradores de la organización comprendan y sigan las políticas establecidas. Sin embargo, la falta de conocimiento sobre estas políticas significa que los empleados pueden estar cometiendo errores que ponen en riesgo la información sensible. Por lo tanto, es importante que la organización cree estrategias para una mejorar la difusión y el cumplimiento de estas políticas, asegurando que todos los empleados estén debidamente informados y capacitados para seguir los procedimientos de seguridad.

Una capacitación en ciberseguridad es la actividad clave para proteger la información en cualquier empresa u organización, y el estudio reveló que la IPS enfrenta ciertos desafíos importantes en este ámbito. La capacitación actual es insuficiente, por lo que resulta en una baja conciencia entre los empleados sobre las amenazas cibernéticas y las mejores prácticas para afrontarlas. Por ejemplo, muchos empleados no reciben formación continua sobre cómo identificar amenazas como el phishing, el programa maligno o las tácticas de ingeniería social, que son los ataques cibernéticos más comunes. Esta falta de capacitación aumenta el riesgo de que los colaboradores caigan en trampas cibernéticas, comprometiendo la seguridad de la información de la organización.

Además, el manejo seguro de contraseñas es otro aspecto crítico donde la capacitación es deficiente. Las contraseñas son una de las primeras estrategias de defensa contra el acceso no autorizado a la información, y con un manejo inadecuado puede dar lugar a brechas de seguridad significativas. Sin una capacitación adecuada, los colaboradores pueden utilizar contraseñas débiles o compartirlas de manera insegura, por lo que facilitarían los ataques cibernéticos. Por lo tanto, es necesario que la organización implemente un plan de capacitación integral que aborde estos aspectos y promueva una cultura de ciberseguridad sólida.

El plan de capacitación debe incluir sesiones regulares de formación que cubran una amplia gama de temas relacionados con la ciberseguridad, desde la identificación de amenazas hasta la respuesta ante incidentes. También es recomendable que la organización realice evaluaciones periódicas de la efectividad de la capacitación, a través de pruebas o simulaciones de ataques cibernéticos, para con ello asegurarse de que los empleados estén preparados para enfrentar los desafíos de seguridad. Este enfoque estructurado no solo mejoraría la competencia del personal en ciberseguridad, sino que también fortalecería la postura general de seguridad de la organización.

Ahora bien, dando una mirando hacia el futuro, es evidente que la IPS debe adoptar un enfoque proactivo para mejorar su seguridad de la información. Esto incluye no solo la actualización y mejora de la infraestructura tecnológica, sino también la creación e implementación de políticas de seguridad internas más robustas y coherentes. La organización debe contemplar la posibilidad de crear un marco de políticas de seguridad de la información

que abarque todas las áreas críticas, desde la protección de datos hasta la gestión de incidentes, y que sea aplicable a todos los niveles de la organización. Estas políticas deben estar alineadas con las mejores prácticas y estándares internacionales de seguridad de la información, como la norma ISO/IEC 27001, para garantizar un enfoque sistemático y efectivo.

También, es crucial que la organización invierta en la formación continua de su personal en ciberseguridad. El rápido crecimiento y evolución de las amenazas cibernéticas requiere que los colaboradores estén constantemente actualizados sobre las últimas técnicas y tácticas utilizadas por los atacantes. Un programa de capacitación regular y bien diseñado no solo aumentará la conciencia de seguridad entre los colaboradores, sino que también les proporcionará las habilidades necesarias para proteger la información de manera efectiva. Este programa debe ser respaldado por la alta dirección y debe formar parte de la cultura organizacional para lograr su éxito.

Por último, la organización podría considerar la implementación de un sistema de monitoreo y auditoría continua de la seguridad de la información. Esto permitiría identificar y corregir rápidamente cualquier vulnerabilidad o incumplimiento de las políticas de seguridad, minimizando así el riesgo de incidentes de seguridad. Un enfoque de monitoreo continuo da a la organización la capacidad de adaptarse rápidamente a nuevas amenazas y de mejorar continuamente su esquema de seguridad.

En conclusión, el análisis de la seguridad de la información en la organización privada IPS revela áreas significativas que requieren atención y mejora. La infraestructura tecnológica, las políticas de seguridad y la capacitación en ciberseguridad son elementos críticos que necesitan ser fortalecidos para proteger adecuadamente la información sensible de la organización. A medida que la IPS continúa creciendo y evolucionando, es importante que adopte un enfoque proactivo e integral para la seguridad de la información, garantizando que todos los aspectos de su operación estén protegidos contra amenazas cibernéticas. Este enfoque no solo mejorará la seguridad de la información, sino que también contribuirá al éxito a largo plazo de la organización en un entorno digital cada vez más complejo y desafiante.

Por último, surgen una serie de preguntas de cara al impacto de la capacitación del personal y la adaptación a nuevas amenazas cibernéticas:

¿Cómo se puede medir de manera efectiva el impacto de la capacitación en la mejora de la seguridad de la información?

¿Qué indicadores pueden ser utilizados para evaluar la efectividad del plan de capacitación propuesto?

¿Cómo puede la IPS mantenerse al día con las amenazas cibernéticas emergentes?

¿Qué estrategias pueden implementarse para asegurar una mejora continua en la seguridad de la información, principalmente en un entorno tecnológico en evolución?

Referencias Bibliográficas

Academia Novasoft. (24 de 01 de 2023). *Novasoft*. Obtenido de https://www.novasoft.com.co/seguridad-de-la-informacion-un-problema-critico-para-las-empresas/

Caamaño Fernández, E. E., & Gil Herrera, R. d. (10 de 2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. Manizales.

Carvajal, D., Cardona, A., & Valencia, F. (30 de 05 de 2019). Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. Manizales, Colombia. doi:https://doi.org/10.31908/19098367.4016

Cervera García, A., & Goussens, A. (13 de 01 de 2024). *ScienceDirect*. doi:https://doi.org/10.1016/j.aprim.2023.102854

Gutiérrez García, S., Barrantes Centurión, J., & Sánchez Silva, J. (2020). Seguridad de la información: Phishing y coronavirus. Alicia - Concytec.

Jarufe Bader, J. P. (14 de septiembre de 2023). *Biblioteca del Congreso Nacional de Chile.* Obtenido de https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/34959/1/Ciberataques_contra_la_infraestructura_de_salud_Experiencia_internacional.pdf

Jarufe Bader, J. P. (14 de septiembre de 2023). *Biblioteca del Congreso Nacional de Chile.* Obtenido de https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/34959/1/Ciberataques_contra_la_infraestructura_de_salud_Experiencia_internacional.pdf

Jiménez Marín, C. A. (21 de 07 de 2024). EntrevistaGerenteIPS. Medellín, Antioquia, Colombia.

Llanos Cardona, J. A., López, F. A., & Mejía Lobo, M. (30 de 11 de 2023). Implementación de un sistema de seguridad de la información en empresa del sector salud: Caso de estudio. Manizales, Caldas, Colombia.

Organización Panamericana de la Salud. (9 de 02 de 2021). De la evolución de los sistemas de información para la salud a la transformación digital del sector de la salud. Informe de la. Washington D.C., Washington D.C., Estados Unidos. Obtenido de https://iris.paho.org/bitstream/handle/10665.2/53801/OPSEIHIS210006_spa.pdf

Preciado Rodríguez, A. J., Valles Coral, M. A., & Lévano Rodríguez, D. (2021). Importancia del uso de sistemas de información en la automatización de historiales clínicos: una revisión sistemática.

Prensario TI Latin America. (08 de 08 de 2023). *Prensariotila*. Obtenido de https://prensariotila.com/desafios-en-la-era-digital-del-sector-salud-en-colombia/

Revista Innovación y Software. (30 de Febrero de 2023). Diagnóstico del nivel de seguridad empresarial y gestión del riesgo de la información basado en ISO/IEC-27001. (U. L. Salle, Ed.) Arequipa, Perú. Obtenido de https://revistas.ulasalle.edu.pe/innosoft

Vilchez Villegas, J. C. (2022). Ciberseguridad y robo de información: Una revisión sistemática de la literatura. Chiclayo.

Zevallos, M. (2 de febrero de 2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. Lima, Lima, Perú.

doi:http://dx.doi.org/10.15381/rpcs.v2i2.17103:citation[oaicite:1]{index=1}.

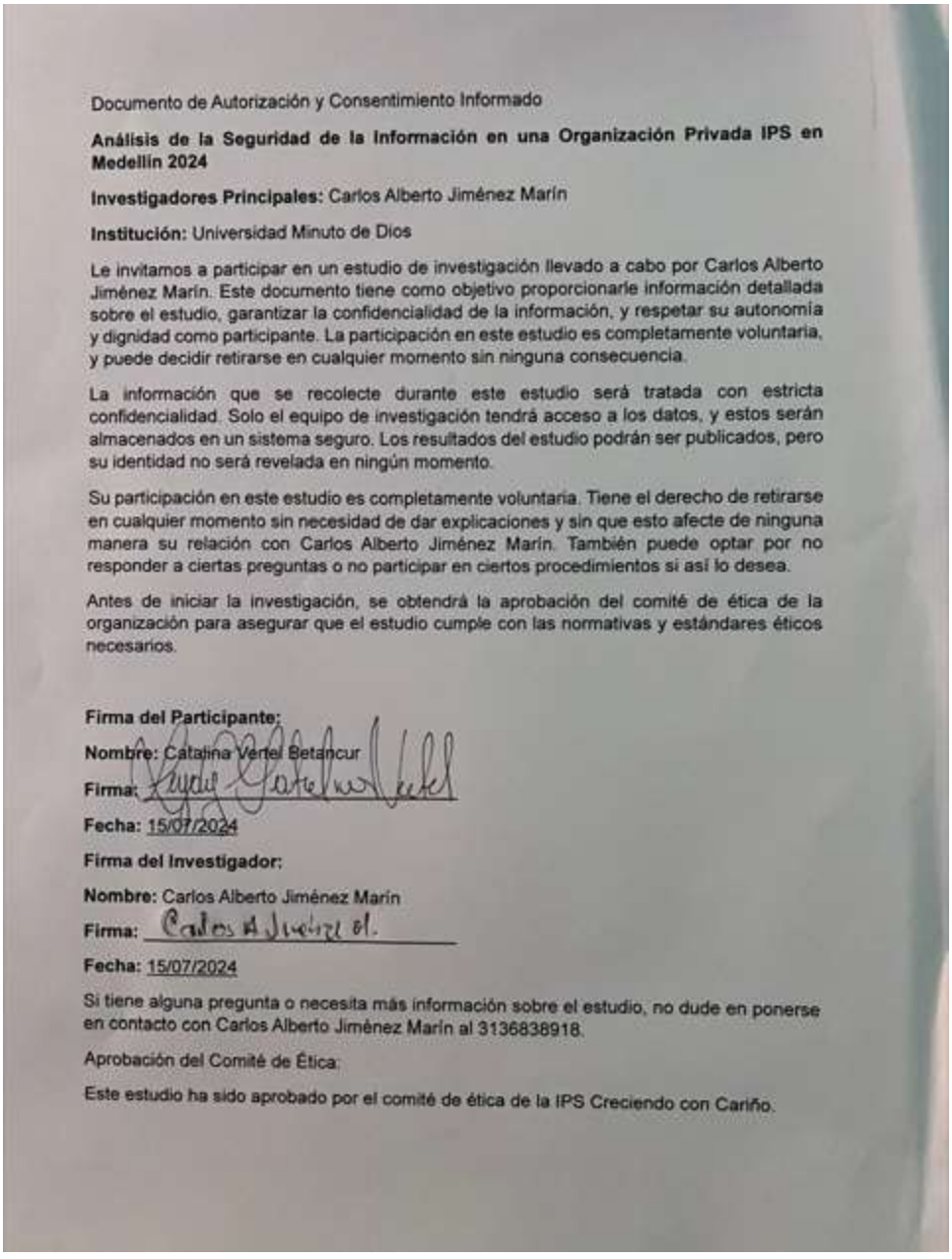
Apéndice A

Instrumentos Aplicados

Se anexa mediante correo los archivos Cuestionario Seguridad IPS y Gráficas Cuestionario.

Apéndice B

Consentimiento Informado



Documento de Autorización y Consentimiento Informado

Análisis de la Seguridad de la Información en una Organización Privada IPS en Medellín 2024

Investigadores Principales: Carlos Alberto Jiménez Marín

Institución: Universidad Minuto de Dios

Le invitamos a participar en un estudio de investigación llevado a cabo por Carlos Alberto Jiménez Marín. Este documento tiene como objetivo proporcionarle información detallada sobre el estudio, garantizar la confidencialidad de la información, y respetar su autonomía y dignidad como participante. La participación en este estudio es completamente voluntaria, y puede decidir retirarse en cualquier momento sin ninguna consecuencia.

La información que se recolecte durante este estudio será tratada con estricta confidencialidad. Solo el equipo de investigación tendrá acceso a los datos, y estos serán almacenados en un sistema seguro. Los resultados del estudio podrán ser publicados, pero su identidad no será revelada en ningún momento.

Su participación en este estudio es completamente voluntaria. Tiene el derecho de retirarse en cualquier momento sin necesidad de dar explicaciones y sin que esto afecte de ninguna manera su relación con Carlos Alberto Jiménez Marín. También puede optar por no responder a ciertas preguntas o no participar en ciertos procedimientos si así lo desea.

Antes de iniciar la investigación, se obtendrá la aprobación del comité de ética de la organización para asegurar que el estudio cumple con las normativas y estándares éticos necesarios.

Firma del Participante:

Nombre: Catalina Vertel Betancur

Firma:

Fecha: 15/07/2024

Firma del Investigador:

Nombre: Carlos Alberto Jiménez Marín

Firma:

Fecha: 15/07/2024

Si tiene alguna pregunta o necesita más información sobre el estudio, no dude en ponerse en contacto con Carlos Alberto Jiménez Marín al 3136838918.

Aprobación del Comité de Ética:

Este estudio ha sido aprobado por el comité de ética de la IPS Creciendo con Cariño.

Apéndice C

Trascripción de Entrevista

Doctora Catalina, primero que todo, muchas gracias por permitirme estar aquí en este momento y poder realizar esta entrevista sobre la seguridad de la información en la IPS Creciendo con Cariño. Doctora, a continuación, le voy a empezar a hacer las preguntas, espero sus respuestas.

Primera pregunta, ¿podría describir su rol en la organización y cómo se maneja la información sensible en su trabajo diario? Buenas tardes, Carlos. Muchísimas gracias por acompañarnos en nuestra IPS Creciendo con Cariño, donde me desempeño como la gerente de la institución.

Para nosotros poder tener el acercamiento a políticas de seguridad, pues en este crecimiento nos hemos enfocado en otros tipos de políticas, entonces es buena hora llegas

a nuestra institución. Muchas gracias. Segunda pregunta. ¿Cómo describiría la información de seguridad de la información en su organización? Bueno, Carlos, nosotros somos una institución que es una institución prestadora de servicios de salud, donde nosotros estamos enfocados en la atención a usuarios víctimas de violencia sexual, por lo tanto, nuestras historias clínicas tienen que estar custodiadas y tienen que estar pues protegidas por la norma de historia clínica, entonces pues directamente con

la política, nosotros sólo contamos con la política de nuestro proveedor de historia clínica que la manejamos con su nube y es una plataforma que está en la nube,

valga la redundancia, y es una política que solo nos protege la historia clínica. Como tal, nosotros no tenemos en este momento una política para la seguridad de la información, porque pues todo lo ponemos

en la nube, cada vez que crecemos más vemos la necesidad de implementar unas políticas.

¿Qué tipos de software de seguridad utilizan regularmente?

Nosotros utilizamos el antivirus normal, el office y la plataforma su nube e IPSA, todo esta en la nube y son plataformas de salud, no utilizamos ninguna otra.

Ok, ahora vamos con unas preguntas respecto a las políticas de seguridad de la información. ¿Qué políticas de la seguridad de la información conoce? Ninguna. Ninguna, perfecto. ¿Cómo se implementan estas políticas en su trabajo diario?

Ninguna, perfecto. ¿Cómo se implementan estas políticas en su trabajo diario? No, como no conocemos ninguna política ni hemos implementado ninguna, pues no. Nosotros solamente trabajamos en este momento con políticas institucionales que tienen que ver más que todo con el CICOP, el SARLAB y el manejo de historia clínica no más.

Muy bien, ¿considera usted doctora que las políticas actuales son efectivas y por qué? Pues mira, con la historia clínica, con plataforma, sí, estamos seguros de que todas las políticas que trabajamos historias clínicas en los computadores pueden manejar información del usuario, dejarlo en los computadores sin ningún control porque no tenemos ninguna política que se establezca y que se pueda publicar. ¿Qué espero yo de este encuentro? Que nos puedas ayudar a realizar esas políticas y capacitar al personal

para poder saber cómo vamos a direccionar toda nuestra política acompañada de tu trabajo. perfecto vamos con la siguiente sección que sobre capacitación de personal ¿ha recibido capacitación en ciberseguridad? ¿si es así puede escribir cómo fue esta experiencia? No, puede ser realmente no hemos tenido una capacitación como te digo la única más cercana es la de su nube y las capacitaciones están más alrededor de cómo funciona la plataforma, pero no desde la ciberseguridad, no. manejar la información de manera segura. Esa pregunta sobra.

Bueno, las siguientes preguntas son sobre opinión general. ¿Ha experimentado o conoce algún accidente, perdón, incidente de seguridad en la organización? ¿Y cómo se manejó? No, pues en ese momento, pues realmente no nos ha pasado nada, pero sí hemos tenido tres incidentes que son tres robos de computador, que siempre nos queda como la sensación de si el usuario estuvo activo, si se logró sacar alguna información, pero hasta el momento no hemos podido comprobar que se hayan robado información, ¿no? Siguiente pregunta. ¿Qué mejoras considera necesarias para mejorar la seguridad de la información en la organización? a todo el personal.

Y la última pregunta. ¿Hay algún otro aspecto relacionado con la seguridad de la información que le gustaría comentar? cuenta lo que piensa el equipo médico y también todo lo que es nuestra plataforma es una nube

y estaría válido que revises un poquito sobre el SICOP, que es el manejo de datos de nuestros usuarios. Es como lo único que te solicitaría al momento de tener claro para las políticas institucionales que vamos a montar.

Muy bien, doctora Catalina, con esto finalizamos y le agradezco mucho por permitirnos este espacio.