UNIVERSIDAD NACIONAL

SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"ESTÁNDAR O-ISM3 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN LA CLÍNICA SAN PABLO S.A.C. – HUARAZ, 2022"

TESIS PARA OPTAR EL TÍTULO DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR:

Bach. López Yauri, Alex Julio

ASESOR:

Mag. Silva Zapata, Miguel Angel

HUARAZ – PERÚ

2022

N° Registro: T132

Repositorio Institucional - UNASAM - Perú

DEDICATORIA

A mis padres Betty y Rafael, por el cuidado y apoyo incondicional que me brindan, por cada gota de sudor derramada en nombre de mi crecimiento profesional.

A mi hija Scarlett, por convertirse en el motor que llego a impulsar mi vida para brindar alegría y motivación para el logro de mis objetivos personales.

A mis familiares y todas las personas que de manera directa e indirecta apoyaron y aportaron a mi formación personal y profesional.

Alex López Yauri

Repositorio Institucional - **UNASAM** - Perú

AGRADECIMIENTO

A dios, por brindarme vida, salud y guiarme en el camino que me permitió llegar a esta etapa de mi vida.

A mis padres, por ser el pilar, apoyo y motivación que siempre me impulsa a cumplir mis metas personales y profesionales a pesar de todos los imprevistos y dificultades presentadas.

A mi alma mater, la Universidad Nacional Santiago Antúnez de Mayolo por abrirme las puertas durante todos los años de estudio de mi formación profesional.

A mi asesor, por la comprensión, orientación y apoyo brindado durante todo este proyecto.

A mis docentes, por la guía y enseñanza brindada que permitió que yo siga avanzando y desempeñándome de manera correcta en mi carrera profesional.

Repositorio Institucional - **UNASAM** - Perú

HOJA DE VISTO BUENO

PRESIDENTE

Ing. Alberto Martin Medina Villacorta

CIP N° 143211

SECRETARIO

Ing. Elizabeth Gladys Arias Lazarte

CIP N° 43138

VOCAL

Ing. Miguel Angel Silva Zapata

CIP N° 96195

Repositorio Institucional - UNASAM - Perú

RESUMEN

En un gobierno que apunta a la transformación digital, la evolución y el uso de las tecnologías ha dado lugar a nuevas vulnerabilidades y amenazas que afectan constantemente la confidencialidad, disponibilidad e integridad de la información. Este contexto no es exclusivo del sector financiero o de las grandes empresas, siendo el sector salud uno de los sectores que afronta este gran reto. En muchos casos las áreas de TI no disponen del conocimiento, herramientas y habilidades para lidiar con las amenazas y vulnerabilidades presentadas y realizar así una adecuada gestión de la seguridad de la información.

La investigación se elaboró a partir de una situación problemática, teniendo como objetivo principal mejorar la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. - Huaraz, mediante un enfoque basado en procesos en niveles operacionales, tácticos, estratégicos y genéricos. La tesis hace uso de un enfoque cuantitativo con nivel correlacional explicativo correspondiente al diseño preexperimental de prueba-post prueba con un solo grupo con una población de 200 trabajadores de la Clínica San Pablo S.A.C. -Huaraz y una muestra conformada por 132 trabajadores de la Clínica San Pablo S.A.C. -Huaraz la cual fue calculada mediante un muestreo aleatorio simple, el instrumento de recolección de datos utilizados fue una encuesta con preguntas pre estructurada y la información recolectada fue procesada mediante el software estadístico SPSS versión 26.

La prueba de Wilcoxon para muestras relacionadas perteneciente a las pruebas no paramétricas, fue la seleccionada para el contraste de las hipótesis, obteniendo como resultante que la seguridad de la información adopta una mejora estadísticamente significativa al igual que sus dimensiones confidencialidad, disponibilidad e integridad logrando así los objetivos planteados y concluyendo que la aplicación del estándar O-ISM3 mejora de manera significativa la seguridad de la información en la Clínica San Pablo S.A.C. sede Huaraz, adicionalmente se concluye que el estándar O-ISM3 permite el incremento de niveles de madurez correspondiente a la seguridad de la información de la organización de un nivel 1 a un nivel 3 dicha mejora abre puertas a una posible implementación de un sistema que ayude a mejorar la gestión de la seguridad de la información y a una posible nueva aplicación con mayor alcance a largo plazo del estándar O-SIM3 u otro estándar internacional que permita a la organización llegar a niveles superiores de seguridad.

Palabras Clave: Modelo de madurez, O-ISM3, procesos O-ISM3, seguridad de la información, transformación digital.

Repositorio Institucional - **UNASAM** - Perú

ABSTRACT

In a government that aims for digital transformation, the evolution and use of technologies has given rise to new vulnerabilities and threats that constantly affect the confidentiality, availability and integrity of information. This context is not exclusive to the financial sector or large companies, with the health sector being one of the sectors facing this great challenge. In many cases, IT areas do not have the knowledge, tools and skills to deal with the threats and vulnerabilities presented and thus carry out adequate information security management.

The research was developed from a problematic situation, with the main objective of improving information security through the application of the O-ISM3 standard at Clínica San Pablo S.A.C. - Huaraz, through a process-based approach at operational, tactical, strategic and generic levels. The thesis makes use of a quantitative approach with an explanatory correlational level corresponding to the pre-experimental test-post test design with a single group with a population of 200 workers from Clínica San Pablo S.A.C. -Huaraz and a sample made up of 132 workers from Clínica San Pablo S.A.C. -Huaraz which was calculated by simple random sampling, the data collection instrument used was a survey with pre-structured questions and the information collected was processed using the SPSS version 26 statistical software.

The Wilcoxon test for related samples belonging to the non-parametric tests was selected to contrast the hypotheses, obtaining as a result that information security adopts a statistically significant improvement as well as its privacy, availability and device dimensions, achieving thus the proposed objectives and concluding that the application of the O-ISM3 standard significantly improves the security of information at Clínica San Pablo S.A.C. Huaraz headquarters, it is also concluded that the O-ISM3 standard allows the increase in maturity levels corresponding to the organization's information security from level 1 to level 3. Said improvement opens doors to a possible implementation of a system that helps to improve the management of information security and to a possible new application with greater long-term scope of the O-SIM3 standard or another international standard that allows the organization to reach higher levels of security.

Keywords: Maturity model, O-ISM3, O-ISM3 processes, information security, Digital transformation.

Repositorio Institucional - **UNASAM** - Perú

ÍNDICE

DEDICATORIA i
AGRADECIMIENTO ii
HOJA DE VISTO BUENO iii
RESUMEN iv
ABSTRACT v
I. INTRODUCCION 1
1.1. Planteamiento del problema 1
1.2. Formulación del problema 2
1.2.1. Problema general 2
1.2.2. Problemas específicos 2
1.3. Objetivo de la investigación 2
1.3.1. Objetivo general 2
1.3.2. Objetivos específicos 3
1.4. Justificación de la investigación 3
1.4.1. Justificación económica 3
1.4.2. Justificación operativa 3
1.4.3. Justificación tecnológica 4
1.4.4. Justificación social 4
1.4.5. Justificación normativa 4
II. MARCO TEORICO 6
2.1. Antecedentes de la investigación 6
2.1.1. Antecedentes internacionales 6
2.1.2. Antecedentes nacionales 8
2.1.3. Antecedentes locales 10
2.2. Bases teóricas 11
2.2.1. Los datos 11
2.2.2. Tipos de datos 11
2.2.3. Fases de vida de los datos 12
2.2.4. Información 13
2.2.5. Los activos de información 14
2.2.6. Seguridad de la información vs seguridad informática 14
2.2.8. El estado peruano y la gestión de seguridad de la información 17
2.2.9. Modelo de madurez 17
2.2.10. El estándar O-ISM3 V 2.0 18

Repositorio Institucional - UNASAM - Perú

2.3. Definición de términos 22
2.4. Hipótesis 23
2.4.1. Hipótesis general 23
2.4.2. Hipótesis específicas 23
2.5. Variables 23
2.5.1. Variable independiente 23
2.5.2. Variable dependiente 23
2.5.3. Operacionalización de variable 23
III. METODOLOGIA 26
3.1. Tipo de estudio 26
3.2. El diseño de investigación 26
3.3. Descripción de la unidad de análisis población y muestra 26
3.3.1. Unidad de análisis 26
3.3.2. Población 26
3.3.3. Muestra 26
3.4. Técnicas de instrumentos de recolección de datos 27
3.5. Técnicas de análisis y prueba de hipótesis 28
3.5.1. Técnicas de análisis 28
3.5.2. Prueba de hipótesis 28
IV. RESULTADOS DE LA INVESTIGACIÓN 30
4.1. Descripción del trabajo de campo 30
4.2. Presentación de resultados 57
4.3. Discusión de resultados 66
V. CONCLUSIONES 68
VI. RECOMENDACIONES 69
VII. REFERENCIAS BIBLIOGRÁFICAS 70
VIII. ANEXOS 73

Repositorio Institucional - UNASAM - Perú

ÍNDICE DE FIGURAS

Figura 1 *Las fases de vida de los datos/información* 12
Figura 2 *Proceso sistémico de la información* 13
Figura 3 *Seguridad de la información vs seguridad informática* 16
Figura 4 *Integración de las dimensiones de seguridad* 17
Figura 5 *Modelo de seguridad O-ISM3* 21
Figura 6 *Fórmula para el cálculo de muestra* 27
Figura 7 *Deficiencias de seguridad* 30
Figura 8 *Modelo de seguridad para Clínica San Pablo S.A.C - Huaraz* 31
Figura 9 *Modelo de madurez propuesto para la Clínica San Pablo S.A.C. - Huaraz* 32
Figura 10 *Brecha de seguridad existente* 34
Figura 11 *Capacitaciones virtuales para replicar el conocimiento* 35
Figura 12 *Versiones del sistema clínico actualizada a la última disponible* 42
Figura 13 *Servidor WSUS implementado* 43
Figura 14 *Herramientas usadas para el respaldo de servidores* 44
Figura 15 *Uso de servidor NAS* 45
Figura 16 *Clasificación de grupos por área* 46
Figura 17 *Creación de grupos de seguridad* 47
Figura 18 *Delimitación de acceso correspondiente a los grupos creados* 47
Figura 19 *Restricción de acceso a repositorios físicos* 48
Figura 20 *Solicitud de creación de usuario* 49
Figura 21 *Gestión de accesos a los usuarios nuevos* 50
Figura 22 *Sensores implementados en el data center* 51
Figura 23 *Aplicativo de monitoreo ambiental* 52
Figura 24 *Tareas de despliegue de antivirus* 53
Figura 25 *Dispositivos administrados por la consola de antivirus* 54
Figura 26 *Directiva de Bloqueo de puertos* 55
Figura 27 *Nuevo nivel de madurez de la Clínica San Pablo S.A.C.* 57

Repositorio Institucional - **UNASAM** - Perú

ÍNDICE DE TABLAS

Tabla 1 *Nivel de capacidad según O-ISM3* 19
Tabla 2 *Operacionalización de variables* 24
Tabla 3 *Normalidad de los datos* 28
Tabla 4 *Nivel de capacidad de los procesos O-ISM3* 56
Tabla 5 *Resultados de la variable de estudio (SI)* 58
Tabla 6 *Resultados de la dimensión Confidencialidad* 58
Tabla 7 *Resultados de la dimensión Disponibilidad* 59
Tabla 8 *Resultados de la dimensión Integridad* 60
Tabla 9 *Contraste de la hipótesis general – Seguridad de la Información* 61
Tabla 10 *Contraste de la hipótesis especifica N°1 – Dimensión Confidencialidad* 63
Tabla 11 *Contraste de la hipótesis especifica N°2 – Dimensión Disponibilidad* 64
Tabla 12 *Contraste de la hipótesis especifica N°3 – Dimensión Integridad* 66

Repositorio Institucional - **UNASAM** - Perú

I. INTRODUCCION

1.1. Planteamiento del problema

El sector salud es una de las industrias más demandadas en nuestro país a causa de la pandemia, por lo cual es fundamental conocer y definir cuán importante es la seguridad de la información en este rubro.

El confinamiento durante el periodo de pandemia a causa de la coyuntura COVID-19 genero cambios en las diversas formas de interacción social, laboral, educativa, etc. A causa de esto la delincuencia intensificó los intentos delictivos de vulnerar la seguridad mediante medios electrónicos, haciendo uso de la ingeniería social o también llamado phishing, las noticias falsas o fake news y actividades mal intencionadas más especializadas como es la inyección de código o malware, por lo cual es importante identificar las prácticas de seguridad de la información en una empresa u organización (Estrada et al., 2021).

Un adecuado cuido de la información significa garantizar la confidencialidad, disponibilidad e integridad de la misma, por lo cual, la identificación de los factores que intervienen en la pérdida de información es un punto fundamental en la protección de la información.

Existen múltiples factores que influyen en la perdida de información, el daño de la imagen y estabilidad de la organización, siendo los más relevantes un bajo nivel de inversión en seguridad, el escaso conocimiento de seguridad de la información, los desastres naturales, los agentes maliciosos y el factor humano (Bustamente et al., 2020).

Una revisión sistemática realizada entre los periodos 2010 al 2021 con la finalidad de poder precisar que tan primordial es la seguridad de la información y el uso de herramientas para protección de datos en el sector salud, saco a flote que las diversas organizaciones del sector salud realizan el control y manutención de los sistemas de seguridad de la información mediante uso de herramientas o estándares como la ISO 27001 y la NTP 27001(Reyes et al., 2022). Siendo estas un pequeño grupo de herramientas dentro del amplio grupo de marcos y normativas de trabajo referentes a la seguridad de la información.

Es fundamental que los diversos rubros de negocio del país conozcan la importancia y hagan uso de herramientas que ayuden a gestionar de manera correcta la seguridad de la información (GSI), el sector de la salud en este caso específico en la Clínica San

Repositorio Institucional - UNASAM - Perú

Pablo S.A.C. sede Huaraz, no se encuentra excluido de esto si lo que desea es encontrarse a la par con las empresas aledañas en su sector. Conocer el estado en el que se encuentra la organización, área o proceso referente a la seguridad de la información resulta fundamental si se desea reducir las brechas existentes, así como tener claros el nivel de seguridad idóneo y objetivos de seguridad que se desean lograr.

Manejar un nivel de seguridad adecuado nos equipa tanto de las herramientas como de la sapiencias requerida para prevenir y hacer frente a problemas e incidentes de seguridad que puedan afectar la confidencialidad de la información al igual que la disponibilidad e integridad, tales como accesos indebidos a los sistemas de información e información confidencial, caída de servidores antes fallas de sistema operativo o cortes eléctricos prolongados, historias clínicas erradas e incompletas, recepción de correos electrónicos mal intencionados (Phishing) y almacenamiento inadecuado de historias clínicas físicas. Incidente que fueron registrados en los últimos 2 años y que a la fecha algunos de ellos aún se presentan.

1.2. Formulación del problema

1.2.1. Problema general

¿De qué manera la aplicación del estándar O-ISM3 mejora la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022?

1.2.2. Problemas específicos

1) ¿De qué manera la aplicación del estándar O-ISM3 mejora la confidencialidad de la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022?

2) ¿De qué manera la aplicación del estándar O-ISM3 mejora la disponibilidad de la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022?

3) ¿De qué manera la aplicación del estándar O-ISM3 mejora la integridad de la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022?

1.3. Objetivo de la investigación

1.3.1. Objetivo general

Mejorar la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022.

Repositorio Institucional - UNASAM - Perú

1.3.2. Objetivos específicos

1) Mejorar la confidencialidad de la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022.
2) Mejorar la disponibilidad de la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022.
3) Mejorar la integridad de la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022.

1.4. Justificación de la investigación

En la presente se plantea la elaboración de un modelo de madurez en base a los lineamientos establecidos por el estándar O-ISM3 que permitió reflejar la brecha de seguridad existente entre el nivel ideal o deseado y el nivel real en el que se encontró la seguridad de la información, cuyo conocimiento generado permitió plantear objetivos de seguridad y tomar medidas en pro de estos objetivos, con el desarrollo de la investigación se implementaron procedimientos y prácticas que beneficiaron a la gestión de seguridad de la información (GSI) permitiéndonos una mejora continua y adecuado control de incidentes que puedan generar pérdidas de información.

1.4.1. Justificación económica

El cuidadoso análisis de los procesos O-ISM3 seleccionados para este estudio generan un mayor beneficio desde el punto de vista económico basado en una relación costo/beneficio esto debido a la capacidad de inversión necesaria correspondiente a los beneficios obtenidos en términos de seguridad, dando como resultados una mejora de esta a bajo costo.

Orientar a la organización a una mejora de la gestión de seguridad de la información permite evitan la ocurrencia de incidentes que puedan generar pérdidas cuantiosas en términos monetarios, punto adicional que brinda la factibilidad a la tesis elaborada.

1.4.2. Justificación operativa

El enfoque de procesos de fácil manejo y aplicación nos brinda la justificación en términos operativos, la aplicación de procesos y controles entendibles y

Repositorio Institucional - UNASAM - Perú

sencillos permiten que toda la organización de estudio se vea beneficiado en términos de gestión referente a la seguridad de la información a un nivel estratégico, táctico, operacional y genérico.

1.4.3. Justificación tecnológica

La mejora de la seguridad facilito a la empresa de estudio el alcance de niveles aceptables de seguridad de la información permitiendo controlar los riesgos generados por el crecimiento tecnológico en pro de la transformación digita en nuestro país, haciendo más seguro el uso de las herramientas tecnológicas que se encuentran al alcance de la organización con miras a la seguridad digital.

Adicionalmente permitiremos que la gerencia general y administrativa tengan un panorama más robusto de las oportunidades de mejora tecnológica que aporten un mayor valor a la seguridad de la información, brindando así el sustento tecnológico requerido.

1.4.4. Justificación social

Conocer y mejorar la seguridad de la información dentro de la organización permitirá manejar procedimientos seguros y controlados, brindando la seguridad y confianza tanto a la población de pacientes como a la población empleada de que su información, tales como datos personales, resultados médicos, procedimientos realizados, contratos laborales entre otros correspondientes al historial clínico del paciente e información organizacional serán tratados de tal forma que la información culmine un adecuado ciclo de vida, desde la generación hasta su destrucción de la misma, brindado así una exitosa gobernanza de datos.

1.4.5. Justificación normativa

El trabajo se encuentra justificado normativamente en el estándar O-ISM3 V2.0, estándar que brinda los lineamientos para lograr un nivel de madurez adecuado de la gestión de seguridad de la información que permite la mejora continua en base a controles y métricas de seguridad, publicada por The Open Group en setiembre del 2017.

En la política de seguridad de la información establecida por la organización de estudio.

Repositorio Institucional - UNASAM - Perú

En la ley N° 29733, ley que hace referencia a la protección de datos personales con la finalidad que las organizaciones puedan garantizar a la protección de datos personales a través de su adecuado tratamiento.

En la Agenda Digital al Bicentenario quien toma la protección de datos como un punto a desarrollar dentro de un marco regulatorio y adicionalmente en la Agenda Digital Andina, el cual establece fortalecer la confianza y seguridad digital dentro de uno de sus ejes y líneas de acción, todo esto orientado a la transformación digital.

Repositorio Institucional - **UNASAM** - Perú

II. MARCO TEORICO

2.1. Antecedentes de la investigación

Después de la recopilación y análisis de información en los diversos repositorios y bases de datos se toma como antecedentes las siguientes exploraciones.

2.1.1. Antecedentes internacionales

Cifre (2020), en su trabajo de maestría "Modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas", Argentina. El tesista se plantea como principal objetivo el concretar un modelo de seguridad examinando los lineamientos establecidos en los estándares O-ISM3 e ISO 27000 mediante la propuesta de acciones específicas por ejecutar para gestionar las vulnerabilidades de los servicios establecidos en nubes de compañas del sector privado. La investigación es realizada mediante un enfoque cuantitativo a un nivel aplicado. La tesis de maestría concluye que la aplicación de los estándares internacionales O-ISM3 e ISO/EIC 27000 ayudan a lograr una eficiente seguridad de la información siendo este uno de los problemas principales de los sistemas informáticos implementados. El modelo propuesto brinda una base para una mejora continua además de mejorar el nivel de madurez mediante buenas prácticas, procesos eficientes de gestión de vulnerabilidades y métricas de control, contribuyendo oportunamente a la creación de un SGSI. La investigación resalta los estándares O-ISM3 e ISO/IEC 27000 como estándares de seguridad con mayor importancia a nivel mundial brindándole mayor solides al presente trabajo de investigación debido a que el estándar O-ISM3 es tomado y aplicado para lograr alcanzar los objetivos planteados.

Al-Matari et al. (2021), en su artículo titulado "Adopting security maturity model to the organizations' capability model", Egipto. Los investigadores proponen un modelo de madurez tomando como referecia el estándar ISM3 que agrupa las tecnologías y capacidades que tiene la organización en cada proceso en 5 niveles de madurez con la finalidad de reducir la brecha existente en la organización de estudio en términos de seguridad de la información, el articulo refleja un enfoque cuantitativo de tipo explicativo. Los investigadores concluyen que el modelo planteado permite evaluar el nivel de madurez de seguridad de la

Repositorio Institucional - UNASAM - Perú

organización y permite que la organización llegue a un nivel adecuado de seguridad ayudando a la organización a disminuir posibles riesgos, además definen que la brecha de seguridad detectada está altamente relacionada con el talento humano y el uso de la tecnología. El artículo aporta significativamente a nuestra investigación ya que define las ventajas de usar un modelo de madurez basado en el estándar ISM3 para disminuir la brecha de seguridad en una organización, lo cual fortalece y brinda mayor sustento a la presente investigación.

Estrada et al. (2021) en el artículo científico "Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá", Colombia. Explican como el confinamiento a causa del COVID-19 abrio puertas a nuevas formas de interacción virtual e indirectamente al incremento de delitos electrónico por lo cual los investigadores se plantean el objetivo de detectar las prácticas principales que se utilizan en una determinada comuna universitaria con respecto a la seguridad de la información basandose en un enfoque de investigación mixto los investigadores plantean una investigación aplicada con el proposito responder a los problemas generados por la coyuntura, para lo cual utilizaron una muestra de 319 personas, obtenida mediante un muestreo aleatorio simple y un 5% de margen de error, los investigadores concluyen que los incidentes correspondientes a la seguridad de la información aumentaron sustancialmente durante la pandemia mas no se observaron vulneraciones significativas en la comunidad de estudio debido a las buenas prácticas aplicadas. El artículo citado aporta favorablemente a nuestra investigación ya que demuestra la importancia de manejar buenas prácticas de seguridad con el proposito de manejar un buen nivel de seguridad de la información ante el incremento de incidentes.

Altamirano (2019) en su artículo científico titulado "Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso", Ecuador. El investigador se propuso el objetivo de implementar un modelo para la gestión de la seguridad de la información establecido con los diferentes estándares de seguridad de la información existentes (entre ellos el estándar ISM3) que permita escalar entre los diversos niveles para hacer la gestión de controles de seguridad

Repositorio Institucional - UNASAM - Perú

menos compleja e incrementar su nivel de madurez y efectividad, para esto se empleó un enfoque cuantitativo con métodos empíricos y teóricos para poder recolectar información mediante entrevistas y encuestas semiestructuradas permitiendo tener un mejor panorama de las debilidades potenciales, el artículo concluye que aproximadamente el 40% de los controles de seguridad brindados por los diferentes estándares internacionales son aplicables y automatizables. El presente artículo constata el efecto favorable que tiene la adecuada gestión de los controles de seguridad y resalta cuán significativo es medir los sistemas de seguridad lo cual produce una mayor efectividad y aporte en la gestión de la seguridad de la información brindando sustento positivo al presente trabajo.

2.1.2. Antecedentes nacionales

Calle y Garcia (2019), en su trabajo de pregrado titulada "Modelo de madurez de protección de datos personales para el sector micro financiero peruano", Perú. Los tesistas tienen como objetivo la ejecución de un modelo de madurez organizacional para medir la capacidad que se tiene para la protección de datos personales en el sector micro financiero peruano, para lo cual los tesistas diseñaron un modelo de madurez tomando en cuenta el poder económico como factor principal para cumplir con el cumplimiento legal del gobierno, brindando adicionalmente un incremento en la cultura y los controles que debe priorizarse para mejorar el nivel de protección de datos, la investigación maneja un enfoque cuantitativo y es de tipo aplicada tomando como muestra de estudio a 5 empresas del sector micro financiero. Los tesistas llegan a la colusión que el modelo de madurez propuesto admite la mejora de la protección de datos personal en empresas de estudio a un bajo presupuesto, así mismo la investigación resalta que el uso del modelo de madurez propuesto es intuitivo y de fácil manejo obteniendo una aprobación del 93%, lo cual evidencia que los modelos de madurez son herramienta factibles para realizar una auto evaluación con el fin de subir de nivel de seguridad mejorando su capacidad y cultura de seguridad proporcionando así mayor sustento al presente trabajo de investigación.

Muedas y Rojas (2019), en su tesis "Modelo de madurez de seguridad de aplicaciones web ante ciberataques para clínicas de nivel 2", Perú. Tienen como objetivo planteado la implementación de un modelo de madurez para mejorar la

Repositorio Institucional - UNASAM - Perú

seguridad de aplicaciones web para prevenir ataques cibernéticos en entidades de salud de nivel 2 basada en la normativa del MINSA con la finalidad de evidenciar las vulnerabilidades de las aplicaciones web y mejorar los aspectos de seguridad, los tesistas manejan un enfoque cuantitativo de tipo descriptivo, obteniendo como resultante que la seguridad de las aplicaciones web se encuentran en un nivel de seguridad medio, siendo esta un nivel 3. Los tesistas concluyeron en base a la investigación que el modelo es de fácil aplicación, detectando la ineficiencia validación de ingreso de información, estas validaciones exponen de forma clara las falencias de seguridad, siendo la lógica con la que cuentan las funcionalidades de la aplicación una de las mayores fallas encontradas. La investigación referenciada muestra claramente como un modelo de madurez ayuda a identificar las falencias en un determinado objeto de estudio en este caso una aplicación web lo cual demuestra que los modelos de madurez pueden ser utilizados en los diversos áreas o aspectos tecnológicos en los que se requiera evaluar o incrementar el nivel de seguridad proporcionando mayor peso y aporte a la presente investigación.

Blas y Pretell (2020) en su investigación de pregrado titulada “Modelo de seguridad de la información para mejorar la gestión informática en la Municipalidad Distrital de Florencia de Mora”, Perú. Se plantean el objetivo de mejorar la seguridad de la información abarcando la seguridad informática haciendo uso de una metodolgia basada en la norma ISO 27002:2013, el trabajo investigativo hac euso del diseño no experimental con corte transversal debido a que los datos son recolectados una sola vez, con un enfoque descriptivo simple. La investigación maneja una población y muestra de 25 empleados debido a que la población de estudios es menor que 30, la investigación obtiene como resultado que existen inconvenientes con los pilares de la seguridad (confidencialidad, disponibilidad e integridad), con el uso de las operaciones y considera que la gestion de la seguridad de la información no se encuentra definida correctamente. Los tesistas concluyen al aplicar el modelo de madurez propuesto para mejorar la seguridad de la información las dimensiones de la seguridad mejoran a un nivel significativo del 2.5% demostrando que el uso de modelos basados en estándares internacionales es una alternativa de solucion a la problemática abarcada en la presente tesis.

Repositorio Institucional - UNASAM - Perú

Huincho (2019) en su investigación de pregrado que lleva como titulo “Sistema de gestión de seguridad de la información para mejorar la protección informática de la comisaria region Huancavelica”, Perú. El tesista se plantea en su investigacion el objetivo de tantear el nivel de dominio de un Sistema de gestión de seguridad de la información en la protección informática de la organización de estudio,para lo cual plantea una tesis aplicada con diseño experimental y manejando un enfoque cuantitativo haciendo uso de un metodo hipotetico deductivo tomando como muestras a 30 policias pertencientes a la organización de estudio obtenida de una población de 32 policias, utilizando la encuesta como instrimneto de recoleccion de información, observacion y entrevista. La investigación obtiene como resultado que el uso de un sistema trdicional orientado de seguridad tiene un nivel de aceptacion menor por parte de la organización a comparacion con el uso de un SGSI, el investigador llega a la conclusion que la implementación de un SGSI permitio aumentar de manera considerable la seguridad de los activos en la entidad de estudio garantizando así que la organización gestione sus riegos de seguridad de forma muy adaptable a cambios que puedan producir el entorno y la tecnología. Esto muestra que el uso de metodologías y sistemas que ayuden a la gestión de seguridad de la información mejoran el nivel de seguridad de una entidad dando así un aporte significativo al presente trabajo de investigación.

2.1.3. Antecedentes locales

Guardia (2020) en su tesis “Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del instituto de educación superior tecnológico público Eleazar Guzmán Barrón - Huaraz”, Perú. Que tiene como objetivo el diseño de un modelo de seguridad de la información que ayude a disminuir los riesgos de información en la gestión académica de la institución de estudio utilizando como base la NTP-ISO/IEC 27001:2014 en complemento con la metodología MAGERIT los investigadores aplican un enfoque de investigación cuantitativo, tipo de investigación: Correlacional y un diseño experimental con corte longitudinal, el trabajo hizo uso de una muestra de 20 colaboradores de la institución y aplico las fichas de resumen y recolección de datos en internet. Los investigadores concluyen que el modelo propuesto logro disminuir los riesgos de los activos de información. La investigación

Repositorio Institucional - UNASAM - Perú

referenciada menciona que la sensibilización del factor humano en temas de seguridad de la información y el uso de controles es fundamental para minimizar los riesgos y por ende para mejorar la seguridad de la información, lo cual aporta una mayor visión de la seguridad de la información al presente trabajo de investigación.

Colonia (2017), en su tesis "Propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la municipalidad distrital de Buena Vista Alta", Chimbote. se pone como objetivo proponer un SGSI basada en la norma ISO/IEC 27001 en la institución de estudio con el fin de minimizar la pérdida de información para ello el tesista realiza un estudio situacional de la seguridad de la información. Haciendo uso de un diseño no experimental con corte transversal, de tipo descriptivo con un enfoque cuantitativo. La investigación llega a la conclusión que el SGSI propuesto logra reducir la pérdida de información considerablemente.

La investigación brinda como principal aporte una mejora considerable en la gestión de la seguridad mediante la implementación de un sistema de gestión de seguridad de la información (SGSI).

2.2. Bases teóricas

2.2.1. Los datos

Proveniente del latín "Datum" que significa "lo que se da", los datos son la representación simbólica mediante letras y numero que indican la situación, condición o algún atributo de un determinado ente, también podemos definir los datos como símbolos numéricos obtenidos en base a algún estudio que nos permitirá realizar cálculos matemáticos para obtener información (Yirda, 2021).

2.2.2. Tipos de datos

Es indispensable saber o clasificar los datos y ver a que categoría pertenece para poder obtener el resultado deseado al momento de procesarlas. El equipo editorial Etecé (2020) define los siguientes tipos de datos como número y texto teniendo estas las siguiente clasificaciones:

1) **Numérico**
   a. **Entero**: formado por una variable número sin decimal.
   b. **Real**: conformado por una parte número y otra decimal.

Repositorio Institucional - UNASAM - Perú

2) **Texto**

a. **Caracter**: conformado por por la integracion de simbolos ya sea numeros o letras.

b. **Cadena:** formado por un conjunto de caracteres con las caracteristicas mencionada anteriormente.

2.2.3. Fases de vida de los datos

Con el rápido crecimiento del big data más creciente desarrollo de Internet de las cosas (IoT) el volumen de datos generados ha sufrido un incremento sustancial a nivel mundial, por lo cual es necesario conocer las fases/ciclo de vida de los datos generados o también llamado fases/ciclo de vida de la información en el ámbito de la transformación digital de las organizaciones este ciclo hace referencia al periodo o etapas por las que los datos pasan durante toda su existencia siendo estas la creación, almacenamiento, uso, archivado y la destrucción de los datos/información (Equipo de colaboradores DocuSing, 2022).

Figura 1

Las fases de vida de los datos/información

Nota: La figura muestra las fases de vida de los datos o también llamado fases de vida de la información. Fuente: Elaboración propia.

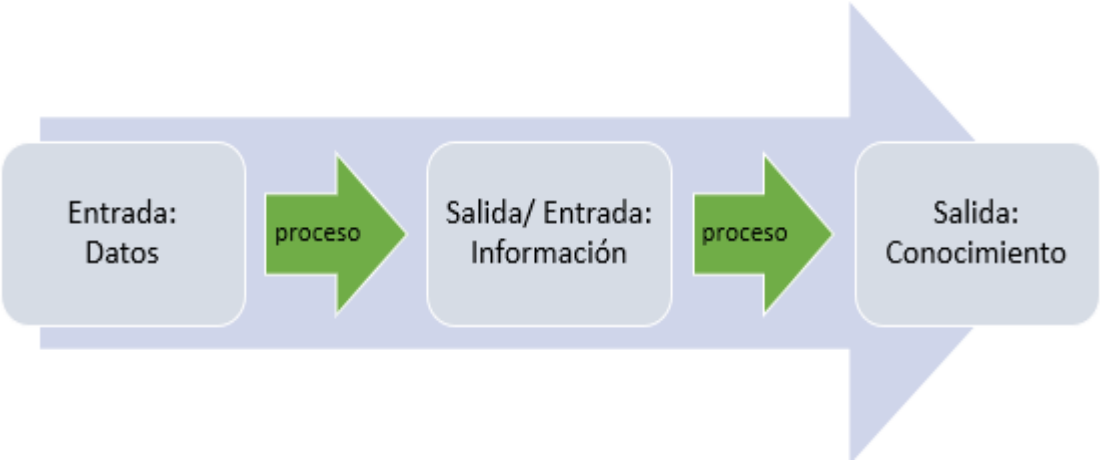
Repositorio Institucional - UNASAM - Perú

2.2.4. Información

La información no es más que la constitución de datos organizados, supervisados y procesados que otorgan un significado a una determinada realidad o contexto cuyo aprovechamiento y entendimiento permite obtener la comprensión necesaria de dicha situación o contexto y así poder tomar mejores decisiones (Pérez y Gardey, 2021).

Figura 2

Proceso sistémico de la información



Nota: La figura muestra el proceso de generación de conocimiento tomando los datos como entrada. Fuente: Elaboración propia.

La información al igual que otros activos comerciales sindo necesario para que una organización marche de forma correcta, la información puede ser almacenada de formas diverzas ya sea de forma digital o forma fisica/material y transmitida por medios físico, electrónicos o verbales por ende debe estar sujeta a una adecuada protección, en la mayoría de las organizaciones la información es dependiente de las TIC, las cuales se convierten en elementos indispensables durante todas las etapas de existencia de la información (International Organization of Standarization [ISO], 2018).

Polo (2020), menciona que la digitalización y la relación constante con la tecnología está generando una transformación en la información tanto en volumen y velocidad en la que esta se genera lo cual causa un impulso a la

Repositorio Institucional - UNASAM - Perú

sociedad digital lo que está provocando que la información esté a la disponibilidad de cualquiera para ser utilizada con fines diferentes, generando así una vigilancia digital o vigilancia de datos que terminara derivando en una sociedad de control como consecuencia de estos cambios.

2.2.5. Los activos de información

Según argumentos de la ISO (2018), todo aquello que se considera valioso para una entidad puede ser considerado como activo de información y por lo tanto debe ser protegida y respaldada ya sean datos/información generados por medios digitales, fisicos u otros medios. El hardware y software utilizado, las pesonas que manejen datos e información o algun tipo de conocimiento de importancia para la organización.

2.2.6. Seguridad de la información vs seguridad informática

Aunque puedan parecer lo mismo o sinónimos y aunque sus acciones de trabajo convivan en armonía cada uno tiene actividades y apuntan a objetivos diferentes sobre todo si se tiene en cuenta que el desarrollo de la tecnología tiende hacia la digitalización y al manejo de cualquier tipo de información a través de sistemas informáticos, entendamos que la seguridad informática comprende los aspectos operacionales y tácticos, mientras que la seguridad de la información comprende los aspectos estratégicos o de gestión correspondiente a seguridad dentro de una organización (ISOTools Excellence, 2017).

2.2.6.1. Seguridad informática

Quiroz y Macías (2017) definen la seguridad informática como la capacidad que tienen las empresas para definir un conjunto de prácticas, políticas, técnicas, reglas y guías de operación con la finalidad de resguardar los recursos informáticos de cualquier daño o sustracción de los que puedan ser víctimas, mediante una gestión de riesgos de tal forma que garanticen el funcionamiento ininterrumpido de dichos recursos informáticos.

Aduanalmente se encarga de salvaguardar a las personas, para lo cual la cultura de seguridad mediante capacitación sobre buenas prácticas y medidas preventivas de seguridad que les ayude a tener noción sobre las amenazas y como prevenirlas debe ser considerada y valorada como una

Repositorio Institucional - UNASAM - Perú

herramienta de seguridad contra la prevención de incidentes, con esto los usuario pueden tomar las medidas preventivas correspondientes y brindarle un mayor nivel de seguridad al desarrollo de sus actividades, existen múltiples términos y problemas como phishing, ingeniería social, troyanos, respaldos de información, etc. Que los usuarios deberían conoces como parte de la cultura de seguridad (Roque y Juárez, 2018).

2.2.6.2. Seguridad de la información

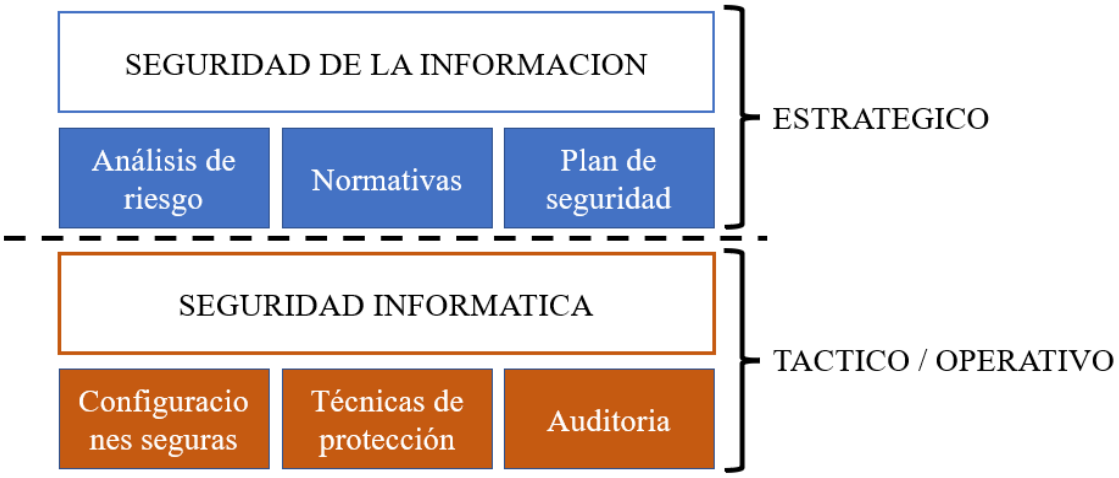
Hablar de seguridad de la información es hablar de riesgos, amenazas, buenas prácticas y estándares o marcos de seguridad que nos llevan al aseguramiento de la tecnología y los procesos para incrementar el nivel de seguridad y confianza en la información durante todas sus fases existenciales para esto se apoya de la seguridad informática de tal manera que se aseguremos el cumplimiento de las dimensiones (Confidencialidad, disponibilidad e integridad) de los activos de información (ISOTools Excellence, 2017).

Tengamos claro que la seguridad total no existe, lo que si existe es un nivel de seguridad determinado que puede ser alto o bajo dependiendo de los procesos implementados, la infraestructura tecnológica manejada, los ambientes utilizados y el nivel de capacitación del personal, por ende, mientras mayor sea el nivel de madurez de la estos factores indispensables para la gestión de seguridad, mayor será el nivel de resguardo de la información de la organización (Cámara de bancos e instituciones financieras de Costa Rica, 2017).

Repositorio Institucional - UNASAM - Perú

Figura 3

Seguridad de la información vs seguridad informática



Nota: Observamos en figura una clara diferencia entre seguridad de la información y seguridad informática. Fuente: ISOTools Excellence (2017).

2.2.7. Gestión de Seguridad de la información

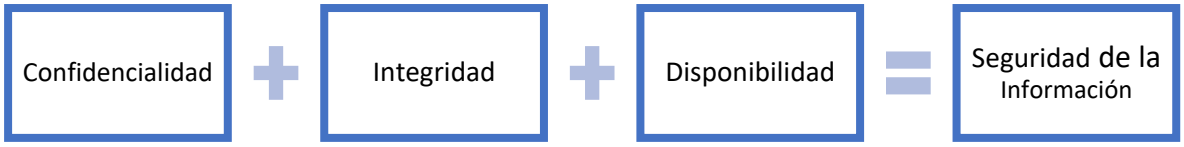
Teniendo muy claro que uno de los principales activos para el correcto funcionamiento de una entidad u organización es la información, la cual se encuentra expuesta a un gran número de amenazas sea de índole natural o por un descuido humano tanto deliberadas como accidentales es necesario definir medidas de protección para esta.

Asegurar la preservación de las dimensiones confidencialidad, disponibilidad e integridad (CDI) de la información es el núcleo de la seguridad de la información (SI) esto implica aplicar y gestionar controles de seguridad apropiados para el amplio número de amenazas latentes de tal manera que podamos avalar la continuidad del negocio y minimizar los estragos ante la posible ocurrencia de un suceso de seguridad que pueda causar daños o perdida a una determinada entidad. Un buen nivel de seguridad está basado en la adecuada implementación de controles de seguridad, los cuales deben ser especificados, implantados, controlados, evaluados y reformados constantemente esperando que estos se integren a los diversos procesos de la organización, los controles deberán ser seleccionados en base a una gestión de riesgos y debidamente gestionados con un SGSI (ISO, 2018).

Repositorio Institucional - UNASAM - Perú

Figura 4

Integración de las dimensiones de seguridad



Nota: observamos que la figura muestra la integración de los pilares que componen la seguridad de la información, las cuales deben ser preservadas mediante una correcta gestión. Fuente: Elaboración propia.

2.2.8. El estado peruano y la gestión de seguridad de la información

Con el proceso de transformación digital del estado peruano surgieron las necesidades de conformar entes reguladores encargados de gestionar, supervisar e integrar las operaciones referentes a la seguridad digital como un apartado más de la seguridad nacional con la finalidad de fortificar la confianza digital del estado peruano, siendo uno de estos entes el Centro Nacional de Seguridad Digital (CNSD), entre los objetivos del CNSD encontramos:

1) establecer la comunicación necesaria entre los entes informáticos de dirección pública para recopilar información que permita generar soluciones para los diferentes incidentes de seguridad.
2) Proponer normas que ayuden a desarrollar mayores niveles de seguridad en los sistemas informáticos y sus recursos.
3) Proteger los sistemas de información y comunicación del sector publico

Adicionalmente, el gobierno peruano cuenta con la Autoridad Nacional de Protección de Datos Personales quien es la encargada de hacer cumplir las normativas existentes referentes a la protección de datos personales (“Gobierno Peruano”, 2022).

2.2.9. Modelo de madurez

Según la Escuela de administración de negocios (ESAN, 2019) Un modelo de madurez es la integración de instrumentos de medición, discernimientos de

Repositorio Institucional - UNASAM - Perú

evaluación, etc. Con la finalidad de definir el nivel en el que una empresa se encuentra haciendo uso de prácticas adecuadas en lo que respecta a la gestión de proyectos.

Según el Software Enginnering Institute (2010) en su marco de trabajo "Capability Maturity Model Integration (CMMI)" describe el modelo de madurez como un conjunto de buenas prácticas para lograr la mejorar determinados procesos que intervienen en el desarrollo de servicio y/o productos de calidad.

2.2.10. El estándar O-ISM3 V 2.0

Estándar que maneja un enfoque basado en procesos con la finalidad de mejorar la gestión de seguridad de la información (GSI), que desglosa la GSI en una cantidad manejable de procesos con controles de seguridad específicos para cada proceso. Este estándar define la madurez de la GSI como una combinación de procesos operados, define la capacidad en términos de métricas de seguridad y prácticas de seguridad (The Open Group, 2017).

O-ISM3 es tecnológicamente neutral por lo que los profesionales de seguridad pueden usar este estándar y técnicas según se acomode a sus objetivos de sus procesos, O-ISM3 define el nivel de madurez de la GSI en base a la capacidad de un determinado número de procesos O-ISM3 definidos para una organización, teniendo en cuenta el nivel de inversión y los beneficios obtenidos a corto, mediano y largo plazo (The Open Group, 2017).

2.2.10.1. Nivel de capacidad según O-ISM3

Los procesos O-ISM3 seleccionados y la capacidad con la que se opera cada proceso determina la madurez de la GSI de una organización. Las métricas son las encargadas de brindar la capacidad de pasar de un estado inicial a un estado optimizado, la siguiente tabla muestra las métricas del nivel de capacidad propuestos por O-ISM3 (The Open Group, 2017).

Repositorio Institucional - UNASAM - Perú

Tabla 1

Nivel de capacidad según O-ISM3

NIVEL DE CAPACIDAD	INICIAL (1)	GESTIONADO (2)	DEFINIDO (3)		CONTROLADO (4)		OPTIMIZADO (5)
Prácticas de gestión implementadas	Auditar y certificar	Pruebas	Planificación	Vigilancia	Ejecución de beneficios	Mejora de la calidad	Mejora del rendimiento
documentación	x	x	x	x	x	x	x
METRICAS ACTIVIDAD			x	x	x	x	x
ALCANCE			x	x	x	x	x
EFICACIA			x	x	x	x	x
CALIDAD					x	x	x
CARGA							x
EFICIENCIA							x

Nota: La tabla muestra la capacidad de los procesos O-ISM3 repartido en niveles establecidos por el estándar O-ISM3 V 2.0 y las métricas necesarias para optar cada nivel, tomado de The open group (2017).

Repositorio Institucional - UNASAM - Perú

2.2.10.2. Nivel de madurez según O-ISM3

O-ISM3 defines cada nivel de madurez en base a una combinación de procesos O-ISM3 que se practican en una determinada organización a un nivel de capacidad determinado teniendo una estrecha correlación entre la cantidad de procesos implementados, el nivel de capacidad de cada proceso la cual definirá el nivel de madurez de la GSI, dicho de otra manera, mientras mayor sea la cantidad de procesos implementados con una mayor capacidad de ejecución mejor será el nivel de madurez (The open group, 2017).

2.2.10.3. Procesos de seguridad O-ISM3

El estándar O-ISM3 define 4 niveles de gestión de seguridad teniendo en cuenta que cada tipo de proceso reporta a la anterior.

a) Procesos Genéricos

Es la responsable de proporcionar la estructura esencial para la ejecución, valoración y progreso de los procesos O-ISM3 definidos (The open group, 2017).

b) Procesos estratégicos

Es la responsable de seleccionar y deseñar servicios teniendo en cuanta los recursos, el costo y el riesgo de la organización, de tal forma que los recursos económicos, humanos, et. Sean utilizados en pro de la GSI (The open group, 2017).

c) Procesos tácticos

Responsable de la administración de recursos asignados a la gestión de la seguridad de la información además de ser responsable de definir el entorno para los procesos operativos (The open group, 2017).

d) Procesos operativos

Es la responsable de emplear operacionalmente los recursos asignados de porfa eficiente (The open group, 2017).

2.2.10.4. O-ISM3 en el contexto empresarial

Los lineamientos para una adecuada GSI establecido por O-ISM3 analiza el impacto que tiene la seguridad de la información en el logro de sus

Repositorio Institucional - UNASAM - Perú

objetivos además de brindar herramientas necesarias para la gestión de la seguridad mediante los procesos O-ISM3.

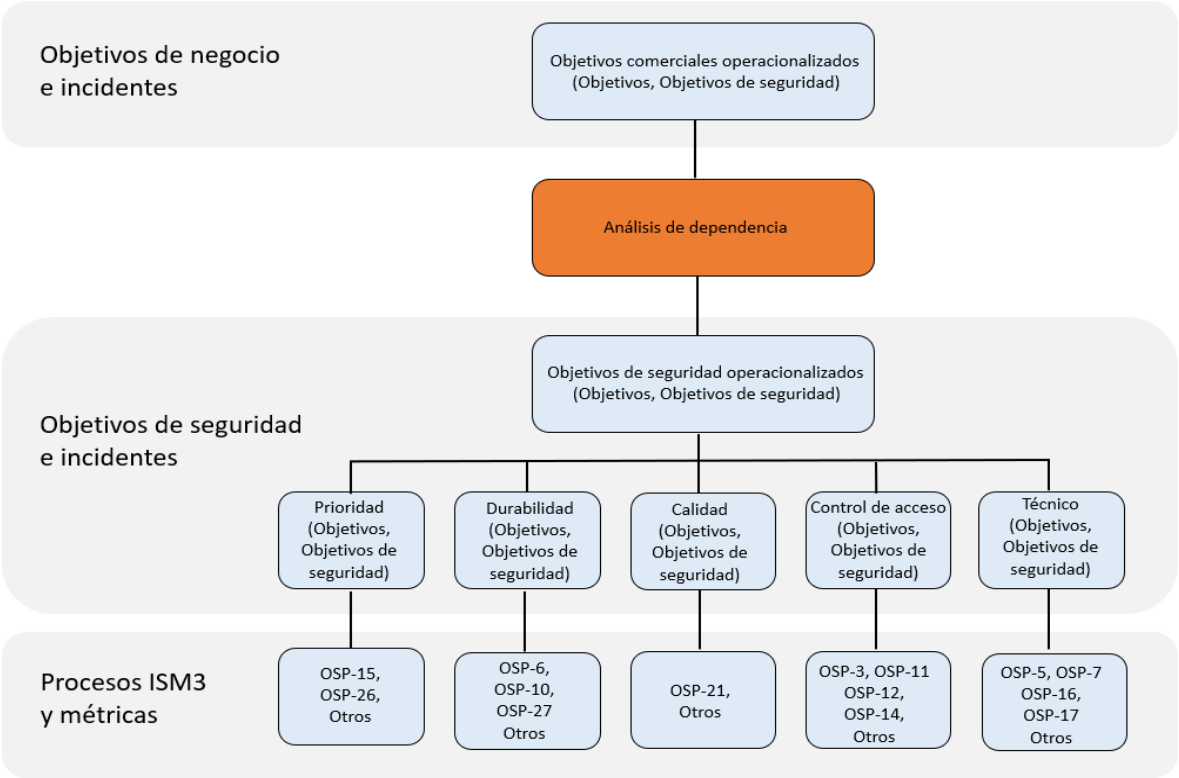
O-ISM3 define la seguridad de la información dependiendo del contexto en el que se trabaja (la organización) algunos procesos y objetivos de seguridad pueden funcionar de forma adecuada en una organización mas no significa que funcionen de la misma forma en otra ya que el contexto y realidad de la organización es completamente diferente (The open group, 2017).

2.2.10.5. Modelo de seguridad O-ISM3

El modelo de seguridad planteado por O-ISM3 según contexto está definido en la figura.

Figura 5

Modelo de seguridad O-ISM3



Nota: La figura plasma el modelo de seguridad definido por los lineamientos de O-ISM3 según el contexto de la organización. Fuente: The open group (2017).

Repositorio Institucional - UNASAM - Perú

2.3. Definición de términos

1) **Confidencialidad**

Propiedad que asegura que los datos/información no están abiertas a individuos, entes o procedimientos no autorizados (ISO, 2018).

2) **Integridad**

Característica de la información que asegura su exactitud y completitud (ISO, 2018).

3) **Disponibilidad**

Característica que asegura que los datos/información están accesibles y utilizables ante la demanda autorizada de una entidad (ISO, 2018).

4) **O-ISM3**

Abreviatura del ingles Open Information Security Management Maturity Model (The open group, 2017).

5) **ISM**

Abreviatura del ingles Information Security Management (The open group, 2017).

6) **ISO**

International Organization of Standarization (ISO, 2018).

7) **Amenaza**

Potencial origen de un incidente que puede generar daños cuantiosos a una organización (ISO, 2018).

8) **Riesgo**

Es la mezcla de las consecuencias y la posibilidad de ocurrencia de un incidente/evento (ISO, 2018).

9) **GSI**

Gestión de seguridad de la información (The open group, 2017).

10) **SGSI**

Sistema de gestión de seguridad e la información (The open group, 2017).

11) **SI**

Seguridad de la información (The open group, 2017).

Repositorio Institucional - UNASAM - Perú

2.4. Hipótesis

2.4.1. Hipótesis general

La aplicación del estándar O-ISM3 mejora de manera significativa la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022.

2.4.2. Hipótesis específicas

1) La aplicación del estándar O-ISM3 mejora de manera significativa la confidencialidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

2) La aplicación del estándar O-ISM3 mejora de manera significativa la disponibilidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

3) La aplicación del estándar O-ISM3 mejora de manera significativa la integridad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

2.5. Variables

2.5.1. Variable independiente

Estándar O-ISM3

2.5.2. Variable dependiente

Seguridad de la información

2.5.3. Operacionalización de variable

Repositorio Institucional - UNASAM - Perú

Tabla 2

Operacionalización de variables

“ESTÁNDAR O-ISM3 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN LA CLÍNICA SAN PABLO S.A.C. – HUARAZ, 2022”					
VARIABLE	**DEFINICIÓN CONCEPTUAL**	**DEFINICIÓN OPERACIONAL**	**DIMENSIONES**	**INDICADORES**	**ESCALA DE MEDICIÓN**
Variable Independiente: **Estándar O-ISM3**	O-ISM3 es el marco para GSI y se enfoca en los procesos comunes de SI que comparten la mayoría de las organizaciones. delimitando las métricas operacionales y sus variaciones. (The Open Group, 2017). O-ISM3 ofrece un enfoque de procesos para la SGI y una amplia lista de procesos implementables a seleccionar de tal manera que permita concretar una mejora continúa haciendo uso de métricas de seguridad (The open group, 2017).	Establecer un modelo de madurez basado en el estándar O-ISM3 para mejorar la seguridad de la información la Clínica San Pablo S.A.C – Huaraz, 2022.	Procesos de seguridad Gestión de seguridad de la información	• Presencia de controles de seguridad en los procesos de gestión de seguridad • Presencia de prácticas de seguridad	La medición de los indicadores será realizada mediante una escala de Likert - de frecuencia con una puntuación del 1 al 5 siendo 1 la mínima y 5 la máxima frecuencia de ocurrencia o repetición.

Repositorio Institucional - UNASAM - Perú

Variable Dependiente: **Seguridad de la información**	Entendamos la seguridad de la información como el aseguramiento y conservación de la confidencialidad, disponibilidad e integridad de la información. (ISO, 2018). Vinculo de medidas anticipadas y reactivas que las entidades y los sistemas deben tener admitiendo el respaldo y protección de la información buscando mantener los pilares o dimensiones de la misma (Cámara de bancos e instituciones financieras de Costa Rica, 2017).	Mejorar la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022 a través de la aplicación del estándar O-ISM3	Confidencialidad Integridad Disponibilidad	• Presencia de procesos de GSI • Nivel de madurez de la capacidad los procesos de GSI

Nota: La tabla muestra la operacionalización de variable del presente trabajo de tesis.

Repositorio Institucional - UNASAM - Perú

III. METODOLOGIA

3.1. Tipo de estudio

Según el enfoque es cuantitativo con nivel correlacional explicativo.

3.2. El diseño de investigación

La presente pertenece al diseño preexperimental de prueba – posprueba con un solo grupo.

G	O1	X	O2

O1: prueba del grupo experimental

X: aplicación del estándar O-ISM3

O2: posprueba del grupo experimental

3.3. Descripción de la unidad de análisis población y muestra

3.3.1. Unidad de análisis

Trabajador de la Clínica San Pablo S.A.C. - Huaraz

3.3.2. Población

Para el desarrollo de la tesis se tomó como población el total de trabajadores de la Clínica San Pablo S.A.C. – Huaraz, siendo este un total de 200 trabajadores.

3.3.3. Muestra

Teniendo en cuenta que la SI involucra a toda la organización siendo compromiso de cada trabajador aportar a la preservación de la información, por lo cual cada individuo de la población tiene una igual de probabilidad para pertenecer a la muestra ya sea personal administrativos o asistenciales.

Dicho esto, se determinó la muestra mediante un muestro aleatorio simple para poblaciones finitas el cual es una técnica de muestreo perteneciente al método de muestreo probabilístico, para ello aplicamos la siguiente formula:

Repositorio Institucional - UNASAM - Perú

Figura 6

Fórmula para el cálculo de muestra

$$\text{Tamaño de muestra} = \frac{NZ^2pq}{e^2(N-1)+Z^2pq}$$

Nota: La figura refleja la fórmula utilizada en el cálculo matemático de la muestra cuando se maneja una población finita/definida. Fuente: Castellanos (2011).

Donde:

Z = Nivel de confianza (95% = 1.96)

p = Probabilidad de aceptación (50% = 0.5)

q = Probabilidad de rechazo (50% = 0.5)

e = Margen de error (5% = 0.05)

N = tamaño de la población (200)

Realizando los cálculos obtenemos:

$$\text{Tamaño de muestra} = \frac{(200)(1.96)^2(0.5)(0.5)}{(0.05)^2(200-1)+(1.96)^2(0.5)(0.5)} = 131.52$$

Por los cálculos realizados, la muestra quedo definida con un total de 132 trabajadores de la Clínica San Pablo S.A.C. - Huaraz.

3.4. Técnicas de instrumentos de recolección de datos

La técnica utilizada en la recolección de información:

1) Encuesta

Es el análisis que el investigador realiza para recopilar información mediante un conjunto de preguntas elaboradas y diseñadas con antelación las cuales fueron dirigidas a los individuos pertenecientes a la muestra calculada, con la finalidad de conocer su percepción sobre la SI.

Para la ejecución de la investigación presente utilizamos preguntas cerradas y una escala de Likert con una valoración del 1 al 5, para entender la frecuencia de ocurrencia de algunos eventos que evidencien el nivel de SI y estuvo dirigido a 132 trabajadores de la Clínica San Pablo S.A.C. - Huaraz.

Repositorio Institucional - UNASAM - Perú

3.5. Técnicas de análisis y prueba de hipótesis

3.5.1. Técnicas de análisis

Se optó por usar un análisis estadístico inferencial con la finalidad de demostrar la hipótesis planteada.

La data recolecta fue procesada mediante el SPSS versión 26, software utilizado para el análisis estadístico.

3.5.2. Prueba de hipótesis

Para someter a prueba el planteamiento de la hipótesis fue necesario elaborar una base de datos para posteriormente construir tablas de distribución de frecuencia unidimensionales y bidimensionales.

Para la contrastación de la hipótesis se tuvo en cuenta el cumplimiento de los datos con los requisitos de normalidad, cuyo cumplimiento fue sometido a una prueba de normalidad tanto en el pre y pos test obteniendo un nivel de significancia menor al establecido ($p<0.05$) comprobando que los datos no cumplen con los requisitos de normalidad, por lo cual se optó por realizar la prueba de hipótesis mediante la prueba no paramétrica de Wilcoxon para muestras relacionadas (pre y pos test).

Tabla 3

Normalidad de los datos

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Confidencialidad en el pre test	,113	132	**,000**	,952	132	,000
Disponibilidad en el pre test	,119	132	**,000**	,917	132	,000
Integridad en el pre test	,133	132	**,000**	,912	132	,000
Seguridad de la información en el pre test	,117	132	**,000**	,885	132	,000
Confidencialidad en el pos test	,143	132	**,000**	,903	132	,000

Repositorio Institucional - UNASAM - Perú

Disponibilidad en el pos test	,127	132	**,000**	,939	132	,000
Integridad en el pos test	,135	132	**,000**	,918	132	,000
Seguridad de la información en el pos test	,159	132	**,000**	,894	132	,000

Nota: La tabla refleja el nivel de significancia de la prueba de Kolmogorov, prueba utilizada debido a que el tamaño de nuestra población es mayor a 30.

Repositorio Institucional - **UNASAM** - Perú

IV. RESULTADOS DE LA INVESTIGACIÓN

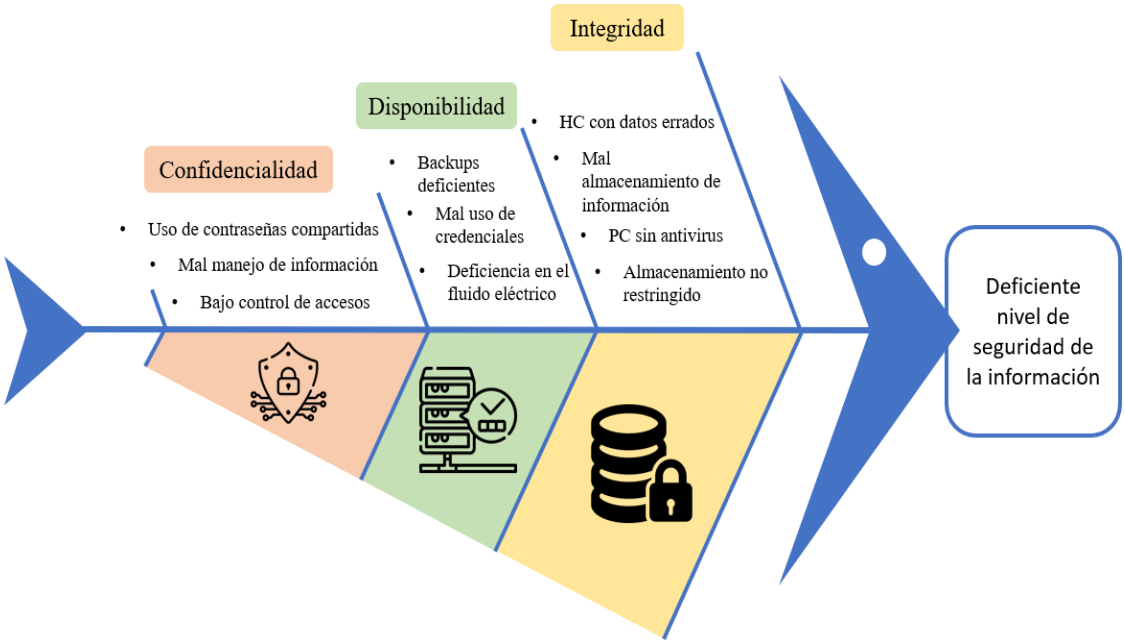
4.1. Descripción del trabajo de campo

4.1.1. Análisis de situación actual

Como acción inicial se realizó un análisis que refleje la realidad actual de la Clínica San Pablo S.A.C. – Huaraz, de tal forma que podamos identificar las deficiencias claras y más recurrentes respecto a la SI, los procesos de seguridad utilizados y la capacidad que manejan de tal forma que nos permita definir el nivel de madurez de la SI que la entidad tenía antes de la implementación del estándar O-ISM3. Si bien es cierto, la empresa realiza y cuenta con algunos procedimientos de seguridad que son realizados de forma reactiva, los cuales no cubren a un nivel aceptable los aspectos de seguridad necesarios para la empresa, además la frecuencia de algunos de estos procedimientos no son las adecuadas como para considerarlas óptimas, algunas de las falencias detectadas se ven reflejadas a continuación.

Figura 7

Deficiencias de seguridad



Nota: La figura muestra las deficiencias detectadas en la Clínica San Pablo con relación a las dimensiones de la SI. Fuente: Elaboración propia.

Repositorio Institucional - UNASAM - Perú

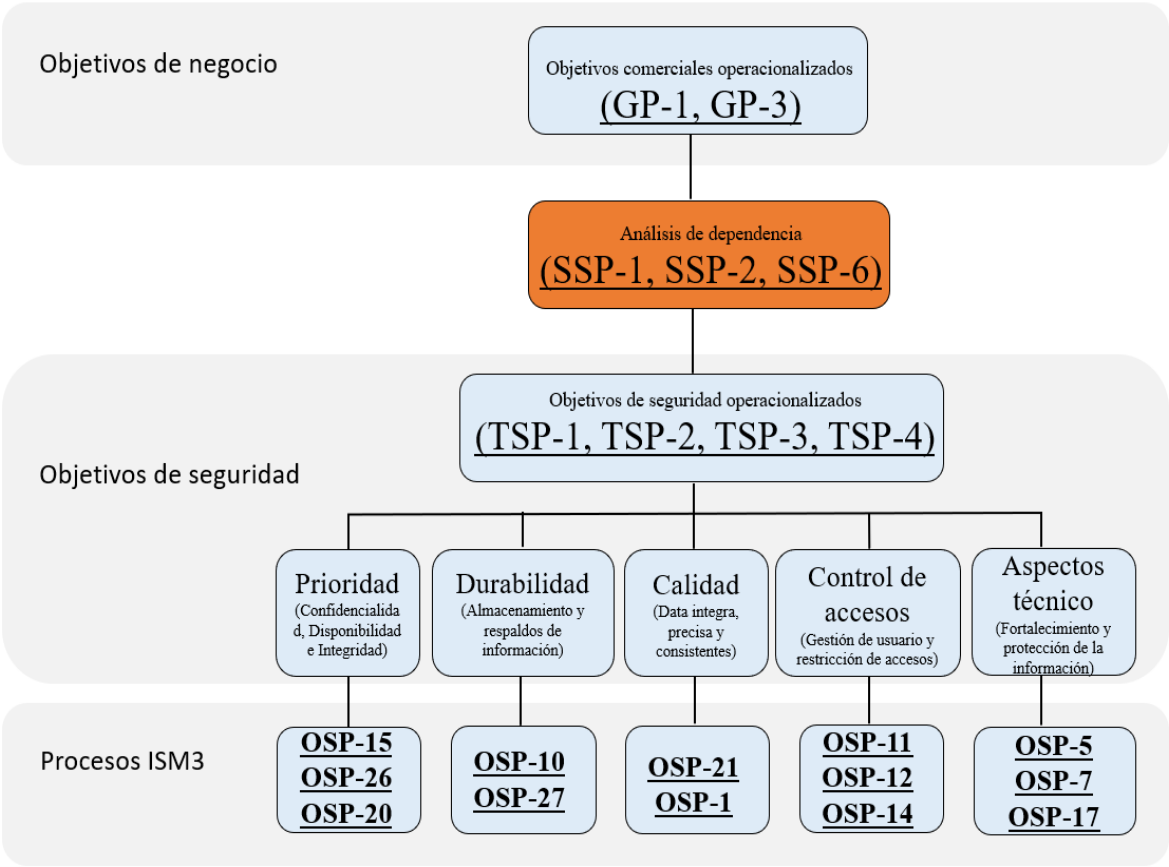
4.1.2. Análisis y selección de Procesos O-ISM3

Para la selección de procesos O-ISM3 fue fundamental realizar un análisis cuidadoso de los procesos en relación a las circunstancias de la organización, políticas de seguridad existente y recursos disponibles, es fundamental tener en cuenta estos aspectos al seleccionar procesos O-ISM3 si lo que se desea es generar el mayor beneficio en relación con la SI.

Adicionalmente se hizo uso del modelo de seguridad definido por O-ISM3 como herramienta para facilitarnos la clasificación de Procesos O-ISM3 idóneos para la Clínica San Pablo. S.A.C.

Figura 8

Modelo de seguridad para Clínica San Pablo S.A.C - Huaraz



Nota: La figura refleja los procesos O-ISM3 seleccionados para la Clínica San Pablo S.A.C. – Huaraz plasmados en el modelo de seguridad O-SIM3. Fuente: Elaboración propia.

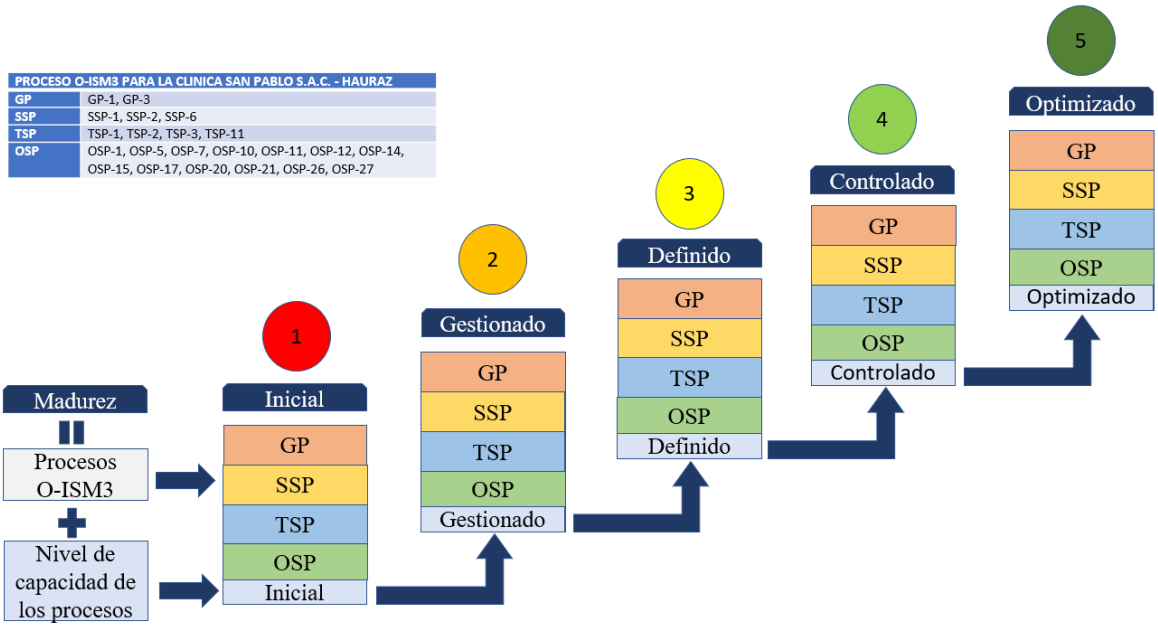
Repositorio Institucional - UNASAM - Perú

4.1.3. Diseño del modelo de madurez de seguridad de la información

El modelo se presentó de manera gráfica y fue diseñada teniendo en consideración lo definido por el estándar O-ISM3, el cual precisa el modelo de madurez como una combinación de procesos previamente seleccionados según contexto y necesidad de la organización y el nivel de capacidad que tiene cada proceso, basado en los procesos seleccionados se procedió con la elaboración del modelo de madurez propuesto para la Clínica San Pablo S.A.C. – Huaraz.

Figura 9

Modelo de madurez propuesto para la Clínica San Pablo S.A.C. - Huaraz



Nota: La figura muestra el modelo de madurez propuesto para la Clínica San Pablo S.A.C. - Huaraz. Fuente: Elaboración propia.

4.1.3.1. Niveles de madurez

Los niveles representan el grado de capacidad de los procesos O-ISM3 respecto al contexto analizado en la Clínica San Pablo S.A.C., los cuales deberán ser escalados con el objetivo de mejorar la SI. Para el modelo propuesto se definieron 5 Niveles de Madurez:

1) **Inicial o nivel 1:** La organización toma este nivel cuando cuenta con procesos los O-ISM3 seleccionados a un nivel de capacidad inicial

es decir con prácticas de gestión no documentados, pero sin manejo de métricas.

2) **Gestionado o nivel 2:** La empresa adopta este nivel cuando cuenta con lo estipulado en el nivel inicial agregándole de manera documenta sin la necesidad de manejar métricas.
3) **Definido o nivel 3:** La empresa adopta este nivel cuando cuenta con lo estipulado en el nivel inicial agregándole prácticas de gestión de planificación y vigilancia con métricas de actividad, alcance y eficacia.
4) **Controlado o nivel 4:** Este nivel es alcanzado cuando la empresa empieza a manejar métricas de calidad adicionalmente a todo lo estipulado en el nivel definido.
5) **Optimizado o nivel 5:** Este es el nivel más alto del modelo y es alcanzado cuando la organización cuenta con los procesos O-ISM3 seleccionados, prácticas de gestión documentadas y todas las métricas definidas por el estándar O-ISM3.

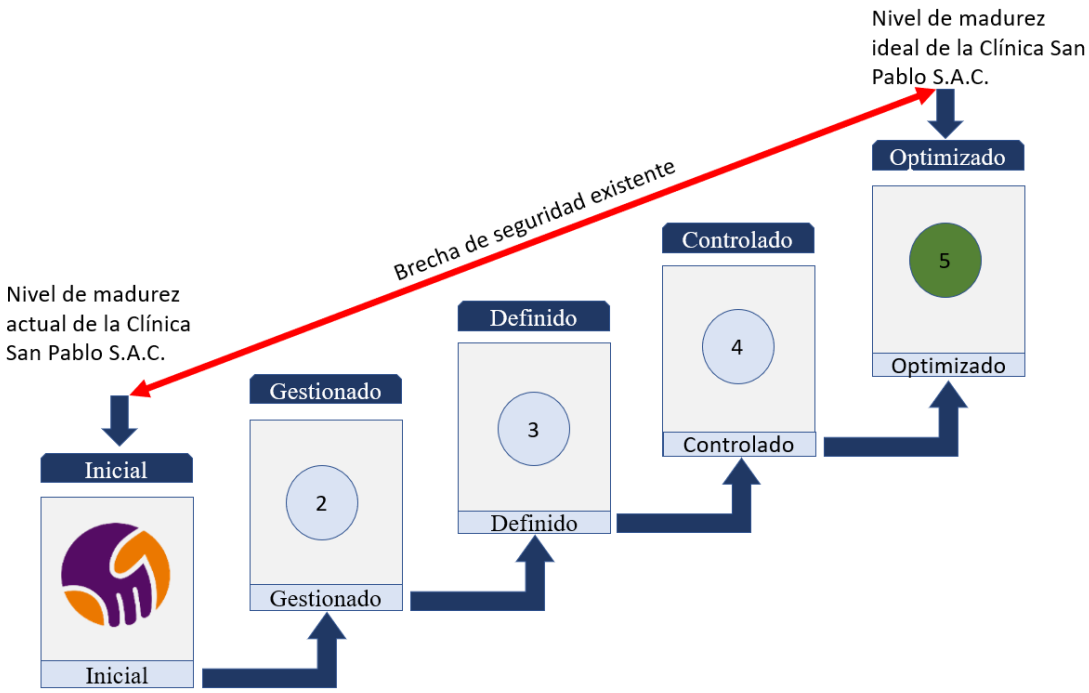
4.1.4. Análisis de brecha

Como se mencionó en el punto anterior el personal de la Clínica San Pablo S.A.C. – Huaraz realiza determinados procedimientos de SI sin embargo estos están mal gestionados, como por ejemplo: la empresa ya cuenta con una política de SI la cual no es de conocimiento de todos los trabajadores así mismo los trabajadores de TI realizan determinados procedimientos de seguridad, pero sin ningún objetivo planteado como por ejemplo: El proceso para realizar respaldos de información o también llamado backups de información los cuales son realizados sin ningún tipo de control, sin una frecuencia definida, sin un alcance definido, en un repositorio no adecuado, falencias como esta fueron analizadas y plasmadas en el modelo de madurez propuesto definiendo así que la Clínica San Pablo S.A.C. -Huaraz, se encuentra en un nivel de madurez inicial o nivel 1 con una brecha de 4 niveles para lograr el nivel de madurez ideal.

Repositorio Institucional - UNASAM - Perú

Figura 10

Brecha de seguridad existente



Nota: La figura muestra la grieta de seguridad existente tomando en cuenta el nivel actual de la Clínica San Pablo con relación a un nivel ideal. Fuente: Elaboración propia.

4.1.5. Implementación del modelo de madurez

Existen dos posibles escenarios en la implementación de un modelo de madurez basado en el estándar O-ISM3: una implementación de arriba hacia abajo o una implementación de abajo hacia arriba para el desarrollo de la presente optamos por realizar una implementación de arriba hacia abajo debido a que la iniciativa de aplicar el estándar O-ISM3 no nació desde la gerencia o cabezas de la organización sino partió de la iniciativa de un personal del área de TI en este caso el investigador.

4.1.5.1. GP-1: Gestión del conocimiento

1. **Descripción del proceso:**

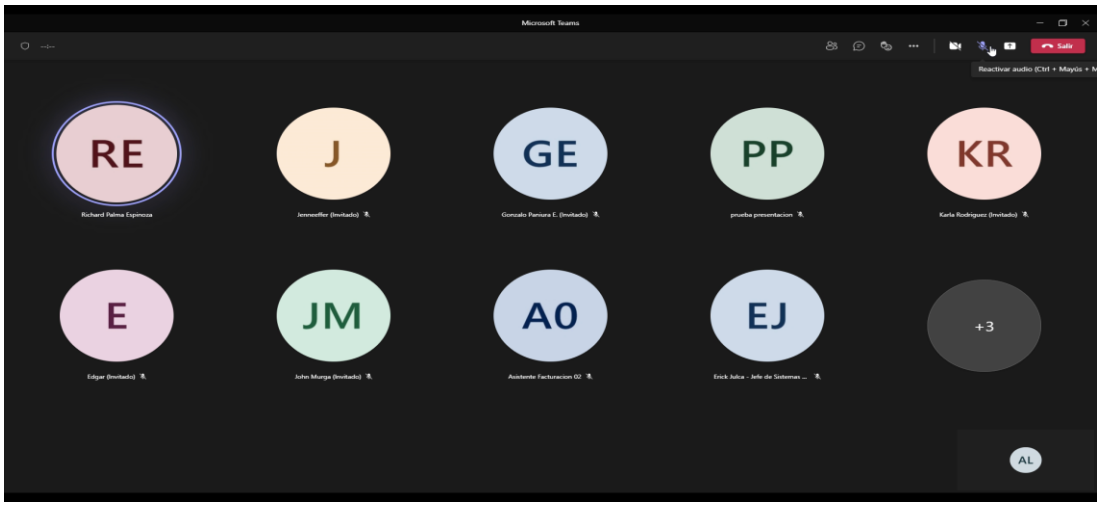
Encargado de recopilar, almacenar y compartir conocimientos dentro de la organización en nuestro caso específico el conocimiento referente a seguridad de la información, procesos adecuados, etc. Con el fin de manejar conocimiento actualizado sobre las nuevas amenazas generadas con el contexto social y desarrollo tecnológico.

2. **Objetivos planteados:**
   a. Manejar conocimiento actualizado sobre seguridad de la información
   b. Asegurar que los procesos se realicen de forma correcta
3. **Propietario del proceso:**
   a. Área de sistemas
   b. Área de Recurso Humanos
   c. Área de Procesos
4. **Actividades realizadas:**

   El proceso fue implementado mediante capacitaciones y reuniones realizadas a en sede y de manera corporativa teniendo al personal de TI de sede y corporativo involucrado en temas de seguridad de la información y al personal de procesos y recursos humanos en las capacitaciones sobre procedimientos correctos, debido a la coyuntura causada por el COVID-19, toda reunión y capacitación fue realizada de manera virtual haciendo uso de la herramienta Microsoft Teams.

Figura 11

Capacitaciones virtuales para replicar el conocimiento



Nota: La figura muestra una de las múltiples capacitaciones realizadas con las que se aplicó el proceso GP-1. Fuente: Elaboración propia.

4.1.5.2. GP-3: Implementación de O-ISM3 o Diseño y evolución de la gestión de seguridad de la información

1. **Descripción del proceso:**

   Este proceso es el encargado de seleccionar los procesos genéricos, estratégicos, tácticos y operativos necesarios para el logro de objetivos de seguridad el cual fue aplicado en base al modelo de seguridad O-ISM, como se puede apreciar en el punto 4.1.2.

2. **Objetivos del proceso:**
   a. Analizar el nivel de madurez actual de la entidad de estudio
   b. Seleccionar los procesos O-ISM3 para la entidad de estudio
   c. Elaborar el modelo de madurez
   d. Efectuar los procesos O-ISM3
   e. Evaluar el nivel de capacidad de los procesos implementados

3. **Propietarios del proceso:**
   a. Área de TI

4. **Actividades realizadas:**

   Las actividades realizadas en este proceso contemplan prácticamente todas las actividades realizadas en implementación del estándar O-SIM3 descrito en la presente investigación.

4.1.5.3. SSP-1: Informes a las partes interesadas

1. **Descripción de proceso:**

   Encargado de reportar el cumplimiento de la implementación del modelo de madurez propuesto y algún punto adicional que la gerencia general (GG), gerencia administrativa (GA) y dirección médica (DM) requieran.

2. **Objetivos planteados:**
   a. Brindar información a la gerencia que le admita tomar acciones con respectos a la seguridad de la información

3. **Propietario del proceso:**
   a. Área de TI

Repositorio Institucional - UNASAM - Perú

b. Gerencia General

4. **Actividades realizadas:**

Para este proceso se estableció inicialmente la realización de reuniones semestrales con próxima modificación a reuniones mensuales siempre y cuando se cumpla con la formación de un comité de SI, en caso este sea concretado la propiedad del proceso se transfiere al comité.

4.1.5.4. SSP-2: Coordinación

1. **Descripción del proceso:**

Proceso encargado de la coordinación entre las partes interesadas (GG, GA, DM) y la parte encargada de la GSI (TI o comité de seguridad de la información)

2. **Objetivos planteados:**

a. Establecer una buena comunicación entre las cabezas a cargo de la entidad y área encargada de la implementación de O-ISM3 o comité de seguridad de la información

3. **Propietario del proceso:**

a. Gerencia general

b. Gerencia administrativa

4. **Actividades realizadas:**

Este proceso fue aplicado mediante el uso de diferentes herramientas de comunicación, tales como: WhatsApp, Reuniones por Microsoft Teams, correo electrónico y a nexo telefónico.

4.1.5.5. SSP-6: Asignar recursos para la seguridad de la información

1. **Descripción del proceso:**

Este proceso es la encargada de asignar recursos monetarios, de personal e instalaciones para que la gestión táctica (TSP) y operativa (OSP) ejecuten sus respectivos procesos con normalidad.

2. **Objetivos planteados:**

a. Brindar los recursos necesarios a los procesos tácticos y operativos

3. **Propietario del proceso:**

a. Gerencia general

b. Gerencia administrativa

Repositorio Institucional - UNASAM - Perú

4. **Actividades realizadas:**

   En este proceso se solicitaron los vistos buenos para la implementación, modificación de los estándares de trabajo utilizados hasta entonces sustentados en los resultados derivados del análisis de situación actual de la entidad de estudio, así como la solicitud de apoyo del personal a las áreas involucradas para poder contar con una ventana de tiempo que nos permita realizar las acciones propuestas adicionalmente se propuso la implementación de algunas herramientas de mayor costo las cuales son detalladas en la gestión operativa (OSP).

4.1.5.6. TSP-1: Reporte a gerencia estratégica

1. **Descripción del proceso:**

   Encargado presentar un informe periódico sobre la seguridad de la información y sobre el uso de los recursos asignados.

2. **Objetivos del proceso:**

   a. Informar a las partes interesadas el rendimiento del modelo de madurez propuesto.

3. **Propietario del proceso:**

   a. Área de TI

4. **Actividades realizadas:**

   Elaboración de reportes que permitieron apreciar las actividades operacionales a favor de la SI como, por ejemplo: Elaboración y actualización de inventario de activos, operatividad de los activos informáticos, distribución correcta de licencias de antivirus, etc.

4.1.5.7. TSP-2: Administrar recursos asignados

1. **Descripción del proceso:**

   Este proceso se encarga de asignar los recursos a la gestión operativa o procesos operacionales especifico (OSP).

2. **Objetivos del proceso:**

   a. Control en la distribución de los recursos para asegurar la correcta GSI.

3. **Propietario del proceso:**

   a. Área de TI

4. **Actividades realizadas:**

Repositorio Institucional - UNASAM - Perú

Elaboración un presupuesto anual presentado a la gerencia teniendo en cuenta los costos económicos que significaría el mantener la seguridad e la información en un nivel de seguridad considerable dentro del presupuesto se tuvieron en cuenta factores como Licencias de Antivirus a utilizar anualmente, Licencias de Windows Server 2022, Renovación de equipo informático para asegurar su disponibilidad, etc.

Adicionalmente se administró recurso humano del área de TI definiendo actividades con una determinada frecuencia en un periodo de tiempo como, por ejemplo: Un personal orientado al seguimiento de los procesos O-ISM3, un personal orientado al seguimiento y elaboración de los respaldos de información, etc.

4.1.5.8. TSP-3: Definir objetivos de seguridad

1. **Descripción del proceso:**

   Precisar los objetivos de seguridad dentro del dominio administrado por TI teniendo en cuenta los requisitos establecidos en el modelo de seguridad O-ISM3 (Prioridad, Durabilidad, Calidad, Control de accesos y aspectos técnicos).

2. **Objetivos del proceso:**

   a. Definir lo que se desea lograr de tal forma que sirva como cimiento para la selección de procesos

3. **Propietario del proceso:**

   a. Área de TI

4. **Actividades realizadas:**

   En este proceso se definieron los objetivos de seguridad los cuales para este caso específico se compartieron los objetivos de investigación planteados adicionando a estos algunos objetivos de seguridad como son:

   - Ofrecer a la organización un modelo de madurez funcional y de fácil entendimiento
   - Incrementar el nivel de madurez de SI de la Clínica San Pablo S.A.C. – Huaraz.
   - Estandarizar las características técnicas de los equipos informáticos de tal forma que podamos asegurar su disponibilidad operativa.

Repositorio Institucional - UNASAM - Perú

- Brindar un soporte adecuado ante algún posible incidente de seguridad.
- Asegurar la confidencialidad, disponibilidad e integridad de la SI.
- Mejorar la cultura organizacional referente a la GSI.

4.1.5.9. TSP-11: Conciencia de seguridad

1. **Descripción del proceso:**

   Responsable de elevar el perfil de seguridad de la información de los usuarios.

2. **Objetivos del proceso:**

   a. Aplicar prácticas de seguridad adecuadas

   b. Capacitar periódicamente a los trabajadores de clínica sobre temas de seguridad de la información

3. **Propietario del proceso:**

   a. Recursos Humanos

   b. Área de TI

4. **Actividades realizadas:**

   Para la ejecución de este proceso fue necesario realizar la coordinación con gerencia para solicitar la autorización de realizar capacitaciones periódicas sobre SI por parte del personal de TI de sede y corporativo.

   Una vez obtenida el visto bueno de gerencia se procedió a coordinar con el área de RR.HH. para la programación de las capacitaciones periódicas llegando a establecer una frecuencia de 3 capacitaciones semestrales con opción a incremento.

   Adicionalmente se dispuso del recurso humano del área de TI encargado de realizar las capacitaciones programadas, dichas capacitaciones se vienen efectuando de manera virtual debido a la coyuntura del COVID-19.

4.1.5.10. OSP-1: Informe a Gestión Táctica

1. **Descripción del proceso:**

   Responsable de presentar un informe de la operatividad de los procesos y el consumo de recursos de manera periódica

2. **Objetivos del Proceso:**

   a. Reflejar el rendimiento de los procesos O-SIM3 implementados

Repositorio Institucional - UNASAM - Perú

3. **Propietarios del proceso:**
   a. Área de TI
4. **Actividades realizadas:**

   Para este proceso se estableció la realización de reuniones semestrales en conjunto con lo indicado en el proceso SSP-1.

4.1.5.11. OSP-5: Parcheo de dominio administrado por TI

1. **Descripción del proceso:**

   Este proceso comprende la actualización continua de los servicios de información con la finalidad de prevenir una posible explotación de vulnerabilidades, mejorando así la confiabilidad de SI.
2. **Objetivos del proceso:**
   a. Actualización de los sistemas
   b. Actualización de los sistemas operativos
3. **Propietarios del proceso:**
   a. Área de TI
   b. Comité de seguridad de la información
4. **Actividades realizadas:**

   Teniendo en cuenta que no toda actualización es efectiva al 100% y que en muchos casos una actualización genera fallas o desperfectos que afectan la operatividad y disponibilidad de los sistemas o por lo menos parte de ellos, fue necesario realizar un respaldo de por lo menos 2 versiones anteriores de los sistemas utilizados en clínica(Sistema clínico, Sistema de archivos y citas, Aplicativo de facturación electrónica, etc.), así mismo se definió un horario de aplicación de las actualizaciones el cual quedo establecido que toda actualización debe ser aplicada en horario de 08:00 am – 01:00 pm, salvo excepciones urgentes para poder tener el tiempo necesario a corregir algún error generado pro dicha actualización.

Repositorio Institucional - UNASAM - Perú

Figura 12

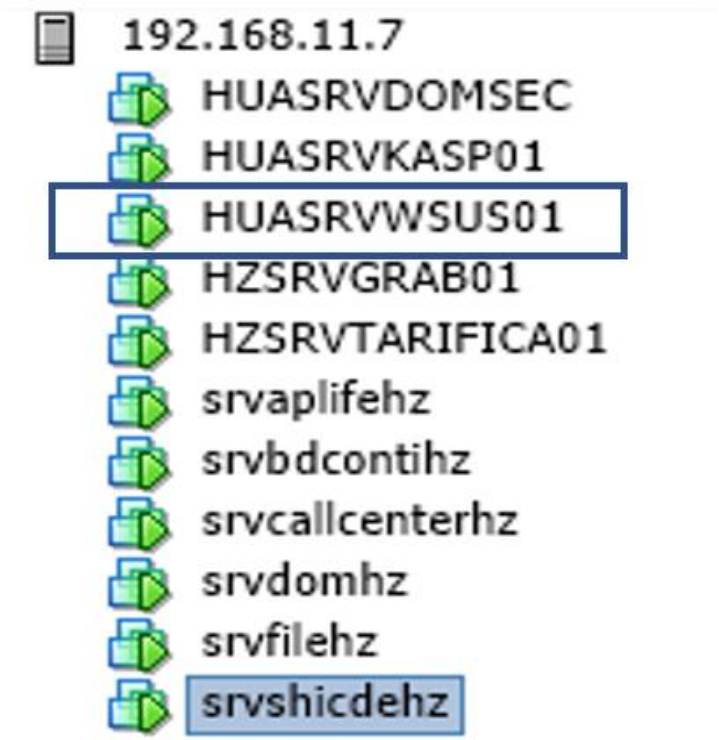
Versiones del sistema clínico actualizada a la última disponible

Nota: La figura muestra uno de los diversos sistemas actualizado a su última versión con Fecha 23-11-2022 Fuente: Elaboración propia.

En cuanto a la actualización de los sistemas operativos se implementó un servidor virtual de actualizaciones (WSUS) encargado de replicar las actualizaciones de seguridad para todos los sistemas operativos de Microsoft alojados en la red corporativa, esto incluye las workstations de nivel usuario y servidores.

Figura 13

Servidor WSUS implementado



Nota: Podemos apreciar el servidor WSUS configurado para la aplicación automática de actualización de seguridad Fuente: Elaboración propia.

4.1.5.12. OSP-10: Gestión de copias de seguridad

1. **Descripción del proceso:**

   Proceso responsable de disminuir en gran parte el impacto sufrido ante la ausencia de información mediante las copias de seguridad, aportando de manera significativa a las dimensiones de la SI.

2. **Objetivos del proceso:**

   a. Garantizar que se salvaguarde la confidencialidad, disponibilidad e integridad de la SI.

   b. Ejecutar copas de seguridad periódicamente

3. **Propietarios del proceso:**

   a. Área de TI

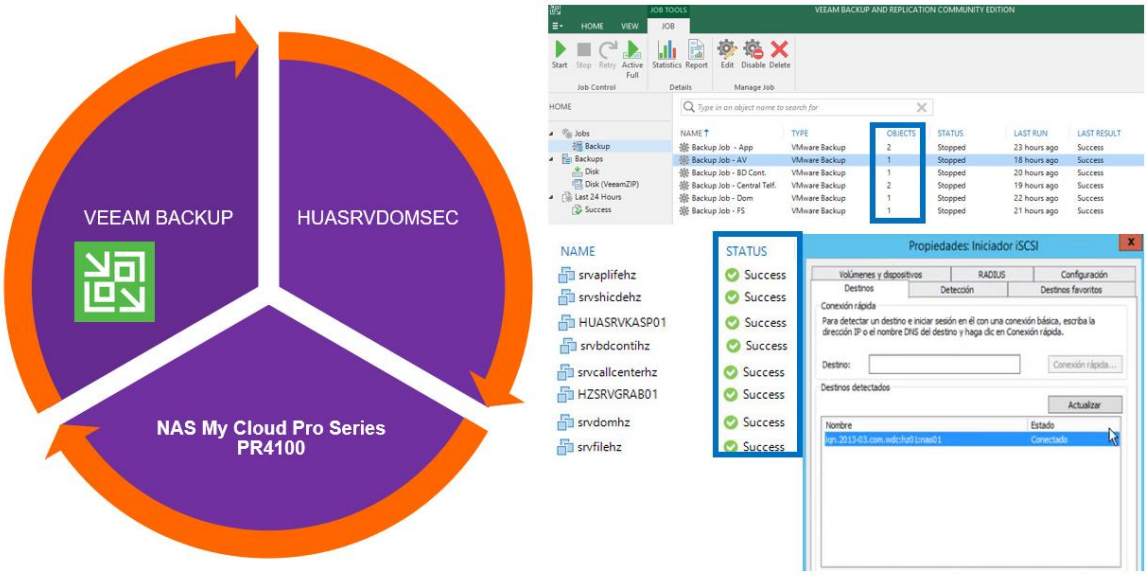
4. **Actividades realizadas:**

Repositorio Institucional - UNASAM - Perú

Dentro del presente proceso se realizaron priorizaron las copias de seguridad de los servidores virtuales mediante la herramienta Veeam Backup adicionalmente el copiado de seguridad del servidor de archivos mediante la herramienta de versiones anteriores y el respaldo de videos de laparoscopia que vienen siendo parte de la HC de los pacientes mediante la configuración y uso de un servidor NAS Qnap.

Figura 14

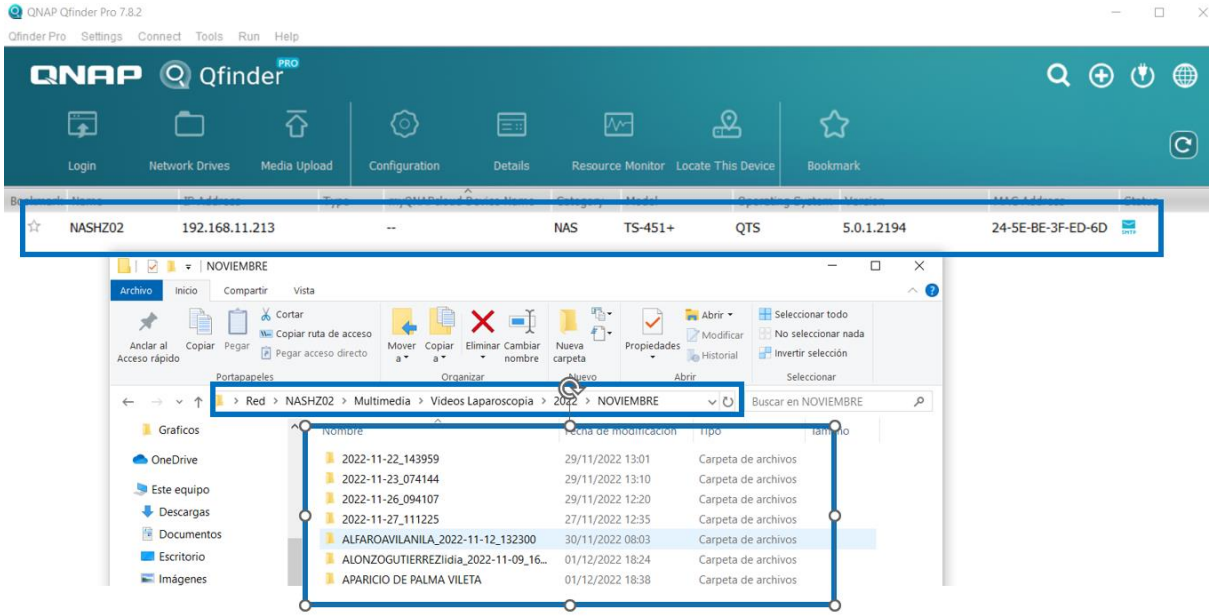
Herramientas usadas para el respaldo de servidores



Nota: En la figura se puede apreciar el uso de la herramienta Veeam Backup para el respaldo de servidores virtuales Fuente: Elaboración propia.

Figura 15

Uso de servidor NAS



Nota: En la figura se puede apreciar el uso de un servidor NAS para respaldar los podeos de laparoscopia los cuales constituyen parte fundamental de las historias clínicas Fuente: Elaboración propia.

4.1.5.13. OSP-11: Control de Accesos

1. **Descripción del proceso:**

   Proceso a cargo de velar que el acceso la información (Física/ digital) se proporcione únicamente a las personas autorizadas, fortaleciendo así la integridad y confidencialidad de la información.

2. **Objetivos del proceso:**
   a. Delimitar el acceso a los repositorios digitales de información (File Server)
   b. Delimitar el acceso a los repositorios físicos de información considerada critica (Historias clínicas)

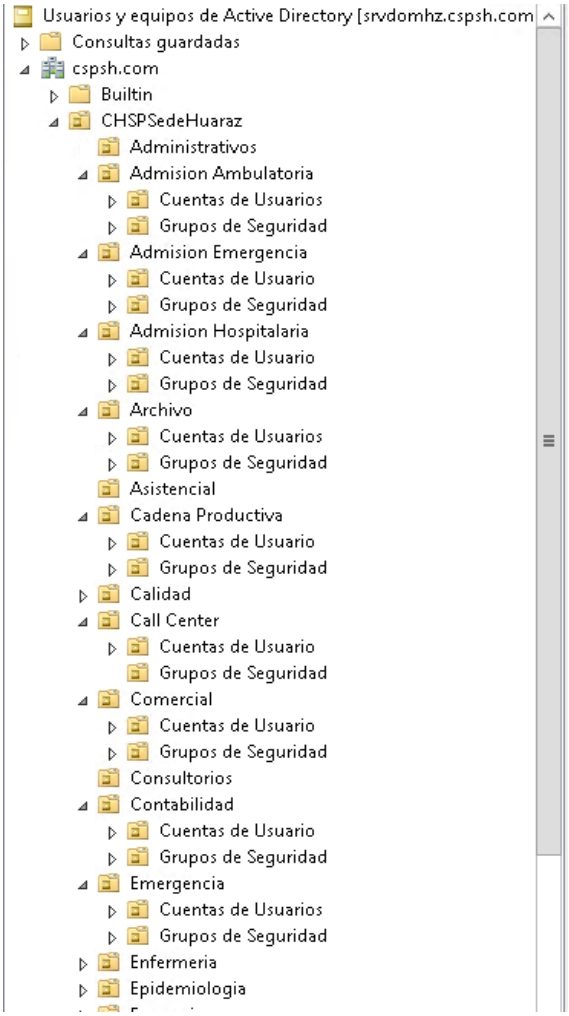
3. **Propietarios del proceso:**
   a. Área de TI
   b. Área de Archivos

4. **Actividades realizadas:**

Este proceso fue seleccionado debido a que se observó una gran problemática a nivel de accesos, en cuanto a los accesos a la información digital en este caso explícito al File Server se verifico que no existía ningún tipo de restricción, por ejemplo: personal de admisión podía acceder de forma libre a información de gerencia quien maneja información más confidencial por lo cual fue necesario realizar una distribución de grupos por área para posteriormente realizar una restricción de accesos totales al personal no autorizadas y brindo acceso a las personas que si tenían autorización, dichas acciones fueron realizadas en el Domain Controller.

Figura 16

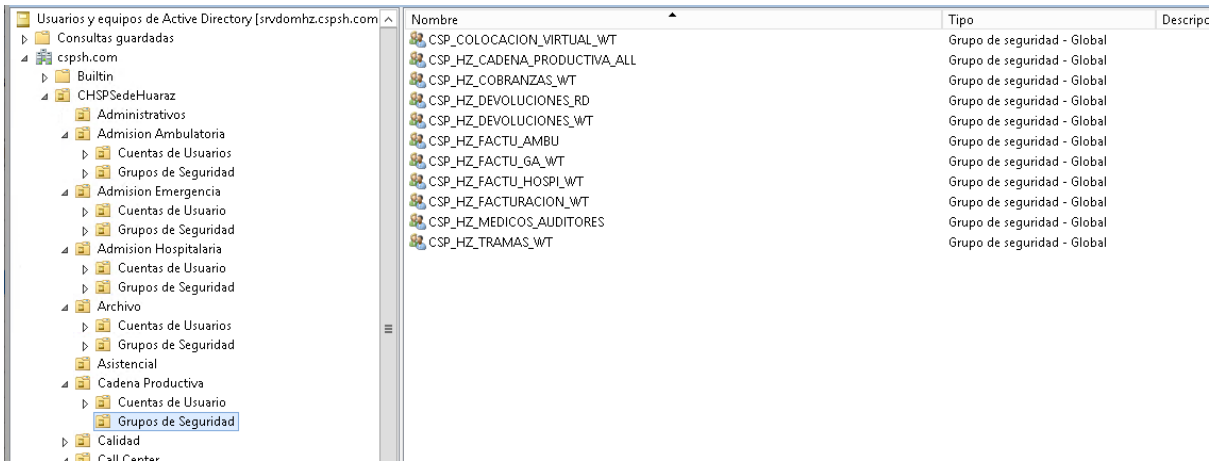
Clasificación de grupos por área



Nota: La figura plasma la clasificación de cuentas de usuario y grupos de seguridad por área en el dominio de la institución de estudio. Fuente: Elaboración propia.

Figura 17

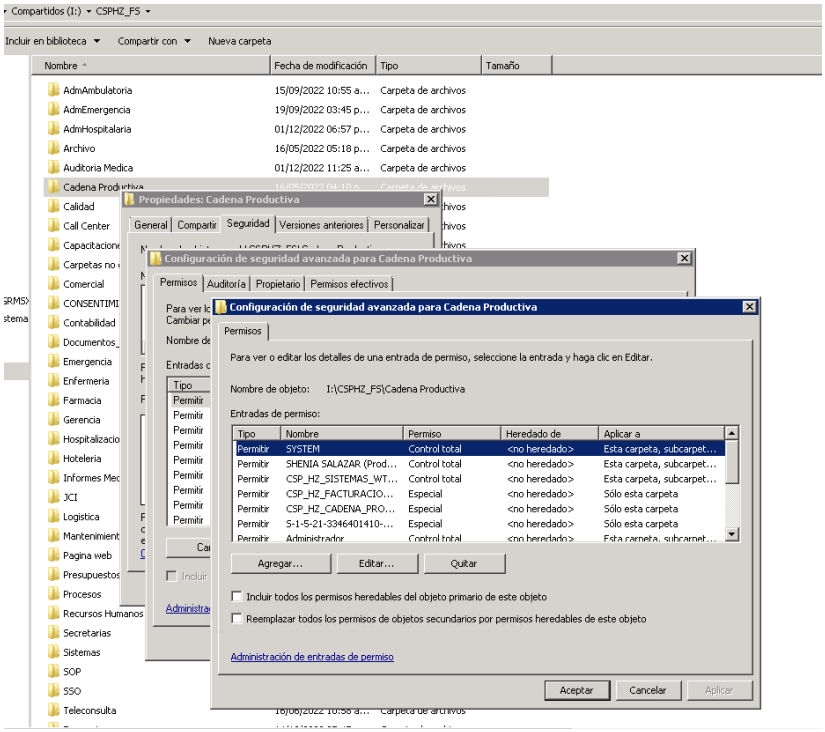
Creación de grupos de seguridad



Nota: La figura muestra los grupos de seguridad creados por cada área dentro de los cuales se integrarán únicamente a los usuarios autorizados Fuente: Elaboración propia

Figura 18

Delimitación de acceso correspondiente a los grupos creados



Nota: La figura muestra los accesos brindados a cada grupo de seguridad según el área y carpeta a la que están autorizados Fuente: Elaboración propia

En cuanto al accesibilidad a la información física en este caso específico el acceso a las historias clínicas físicas también enfrentamos un gran inconveniente ya que el almacenamiento de estas no eran las correcta además de que cualquier personal podía entrar al ambiente donde eran almacenadas dando cabida a cualquier acto mal intencionado que afecte la integridad de dichas historias clínicas, como acción correctiva se orientó al personal sobre el cuidado y correcto almacenamiento de las historias además de restringir el acceso a personal no autorizado.

Figura 19

Restricción de acceso a repositorios físicos

Nota: La figura muestra la restricción de accesos implementada para evitar algún incidente mal intencionado que genere perdida de historias clínicas Fuente: Elaboración propia

4.1.5.14. OSP-12: Registro de usuarios

1. **Descripción del proceso:**

   En este proceso cubriremos la gestión de usuarios desde su creación hasta la baja, comprendiendo que existen usuarios para acceso de diversos sistemas y repositorios de información.

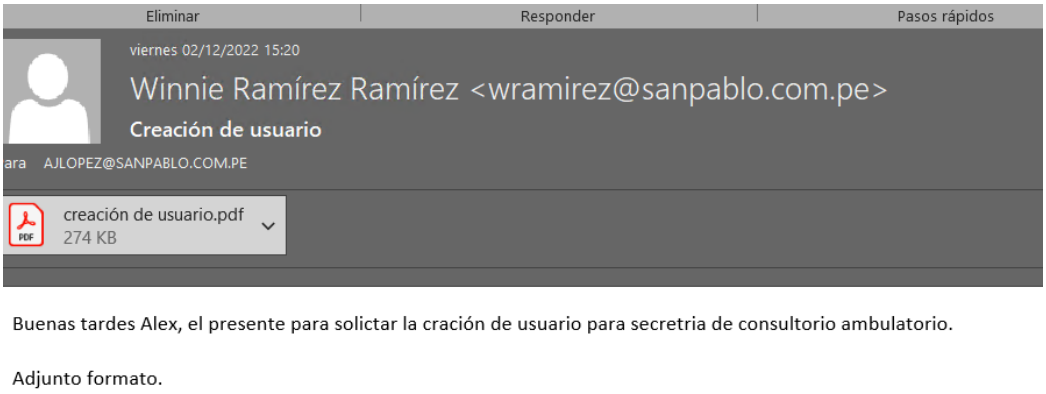
2. **Objetivos del proceso:**
   a. Establecer procedimientos para la adecuada creación de usuarios
   b. Brindar accesos correspondientes al cargo del personal para evitar que cuente con accesos a funciones que puedan vulnerar la integridad de la SI.
3. **Propietarios del proceso:**
   a. Área de TI
4. **Actividades realizadas:**

   En este proceso se definió y oriento el procedimiento correcto para la solicitud de creación de usuario definiendo así lo siguiente:

   - Toda solicitud de creación de usuario debe ser solicitada por la jefatura de área presentando el formato correspondiente

Figura 20

Solicitud de creación de usuario

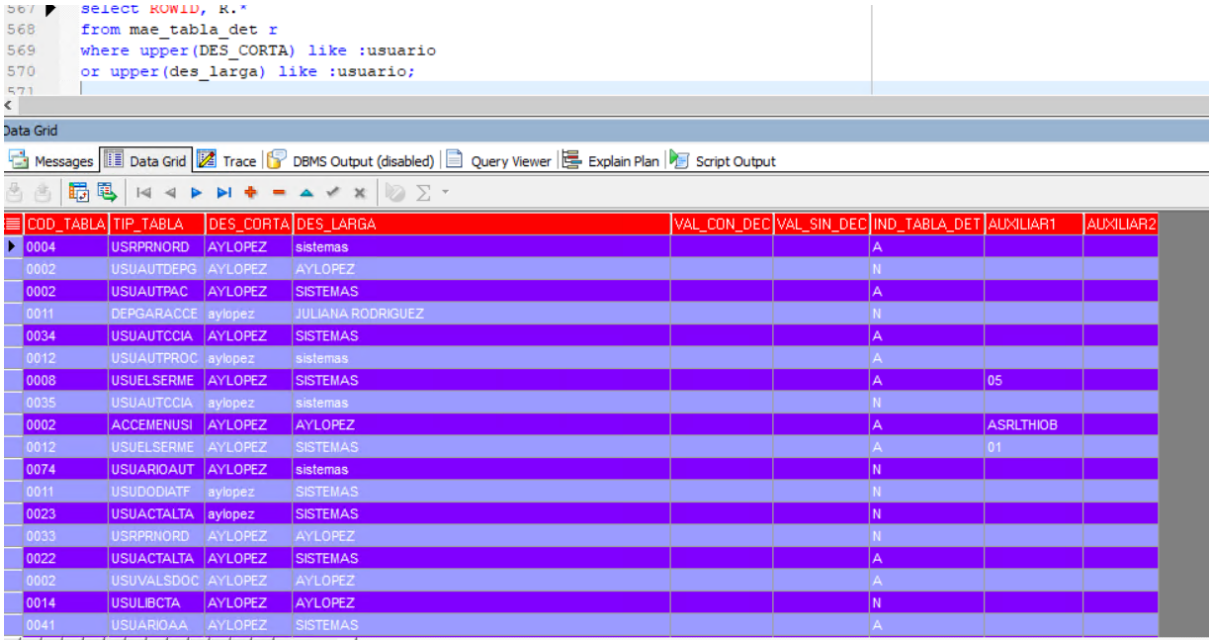


Nota: La figura muestra parte del procedimiento del proceso OSP-12 (Solicitud de creación de usuario) Fuente: Elaboración propia

- Una vez validado el formato se procede a denegar o aceptar la solicitud
- En caso ser aceptada se solicita la creación a la sede central y se espera la respuesta con las credenciales de acceso
- Una vez creado el usuario, el personal de sistemas procede a brindar los accesos a los módulos y funciones de los diversos sistemas

Figura 21

Gestión de accesos a los usuarios nuevos



```
select ROWID, R.*
from mae_tabla_det r
where upper(DES_CORTA) like :usuario
or upper(des_larga) like :usuario;
```

Data Grid

Messages | Data Grid | Trace | DBMS Output (disabled) | Query Viewer | Explain Plan | Script Output

COD_TABLA	TIP_TABLA	DES_CORTA	DES_LARGA	VAL_CON_DEC	VAL_SIN_DEC	IND_TABLA_DET	AUXILIAR1	AUXILIAR2
0004	USRPRNORD	AYLOPEZ	sistemas			A		
0002	USUAUTDEPG	AYLOPEZ	AYLOPEZ			N		
0002	USUAUTPAC	AYLOPEZ	SISTEMAS			A		
0011	DEPGARACCE	aylopez	JULIANA RODRIGUEZ			N		
0034	USUAUTCCIA	AYLOPEZ	SISTEMAS			A		
0012	USUAUTPROC	aylopez	sistemas			A		
0008	USUELSERME	AYLOPEZ	SISTEMAS			A	05	
0035	USUAUTCCIA	aylopez	sistemas			N		
0002	ACCEMENUSI	AYLOPEZ	AYLOPEZ			A	ASRLTHIOB	
0012	USUELSERME	AYLOPEZ	SISTEMAS			A	01	
0074	USUARIOAUT	AYLOPEZ	sistemas			N		
0011	USUDODIATF	aylopez	SISTEMAS			N		
0023	USUACTALTA	aylopez	SISTEMAS			N		
0033	USRPRNORD	AYLOPEZ	AYLOPEZ			N		
0022	USUACTALTA	AYLOPEZ	SISTEMAS			A		
0002	USUVALSDOC	AYLOPEZ	AYLOPEZ			A		
0014	USULIBCTA	AYLOPEZ	AYLOPEZ			N		
0041	USUARIOAA	AYLOPEZ	SISTEMAS			A		

Nota: La figura muestra cómo se brinda accesos a los usuarios nuevos mediante base de datos, adicionalmente este proceso se complementa con el proceso OSP-11 Fuente: Elaboración propia

4.1.5.15. OSP-14: Gestión de protección del medio ambiente físico

1. **Descripción del proceso:**

   Este proceso comprende la protección de los ambientes que albergan repositorios o interfases críticas contra incendios, temperaturas extremas, inundaciones, humedad o accesos no autorizados.

   En nuestro especifico la protección de la data center de la Clínica.

2. **Objetivos del proceso:**

   a. Protección de la data center contra factores ambientales

3. **Propietarios del proceso:**

   a. Área de TI

   b. Área de mantenimiento

4. **Actividades realizadas:**

   Para cubrir con este proceso se propuso la implementación de un sistema de monitoreo ambiental el cual cubre todos los puntos de protección delimitados en la descripción, la propuesta fue aprobada por gerencia y

Repositorio Institucional - UNASAM - Perú

gestionada rápidamente actualmente se viene haciendo del sistema de monitoreo ambiental de la empresa Firecity, el cual permite llevar un monitoreo de los sensores implementados mediante un aplicativo móvil.

Figura 22

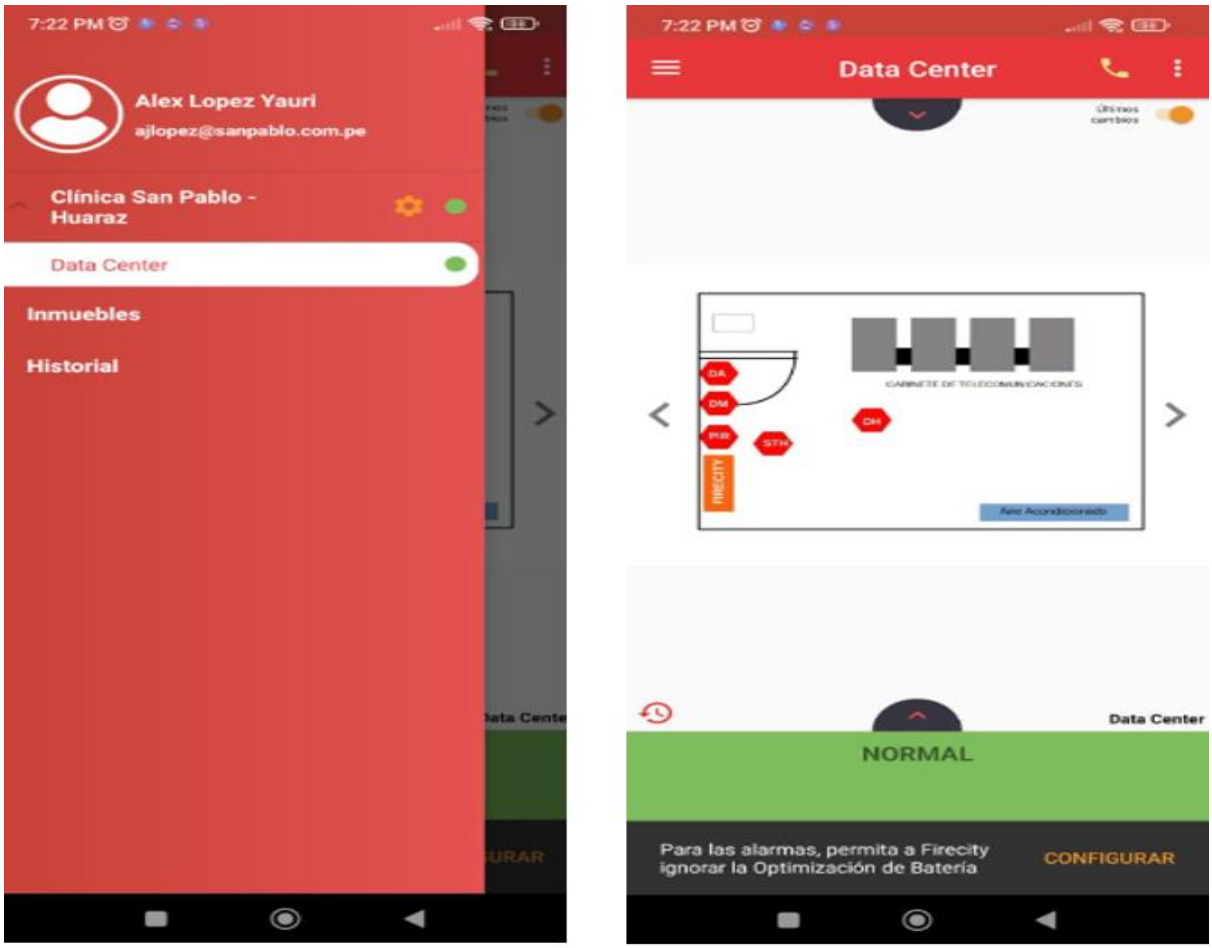
Sensores implementados en el data center

Nota: La figura muestra los sensores implementados en el data center de la Clínica San Pablo S.A.C sede Huaraz. Fuente: Elaboración propia

Repositorio Institucional - **UNASAM** - Perú

Figura 23

Aplicativo de monitoreo ambiental



Nota: La figura muestra los sensores el aplicativo de monitoreo ambiental implementado en el data center de la Clínica San Pablo S.A.C sede Huaraz. Fuente: Elaboración propia

4.1.5.16. OSP-17: Gestión de protección contra malware

1. **Descripción del proceso:**

   Responsable de implementar un conjunto de medidas de seguridad para asegurar el amparo de la información en contra de algún malware como, por ejemplo: Virus, Troyano, Phishing, etc.

2. **Objetivos del proceso:**

   a. Resguardar la integridad de la información contra malware.

3. **Propietarios del proceso:**

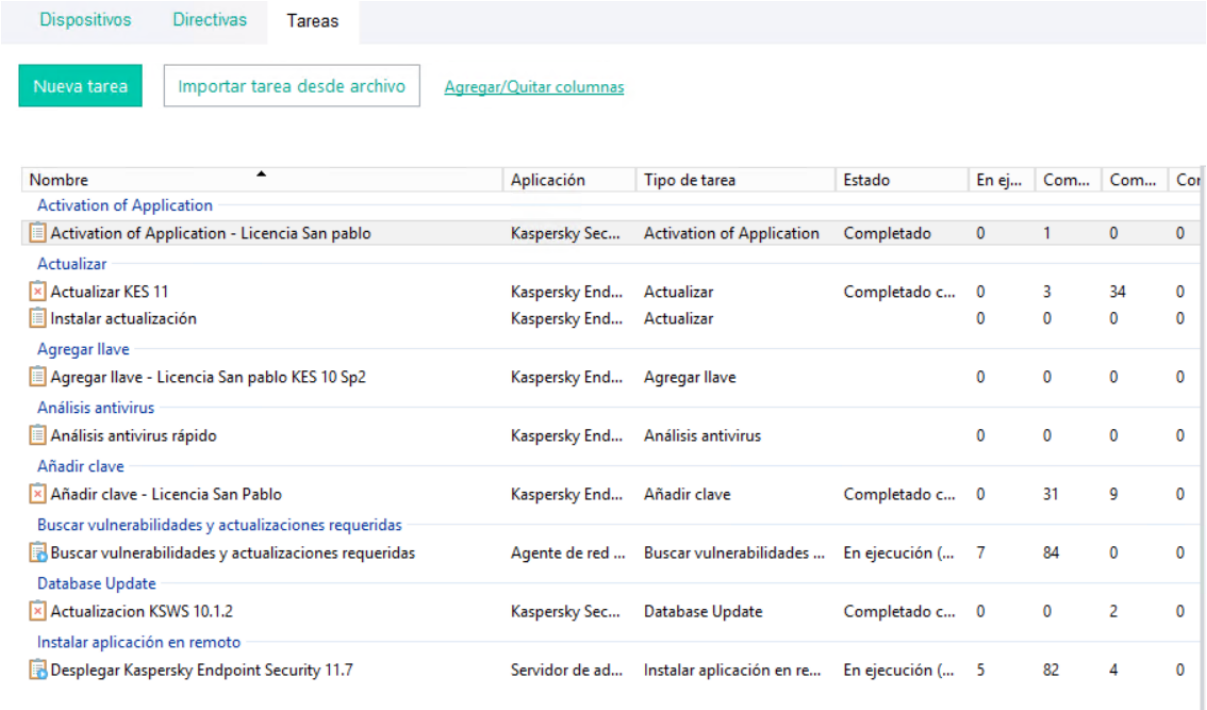
   a. Área de TI

4. **Actividades realizadas:**

Para la ejecución de este proceso fue necesario administrar de manera correcta el recurso con el que se contaba, en este caso la organización contaba con licencias de Antivirus las cuales no eran gestionadas de forma adecuada, en palabras simples muchos de los dispositivos informáticos que se encontraban en la red no se encontraban bajo la administración del antivirus y en algunos casos los equipos tenían instaladas versiones antiguas de antivirus por lo cual fue necesario crear nuevas tareas para el despliegue de los agentes y antivirus actualizados.

Figura 24

Tareas de despliegue de antivirus

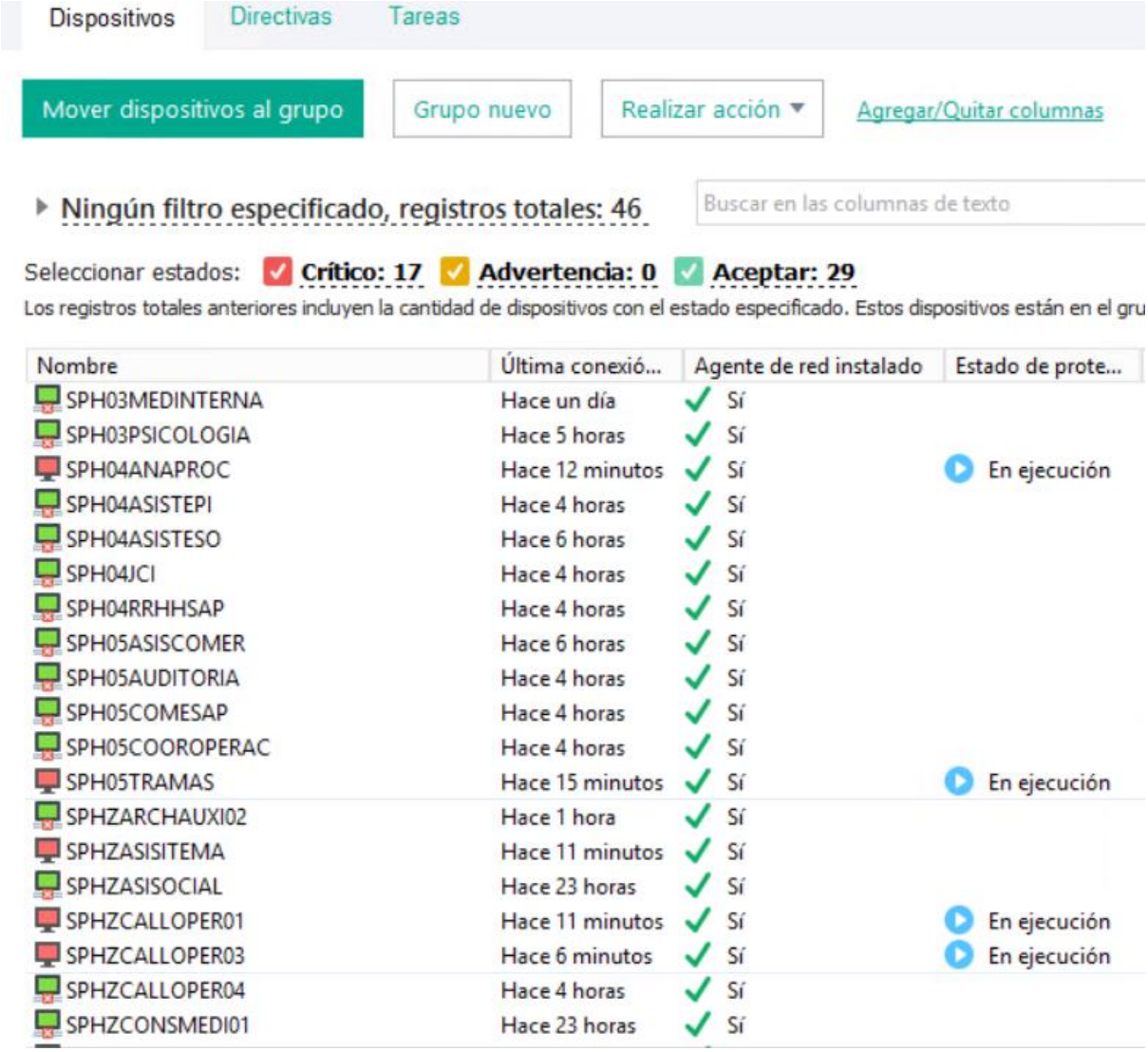


Nombre	Aplicación	Tipo de tarea	Estado	En ej...	Com...	Com...	Cor
Activation of Application							
Activation of Application - Licencia San pablo	Kaspersky Sec...	Activation of Application	Completado	0	1	0	0
Actualizar							
Actualizar KES 11	Kaspersky End...	Actualizar	Completado c...	0	3	34	0
Instalar actualización	Kaspersky End...	Actualizar		0	0	0	0
Agregar llave							
Agregar llave - Licencia San pablo KES 10 Sp2	Kaspersky End...	Agregar llave		0	0	0	0
Análisis antivirus							
Análisis antivirus rápido	Kaspersky End...	Análisis antivirus		0	0	0	0
Añadir clave							
Añadir clave - Licencia San Pablo	Kaspersky End...	Añadir clave	Completado c...	0	31	9	0
Buscar vulnerabilidades y actualizaciones requeridas							
Buscar vulnerabilidades y actualizaciones requeridas	Agente de red ...	Buscar vulnerabilidades ...	En ejecución (...	7	84	0	0
Database Update							
Actualizacion KSWS 10.1.2	Kaspersky Sec...	Database Update	Completado c...	0	0	2	0
Instalar aplicación en remoto							
Desplegar Kaspersky Endpoint Security 11.7	Servidor de ad...	Instalar aplicación en re...	En ejecución (...	5	82	4	0

Nota: En la figura se puede apreciar las tareas de despliegue de agente y antivirus como parte del proceso OSP-17 Fuente: Elaboración propia.

Figura 25

Dispositivos administrados por la consola de antivirus



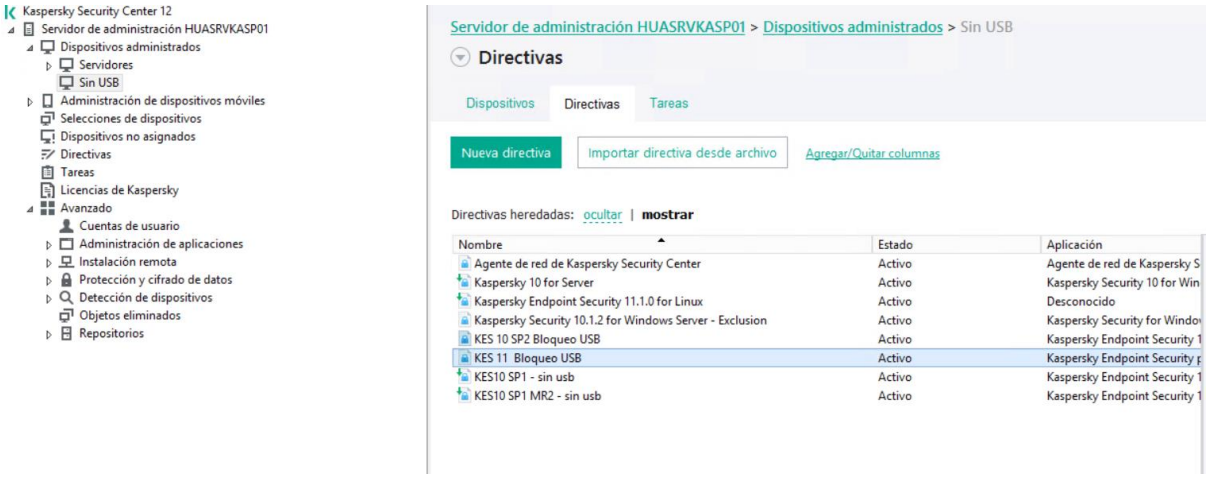
Nota: En figura podemos aprecia ni siquiera el 50% de los dispositivos totales de la Clínica son administrados por la consola de AV. Fuente: Elaboración propia.

Adicionalmente se realizó un bloque de puertos aprovechando las funcionalidades del Security Center del antivirus manejado para evitar que algún malware se filtre mediante algún dispositivo de almacenamiento externo, tener en cuenta que este proceso se complementa con el proceso OSP-5.

Repositorio Institucional - UNASAM - Perú

Figura 26

Directiva de Bloqueo de puertos



Nota: La figura muestra la directiva creada para el bloqueo de puertos USB con la finalidad de evitar el filtrado de algún malware que afecte la seguridad de la información de la Clínica San Pablo S.A.C. sede Huaraz Fuente: Elaboración propia.

4.1.5.17. OSP-21: Calidad de la información y sondeo de cumplimiento

1. **Descripción del proceso:**

   Proceso a cargo de la evaluación habitual de la información y los procesos O-ISM3 implementados

2. **Objetivos del proceso:**

   a. Asegurar el cumplimiento de los procesos O-ISM3.

3. **Propietario del proceso:**

   a. Área de TI

4. **Actividades realizadas:**

   Para el cumplimiento de este proceso todo el equipo de TI debe raizar una evaluación trimestral de los procesos O-ISM3 y una evaluación a mejora del modelo de madurez propuesto con la finalidad de seguir escalando niveles en pro de la SI.

4.1.6. Evaluación del nivel de capacidad de cada proceso

Posteriormente a la implementación se evaluó el nivel de capacidad de los procesos implementados en la organización de estudio.

Tabla 4

Nivel de capacidad de los procesos O-ISM3

Proceso	Nivel 1 Inicial	Nivel 2 Gestionado	Nivel 3 Definido	Nivel 4 Controlado	Nivel 5 Optimizado
Procesos Generales					
GP-1: Gestión del conocimiento de SI			X		
GP-3: Implementación de O-ISM3			X		
Procesos Estratégicos Específicos					
SSP-1: Informe a las partes interesadas			X		
SSP-2: Coordinación			X		
SSP-6: Asignar recursos para la seguridad de la información			X		
Procesos Tácticos Específicos					
TSP-1: Reporte a gerencia estratégica			X		
TSP-2: Administración recursos fijados			X		
TSP-3: Definir objetivos de seguridad			X		
TSP-11: Conciencia de seguridad			X		
Procesos Operacionales Específicos					
OSP-1: Informe a Gestión Táctica			X		
OSP-5: Parcheo de dominio administrado por TI				X	
OSP-10: Gestión de copias de seguridad				X	
OSP-11: Control/gestión de Accesos			X		
OSP-12: Registro de usuarios			X		
OSP-14: Gestión de protección del medio ambiente físico					X
OSP-17: Gestión de protección contra malware			X		
OSP-21: Calidad de la información y sondeo de cumplimiento			X		

Nota: La tabla muestra los niveles de capacidad de los procesos O-ISM3 implementados para la Clínica San Pablo, donde observa que la mayoría de procesos cuenta con un nivel de capacidad definido.

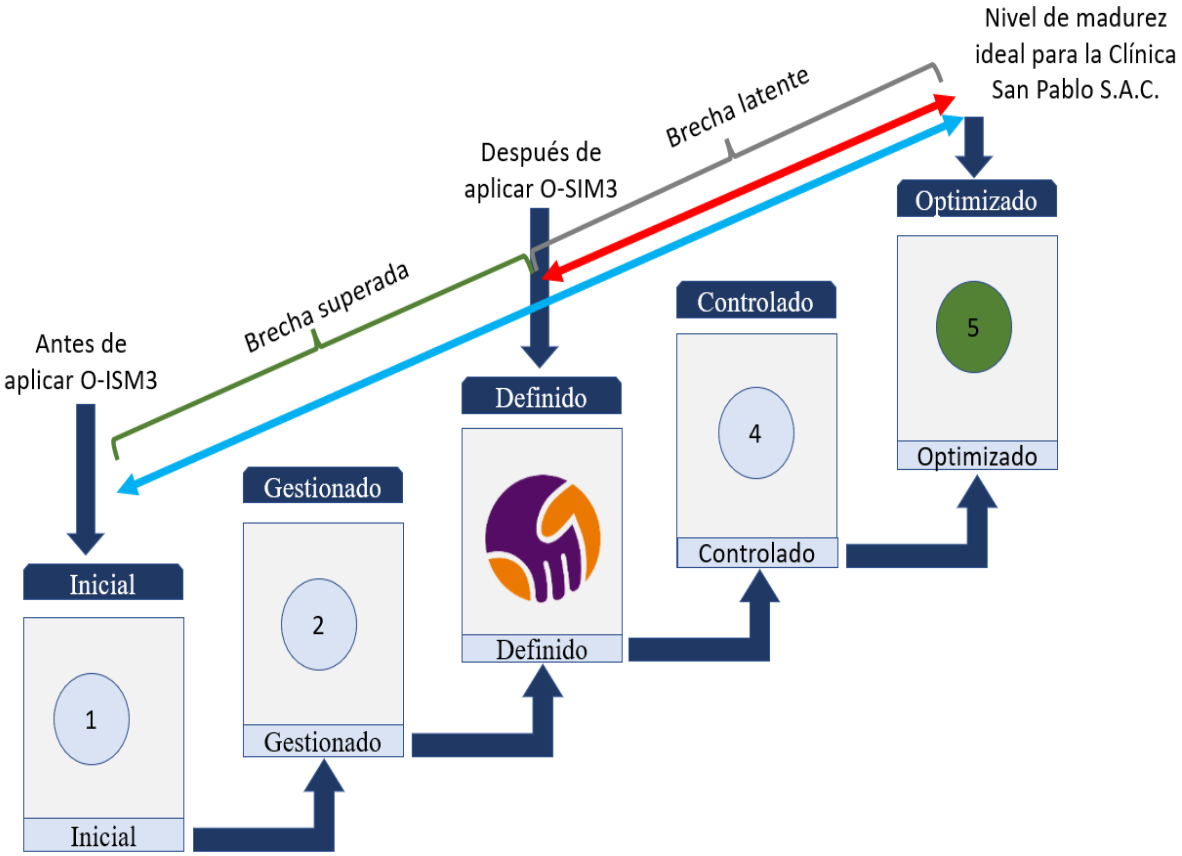
Repositorio Institucional - UNASAM - Perú

4.1.7. Evaluación del nivel del nuevo nivel de madurez

Posterior a la valoración de la capacidad de los procesos implementados procedemos a realizar una reevaluación del nivel de madurez de la SI para verificar si la Clínica San Pablo S.A.C. – Huaraz incremento su nivel de seguridad.

Figura 27

Nuevo nivel de madurez de la Clínica San Pablo S.A.C.



Nota: La figura muestra el incremento de nivel de la entidad de estudio de un nivel 1 a un nivel 3 Fuente: Elaboración propia.

4.2. Presentación de resultados

4.2.1. Resultados de la variable de estudio: Seguridad de la información

Resultados obtenidos según el objetivo general planteado: Mejorar la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022.

Repositorio Institucional - UNASAM - Perú

Tabla 5

Resultados de la variable de estudio (SI)

Resultado	Test	
	Pre (%)	Pos (%)
De 15 a 30	6 (4,5)	1 (0,8)
De 31 a 45	7 (5,3)	4 (3,03)
De 46 a 60	75 (56,8)	54 (40,91)
De 61 a 75	44 (33,3)	73 (55,30)
Total	132 (100)	132 (100)

Los datos mostrados en la tabla precedente reflejan los resultados derivados del pre y pos test, teniendo en consideración la variable de estudio definido en el objetivo general. En el cual se puede apreciar que dentro de una puntuación mínima de 15 puntos y una máxima de 75 puntos en el pre test, el 4,5 % valora la seguridad de la información con una puntuación de entre 15 a 30 puntos, el 5,3 % de entre 31 a 45 puntos, el 56,8% de entre 46 a 60 puntos y el 33.3% de entre 61 a 75 puntos, mientras que en el pos test solo el 0,76% valora la seguridad de la información con un puntaje de entre 15 a 30 puntos, el 3,03% de entre 31 a 45 puntos, 40,91% de entre 46 a 60 puntos y 55,30% de entre 61 a 75 puntos.

4.2.2. Resultados de la dimensión N°1: Confidencialidad

Resultados obtenidos según el objetivo específico N°1 planteado: Mejorar la confidencialidad de la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022.

Tabla 6

Resultados de la dimensión Confidencialidad

Resultado	Test	
	Pre (%)	Pos (%)
De 5 a 10	7 (5,3)	3 (2,3)
De 11 a 15	21 (15,9)	7 (5,3)
De 16 a 20	56 (42,4)	50 (37,9)
De 21 a 25	48 (36,4)	72 (54,5)
Total	132 (100)	132 (100)

Repositorio Institucional - UNASAM - Perú

Los datos mostrados en la tabla precedente reflejan los resultados obtenidos en el pre y pos test del grupo experimental, teniendo en consideración la dimensión de estudio definido en el objetivo específico N°1. En el cual se puede apreciar que dentro de un puntaje mínimo de 5 y una máxima de 25 en el pre test, el 5,3 % valora la seguridad de la información con una puntuación de entre 5 a 10 puntos, el 15,9 % de entre 11 a 15 puntos, el 42,4% de entre 16 a 20 puntos y el 36,4% de entre 20 a 25 puntos, mientras que en el pos test solo el 2,3% valora la seguridad de la información con un puntaje de entre 5 a 10 puntos, el 5,3% de entre 11 a 15 puntos, 37,9% de entre 16 a 20 puntos y 54,5% de entre 21 a 25 puntos.

4.2.3. Resultados de la dimensión N°2: Disponibilidad

Resultados obtenidos según el objetivo específico N°1 planteado: Mejorar la disponibilidad de la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022.

Tabla 7

Resultados de la dimensión Disponibilidad

Resultado	Test	
	Pre (%)	Pos (%)
De 5 a 10	8 (6,1)	4 (3,0)
De 11 a 15	19 (14,4)	12 (9,1)
De 16 a 20	61 (46,2)	65 (49,2)
De 21 a 25	44 (33,3)	51 (38,6)
Total	132 (100)	132 (100)

Los datos mostrados en la tabla precedente reflejan los resultados obtenidos en el pre y pos test del grupo experimental, teniendo en consideración la dimensión de estudio definido en el objetivo específico N°2. En el cual se puede apreciar que dentro de un puntaje mínimo de 5 y una máxima de 25 en el pre test, el 6,1 % valora la seguridad de la información con una puntuación de entre 5 a 10 puntos, el 14,4 % de entre 11 a 15 puntos, el 46,2% de entre 16 a 20 puntos y el 33,3% de entre 20 a 25 puntos, mientras que en el pos test solo el 3,0% valora la seguridad de la información con un puntaje de entre 5 a 10 puntos, el 9,1% de entre 11 a 15 puntos, 49,2% de entre 16 a 20 puntos y 38,6% de entre 21 a 25 puntos.

Repositorio Institucional - UNASAM - Perú

4.2.4. Resultados de la dimensión N°3: Integridad

Resultados obtenidos según el objetivo específico N°1 planteado: Mejorar la disponibilidad de la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022.

Tabla 8

Resultados de la dimensión Integridad

Resultado	Test	
	Pre (%)	Pos (%)
De 5 a 10	8 (6,1)	2 (1,5)
De 11 a 15	23 (17,4)	11 (8,3)
De 16 a 20	64 (48,5)	51 (38,6)
De 21 a 25	37 (28,0)	68 (51,5)
Total	132 (100)	132 (100)

Los datos mostrados en la tabla precedente reflejan los resultados obtenidos en el pre y pos test del grupo experimental, teniendo en consideración la dimensión de estudio definido en el objetivo específico N°2. En el cual se puede apreciar que dentro de un puntaje mínimo de 5 y una máxima de 25 en el pre test, el 6,1 % valora la seguridad de la información con una puntuación de entre 5 a 10 puntos, el 17,4 % de entre 11 a 15 puntos, el 48,5% de entre 16 a 20 puntos y el 28,0% de entre 20 a 25 puntos, mientras que en el pos test solo el 1,5% valora la seguridad de la información con un puntaje de entre 5 a 10 puntos, el 8,3% de entre 11 a 15 puntos, 38,6% de entre 16 a 20 puntos y 51,5% de entre 21 a 25 puntos.

4.2.5. Prueba de hipótesis

4.2.5.1. Hipótesis General planteada

La aplicación del estándar O-ISM3 mejora de manera significativa la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022.

Paso 1: Formulación de Hipótesis estadísticas

H_0: La aplicación del estándar O-ISM3 no mejora de manera significativa la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022.

Repositorio Institucional - UNASAM - Perú

H_1: La aplicación del estándar O-ISM3 mejora de manera significativa la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022.

Paso 2: Elección del nivel de significancia

La significancia usada en la investigación fue del 5% (α=0.05).

Paso 3: Elección del estadígrafo de prueba

$$Z = \frac{W - \left[\frac{n(n+1)}{4}\right]}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

El contraste de hipótesis se trabajó mediante la prueba estadística de Wilcoxon, esta prueba es utilizada para muestras relacionadas (pretest-postest) cuando los datos de análisis no cuentan con las propiedades necesarias de normalidad y las variables son de naturaleza cualitativa.

Paso 4: Calculo realizado mediante el programa SPSS 26

Tabla 9

Contraste de la hipótesis general – Seguridad de la Información

Resultados del grupo experimental	Z	Valor p
Pre test vs Pos test	-7,212864	5,4787E-13

Nota: La tabla muestra los resultados de la prueba de hipótesis donde se observa el valor "p" de la seguridad de la información entre el pre y pos test.

Paso 5: Regla de decisión estadística

En caso se obtenga un valor p es menor que 0,05 (p<0,05) se opta por rechazar la hipótesis nula (H_0), con un nivel de confianza de 95%.

Paso 6: Toma de decisión

Repositorio Institucional - UNASAM - Perú

Se ha obtenido Z= -7,212864 con un valor p = 5,4787E-13 ($p < 0,05$) tal como se muestra en el paso 4, por lo que optamos por rechazar la hipótesis nula.

Como la hipótesis nula ha sido rechazada, se concluye que la aplicación del estándar O-ISM3 mejora de manera significativa la seguridad de la información en la Clínica San Pablo S.A.C – Huaraz, 2022. Confirmando así la hipótesis general planteada en la presente investigación.

4.2.5.2. Hipótesis especifica N°1

La aplicación del estándar O-ISM3 mejora de manera significativa la confidencialidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

Paso 1: Formulación de Hipótesis estadísticas

H_0: La aplicación del estándar O-ISM3 no mejora de manera significativa la confidencialidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

H_1: La aplicación del estándar O-ISM3 mejora de manera significativa la confidencialidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

Paso 2: Elección del nivel de significancia

La significancia usada en la investigación fue del 5% (α=0.05).

Paso3: Elección del estadígrafo de prueba

$$Z = \frac{W - \left[\frac{n(n+1)}{4}\right]}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

El contraste de hipótesis se trabajó mediante la prueba estadística de Wilcoxon, esta prueba es utilizada para muestras relacionadas (pretest-postest) cuando los datos de análisis no cuentan con las propiedades necesarias de normalidad y las variables son de naturaleza cualitativa.

Paso 4: Calculo realizado mediante el programa SPSS 26

Repositorio Institucional - UNASAM - Perú

Tabla 10

Contraste de la hipótesis especifica N°1 – Dimensión Confidencialidad

Resultados del grupo experimental	Z	Valor p
Pre test vs Pos test	-4,222146	0,000024

Nota: La tabla muestra los resultados de la prueba de hipótesis donde se observa el nivel de significancia de la confidencialidad de la SI entre el pre y pos test.

Paso 5: Regla de decisión estadística

En caso se obtenga un valor p es menor que 0,05 ($p<0,05$) se opta por rechazar la hipótesis nula (H_0), con un nivel de confianza de 95%.

Paso 6: Toma de decisión

Se ha obtenido Z= -4,222146 con un valor p = 0,000024 ($p < 0,05$) tal como se muestra en el paso 4, por lo que optamos por rechazar la hipótesis nula.

Como la hipótesis nula ha sido rechazada, se concluye que la aplicación del estándar O-ISM3 mejora de manera estadísticamente significativa la confidencialidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022. Confirmando así la hipótesis especifica N°1 planteada en la presente investigación.

4.2.5.3. Hipótesis especifica N°2

La aplicación del estándar O-ISM3 mejora de manera significativa la disponibilidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

Paso 1: Formulación de Hipótesis estadísticas

Repositorio Institucional - UNASAM - Perú

H_0: La aplicación del estándar O-ISM3 no mejora de manera significativa la disponibilidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

H_1: La aplicación del estándar O-ISM3 mejora de manera estadísticamente significativa la disponibilidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

Paso 2: Elección del nivel de significancia

La significancia usada en la investigación fue del 5% (α=0.05).

Paso3: Elección del estadígrafo de prueba

$$Z = \frac{W - \left[\frac{n(n+1)}{4}\right]}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

El contraste de hipótesis se trabajó mediante la prueba estadística de Wilcoxon, esta prueba es utilizada para muestras relacionadas (pre test-pos test) cuando los datos de análisis no cuentan con las propiedades necesarias de normalidad y las variables son de naturaleza cualitativa.

Paso 4: Cálculo realizado mediante el programa SPSS 26

Tabla 11

Contraste de la hipótesis especifica N°2 – Dimensión Disponibilidad

Resultados del grupo experimental	Z	Valor p
Pre test vs Pos test	-2,303118	0,021272

Nota: La tabla muestra los resultados de la prueba de hipótesis donde se observa el nivel de significancia de la disponibilidad de la SI entre el pre y pos test.

Paso 5: Regla de decisión estadística

En caso se obtenga un valor p es menor que 0,05 (p<0,05) se opta por rechazar la hipótesis nula (H_0), con un nivel de confianza de 95%.

Repositorio Institucional - UNASAM - Perú

Paso 6: Toma de decisión

Se ha obtenido Z= -2,303118 con un valor p = 0,021272 (p < 0,05) tal como se muestra en el paso 4, por lo que optamos por rechazar la hipótesis nula.

Como la hipótesis nula ha sido rechazada, se concluye que la aplicación del estándar O-ISM3 mejora de manera significativa la disponibilidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, confirmando así la hipótesis especifica N°2 planteada en la presente investigación.

4.2.5.4. Hipótesis especifica N°3

La aplicación del estándar O-ISM3 mejora de manera significativa la integridad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

Paso 1: Formulación de Hipótesis estadísticas

H_0: La aplicación del estándar O-ISM3 no mejora de manera significativa la integridad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

H_1: La aplicación del estándar O-ISM3 mejora de manera significativa la integridad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.

Paso 2: Elección del nivel de significancia

La significancia usada en la investigación fue del 5% (α=0.05).

Paso3: Elección del estadígrafo de prueba

$$Z = \frac{W - \left[\frac{n(n+1)}{4}\right]}{\sqrt{\frac{n(n+1)(2n+1)}{24}}}$$

El contraste de hipótesis se trabajó mediante la prueba estadística de Wilcoxon, esta prueba es utilizada para muestras relacionadas (pretest-

Repositorio Institucional - UNASAM - Perú

postest) cuando los datos de análisis no cuentan con las propiedades necesarias de normalidad y las variables son de naturaleza cualitativa.

Paso 4: Calculo realizado mediante el programa SPSS 26

Tabla 12

Contraste de la hipótesis especifica N°3 – Dimensión Integridad

Resultados del grupo experimental	Z	Valor p
Pre test vs Pos test	-6,011688	1,836E-9

Nota: La tabla muestra los resultados de la prueba de hipótesis donde se observa el nivel de significancia de la integridad de la SI entre el pre y pos test.

Paso 5: Regla de decisión estadística

En caso se obtenga un valor p es menor que 0,05 ($p<0,05$) se opta por rechazar la hipótesis nula (H_0), con un nivel de confianza de 95%.

Paso 6: Toma de decisión

Se ha obtenido Z= -6,011688 con un valor p = 1,836E-9 ($p < 0,05$) tal como se muestra en el paso 4, por lo que optamos por rechazar la hipótesis nula.

Como la hipótesis nula ha sido rechazada, se concluye que la aplicación del estándar O-ISM3 mejora de manera significativa la integridad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, confirmando así la hipótesis especifica N°2 planteada en la presente investigación.

4.3. Discusión de resultados

Los resultados plasmados en la presente se puede apreciar que la aplicación del estándar O-ISM3 mejora significativamente la seguridad de la información mediante una GSI eficiente, en coincidencia con Cifre (2020), quien en su trabajo de posgrado se plantea el objetivo de concretar un modelo de seguridad basado en los lineamientos de O-ISM3 e ISO/IEC 27000 concluyendo que la aplicación de dichos estándares

Repositorio Institucional - UNASAM - Perú

internacionales ayudan a lograr una eficiente seguridad de la información siendo este uno de los problemas principales de los sistemas de información.

Así mismo la mejora de la SI en la organización de estudio permitió reducir la brecha de seguridad existente, lo cual coincide con el articulo científico publicado por Al-Matari et al. (2021) quienes logran demostrar que el modelo de madurez planteado por la norma O-ISM3 permite evaluar y mejorar el nivel de SI. Así mismo considerando que la SI abarca también la seguridad informática y protección de datos personales se puede deducir que una mejora significativa en la SI equivale también una mejora en la protección de datos personales lo cual concuerda con el trabajo realizado por Calle y Garcia (2019) quienes se plantearon como objetivo la consumación de un modelo de madurez organizacional para medir la capacidad de protección de datos personales y concluyeron que el modelo de madurez propuesto admite el incremento de la protección de datos personal en empresas de estudio a un bajo presupuesto.

De igual manera se observa en los resultados que las dimensiones confidencialidad, disponibilidad e integridad de la SI mejoran significativamente cuyo resultado es concordante con la tesis de pregrado de Blas y Pretell (2020), quienes concluyeron que la aplicación del modelo de madurez de SI propuesto mejoran las dimensiones de la seguridad de la información a un nivel significativo del 2.5% demostrando así que el uso de modelos basados en estándares internacionales como O-ISM3 es una alternativa de solución a la problemática que abarcamos en el trabajo presente.

Adicionalmente la investigación demuestra que la aplicación del estándar O-ISM3 permite a la organización el incremento de la madurez de la SI a un nivel aceptable lo cual concuerda con la tesis realizada por Muedas y Rojas (2019), quienes lograron demostrar el incremento de madurez de un nivel 1 a un nivel 3.

Repositorio Institucional - UNASAM - Perú

V. CONCLUSIONES

1. Mediante la aplicación del estándar O-ISM3 se logró mejorar de forma significativa la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022. Según los resultados estadísticos obtenidos.
2. La aplicación del estándar O-ISM3 permite mejorar de manera estadísticamente significativa la confidencialidad de la seguridad de la información en la entidad de estudio.
3. La aplicación del estándar O-ISM3 permite mejorar de manera estadísticamente significativa la disponibilidad de la seguridad de la información en la entidad de estudio.
4. La aplicación del estándar O-ISM3 permite mejorar de manera estadísticamente significativa la integridad de la seguridad de la información en entidad de estudio.
5. Mediante la aplicación del estándar O-SIM3 se logró incrementar el nivel de madurez de la GSI de la Clínica San Pablo de un nivel 1 - Inicial a un nivel 3 – Definido.
6. Respecto a las limitaciones presentadas en la presente investigación se tienen dos factores limitantes: La poca disponibilidad del personal asistencial tanto en el pre como en el pos test y el poco tiempo para el desarrollo de la investigación.

Repositorio Institucional - **UNASAM** - Perú

VI. RECOMENDACIONES

1. Aplicar el estándar O-ISM3 u otro estándar internacional con mayor inversión económica y a largo plazo, a fin de obtener un mejor nivel de madurez de la seguridad de la información.
2. La creación de un comité de seguridad de la información que se encargue de gestionar todos los temas correspondientes y proponer alternativas de mejora tomando como base la presente investigación.
3. Basado en el estudio realizado se recomienda la implementación de un sistema de SGSI con la finalidad de obtener una certificación.
4. Promover el reforzamiento de la cultura organizacional en temas de seguridad de la información mediante, capacitaciones constantes al personal, publicaciones y actividades técnicas y de sensibilización.
5. Seguir aplicando y ampliar la cantidad de procesos O-ISM3 aplicados en la entidad con miras a incrementar el nivel de seguridad.
6. Proponer la implementación del estándar O-ISM3 a nivel corporativo ya que algunos servicios están bajo la administración de la sede central, esto ayudaría a mejorar los niveles de seguridad en todas las sedes dependientes.
7. Mejorar la infraestructura tecnológica para asegurar la disponibilidad de los sistemas y servicios brindados, para el funcionamiento de la empresa y la continuidad del negocio.

Repositorio Institucional - UNASAM - Perú

VII. REFERENCIAS BIBLIOGRÁFICAS

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Adopting security maturity model to the organizations' capability model. *Egyptian Informatics Journal, 22*(2), 7. doi:https://doi.org/10.1016/j.eij.2020.08.001

Altamirano, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Instituto de Información Científica y Tecnológica, 21*(2), 248-263. Recuperado el 25 de agosto de 2022, de https://www.redalyc.org/journal/6378/637869113010/html/

Blas, W., & Pretell, G. (2020). *Modelo de seguridad de la información para mejorar la gestión informática en la Municipalidad Distrital de Florencia de Mora.* Trujillo. Recuperado el 04 de Setiembre de 2022, de https://dspace.unitru.edu.pe/handle/UNITRU/16156

Bustamente, S., Valles, M., & Levano, D. (2020). Factores que contribuyen en la pérdida de información en las organizaciones. *Revista Cubana de Ciencias Informáticas*, 19. doi:http://orcid.org/0000-0002-8173-203X

Calle, l., & Garcia, A. (2019). *Modelo de madurez de protección de datos personales para el.* Universidad Peruana de Ciencias Aplicadas. Lima: Universidad Peruana de Ciencias Aplicadas (UPC). doi:https://doi.org/10.19083/tesis/625502

Cámara de bancos e instituciones financieras de Costa Rica. (2017). *MODELO DE MADUREZ DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.* Costa Rica. Recuperado el 25 de Julio de 2022

Castellanos, M. H. (2011). FORMULA PARA CÁLCULO DE LA MUESTRA POBLACIONES FINITAS. Obtenido de https://investigacionpediahr.files.wordpress.com/2011/01/formula-para-cc3a1lculo-de-la-muestra-poblaciones-finitas-var-categorica.pdf

Cifre, S. (2020). *Modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas.* Tesis de maestría, Universidad Tecnológica Nacional Facultad Regional Santa Fe, Argentina.

Colonia, P. (2017). *Propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la municipalidad distrital de buena vista alta - casma.* Tesis de pregrado, Universidad Católica Los Ángeles de Chimbote, Casma. Recuperado el 28 de Julio de 2022, de https://purl.org/pe-repo/ocde/ford#2.02.04

Equipo de colaboradores DocuSing. (2022). *DocuSing*. Recuperado el 22 de Julio de 2022, de https://www.docusign.mx/blog/ciclo-de-vida-de-datos#:~:text=Ciclo%20de%20vida%20de%20datos%3A%20%C2%BFQu%C3%A9%20es%3F,la%20primera%20captura%20en%20adelante.

Equipo editorial Etecé. (2020). *Concepto*. Recuperado el 18 de Julio de 2022, de https://concepto.de/dato/

Escuela de administración de negocios. (2019). *Conexion ESAN*. Recuperado el 31 de Agosto de 2022, de https://www.esan.edu.pe/conexion-esan/cual-es-el-modelo-de-madurez-de-tu-organizacion#:~:text=El%20modelo%20de%20madurez%20(CMM,criterios%20de%20evaluaci%C3%B3n%2C%20entre%20otros.

Estrada, R., Unás, J., & Flórez, O. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, Sede Tulúa. *Revista Logos Ciencia & Tecnología*, 98. doi:https://doi.org/10.22335/rlct.v13i3.1446

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2017). La seguridad informática y la seguridad de la información. *Polo del conocimiento, 2*(12), 155. doi:10.23857/pc.v2i12.420

Gobierno Peruano. (2022). *Plataforma digital única del estado peruano*. Recuperado el 02 de Setiembre de 2022, de https://www.gob.pe/

Guardia, R. (2020). *Diseño de un modelo de seguridad de la información para minimizar los riesgos informaticos en la gestión académica del Instituto de Educación Superior Tecnológico Publico Eleazar Guzmán Barrón.* Huaraz. Recuperado el 27 de 08 de 2022, de http://repositorio.unasam.edu.pe/handle/UNASAM/4212

Huincho, W. (2019). *Sistema de gestión de seguridad de la información para mejorar la protección informática de la comisaria region Huancavelica.* Cerro de pasco. Recuperado el 05 de Setiembre de 2022

International Organization of Standarization. (2018). *ISO/IEC 27000.* Suiza. Recuperado el 29 de Julio de 2022

ISOTools Excellence. (2017). *Blog especializadoen seguridad de la información y ciberseguridad*. Recuperado el 28 de Julio de 2022, de https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Muedas, A., & Rojas, R. (2019). *Modelo de madurez de seguridad de aplicaciones web ante ciberataques para clínicas de nivel 2.* Universidad Peruana de Ciencias Aplicadas. Lima: Universidad Peruana de Ciencias Aplicadas (UPC). Recuperado el 10 de 07 de 2020, de http://hdl.handle.net/10757/628108

Pérez, J., & Gardey, A. (2021). *Definición*. Obtenido de https://definicion.de/informacion/

Polo, A. (2020). Sociedad de la Información, Sociedad Digital, Sociedad de Control. *Inguriak revista vasca de sociologia y ciencia política*(68), 77. Recuperado el 10 de Agosto de 2022, de https://dialnet.unirioja.es/servlet/articulo?codigo=7526046

Quiroz, S., & Macías, D. (2017). Seguridad en informática: consideraciones. *Dominio de las ciencias, 3*(5), 676-688. doi:http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.5.jul.72-88

Reyes, C., Vera, T., & Mendoza, A. (2022). La importancia de la seguridad de la información de un paciente en el sector salud entre los años 2010 al 2021. *Revista De Investigación Multidisciplinaria CTSCAFE*, 19. doi:https://orcid.org/0000-0002-0469-915X

Roque, R., & Juárez, C. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. *Revista de tecnología y sociedad, 8*(14). doi:http://dx.doi.org/10.32870/Pk.a8n14.318

Software Enginnering Institute. (2010). *CMMI-DEV, V1.3.* Obtenido de http://www.sei.cmu.edu

The open group. (2017). *Open Information Security Management Maturity Model (O-ISM3), Version 2.0.* Reino Unido: The Open Group. Recuperado el 15 de 06 de 2022

Yirda, A. (2021). *ConceptoDefinición*. Recuperado el 29 de 07 de 2022, de https://conceptodefinicion.de/datos/

Repositorio Institucional - **UNASAM** - Perú

VIII. ANEXOS

Repositorio Institucional - UNASAM - Perú

ANEXO 1: "MATRIZ DE CONSISTENCIA DE LA INVESTIGACION"

"ESTÁNDAR O-ISM3 PARA MEJORAR LA SEGURIDAD EN LA INFORMACIÓN EN LA CLÍNICA SAN PABLO S.A.C. – HUARAZ, 2022"

Problema	Objetivos	Hipótesis	Variables y dimensiones	Metodología
Problema general: ¿De qué manera la aplicación del estándar O-ISM3 mejora la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022? **Problemas específicos** **P1**: ¿de qué manera la aplicación del estándar O-ISM3 mejora la confidencialidad de la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022? **P2**: ¿de qué manera la aplicación del estándar O-ISM3 mejora la integridad de la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022? **P3**: ¿de qué manera la aplicación del estándar O-ISM3 mejora la disponibilidad de la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022?	**Objetivo general:** Mejorar la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022. **Objetivos específicos:** **O1:** Mejorar la confidencialidad de la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022. **O2:** Mejorar la disponibilidad de la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022. **O3:** Mejorar la integridad de la seguridad de la información mediante la aplicación del estándar O-ISM3 en la Clínica San Pablo S.A.C. – Huaraz, 2022.	**Hipótesis general:** La aplicación del estándar O-ISM3 mejora de manera significativa la seguridad de la información en la Clínica San Pablo S.A.C. – Huaraz, 2022. **Hipótesis específicas:** **H1:** La aplicación del estándar O-ISM3 mejora de manera significativa la confidencialidad de la seguridad de la información en la clínica San Pablo S.A.C. - Huaraz, 2022. **H2:** La aplicación del estándar O-ISM3 mejora de manera significativa la integridad de la seguridad de la información en la clínica San Pablo S.A.C. - Huaraz, 2022. **H3:** La aplicación del estándar O-ISM3 mejora de manera significativa la disponibilidad de la seguridad de la información en la clínica San Pablo S.A.C. -Huaraz, 2022.	**Variable Independiente** Estándar O-ISM3. **Dimensiones:** • Procesos de seguridad • Gestión de seguridad de la información. **Variable Dependiente** Seguridad de la información. **Dimensiones**: • Confidencialidad • Integridad. • Disponibilidad.	**Tipo de investigación:** según el enfoque es cuantitativo con nivel correlacional explicativo **Diseño de la investigación** corresponde al diseño preexperimental de prueba – posprueba con un solo grupo **Población:** el total de trabajadores de la Clínica San Pablo S.A.C. – Huaraz, siendo este un total de 200 trabajadores **Muestra:** la muestra queda definida con un total de 132 trabajadores de la Clínica San Pablo S.A.C -Huaraz.

Repositorio Institucional - UNASAM - Perú

ANEXO 2: "INSTRUMENTO DE RECOLECCION DE DATOS"

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO

Escuela profesional de ingeniería de sistemas e informática

ENCUESTA PARA MEDIR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN EN LA CLÍNICA SAN PABLO S.A.C. – HUARAZ.

Lea detenidamente las preguntas y responda con la mayor veracidad y sinceridad marcando una de la opción que se acomode más a su respuesta		**Nunca**	**Casi nunca**	**Ocasionalmente**	**Casi siempre**	**Siempre**
CONFIDENCIALIDAD	¿conoce o se le orienta periódicamente sobre las políticas de seguridad de la información de la empresa?	1	2	3	4	5
	¿Tiene acceso restringido a los sistemas e instalaciones que alojen información que no sea relevante para sus funciones? (Ejemplo: Ambientes donde se alojen las HC, Sistema clínico, Archivos y citas, Farmacia, Shicde, Data center)	1	2	3	4	5
	¿Evita compartir con sus compañeros sus credenciales de acceso a los sistemas y equipos infor0máticos? (Ejemplo: PC, Laptops, Correo, Sistema clínico, Archivos y citas, Farmacia, Shicde, etc.)	1	2	3	4	5
	¿Sigue algún procedimiento de confidencialidad afines a sus obligaciones contractuales, legislativas y regulatorias con la empresa respecto a seguridad de la información? (Ejemplo: Contrato, acuerdo de confidencialidad)	1	2	3	4	5
	¿Maneja cuidadosamente información considerada privada/confidencial durante el desarrollo de sus funciones? (Ejemplo: Historias clínicas, contratos, datos personales de los pacientes, proveedores, etc.)	1	2	3	4	5

Repositorio Institucional - UNASAM - Perú

DISPONIBILIDAD	¿Le brindan los respaldos de información (física/Digital) ante cualquier falla del sistema, equipo informático o perdida de información, de tal forma que no retrase sus labores? (Ejemplo: documentos compartidos, reportes de base de datos, HC, correos, etc.)	1	2	3	4	5
	¿Los sistemas y equipos informáticos utilizados en sus labores están disponibles para su uso incluso ante un corte del fluido eléctrico?	1	2	3	4	5
	¿Los equipos informáticos que utiliza le permite acceder a los diversos sistemas y repositorios de información necesarios para su trabajo sin presentar inconvenientes? (Ejemplo: lentitud, reinicios y apagados espontáneos, pantalla azul, etc.)	1	2	3	4	5
	¿El servicio de Internet le permite acceder a los diversos sistemas web necesarios para el desarrollo de sus funciones? (Ejemplo: Tableu, monitor de FE, páginas de seguros, etc.)	1	2	3	4	5
	¿El servicio de Internet le restringe el acceso libre a las diversas páginas que no son relevantes para el desarrollo de sus funciones? (Ejemplo: Youtube, páginas de compras, etc.)	1	2	3	4	5
INTEGRIDAD	¿Toda alteración de información relevante/importante es autorizada por el área o jefatura correspondiente? (Ejemplo: modificación de HC, Modificación de datos personales en la base de datos, modificación de facturas etc.)	1	2	3	4	5
	¿La información (Física/Digital) que maneja en sus labores es confiable, coherente de tal forma que le permite ser utilizada sin necesidad de realizar modificaciones o correcciones? (Ejemplo: Historias clínicas,)	1	2	3	4	5
	¿La empresa controla y restringe el acceso de personas no autorizadas a las instalaciones o sistemas que alojen información (física/digital) considerada de importancia para el desarrollo de sus funciones? (Ejemplo: Control de acceso a zonas no autorizadas a las personas externas, personal que esté a punto de culminar su vínculo laboral con la empresa, uso de cámaras de vigilancia)	1	2	3	4	5

Repositorio Institucional - UNASAM - Perú

	¿Los sistemas y equipos informáticos utilizados en el desarrollo de sus funciones son actualizados constantemente?	1	2	3	4	5
	¿los equipos informáticos que utiliza en sus labores cuentan con antivirus instalado y actualizado?	1	2	3	4	5

Repositorio Institucional - **UNASAM** - Perú

ANEXO 3: "INFORME DE OPINION DE EXPERTO N° 1"

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO

"Una nueva universidad para el desarrollo"

Facultad de Ciencias – Escuela Profesional de Ingeniería de Sistemas e Informática

INFORME DE OPINION DE EXPERTO

I. DATOS DEL EXPERTO

Apellidos Y Nombres Del Evaluador: Walter Junior Medina López

Profesión: Ing. Sistemas e Informática

Grado Académico: Mag. Ciencias e Ingeniería con mención en Tecnologías de la Información y Sistemas Informáticos

Centro De Labores: UNASAM

II. MATRIZ EVALUACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Indicador de Evaluación	Criterio de evaluación	Deficiente	Regular	Bueno	Excelente	Observaciones del experto
Adecuación	Es adecuado y comprensible			X		
Pertinencia	Es pertinente para el logro de objetivos			X		
claridad	Está formulado con un lenguaje claro				X	
Objetividad	No presenta sesgo ni induce a respuestas				X	
Coherencia	Hay relación entre variables, dimensiones e indicadores				X	
Organización	Existe una organización lógica y coherente de los ítems		X			
Intencionalidad	Adecuado para establecer asociación			X		

III. VALORACIÓN GENERAL DEL INSTRUMENTO:

Deficiente	Regular	Bueno	Excelente
		X	

Firma

Repositorio Institucional - UNASAM - Perú

ANEXO 4: "INFORME DE OPINION DE EXPERTO N° 2"

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO
"Una nueva universidad para el desarrollo"
Facultad de Ciencias – Escuela Profesional de Ingeniería de Sistemas e Informática

INFORME DE OPINION DE EXPERTO

I. DATOS DEL EXPERTO

Apellidos Y Nombres Del Evaluador: JAMANCA RAMIREZ MARCO ANTONIO

Profesión: INGENIERO DE SISTEMAS

Grado Académico: MAESTRO EN ING. DE SEGURIDAD INFORMÁTICA

Centro De Labores: UNASAM

II. MATRIZ EVALUACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Indicador de Evaluación	Criterio de evaluación	Deficiente	Regular	Bueno	Excelente	Observaciones del experto
Adecuación	Es adecuado y comprensible			X		LAS PREGUNTAS DEBEN SER GENERALES CON RESPECTO A LA ORGANIZACIÓN, NO PERSONALES
Pertinencia	Es pertinente para el logro de objetivos				X	LAS PREGUNTAS DEBEN SER GENERALES CON RESPECTO A LA ORGANIZACIÓN, NO PERSONALES
claridad	Está formulado con un lenguaje claro			X		LAS PREGUNTAS DEBEN SER GENERALES CON RESPECTO A LA ORGANIZACIÓN, NO PERSONALES
Objetividad	No presenta sesgo ni induce a respuestas			X		LAS PREGUNTAS DEBEN SER GENERALES CON RESPECTO A LA ORGANIZACIÓN, NO PERSONALES
Coherencia	Hay relación entre variables, dimensiones e indicadores			X		LAS PREGUNTAS DEBEN SER GENERALES CON RESPECTO A LA ORGANIZACIÓN, NO PERSONALES
Organización	Existe una organización lógica y coherente de los ítems			X		LAS PREGUNTAS DEBEN SER GENERALES CON RESPECTO A LA ORGANIZACIÓN, NO PERSONALES
Intencionalidad	Adecuado para establecer asociación			X		LAS PREGUNTAS DEBEN SER GENERALES CON RESPECTO A LA ORGANIZACIÓN, NO PERSONALES

III. VALORACIÓN GENERAL DEL INSTRUMENTO:

Deficiente	Regular	Bueno	Excelente
		X	

MARCO ANTONIO JAMANCA RAMIREZ
INGENIERO DE SISTEMAS
C.I.P. N° 123333

Firma

Repositorio Institucional - UNASAM - Perú

ANEXO 5: "INFORME DE OPINION DE EXPERTO N° 3"

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO

"Una nueva universidad para el desarrollo"

Facultad de Ciencias – Escuela Profesional de Ingeniería de Sistemas e Informática

INFORME DE OPINION DE EXPERTO

I. DATOS DEL EXPERTO

Apellidos Y Nombres Del Evaluador: Joseph Darwin Alvarado Tolentino

Profesión: Ing. Sistemas e Informática

Grado Académico: Maestro en ciencias e Ingeniería con mención en auditoria y seguridad informática

Centro De Labores: UNASAM

II. MATRIZ EVALUACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Indicador de Evaluación	Criterio de evaluación	Deficiente	Regular	Bueno	Excelente	Observaciones del experto
Adecuación	Es adecuado y comprensible			X		
Pertinencia	Es pertinente para el logro de objetivos		X			
claridad	Está formulado con un lenguaje claro				X	
Objetividad	No presenta sesgo ni induce a respuestas			X		
Coherencia	Hay relación entre variables, dimensiones e indicadores			X		
Organización	Existe una organización lógica y coherente de los ítems			X		
Intencionalidad	Adecuado para establecer asociación		X			

III. VALORACIÓN GENERAL DEL INSTRUMENTO:

Deficiente	Regular	Bueno	Excelente
		X	

Firma

Repositorio Institucional - UNASAM - Perú