FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Sistema de Gestión de Seguridad de la Información de Servicios en la nube basado en ISO/IEC-27017 para Instituciones Públicas

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR

Bach. Davila Chunga Dayan Ray

https://orcid.org/0000-0002-9676-8908

Asesor:

Mg. Mejia Cabrera Heber Ivan

https://orcid.org/ 0000-0002-0007-0928

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel - Perú

2024

Aprobación del Jurado

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN ISO/IEC-27017 PARA INSTITUCIONES PÚBLICAS

_____

Bach. Davila Chunga Dayan Ray

Autor

_____

Mg. Mejia Cabrera Heber Ivan

Asesor

_____ _____

Mg. Asenjo Carranza Enrique David

Presidente de Jurado

Mg. Alva Zapata Juliana Del Pilar

Secretario de Jurado

_____

Mg. Mejia Cabrera Heber Ivan

Vocal de Jurado

NOMBRE DEL TRABAJO

DAVILA_CHUNGA_DAYAN_RAY-TURNITIN.docx

RECUENTO DE PALABRAS

42066 Words

RECUENTO DE CARACTERES

229394 Characters

RECUENTO DE PÁGINAS

229 Pages

TAMAÑO DEL ARCHIVO

10.6MB

FECHA DE ENTREGA

Sep 10, 2024 10:30 AM GMT-5

FECHA DEL INFORME

Sep 10, 2024 10:33 AM GMT-5

14% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 12% Base de datos de Internet
- 4% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 7% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)

Declaración jurada de originalidad

Universidad Señor de Sipán

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la **DECLARACIÓN JURADA**, es **EGRESADO** del Programa de Estudios de **Ingeniería de Sistemas** de la Universidad Señor de Sipán S.A.C, y, declaro bajo juramento que soy autor del trabajo titulado:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN ISO/IEC-27017 PARA INSTITUCIONES PÚBLICAS

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informamos que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firma:

DAVILA CHUNGA DAYAN RAY	DNI: 10467519	

Pimentel, 1 de julio del 2024.

Dedicatoria

A mis padres, esposa e hijo.

Davila Chunga Dayan Ray

Agradecimientos

Un agradecimiento especial al Mg. Heber Ivan Mejia Cabrera quien, con su valioso aporte y experiencias, me permitieron el logro de este trabajo de grado.

Dávila Chunga Dayán Ray

Índice

Índice de figuras

Índice de tablas

Índice de anexos

Resumen

Un SGSI basado en la ISO/IEC 27017 es crucial para las instituciones del sector salud en Perú, ya que proporciona un marco sólido para garantizar la seguridad de la información, cumplir con los requisitos normativos, proteger los datos sensibles de los pacientes y gestionar los riesgos asociados con los servicios en la nube. Esto no solo ayuda a proteger la información crítica de la institución caso de estudio, sino que también contribuye a mantener la confianza del público en los servicios de salud ofrecidos. Por esta razón, primeramente, se seleccionó el estándar más adecuado para la seguridad de la información para servicios en la nube; luego, se diagnosticó el estado actual de la seguridad de la información en una institución pública peruana; después, se procedió a diseñar dicho SGSI considerando el estándar seleccionado previamente; posteriormente, se validó mediante juicio de expertos dicho modelo y, finalmente, se ejecutó una prueba piloto de dicho SGSI en una institución pública peruana del sector salud. Los resultados evidenciaron que, el SGSI obtuvo una puntuación de 92.90% de aprobación por parte de los expertos quienes lo consideraron como “Excelente” para su aplicabilidad, asimismo, en cuanto a la ejecución de la prueba piloto del SGSI para servicios en la nube en el MINSA, se logró mejorar el nivel de la seguridad de la información en el 100% de las cláusulas, al obtener un nivel de madurez INICIAL en el PRE TEST (1.15) y un nivel de madurez DEFINIDO en el POST TEST (2.53), luego de haber desarrollado el SGSI de servicios en la nube. Se concluyó que, el desarrollo de un SGSI de servicios en la nube basado en la norma ISO/IEC 27017 sí logró mejorar la seguridad de la información en instituciones públicas de salud peruanas.

Palabras claves: Computación en la Nube, Seguridad en la Nube, SGSI, Seguridad de la Información, ISO/IEC 27017.

Abstract

An ISMS based on ISO/IEC 27017 is crucial for healthcare institutions in Peru as it provides a solid framework to ensure information security, comply with regulatory requirements, protect sensitive patient data, and manage risks associated with cloud services. This not only helps protect critical information of the case study institution but also contributes to maintaining public trust in healthcare services offered. For this reason, firstly, the most suitable standard for information security for cloud services was selected; then, the current state of information security in a Peruvian public institution was diagnosed; next, the ISMS was designed considering the previously selected standard; subsequently, this model was validated by expert judgment, and finally, a pilot test of the ISMS was executed in a Peruvian public healthcare institution. The results showed that the ISMS obtained a 92.90% approval rating from the experts, who considered it "Excellent" for its applicability. Additionally, regarding the execution of the pilot test of the ISMS for cloud services in the MINSA, the level of information security was improved in 100% of the clauses, achieving an INITIAL maturity level in the PRE TEST (1.15) and a DEFINED maturity level in the POST TEST (2.53), after developing the cloud services ISMS. It was concluded that the development of a cloud services ISMS based on ISO/IEC 27017 did improve information security in Peruvian public healthcare institutions.

Keywords: Cloud Computing, Cloud Security, ISMS, Information Security, ISO/IEC 27017.

I. INTRODUCCIÓN

1.1. Realidad problemática

La computación en la nube (o conocido como “Cloud Computing” por su traducción al inglés) es un modelo de prestación de servicios de Tecnología de la Información (en adelante “TI”) que ofrece accesibilidad a recursos compartidos, tales como, verbigracia, almacenamiento, servidores y aplicaciones, por medio de Internet según la demanda acaecida. En lugar de gestionar sus propias infraestructuras, las organizaciones pueden utilizar los recursos proporcionados por proveedores externos, pagando solo por los servicios que necesitan. Esto les proporciona flexibilidad, escalabilidad y eficiencia operativa [1].

El uso cada vez mayor de la computación en la nube (en adelante “CC”) hace que las organizaciones y/o empresas que hacen uso de este tipo de tecnologías tengan que disponer de altos estándares, normas, marcos metodológicos, entre otros, relativos a la seguridad de la información (SI). Debido a la facilidad de acceso que da el almacenamiento en la nube, es muy vulnerable porque todos los datos están en Internet. En la actualidad, las organizaciones que manejan una alta cantidad de información, como es el caso de las instituciones públicas, requieran de estándares ligados a los sistemas de seguridad en entornos CC y en la toma de informaciones junto con decisiones informadas porque tendrá un impacto fatal en ellas.

El uso de la tecnología CC se ha convertido en una de las innovaciones más interesantes y desafiantes en el campo de las TI, ya que suministra métodos elásticos, flexibles, así como de almacenamiento de acuerdo a la demanda y proporciona servicios de computación a los clientes. En [2] se reveló la tasa de acrecentamiento anual en el transcurso del periodo comprendido entre los años 2021 - 2028 del tamaño del mercado y los ingresos compartidos de la demanda de computación en nube a nivel mundial es del 15,80%, lo que indica que habrá un aumento en el uso de tecnologías CC. Asimismo, en este estudio se estimó que, el tamaño del mercado y los ingresos compartidos de la computación en nube en

el país asiático de Indonesia aumentarán con una tasa de crecimiento anual durante 2021-2028 del 28-33%.

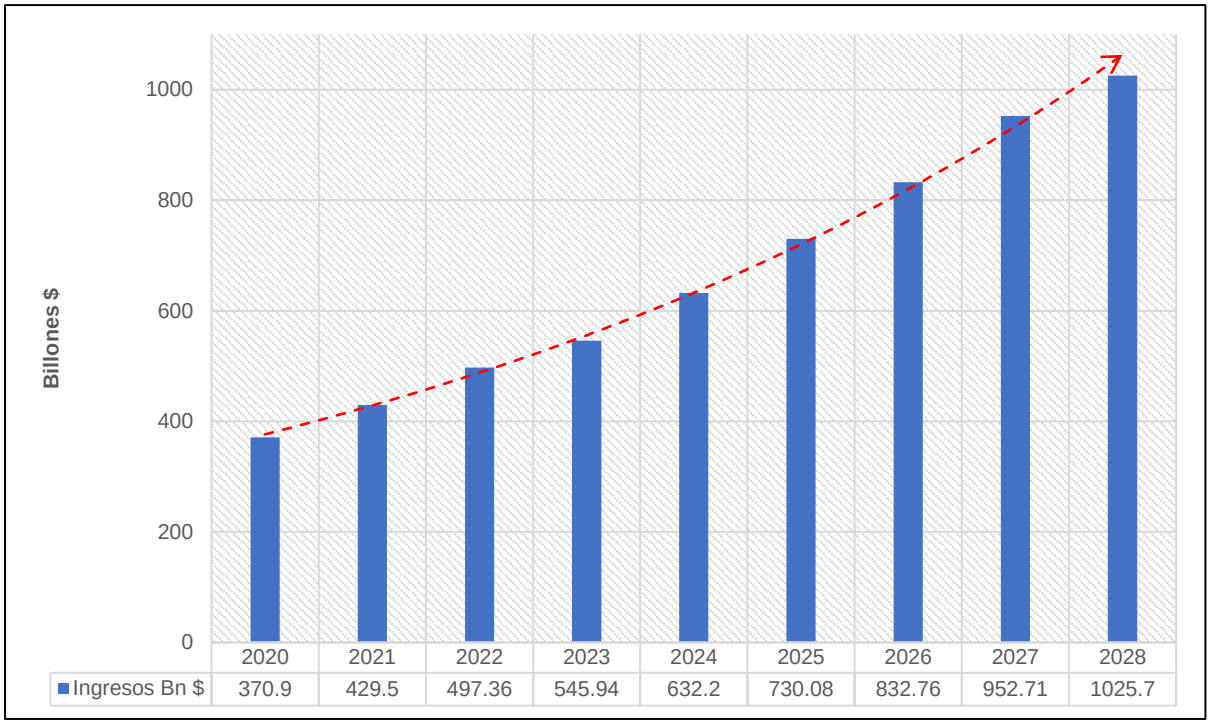


Fig. 1. Mercado mundial de la computación en nube 2030 [2].

Respecto a este incremento de las tecnologías de Cloud Computing, un estudio ejecutado por eHealth [3], revista especializada en Reportes de Salud en Latinoamérica, reveló un informe en el cual revela la adaptabilidad de tecnologías CC en nosocomios públicos y privados de la región, contando con la participación de 169 profesionales del sector, incluyendo CEOs, CIOs, directores médicos y responsables de sistemas, provenientes de 11 países de América Latina. Los resultados del estudio revelaron que, el 46% de los encuestados indicaron que sus organizaciones de salud actualmente utilizan servicios en la nube, mientras que otro 40% aún no lo hace, pero planea hacerlo en el futuro. Entre los usos que más hacen de esta tecnología se encuentran su usanza como backup de información (59.5%), almacenamiento de datos clínicos (55.90%), intercambio de información en salud (50.3%) y almacenamiento y gestión de historias clínicas (49.0%). En total, el 90% de los encuestados mostraron disposición a emplear la computación en la nube en sus instituciones.

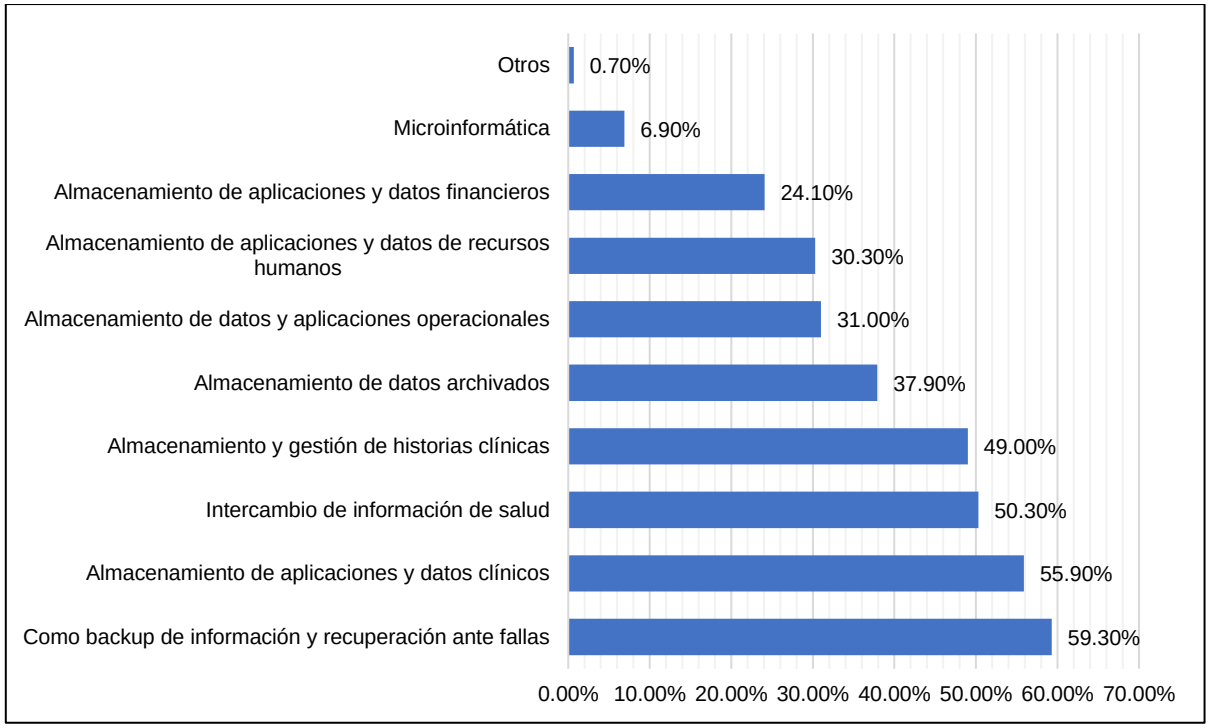


Fig. 2. Finalidad del uso de computación en nube en sector salud latinoamericano [3].

Por otra parte, el enfoque de “software como servicio” (SaaS), es uno de los modelos que posee la tecnología CC junto al de “Infraestructura como servicio” (IaaS) y al de “Plataforma como servicio” (PaaS), sin embargo, este implica que las aplicaciones están alojadas en los servidores de un proveedor de servicios, quien las ofrece a través de Internet, permitiendo de esta manera, a las instituciones públicas del sector salud acceder a los softwares mediante un modelo de alquiler o suscripción durante un período de tiempo específico, sin que ello involucre la necesidad de apostar por la inversión en infraestructura, hardware, implementación o actualizaciones continuas. Al igual que en otras partes del mundo, el SaaS, que incluye las historias clínicas electrónicas, se destaca como el tipo de servicio CC de mayor usanza o planificado para su uso en la región, representando casi el 50% del total. Este modelo proporciona una alternativa rentable y flexible para las instituciones de salud, permitiéndoles adaptar y escalar sus necesidades de software de manera más eficiente, sin comprometer la calidad o la seguridad de la atención médica.

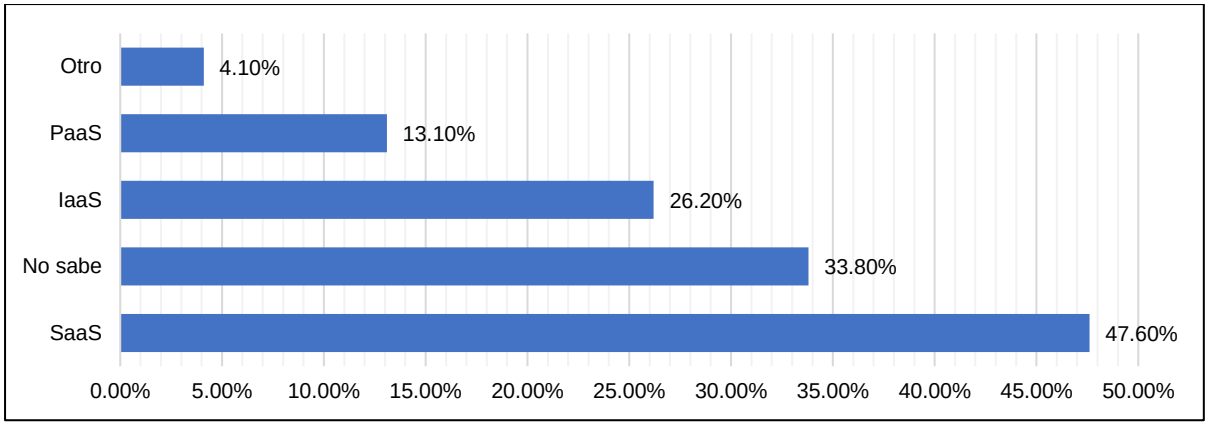


Fig. 3. Tipo de servicio en la nube utilizado en sector salud latinoamericano [3].

Se entiende que, según estos informes y estudios previos, el uso de CC en América Latina, sobre todo el sector de la salud, ha logrado una experimentación creciente y significativa en el último decenio. Aunque las cifras específicas pueden variar según el país y la fuente de los datos, algunas tendencias generales incluyen que, más hospitales, clínicas y proveedores de servicios de salud están recurriendo a la nube para almacenar, procesar y compartir datos médicos y administrativos. Así como también que, se están realizando inversiones significativas en infraestructura de TI y tecnologías de la información en los sectores de la salud en dicha región latinoamericana. Esto incluye, en definitiva, la adopción de soluciones basadas, no solamente en la nube para mejoramiento de la eficiencia operacional, sino que también hacen eco en la interoperabilidad de los sistemas TI y la calidad de la atención médica.

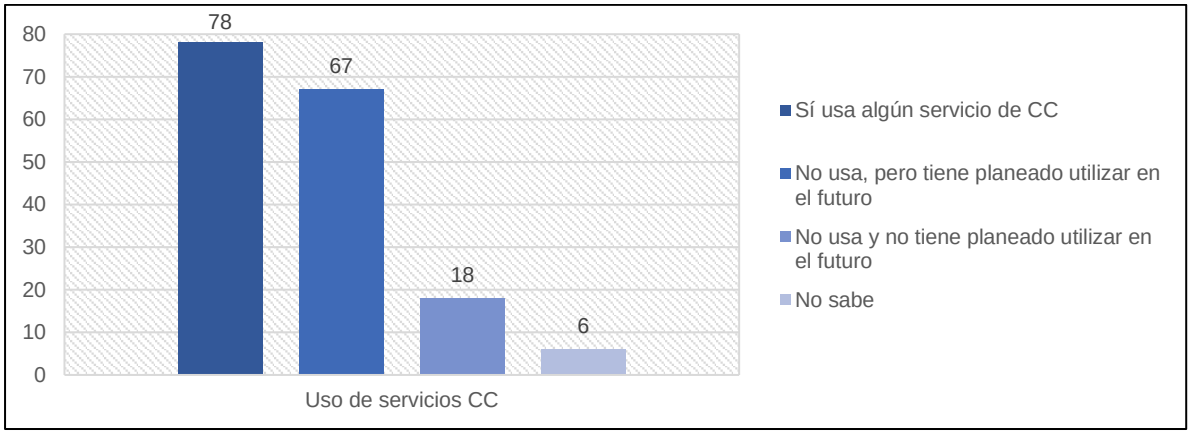


Fig. 4. Uso de servicios CC en sector salud latinoamericano [3].

En [4] se reveló que, en los últimos años, se evidenció de manera clara un incremento característico y revelador en el uso de CC en el sector de salud en Perú. Este fenómeno se debe a diversos motivos, como la búsqueda de mejoras en la eficiencia operacional, el aminoramiento de costes y la necesidad de accesibilidad rápida, fluida y de modo más legible hacia informaciones de tipo médicas. La adopción de la nube ha permitido a las instituciones de salud peruana acceder a tecnologías avanzadas para el análisis, almacenamiento y procesamiento de informaciones, lo que les ha facilitado gestionar de manera más efectiva los registros médicos electrónicos, compartir información entre distintos departamentos y mejoramiento de la calidad de las atenciones médicas. Además, las tecnologías CC ofrecen una mayor flexibilidad y escalabilidad, permitiendo mediante ello a instituciones de salud acomodarse rápidamente frente a los cambios en el sector y brindar servicios de salud de manera más ágil y eficiente a la población peruana.

Esto indica que, el adoptabilidad de tecnologías CC aumenta cada año según los resultados de las previsiones mundiales. Esta afirmación se ve reforzada por la presencia de muchos proveedores de servicios en nube en todas partes del mundo, no siendo ajeno el Perú donde, según [5] a finales del año 2022, el mercado de tecnologías CC logró la obtención de $706.42 millones. Además de ello, se evidenció un acrecentamiento sumamente relevante de este tipo de tecnologías CC en detrimento de los servicios de TI habituales u ortodoxos de datas center, los cuales tan solamente lograron cerrar con $247,91 millones el año anterior. Esto no hace más que evidenciar la existencia de oportunidades importantes para tercerizar las operaciones y, también, las gestiones de las cargas laborales efectuadas en nubes públicas, “el cual representó el 8.1% del total del mercado de servicios gestionados frente a los 6.2% de los servicios gestionados en nube privada” [5].

Por otra parte, para este año en curso, 2024, en gran parte, el heredamiento de aplicaciones obtendrá algún tipo de presupuesto para inversiones en cuanto a modernización de servicios y, por tanto, con servicios CC empleados a razón de un 65% del total general, este tipo de aplicaciones heredadas buscarán ampliarse en términos de reemplazamiento de

códigos ineficientes o funcionalidad, según revela un estudio ejecutado por la marca Gartner [6]. “Los servicios en la nube aparecen como un aliado importante en este movimiento, ya que permiten a los desarrolladores crear rápidamente proyectos nativos de nube híbrida, escalar continuamente a través de múltiples nubes y geografías y reducir la complejidad” [7].

En [8] se analizó cómo la adopción de TI en la nube está influyendo en la economía del Perú. Destaca cómo la migración hacia la nube puede generar importantes beneficios económicos para las instituciones peruanas, incluyendo la reducción de costos operativos, la optimación de recursos y mejoramiento de la productividad. Se resalta, con ello, el potencial de la nube como motor impulsor de acrecentamiento e innovación empresarial, así como su papel en la generación de empleo y el reforzamiento y la potenciación de la competitividad del Perú a nivel planetario al permitir un incremento de alrededor de 8.6 millones de empleo a nivel regional, más específicamente en el Perú un total de 1.4 millones de puestos laborales durante próximos tres lustros. Además, el artículo aborda los desafíos y oportunidades que enfrentan las empresas peruanas en su proceso de adoptabilidad de tecnologías CC, y destaca la importancia de políticas y programas de apoyo para fomentar la integración efectiva de estas tecnologías en el tejido empresarial del país.

Un estudio ejecutado en [9] examinó el perenne crecimiento, progreso y perfeccionamiento de tecnologías en la nube en el contexto nacional. Se resalta cómo la demanda de servicios en la nube sigue en aumento, impulsada por la imprescindibilidad de las compañías de mejoramiento de su agilidad, escalabilidad y eficiencia operativa. El artículo subrayó el papel clave que juegan los proveedores de servicios CC en la expansión de esta tecnología en el país, así como la relevancia de las inversiones en infraestructuras y recursos humanos para satisfacer la creciente demanda. Además, se discuten las tendencias emergentes en el mercado de la nube, como la adopción de soluciones híbridas y multi-nube, y se exploran los desafíos y oportunidades que enfrentan tanto los proveedores como los usuarios de servicios CC en Perú, finalmente considerando a la seguridad como la segunda barrera más alta para que las organizaciones desplieguen sus estrategias de Cloud

Computing. En conclusión, el artículo destacó el impacto positivo que la tecnología en la nube está teniendo en la economía y el panorama empresarial del país, y proyecta un futuro prometedor para su continuo crecimiento y desarrollo.

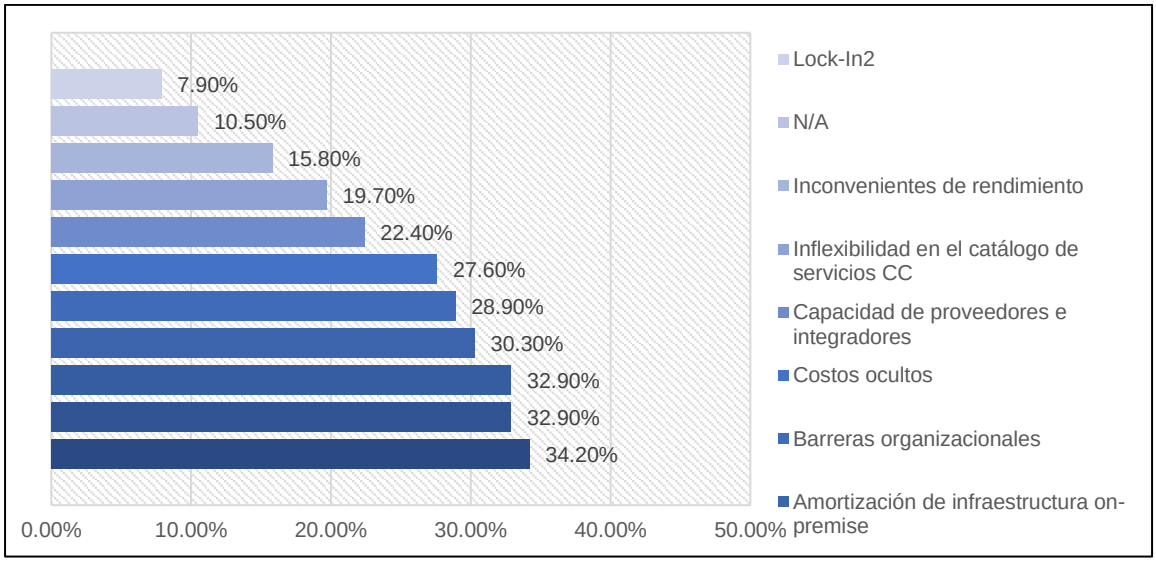


Fig. 5. Barreras existentes para el despliegue de servicios CC en sector salud [9].

En contraste con todo este panorama alentador en cuanto a uso de Cloud Computing, aparecen los problemas correlacionados con la carencia de Seguridad de la Información (SI) de los servicios CC. Por una parte, un estudio referido a esto por parte de Oracle [10] menciona que, los delincuentes ahora están robando informaciones mediante phishing dirigido para obtener accesibilidad a los servicios críticos CC de una organización, así como a los datos asociados con esos servicios. Una conclusión clave del informe sobre amenazas a la nube de este año es que las credenciales de usuarios son compartidas con miembros de la organización, lo que ya ha traído consecuencias como que el 59% de ellos habían sido comprometidos con casos de phishing. La actual alta tasa de incidentes de phishing y el hecho de que los piratas informáticos han aumentado las apuestas al buscar más y mejores prácticas de hacking en la nube, es necesario revisar un conjunto de mejores praxis para mitigar la amenaza predominante e incesante de los ataques por parte de los ciberdelincuentes.

En Reino Unido [11] en mayo del 2017 aconteció un caso significativo de ataque a la SI del entorno CC en el sector salud en el momento en que, el Servicio Nacional de Salud británico (NHS por su acrónimo de “National Health Service”) fue blanco de una embestida cibernética mediante ransomware denominado WannaCry, el mismo que logró la afectación de sistemas informáticos, no solamente en centros de atención médica, sino que también afectó a los diversos nosocomios existentes en todo el territorio británico. El ataque paralizó las operaciones de muchos hospitales y clínicas del NHS, interrumpiendo servicios médicos críticos, como la atención de emergencia y la programación de citas médicas. Los hackers cifraron los datos en los sistemas informáticos y exigieron un rescate para su liberación. Este ataque resaltó las vulnerabilidades existentes en los SI pertenecientes a la salud pública ante las amenazas cibernéticas y reveló la necesidad de mejorar la SI en dicho sector estatal. También subrayó la importancia de contar con planes de respuesta a incidentes cibernéticos y de mantener actualizadas las medidas de SI para la protección de las informaciones médicas sensibles almacenados en este tipo de entornos CC.

En Canadá [12] en octubre del 2019 se registró un destacado incidente de violación de SI en un entorno CC en el ámbito de la salud, protagonizado por la empresa de tecnología médica LifeLabs. Durante este evento, perpetradores cibernéticos lograron tener accesibilidad a los sistemas de LifeLabs, comprometiendo informaciones confidenciales y médicas de alrededor de 15 millones de pacientes. Los datos afectados incluían informaciones tales como, verbigracia, nombres, direcciones, números de seguro social, resultados médicos, etcétera. Dicha empresa de tecnología médica confirmó que los datos de los pacientes estaban almacenados en la nube y fueron comprometidos como resultado del ataque cibernético. Esta situación suscitó preocupación en la comunidad de la salud, evidenciando los riesgos inherentes al almacenamiento y procesamientos de informaciones sensibles en sus entornos en la nube. Asimismo, resaltó la relevancia de plantear e implantar medidas de SI sólidas y estar preparados para enfrentar amenazas cibernéticas cada vez más sofisticadas, especialmente en contextos donde se manejan datos médicos delicados.

Además, subrayó la necesidad de transparencia por parte de las organizaciones en asociación con la gestión de la SI y la notificación oportuna a los pacientes afectados en caso de brechas de datos.

En Irlanda [13] en mayo de 2021, se experimentó un grave ciberataque que obligó a cerrar el sistema informático de su sistema de salud pública, el Servicio de Salud Ejecutivo (HSE, por sus siglas en inglés). Este ataque, identificado como un ransomware, afectó significativamente las operaciones del sistema de salud, lo que llevó a la cancelación de citas médicas, la reprogramación de cirugías y la interrupción de servicios críticos de atenciones médicas en todo el país isleño. El ransomware utilizado en este ataque, conocido como Conti, se infiltró en la red del HSE y cifró los archivos, exigiendo un rescate para su liberación. Ante la gravedad del incidente, el HSE se vio obligado a desconectar gran parte de su infraestructura informática para contener la propagación del malware y evitar daños mayores. Este ciberataque resaltó las vulnerabilidades de los SI de salud pública frente a las amenazas tipo cibernéticas y subrayó las necesidades de reforzar las regulaciones de SI en este sector. Además, generó preocupación sobre la capacidad de respuesta de Irlanda y otros países frente a futuros ataques cibernéticos dirigidos a infraestructuras en la nube críticas como la salud pública.

Por otra parte, en un estudio en [14], examinó la creciente preocupación por la vulnerabilidad del sector de la salud ante posibles ataques a la SI. Se destaca cómo los sistemas informáticos y los datos sensibles de los pacientes se han vuelto cada vez más susceptibles a amenazas cibernéticas, lo que podría tener consecuencias de gran significancia en la SI y la calidad de las atenciones médicas. El artículo resalta la importancia de fortalecer las medidas de SI en las instituciones de salud, así como de mejorar la conciencia y capacitación del personal en materia de ciberseguridad. Además, se discuten las posibles consecuencias de un ataque a la SI en el sector salud, incluyendo la interrupción de los servicios médicos, el robo de informaciones confidenciales y sus riesgos para la salud y la seguridad de los pacientes. Se subraya la urgencia de abordar las vulnerabilidades y

mejorar la resiliencia del sector de la salud para contrarrestar las crecientes amenazas ciber-delincuenciales.

Como bien se logra distinguir, el sector salud se encuentra vulnerable a este tipo de situaciones que afectan la confidencialidad, integridad y disponibilidad de las informaciones. En [15] se evidenció la necesidad de establecer directrices claras y efectivas para certificar las protecciones adecuadas de las informaciones en entornos CC. En la medida en que los tiempos pasan, muchas más son las organizaciones que logran el adoptabilidad de entornos CC para almacenar, procesar y compartir datos, surge la preocupación por los potenciales riesgos de SI correlacionados con esta tecnología. Ante ello, las ISO proporcionan un marco referencial en mención con propósitos de establecer controles de SI efectivos en cualquier entorno de TI, incluidos los entornos de nube. Sin embargo, adaptar estos estándares y modelos a las especificidades de la computación en la nube presenta desafíos únicos, sobre todo para las instituciones públicas del sector salud.

Por una parte, se han creado varios estándares tanto a nivel global, como la Norma lSO 27001, y a nivel nacional, como la Norma Técnica Peruana NTP lSO/lEC 17799:2007 EDl, que definen los componentes esenciales de un “Sistema de Gestión de la Seguridad de la Información” (en adelante “SGSI”) a manera de una guía general, sin detallar la manera específica en que deben ser implementados. Esta responsabilidad recae en las organizaciones, por lo que la situación se complica aún más en este aspecto. Por otra parte, “en el Perú al respecto existe el marco legal que norma a través de la Resolución Ministerial N° 187-2010-PCM de la Presidencia del Consejo de Ministros la obligatoriedad de implementar en cada institución pública un Sistema de Seguridad de la Información basado en la Norma Técnica Peruana antes mencionada” [16]. Respecto al alcance que dicho documento oficial tiene, logra incluir consecuentemente al MINSA como instituciones cuyo patrocinio pende del Estado Peruano, empero, esta resolución no especifica el arranque o activación de SGSI de servicios en la nube.

En ese sentido, la institución pública caso de estudio, no cuenta con un SGSI específicamente para servicios en dichos entornos CC, lo que representa un riesgo significativo para la protección de informaciones de naturaleza sensible y críticos relacionados con la salud entera de la población. Sin un sistema adecuado de gestión de SI en entornos CC como estos, el MINSA podría enfrentarse a diversos desafíos y problemáticas, tales como:

a. Vulnerabilidades de seguridad: La falta de controles y medidas de SI específicas para los servicios en entornos CC podría dejar al MINSA expuesto a vulnerabilidades y ataques cibernéticos, comprometiendo la confidencialidad, integridad y disponibilidad de las informaciones médicos y administrativos.

b. Riesgo de pérdida de datos: La ausencia de un SGSI para entornos CC podría aumentar el riesgo de pérdida o robo de datos, lo que podría tener consecuencias graves para las investigaciones, las atenciones médicas y la planificación de políticas de salud.

c. Incumplimiento normativo: La carencia de medidas de SI apropiadas para entornos CC podría resultar en el incumplimiento de regulaciones y leyes correlacionadas con la protección de informaciones plenamente personales y la privacidad de las informaciones de salud, conllevando con ello a potenciales sanciones legales y pérdidas en cuanto a la confiabilidad pública por parte de los conciudadanos, más aún, considerando que si existen Resoluciones Ministeriales.

d. Falta de transparencia y control: Sin un SGSI para entornos CC, el MINSA podría carecer de la capacidad para monitorear cabalmente y auditar adecuadamente el acceso y uso de los datos, lo que dificultaría la identificación y respuesta a incidencias de SI.

Para solucionar este tipo de problemáticas, diversos autores han ejecutado investigaciones a nivel internacional y nacional, los cuales identificaron casuísticas propias, pero ligadas a la SI en entornos CC y las cuales han solucionado de distintas maneras. Entre estos se tienen:

En Bandung, Indonesia [17], se reveló que, una compañía proveedora de servicios CC, denominada PT.XYZ, trabajaba con diversos clientes a los que proveía de servicios en la nube, sin embargo, existía aún una brecha en cuanto a la preocupación de sus clientes respecto a la SI, pues en estos tiempos existen fugas de información, privacidad de la información, etcétera. Además de ello, PT.XYZ requería certificarse en la lSO/IEC 27017, para brindarle confianza a sus clientes, por lo que ejecutó una auditoría a una de sus empresas clientes para conocer el grado de cumplimiento con la ISO y el nivel de madurez de SI alcanzado y buscar el mejoramiento de sus servicios. Por esta razón, ejecutaron una auditoría fundamentada en la norma lSO/lEC 27017:2015 para reconocer el estado actual de una empresa a la que proveían de servicios en la nube, de modo que pudieran identificar oportunidades de mejora. Los resultados permitieron distinguir que, PT.XYZ había implementado solamente 97 de los 121 objetivos de control alineados a la norma, por lo que se encontraban en un 80.16% de cumplimiento; además de ello, la empresa cliente se encontraba en un Nivel Gestionado (2.317) estando aún muy por debajo del nivel mínimo esperado, el Nivel Gestionado Cuantitativamente (4.1). Se concluyó que, para poder certificarse en la norma ISO/IEC 27017:2015, PT.XYZ debe cumplir al 100% con los objetivos de control y, además, enfocarse en aquellas cláusulas en las que ha obtenido el menor nivel de madurez, como, por ejemplo, criptografía, control de acceso y seguridad física.

En Selangor, Malasia [18], se reveló que, las TI de la computación en la nube han logrado atraer el interés mundialmente por su capacidad de ofrecer servicios adaptables, rentables y flexibles en el despliegue de soluciones informáticas, sin embargo, aún existe una brecha en cuanto al resguardo de la confidencialidad, integridad y disponibilidad de dichas informaciones en entornos CC desencadenando incidentes como la perdición de informaciones y la violación de las mismas. Por esta razón, primeramente, se ejecutó una revisión de literatura concerniente sobre todo con la usanza de los servicios en entornos CC por parte de las organizaciones; luego, se evaluaron comparativamente cuatro (04) modelos existentes de preparación para la seguridad en la nube; después, seleccionaron mediante

criterios de selección de dominios para el desarrollo de un modelo para la SI en la nube; posteriormente, diseñaron un modelo de siete (07) dominios y cuarenta y cuatro (44) controles considerando la ISO/IEC 27017 considerando tres fases: (i) desarrollo del modelo preliminar; (ii) verificación del modelo preliminar; y (iii) validación del modelo final y; finalmente validaron el modelo por expertos. Los resultados obtenidos evidenciaron que, el 45,5% de los profesionales que están totalmente de acuerdo con la eficacia de las pruebas del prototipo, un 54,5% de los profesionales que estuvieron muy de acuerdo con el nivel de eficiencia de las pruebas de prototipo. Se concluyó que, el modelo desarrollado sirve como guía para cualquier organización en su esfuerzo por brindar servicios de cómputo en la nube seguros que puedan ser acreditados por un estándar de certificación reconocido mundialmente.

En Yakarta, Indonesia [19], se reveló que, el Cloud Computing se está implantando en la totalidad de los sectores laborales del planeta, no siendo ajena el ámbito de la enseñanza superior, tal y como es el caso de las más relevantes casas de estudios privadas de Indonesia y que según sus estadísticas, viene siendo atacada a razón de 1 millón de intrusiones por año en cuanto a su computación en nube privada. Por esta razón, se propuso ejecutar una evaluación de la SI en entornos CC, más aún, considerando que ya lleva +5 años empleando este tipo de tecnologías. Para ello, hizo empleo de la ISO/IEC 27001, considerando las 14 cláusulas que, coincidentemente son las que posee la ISO/IEC 27017 y de una escala de seis niveles basada en el SSE-CMM y la ISO 21827:2008 para evaluar el nivel de madurez actual. Los resultados obtenidos evidenciaron que la SI en dicho entorno CC estaba actualmente en un “Nivel Gestionado” (2.31), por lo que existía una brecha muy amplia para llegar al nivel de madurez esperado de 5.00. Dentro de cláusulas con mayor brecha se identificaron a Criptografía (3.59), Relaciones con los Proveedores (3.11) y Conformidad (3.06), todas ellas reflejadas en la falta de controles criptográficos, la no aplicabilidad de políticas de vigilancia de accesos a las informaciones, ausencia de auditorías, etcétera. Se concluyó que, el modelo de evaluación proporciona beneficios de análisis para mapear aquellos puntos débiles a atacar y en donde existen oportunidades de mejora,

asimismo también se evidenció la amplia brecha que posee la Universidad XYZ para llegar al nivel esperado de madurez.

En Selangor, Malasia [20], se reveló que, la creciente tendencia a la computación en nube ha atraído a muchas organizaciones a esta tecnología por su capacidad de ofrecer servicios escalables y flexibles, su rentabilidad y la disponibilidad de los datos. Sin embargo, la preocupación por la SI seguía siendo el obstáculo principal para la adecuación de los servicios en la nube, no siendo ajenas las compañías malayas. Por esta razón, primeramente, se caracterizó la coyuntura actual de la usanza de CC por organizaciones en dicho país asiático; luego, se diseñó un SGSI acorde a las necesidades de esta coyuntura local considerando la ISO/IEC 27017; posteriormente, se implementó dicho modelo en un caso de estudio local y; finalmente se evaluaron los resultados. Los resultados obtenidos mostraron que, se mejoraron los niveles de SI en dicho caso de estudio, evidenciándose mejoras en cuanto a la pérdida de control y gobernanza es especialmente porque los CSP anteriormente no eran fiables ni transparentes. Se concluyó que, este modelo sirve de soporte a los CSP malayos en el cumplimiento de las normas específicas de la nube para certificar la SI de las informaciones de las clientelas y que todos los recursos estén bien protegidos.

En Ibarra, Ecuador [21], se reveló que, con la evolución de las TI, logró darse la conceptualización nueva de computación en la nube, por lo que suministradores de TI tuvieron que orientar sus operaciones hacia dichos servicios, tal es el caso de la compañía caso de estudio quien ofrecía diversas soluciones cloud en modalidad SaaS pero que, aún poseía brechas diversas en cuanto a la SI con los servicios en la nube que ofrecía. Por esta razón, primeramente, caracterizaron los estándares de SI existentes en la literatura; luego, analizaron la situación actual de dicha compañía en cuanto a infraestructura, niveles de seguridad, planes de contingencia, análisis de riesgos y vulnerabilidades, etcétera; posteriormente desarrollaron el SGSI para servicios en la nube considerando la ISO en mención y el apoyo del Ciclo PDCA y; finalmente validaron dicha propuesta por juicio de expertos en SI para llevarlo a la práctica en el caso de estudio. Los resultados obtenidos

mostraron que, luego de implementar dicho SGSI, se logró obtener un nivel de cumplimiento del 80% de cada uno de los criterios asociados a un cumplimiento “alto”. Se concluyó que, dicho SGSI es un punto de partida para que dicha compañía pueda certificarse en la normativa ISO/IEC 27017 y así pueda seguir logrando el aminoramiento de los riesgos y vulnerabilidades de SI.

En Alcalá de Henares, España [22], se reveló que, actualmente las empresas hacen uso de servicios cloud, lo cual les permite externalizar su administración e infraestructura, por lo que han aparecido compañías dedicadas a prestar dichos servicios cloud, para lo cual existen diversos estándares, marcos y normas que coadyuvan a las compañías refuercen sus estrategias de SI en cloud. Por esta razón, primeramente, describieron la SI en cuanto a marcos existentes, tipos de cloud, etcétera; luego, caracterizaron la situación presente en cuanto a SI de la compañía española caso de estudio; después, diseñaron el SGSI fundamentado en la norma en IS0/IEC 27017 y considerando la metodología MAGERIT como soporte en la gestión de riesgos; posteriormente implementaron dicho SGSI, para; finalmente evaluar los resultados de dicha implantación. Los resultados obtenidos evidenciaron que, el proceso de explotación CMS cloud poseía valores altos (3-Alto) en cuanto a DICAT con un valor de negocio de € 292.682.927; asimismo, la integridad y disponibilidad asumirían más riesgos con un 24% y 31% respectivamente. Se concluyó que, el SGSI fundamentado en la IS0/IEC 27017 sí cumple con mejorar el nivel de SI en una compañía peruana de software que suministra software como PaaS.

En Riobamba, Ecuador [23], se reveló que, en la actualidad, con las grandes cantidades de información que se manejan en las diversas compañías es necesario que estas realicen copias de seguridad en las nubes, sin embargo, estos nuevos servicios plantean nuevos desafíos en cuanto a la seguridad de la información, no siendo ajeno el país ecuatoriano en donde no se han visto normativas en cuanto a esta temático, evidenciándose el requerimiento de disponer de un modelo de seguridad que mitigue dichas vulnerabilidades. Por esta razón, primeramente, se caracterizaron las ISO/IEC 27017 y 27018; luego, se diseñó

el SGSI considerando las ISO anteriormente mencionadas y fundamentado en Seguridad del Entorno, Conocer & Limite de Acceso, Detección y Respuesta; después, implementaron el modelo haciendo uso de herramientas tales como Mantis Bug Tracker, ClamAV, Aide, etcétera; finalmente, evaluaron los resultados de las pruebas obtenidas. Los resultados obtenidos evidenciaron que, el modelo de SGSI ayudó en el mejoramiento de los niveles de SI y en la mitigación de vulnerabilidades en un 75.0%. Se concluyó que, el modelo de SGSI ayudó al mejoramiento de los niveles de SI en la nube en cuanto a cantidades de logs, riesgos mitigados y vulnerabilidades.

En Callao, Perú [24], se reveló que, en la actualidad la información es una pieza ampliamente trascendental en las organizaciones de Ia totalidad los sectores, pero que, sin embargo, desde el punto de vista gerencial aún existe una brecha en cuanto a la aceptabilidad de esta cultura de SI pues muchas veces no es parte de los presupuestos de tales organizaciones. Asimismo, se reveló que, en este país, existe una norma que obliga a todas las instituciones públicas a la implementación de un SGSI, no siendo ajenas las universidades. Por esta razón, desarrolló una estrategia para la implantación de un SGSI de servicios en entornos CC para migrar las informaciones físicas de la que disponía una universidad, caso de estudio, a un entorno cloud. Para ello, se desarrolló la propuesta fundamentada en la ISO/IEC 27017 y en un total de cinco (05) etapas las cuales tenían una mejora continua mediante el Ciclo de Deming: a) Desarrollo del SGSI, b) preparación para la migración en la nube, c) implementación en la nube, d) implementación de los controles y e) evaluación de los controles establecidos. Los resultados obtenidos mostraron que, en efecto, no existían controles por lo que la propuesta también trajo consigo una escala para la evaluabilidad del nivel de madurez la cual constó de cinco (05) niveles. Se concluyó que, el SGSI para servicios en entornos CC sí permite la mejora de la SI en las universidades públicas peruanas.

En La Habana, Cuba [25], se revelo que, las organizaciones cubanas con limitaciones de financiamiento y que poseían centro de datos virtualizados, tenía inconvenientes para

elegir aquellos controles y dominios de SI, que les admitan la mantenibilidad de la confidencialidad, integridad y disponibilidad de sus informaciones. Por esta razón, los autores plantearon una propuesta basada en los mejores estándares y documentos que existen en EEUU y en dicho país caribeño. Primero, ejecutaron una revisión de la literatura en la que lograron distinguir cinco (05) directrices. ISO 27017, SP 800/53, CCM, CIS y la resolución n0 127 del Ministerio de Comunicaciones cubano. Luego de hacer el análisis exhaustivo de estas cinco directrices, primeramente, depuraron varios controles que no eran acordes a este tipo de organizaciones, para posteriormente, plantear su propuesta en un total; de 41 controles que fueron agrupados en 14 dominios totales. Además de ello, dieron alcance de algunas herramientas para estos controles propuestos, tales como OCS Inventory para el inventario de activos o Moodle para la capacitación del recurso humano, entre otros. Se concluyo que, los dominios y controles propuestos en esta investigación, aseguran los requisitos mínimos de confidencialidad, integridad y disponibilidad de las informaciones de aquellas organizaciones que poseen limitancias económicas y que además de ello, estos controles y dominios son el punto de partida para que estas organizaciones puedan actualizar y seguir mejorando sus SGSI constantemente.

En Quito, Ecuador [26], se reveló que, el CC es un paradigma moderno que accede brindar a las compañías un tecnológico en cuanto a la información, teniendo una gran acogida e impacto por la amplia gama de beneficios que ofrece en sus servicios IaaS, PaaS y SaaS. Sin embargo, ante tal acogida, este paradigma ha introducido con él un nuevo manejo de informaciones que deben de ser resguardadas, por lo que se hace necesario el desarrollo de soluciones que admitan resguardar la confidencialidad, integridad y disponibilidad de ellos. Ante tal panorama, no solamente los proveedores de servicios deben buscar nuevas formas de proteger dichas informaciones, sino que también deben hacerlo las empresas clientes. Por esta razón, se planteó una propuesta de SGSI basado en la familia 27K para ambientes cloud de manera que fuera implementada en una compañía de TI que venía realizando la migración parcial de sus informaciones la nube. Para ello, tomaron como referencia la ISO/IEC

27001:2013, la cual analizaron a detalle en cada una de sus fases, documentos y registros, para posteriormente, adaptarla al caso de estudio. Los resultados obtenidos mostraron que, mediante la usanza de esta ISO en mención se lograron proponer siete (07) fases para este tipo de coyuntura cloud. Se concluyó que, la familia ISO 27K brinda una hoja de ruta, tanto a las clientelas, como a los proveedores de servicios CC, una opción para poder monitorear los recursos cloud previamente sin permitir que sus informaciones se vean comprometidas al migrar de data center físicos a entornos cloud.

En Bogotá, Colombia [15], se reveló que, ante el incremento exponencial de los datos e informaciones, las empresas han visto con buenos ojos almacenar dichas informaciones a la nube, es por ello que contratan a empresas que ofrecen este tipo de servicios. Además de ello, es importante mencionar que, el incremento del uso de tecnologías cloud trajo consigo también el acrecentamiento de problemas relacionados con la SI, por ello es menester que las organizaciones cuenten con mecanismos para la mantenibilidad de la confidencialidad, integridad y disponibilidad, pero basados estándares y modelos de aceptación internacional. Por esta razón, se ejecutó una revisión de la literatura en la que se distinguieron varios modelos para proteger el entorno de las informaciones, tales como el Modelo Bell-Lapadula, Modelo Clark-Wilson, Modelo Graham-Denning, etc. Posterior a ello, se ejecutó también una correlación de los criterios de SI con los modelos y estándares encontrados previamente, para posterior a ello, proponer recomendaciones útiles para este fin. Los resultados evidenciaron que, existen 14 criterios para la buena gestión de la SI en un entorno CC. Se concluyó que, las recomendaciones brindadas, son una hoja de ruta para las instituciones que buscan adquirir servicios cloud, proponiendo recomendaciones que han sido elaboradas partiendo de los análisis previos realizados a los estándares, modelos y prácticas existentes, entre los cuales destacan la ISO/IEC 27017.

En Viena, Austria [27], se reveló que, el rápido crecimiento la IaaS basado en la nube plantea la cuestión de cómo sostener y garantizar la seguridad de las operaciones, por lo que necesitan de lineamientos para los controles de SI ajustables a las prestaciones y la usanza

de los servicios CC, más aún, considerando a los proveedores de este tipo, siendo estos últimos, los responsables de proporcionar una plataforma IaaS que sea elástica, fiable y segura para el consumidor de la nube, que les permita ser utilizada por otros servicios cloud, tales como PaaS o SaaS. Por esta razón, se ejecutó una revisión de aquellas directrices que existen para la seguridad de las operaciones en la nube, distinguiéndose varias, entre las cuales destacan, NIST SP 800-82, NIST SP 800-184, CTP (Cloud Trust Protocol) y la familia 27K, siendo de este último grupo, la ISO/IEC 27017:2015 la que evaluaron por ser aquella que está ligada estrechamente a la SI en entornos CC, más específicamente la evaluaron en su Cláusula 12, referida a la Seguridad de la Operaciones mediante su aplicabilidad en las plataformas OpenStack y VMware vSphere, ambas plataformas IaaS. Los resultados obtenidos evidenciaron que, los controles de seguridad 12.3.1 (Respaldo de Informaciones) y 12.2.1 (Controles contra el Malware) son los menos compatibles con las plataformas OpenStack y VMware vSphere, así como también, los controles de seguridad 12.1.4 (Separación de entornos para desarrollo, prueba y operación) y 12.6.2 (Restricciones en Ia instalación de Software) sólo pueden aplicarse con un esfuerzo adicional en las plataformas evaluadas. Se concluyó que, la seguridad de las operaciones requiere una definición clara de los procesos operativos en materia de seguridad, así como de los servicios de infraestructura de apoyo.

En Jouribga, Marruecos [28], se reveló que, al igual que la progresiva demanda de servicios CC en la actualidad, con ello, también crecen las amenazas de seguridad, vulnerabilidades y ataques a este tipo de tecnologías, por lo que, el mundo debe ser consciente acerca de la necesidad que tiene por tomar medidas preventivas y controles idóneos para la identificación, valuación y gestión de la SI en entornos CC. Por esta razón, en este artículo, se ejecutó un análisis de aquellos estándares que existen en la literatura para Ia gestión de la SI en entornos Cloud Computing y a partir de ellos plantear un marco conceptual que permita a las organizaciones obtener información acerca de cómo establecer un enfoque adecuado de gestión de riesgos de SI en este tipo de entornos Cloud Computing

o, en todo caso, complementar los procesos existentes que ya poseen. Los resultados obtenidos mostraron la existencia de las lSO 27001, lSO 27002, lSO 27017, lSO 27032 y el NIST Cybersecurity Framework (CSF); asimismo, en base a una combinación de las buenas prácticas internacionales mencionadas previamente, se propuso un marco para la SI para servicios CC el cual se compuso de 21 pasos. Se concluyó que, el modelo propuesto es una guía completa para las organizaciones que deseen establecer su enfoque adecuado de gestión de SI en entornos CC.

En Quito, Ecuador [29], se ejecutó un estudio enfocado en la falta de recursos y conocimientos especializados sobre SI en PYMES ecuatorianas. Muchas pymes de la localidad de Ambato, carecen de la capacidad para implementar medidas adecuadas de autenticación y seguridad en entornos CC, lo que las deja vulnerables a diversas amenazas cibernéticas, como el robo de datos, accesos no autorizados y los ataques de malware, lo cual, inevitablemente sabría traerle consecuencias de gran valor tales como, verbigracia, pérdidas de datos críticos, daños al prestigio de la compañía y pérdidas monetarias, por lo que es menester poner sobre la marcha diversos tipos de estrategias y herramientas de manera que se puedan fortalecer sus posturas de seguridad en entornos cloud y proteger sus activos digitales de manera efectiva, a pesar de las limitancia de recursos y conocimientos. Por esta razón, se proporcionó un marco detallado y recomendaciones prácticas para la implantación de reglas de autentificación y SI en entornos CC, adaptadas específicamente a las necesidades y capacidades de las PYMES ecuatorianas, teniendo en consideración la ISO/IEC 27017. Los resultados evidenciaron que, las PYMES ecuatorianas poseían un nivel de madurez “en procesos” en cuanto al Cloud Computing (35.30%), desconocían de los mecanismos de seguridad en dichos entornos (41.20%), entre otras brechas. Se concluyó que, adoptando un enfoque proactivo hacia la SI en entornos Cloud Computing fundamentado en la lSO/IEC 27017, las PYMES ambateñas pueden proteger su reputación, manteniendo la confianza de sus clientelas y asegurando con ello el éxito en un horizonte futuro en entornos digitales que cada vez, en demasía, es más complejo y sobre todo peligroso.

En [30], se reveló la carencia de claridad y comprensión sobre qué estándares de SGSI son más apropiados y efectivos para entornos Cloud Computing. Dado el crecimiento y la complejidad del Cloud Computing, las organizaciones se enfrentan a desafíos para garantizar la SI y el cumplimiento normativo en este entorno dinámico y compartido, por tanto, se hace trascendental comprender y comparar exhaustivamente los diferentes estándares de SGSI y su implicancia en la SI en entornos CC, con el fin de ayudar a organizaciones a asumir decisiones informadas y estratégicas acerca de cómo dar protección a sus datos y sistemas en dichos entornos. Por esta razón, se ejecutó un análisis comparativo de diez (10) estándares internacionales de SGSI y su impacto en el entorno Cloud Computing. Los resultados obtenidos evidenciaron diez (10) estándares de SGSI ampliamente reconocidos a nivel internacional, como ISO/IEC 27001, NIST SP 800-53, PRINCE-2, CSA CCM, entre otros; comparándolos y contrastándolos en términos de su alcance, enfoque, requisitos clave y su aplicabilidad específica a entornos Cloud Computing. Se concluyó que, si bien es cierto, algunos estándares son más amplios y generales en su alcance, otros están más centrados en aspectos específicos de la SI, tales como la lSO/IEC 27017, que es específica para entornos Cloud Computing, pero que, sin embargo, la elección del estándar más adecuado para una organización dependerá de diversos factores, como su tamaño, industria, ubicación geográfica y requisitos normativos existentes.

Los objetivos de la seguridad de las operaciones consisten en respaldar fielmente la planificación y la mantenibilidad de los procesos cotidianos que son críticos con respecto a la seguridad de los entornos de información. En este trabajo ofrecemos un análisis detallado de la norma ISO 27017 en lo que concierne a controles de SI e investigamos en qué medida las plataformas en nube más populares pueden darles cabida. Este informe surgió como una ayuda a la comunidad de SI, porque al analizar un caso de estudio de un SGSI de servicios en la nube para el caso de estudio de instituciones públicas peruanas, con el objetivo de investigar las causas que se afecta el proceso de monitoreo de acceso no autorizado que afecta las citas, entre otros, además de apoyar la toma de decisiones como parte del propósito

de mejorar la SI.

Esta investigación, basada en estándares internacionales como la norma IS0 27017, adoptó una nueva perspectiva en instituciones públicas peruanas, donde una de las mayores barreras es el alineamiento a entidades mayores, dependiendo de las jerarquías organizativas, y que además de ello, dispongan de servicios en entornos CC, por ejemplo, en el caso de los ministerios, verbigracia, el caso del MINSA, en la cual, sus áreas internas a veces no se comunican de manera correcta dentro de la misma institución y este al ser un ministerio depende de las directrices que establece el gobierno de turno.

Esta investigación aprobada por la Universidad Señor de Sipán, permitió identificar el recurso de investigación asociados con los objetivos de salud que ayuden a la sociedad de manera exitosa impulsando el bienestar y confidencialidad de los pacientes en un mundo más digital pero seguro.

Finalmente, en cuanto a pertenencia, el presente informe perteneció a la Línea de Investigación “Infraestructura, Tecnología y Medio Ambiente” línea propuesta por esta casa de estudios superiores, en el Área de “Tecnologías de la Información”, más específicamente en la temática “Seguridad Informática” pues, se desarrolló un SGSI de servicios en la nube, el cual estuvo fundamentado en la norma IS0/IEC 27017 para optimar la SI en instituciones públicas de salud peruanas.

1.2. Formulación del problema

¿El desarrollo de un sistema de gestión de seguridad de la información de servicios en la nube basado en la ISO/IEC-27017 mejora la seguridad de la información en instituciones públicas?

1.3. Hipótesis

Mediante el desarrollo de un sistema de gestión de seguridad de la información de servicios en la nube basado en la ISO/IEC-27017 se mejorará la seguridad de la información en instituciones públicas

1.4. Objetivos

1.4.1. Objetivo general

Desarrollar un sistema de gestión de seguridad de la información de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas

1.4.2. Objetivos específicos

- Seleccionar el estándar más adecuado para la seguridad de la información en entornos de servicios en la nube.
- Diagnosticar el nivel de cumplimiento actual de políticas de seguridad de la información en el entorno de servicios en la nube que existe en una institución pública de salud peruana.
- Diseñar un sistema de gestión de seguridad de la información considerando un entorno de servicios en la nube y basado en el cumplimiento del estándar seleccionado.
- Validar mediante juicio de expertos el sistema de gestión de seguridad de la información propuesto.
- Ejecutar una prueba piloto del sistema de gestión de seguridad de la información para servicios en la nube en el caso de estudio.

1.5. Teorías relacionadas al tema

1.5.1. Cloud Computing

1.5.1.1. Definición de Cloud Computing

El Cloud Computing, también conocido como computación en la nube, es “un modelo de prestación de servicios de tecnología de la información que permite acceder y utilizar recursos informáticos, como servidores, almacenamiento, bases de datos, redes, software y otros servicios, a través de internet de manera flexible y escalable, según la demanda del usuario” [31].

En lugar de que las organizaciones mantengan sus propias infraestructuras de TI físicas, el Cloud Computing les proporciona la capacidad de valerse de recursos informáticos introducidos en data centers remotos, operados por proveedores de servicios CC. Dichos recursos son compartidos entre múltiples usuarios y pueden ser aprovisionados y des aprovisionados rápidamente según las necesidades del usuario [1].

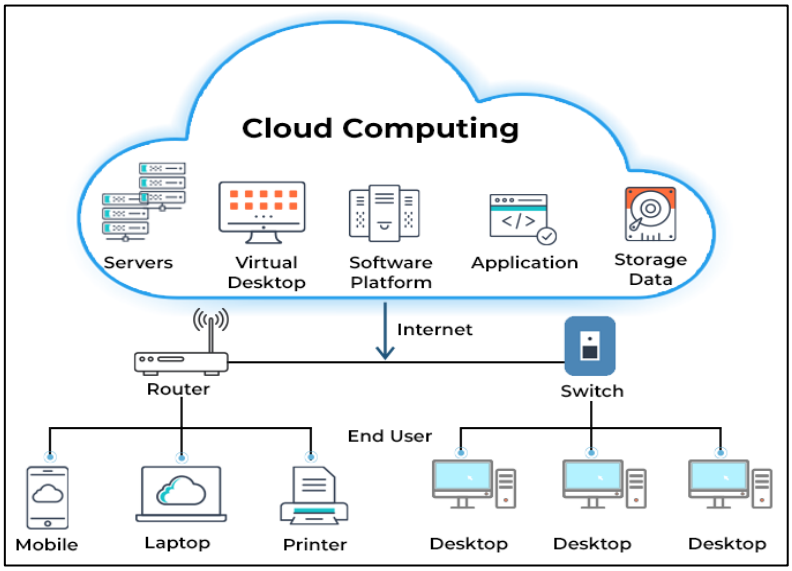


Fig. 6. Arquitectura Cloud Computing.

El CC se basa en la virtualización, Ia automatización y la distribución de recursos informáticos para ofrecer una variedad extensa de servicios, incluyendo:

- Infraestructura como servicio (IaaS): que, “proporciona acceso a recursos informáticos fundamentales, como servidores virtuales y almacenamiento” [31].
- Plataforma como servicio (PaaS): que, “ofrece un entorno de desarrollo y ejecución para aplicaciones, incluyendo herramientas y servicios para facilitar el desarrollo, la implementación y la administración de aplicaciones” [31].
- Software como servicio (SaaS): que, “ofrece aplicaciones y software alojados en entornos CC y accesibles a través de internet, eliminando la necesidad de instalar y mantener software en los dispositivos del usuario” [31].

EI CC ofrece un abanico de beneficios, incluyendo la capacidad de reducir costos operativos, mejorar la agilidad y la flexibilidad de las organizaciones, y permitir la innovación y la escalabilidad rápida de los servicios. Sin embargo, también traza desafíos en cuanto a privacidad, seguridad, cumplimiento normativo y dependencia de terceros proveedores de servicios en entornos CC [31].

1.5.1.2. Características del Cloud Computing

Según Rashid et al. [32] el Cloud Computing exhibe una serie de atributos esenciales y trascendentales que lo distinguen en el ámbito de la TI. Estos aspectos característicos delinean su naturaleza y operatividad de manera significativa y son los siguientes:

- Flexibilidad Elástica: Se refiere a la habilidad del CC para ajustar la cantidad de recursos informáticos de carácter dinámica, en concordancia con los requerimientos variables y fluctuantes del usuario. Esta capacidad permite una adaptación rápida y eficaz de los recursos disponibles, otorgando mayor

versatilidad para satisfacer las peticiones variables de las aplicaciones y los usuarios [32].

- Auto Servicio a Demanda: Este aspecto admite a los usuarios la accesibilidad a los recursos informáticos en concordancia con su necesidad, sin requerir intermediación humana directa proveniente de los proveedores de servicios CC. Así, se facilita la provisión automática y veloz de recursos, simplificando su gestión para los usuarios [32].
- Accesibilidad Universal: El Cloud Computing brinda acceso a los recursos informáticos por intermedio de internet, sin restricciones geográficas y en cualquier momento. Esta característica elimina las barreras de ubicación y posibilita a los diferentes usuarios la accesibilidad a sus aplicaciones e informaciones desde diversos dispositivos y plataformas [32].
- Agrupamiento de Recursos: Los recursos informáticos se consolidan y colaboran considerando que estos puedan ser varios usuarios en dicho entorno CC, maximizando su eficiencia y utilización. Este enfoque forja economías de escala y aminora costes operativos tanto para usuarios, como para proveedores de servicios CC [32].
- Medición y Control de Servicio: El Cloud Computing permite medir y gestionar con precisión el uso de los recursos informáticos. Esto posibilita a usuarios y proveedores monitorear y optimizar el rendimiento, así como facturar y contabilizar el uso de los recursos de manera precisa [32].
- Resiliencia y Disponibilidad: Los servicios CC se encuentran desarrollados para ser altamente disponibles y resilientes, incorporando redundancia y capacidades de recuperación ante desastres. Esta disposición garantiza la continuidad del servicio y minimiza el riesgo de interrupciones no planificadas [32].

Estas características fundamentales del Cloud Computing definen su capacidad para ofrecer servicios de TI eficientes, flexibles y escalables, lo que conlleva a convertirlo alternativa atractiva para organizaciones de cualquier que sean sus tamaños y sectores.

1.5.1.3. Modelos de servicios del Cloud Computing

Según Kim [33] el concepto del Cloud Computing proporciona una variedad de modelos de servicios diseñados para satisfacer las distintas necesidades y exigencias de los usuarios. Estos modelos, identificados previamente como SaaS, IaaS y PaaS, presentan diversos grados de abstracción y responsabilidad en cuanto a la administración de la infraestructura y las aplicaciones.

Los servicios en la nube, también conocidos como servicios de CC, se refieren a recursos informáticos y servicios que se ofrecen por intermediación del internet, permitiendo a usuarios la accesibilidad a ellos de forma remota y bajo demanda, existiendo muchas herramientas CC en el mundo actualmente. Dichos servicios anteriormente mencionados, son suministrados por proveedores de servicios CC, que gestionan y mantienen infraestructuras subyacentes necesaria para ofrecerlos. A continuación, se detallan en profundidad estos modelos:

A. Software as a Service (SaaS):

"Este modelo proporciona aplicaciones de software alojadas en la nube y accesibles a través de internet. Los usuarios pueden utilizar estas aplicaciones sin necesidad de instalarlas en sus dispositivos locales, ya que son ejecutadas y mantenidas por el proveedor de servicios en la nube. El SaaS ofrece una amplia gama de aplicaciones, desde herramientas de productividad como suites de oficina y aplicaciones de correo electrónico, hasta aplicaciones empresariales complejas como sistemas de gestión de relaciones con los clientes (CRM) y sistemas de gestión de recursos empresariales (ERP). Los usuarios acceden a estas aplicaciones a través de un navegador web o una interfaz de usuario específica,

pagando por su uso en función de un modelo de suscripción o tarifa de uso” [33].

B. Infrastructure as a Service (IaaS):

“En este modelo, los proveedores de servicios en la nube ofrecen recursos informáticos fundamentales, como capacidad de procesamiento, almacenamiento y redes, como servicios virtualizados a través de internet. Los usuarios pueden aprovisionar y gestionar estos recursos de manera flexible y bajo demanda, sin necesidad de adquirir ni mantener su propia infraestructura física. El IaaS proporciona una base sólida para construir y desplegar aplicaciones, permitiendo a los usuarios tener un mayor control y flexibilidad sobre el entorno de computación. Los servicios comunes incluidos en el IaaS son máquinas virtuales, almacenamiento en la nube, redes virtuales y balanceadores de carga, entre otros” [33].

C. Platform as a Service (PaaS):

“Este modelo ofrece un entorno completo de desarrollo y ejecución para la creación, prueba, implementación y gestión de aplicaciones en la nube. Los proveedores de servicios en la nube proporcionan una plataforma de software y hardware que incluye herramientas y servicios necesarios para el desarrollo de aplicaciones, como sistemas operativos, entornos de desarrollo integrados (IDE), bases de datos, servicios de mensajería y herramientas de monitoreo. Los usuarios pueden desarrollar y desplegar aplicaciones en la plataforma sin preocuparse por la gestión de la infraestructura subyacente, lo que les permite centrarse en la creación de aplicaciones de manera rápida y eficiente. El PaaS es especialmente adecuado para el desarrollo de aplicaciones web, móviles y de análisis de datos” [33].

Estos modelos de servicios CC un abanico de diversos niveles de abstracción y responsabilidad, admitiendo a los usuarios optar por aquella opción con mejores prestaciones

para ser adaptada a las necesidades, objetivos y metas propias. Desde aplicaciones listas para usar hasta infraestructura y plataformas personalizables, el Cloud Computing ofrece una diversidad de posibilidades para satisfacer las demandas de los usuarios en diferentes contextos y escenarios.

Respecto a esto, existe un modelo de Responsabilidad Compartida en la Nube el mismo que es “un enfoque de gestión de seguridad que distribuye los roles y responsabilidades entre el proveedor de servicios en la nube y el cliente. Este modelo reconoce que tanto el proveedor como el cliente tienen funciones específicas en la protección de los datos y la seguridad de la información en el contexto de la nube. Mientras que el proveedor de servicios en la nube asume la responsabilidad de salvaguardar la infraestructura subyacente y los servicios ofrecidos, el cliente es encargado de proteger los datos y las aplicaciones utilizadas en la nube. Esta perspectiva promueve la cooperación entre ambas partes con el fin de garantizar un nivel adecuado de seguridad en el entorno de la nube, lo que permite mitigar los riesgos y asegurar la integridad, confidencialidad y disponibilidad de los datos” [34].

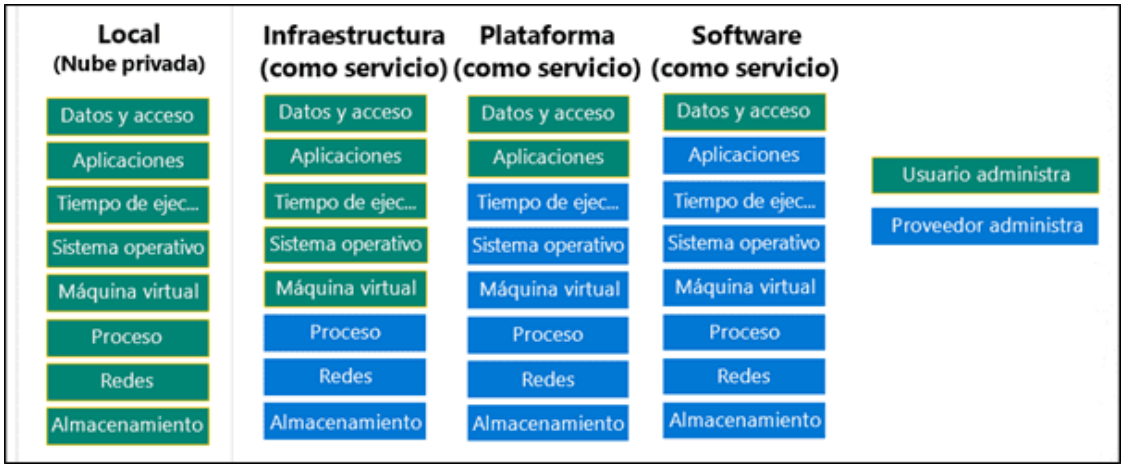


Fig. 7. Niveles de responsabilidad entre proveedor y cliente de servicios en la nube [34]

1.5.1.4. Ventajas y desventajas del Cloud Computing

Según Condori [35] estas son algunas de las más relevantes ventajas y desventajas de la usanza de Cloud Computing, cada una con su debida implicancia en la eficiencia operativa, la seguridad de los datos y la flexibilidad de las organizaciones:

TABLA I.

Ventajas y desventajas del Cloud Computing

Ventajas	Desventajas
Flexibilidad y Escalabilidad: “Permite escalar los recursos informáticos según la demanda del usuario de manera rápida y eficiente” [35].	Dependencia de la Conectividad: “Requiere una conexión a internet estable para acceder a los servicios en la nube” [35].
Reducción de Costes: “Elimina la necesidad de invertir en infraestructura física y permite a las organizaciones pagar solo por los recursos que utilizan” [35].	Seguridad y Privacidad: “Preocupaciones sobre la seguridad y privacidad de los datos almacenados en la nube, especialmente en entornos públicos” [35].
Agilidad y Velocidad: “Facilita el desarrollo, la implementación y la entrega rápida de aplicaciones y servicios” [35].	Riesgo de Bloqueo de Proveedor: “Posibilidad de quedar bloqueado en un proveedor de servicios en la nube debido a la dificultad de migrar datos y aplicaciones entre plataformas” [35].
Acceso Universal: “Permite acceder a los recursos informáticos desde cualquier ubicación y en cualquier momento, facilitando el trabajo remoto y la colaboración” [35].	Disponibilidad y Tiempo de Inactividad: “Riesgo de tiempo de inactividad y falta de disponibilidad de servicios en entornos CC debido a problemas técnicos o fallas del proveedor” [35].
Actualizaciones Automáticas: “Las actualizaciones de software y parches de seguridad se aplican automáticamente por el proveedor de servicios en la nube” [35].	Limitaciones de Personalización: “Algunas soluciones en la nube pueden tener limitaciones en cuanto a la personalización y adaptación a las necesidades específicas de la organización” [35].

Nota. Fuente, adaptado de [35].

1.5.1.4. Cloud Computing en el sector salud

El uso de Cloud Computing en el sector de la salud a nivel mundial ha venido logrando

experimentar un notable progreso, presentando una cadena de beneficios y retos significativos. En términos generales, la adopción de esta tecnología ha permitido a las instituciones sanitarias mejorar la eficiencia operativa, optimizar el intercambio de información entre profesionales médicos y pacientes, así como facilitar el acceso a registros médicos electrónicos desde cualquier ubicación. Además, el almacenamiento y procesamientos de volúmenes grandes de datos clínicos en entornos CC ha posibilitado ampliamente el desarrollo de herramientas de análisis avanzado, como el aprendizaje de máquina automático y la inteligencia artificiaI, que han contribuido a mejoramiento de la precisión del diagnóstico y el tratamiento de enfermedades. Sin embargo, a pesar de estas ventajas, la usanza de CC en el sector salud también plantea inquietudes correlacionadas con la privacidad y la seguridad de informaciones médicos, así como cuestiones regulatorias y de cumplimiento normativo, que deben abordarse de manera adecuada para certificar, de ese modo, la confianza y la integridad de Ia información del paciente.

Por una parte, Rai et al. [36] exploró las oportunidades y desafíos asociados con el uso de CC en ámbitos de la salud. Se destaca que esta tecnología ofrece oportunidades significativas para mejorar la eficiencia operativa, facilitando el tráfico de informaciones médica y promover la innovación en eI diagnóstico y tratamiento de enfermedades. Empero, también se identifican desafíos importantes, como preocupaciones sobre la privacidad y SI personales de los pacientes, así como cuestiones relacionadas con la interoperabilidad de sistemas y el cumplimiento normativo. El estudio subraya la importancia de abordar estos desafíos de manera efectiva para aprovechar plenamente el potencial de CC en el ámbito de la salud, garantizando al mismo tiempo la protección y confidencialidad de la información médica.

Por otra parte, Bamiah et al. [37] examinaron la importancia de adoptar el paradigma del CC en el sector sanitario. Se resalta que la implementación de CC en este ámbito ofrece numerosos beneficios, incluida la optimación de la eficiencia operativa, la accesibilidad a las

informaciones médica desde cualquier ubicación y el aminoramiento de costes ligados con la gestión de infraestructura física. Además, se destaca el potencial de Cloud Computing para facilitar la colaboración entre profesionales médicos, así como para promover la innovación en la constructiva de aplicaciones y servicios de salud. Sin embargo, el estudio también reconoce la necesidad de abordar desafíos importantes, como preocupaciones sobre la privacidad y la SI, asimismo como barreras relacionadas con la interoperabilidad de sistemas y el cumplimiento normativo. En general, se concluye que la adoptabilidad de CC en el sector sanitario es fundamental para avanzar hacia una atención médica mucho más eficiente, accesible y centralizada en el activo más relevante, el paciente.

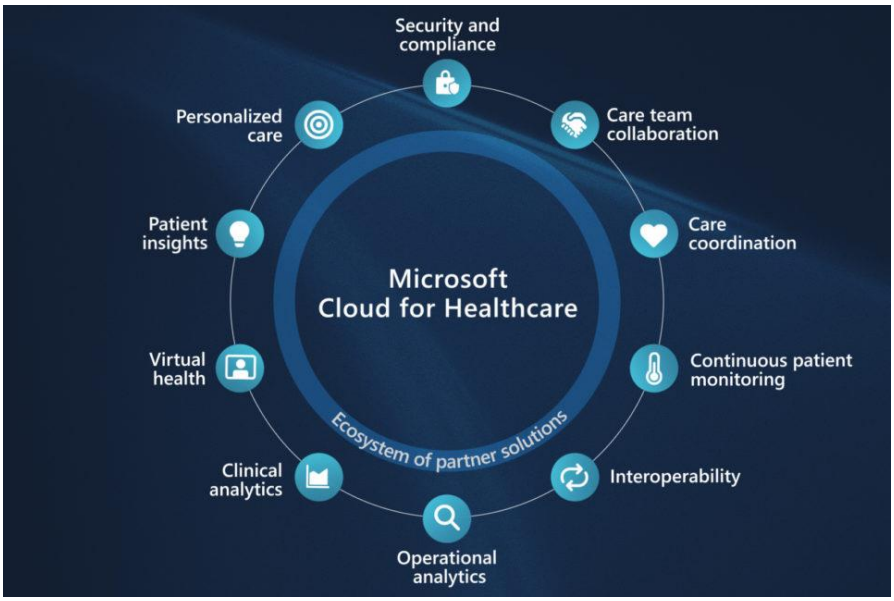


Fig. 8. Cloud Computing en el sector salud [38].

En resumen, el Cloud Computing ha transformado la prestación de servicios de salud a nivel mundial, ofreciendo oportunidades significativas para mejorar la atención médica, aunque también plantea desafíos que deben ser gestionados de manera eficaz para maximizar sus beneficios.

1.5.2. Seguridad de la Información

1.5.2.1. Definición de Seguridad de la Información

Gillies [39] reveló que, “la SI comprende un conjunto de prácticas, políticas y procedimientos destinados a resguardar la confidencialidad, integridad y disponibilidad de los datos. Esto implica la implementación de medidas técnicas, como firewalls y cifrado, junto con la adopción de políticas de seguridad y la capacitación del personal para mitigar el riesgo de acceso no autorizado, alteración o pérdida de la información sensible. El propósito es asegurar que los datos solo sean accesibles por personal autorizado, manteniendo su integridad y estando disponibles cuando se requiera, protegiéndolos contra amenazas tanto internas como externas”.

Tøndel et al. [40] reveló que, la SI es un conjunto de prácticas, normativas y tecnologías orientadas a salvaguardar la integridad, confidencialidad y disponibilidad de las informaciones y sistemas informáticos de una organización. Esto implica la implantación de controles para la accesibilidad, políticas de gestión de riesgos, encriptación de informaciones y medidas de prevención y detección de amenazas, con el fin de minimizar riesgos ligados con accesos no permitidos, la pérdida de datos e incidentes de SI. La meta es certificar la protección de informaciones sensibles y crítica de la organización, asegurando su confidencialidad, integridad y disponibilidad en cualquier situación acaecida.

1.5.2.2. Ciclo de Deming y Seguridad de la Información

El ciclo Deming, “también conocido como PDCA (Planificar, Hacer, Verificar, Actuar), es un enfoque de mejora continua que se puede aplicar eficazmente a la seguridad de la información” [41]. Comienza con la etapa de Planificar, donde se instituyen los objetivos de seguridad y se mapean riesgos potenciales. Luego, en la etapa de Hacer, se efectúan pautas de seguridad según el plan establecido. La etapa de Verificar contempla monitorear y evaluar

el desempeño de las medidas de SI implantadas, asimismo también identificar posibles áreas de mejora. Finalmente, en la etapa de Actuar, se toman acciones correctoras de modo que se aborden cualquier riesgo o problema identificado durante la fase de Verificar, y se ajustan los planes y procesos de seguridad según sea necesario. Este ciclo se repite continuamente para garantizar una mejora constante en la SI de la organización [42].

"El ciclo PDCA es un marco de trabajo del SGSI basado en el concepto de que la gestión de la SI es un proceso continuo para salvaguardar la integridad y la disponibilidad de los activos de información de las compañías" [43].

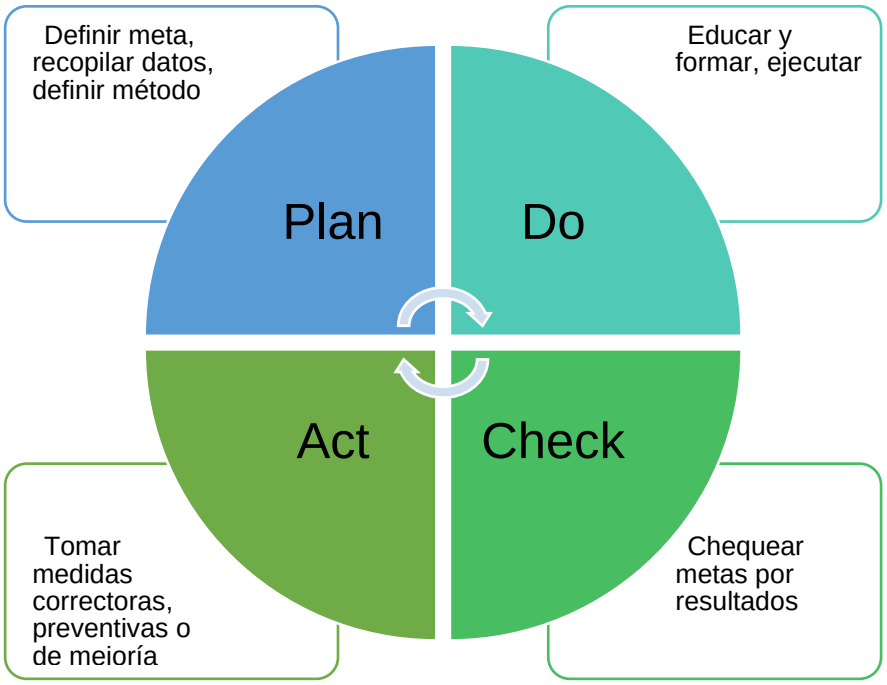


Fig. 9. Ciclo PDCA [4].

Tal y como ha podido visualizarse en la imagen anterior, el ciclo PDCA consta de cuatro (04) fases.

a. La fase de planificación (PLAN) implica la elaboración de estrategias de políticas y controles de seguridad necesarios; este paso es crucial, ya que traza la visión inicial de los niveles de SI deseados en la organización [15].

b. La fase de ejecución (DO) abarca todas las implementaciones técnicas necesarias para lograr un sistema de SI funcional que se planificó en el paso anterior [15].

c. La fase de comprobación (CHECK) comprende las evaluaciones técnicas necesarias para garantizar la funcionalidad a largo plazo del sistema de SI, así como los procedimientos de auditoría de SI que deben seguirse para garantizar continuamente el nivel de SI del sistema en la empresa [15].

d. La fase de actuación (ACT) implica preservar la calidad del nivel de garantía de la seguridad fundamentándose en las informaciones recibidas de la fase de comprobación, pudiendo promoverse nuevas actualizaciones o implementaciones en función de las nuevas incorporaciones al sistema o de las amenazas descubiertas y de los resultados de la valuación de riesgos [15].

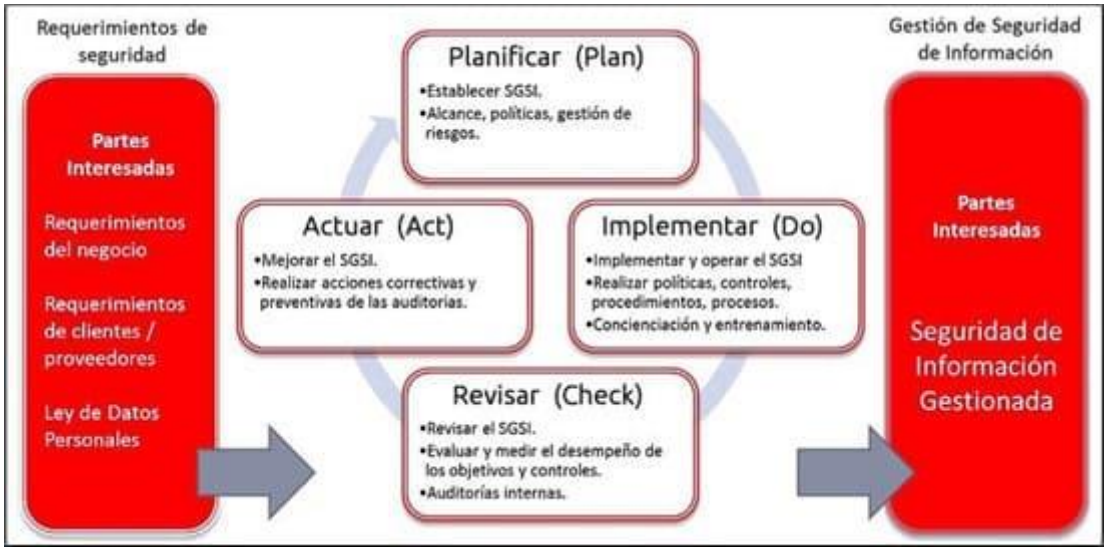


Fig. 10. Ciclo PDCA aplicado a los procesos del SGSI [43].

La tabla siguiente resume las operaciones básicas de cada fase:

TABLA II.

Resumen del Ciclo PDCA.

Fase	Descripción
PLAN (establecer el SGSI)	"Establecer la política, los objetivos, los procesos y los procedimientos del SGSI relevantes para la administración de los riesgos y la mejora de la SI para la obtención de resultados en concordancia con los objetivos y las políticas integrales de las compañías" [43]
DO (aplicar y hacer funcionar el SGSI)	"Aplicar y hacer funcionar la política, los controles, los procesos y los procedimientos del SGSI" [43]
CHECK (supervisar y revisar el SGSI)	"Valuar y, en su caso, llevar a cabo la medición del desempeño de los procesos con respecto a la política, los objetivos y la experiencia en la praxis del SGSI e informar a dirección de los resultados obtenidos para su posterior evaluación" [43].
ACT (mantener y mejorar el SGSI)	"Aquí se consideran medidas preventivas y correctivas, basadas en los resultados de las auditorías internas del SGSI y la revisión de la gestión u otra pertinente información, para la consecución de la mejora continua del SGSI" [43].

Nota. Adaptado de Arafat [43].

En resumen, el ciclo de Deming suministra un enfoque estructurado y sistémico para gestionar la SI, admitiendo a las organizaciones el reconocimiento pleno de áreas de mejoramiento continua y adaptar sus estrategias de SI de modo de réplica a cambios en un contexto de amenazas y tecnológico, considerando las cuatro (04) etapas mencionadas previamente (Planificar, Hacer, Verificar y Actuar).

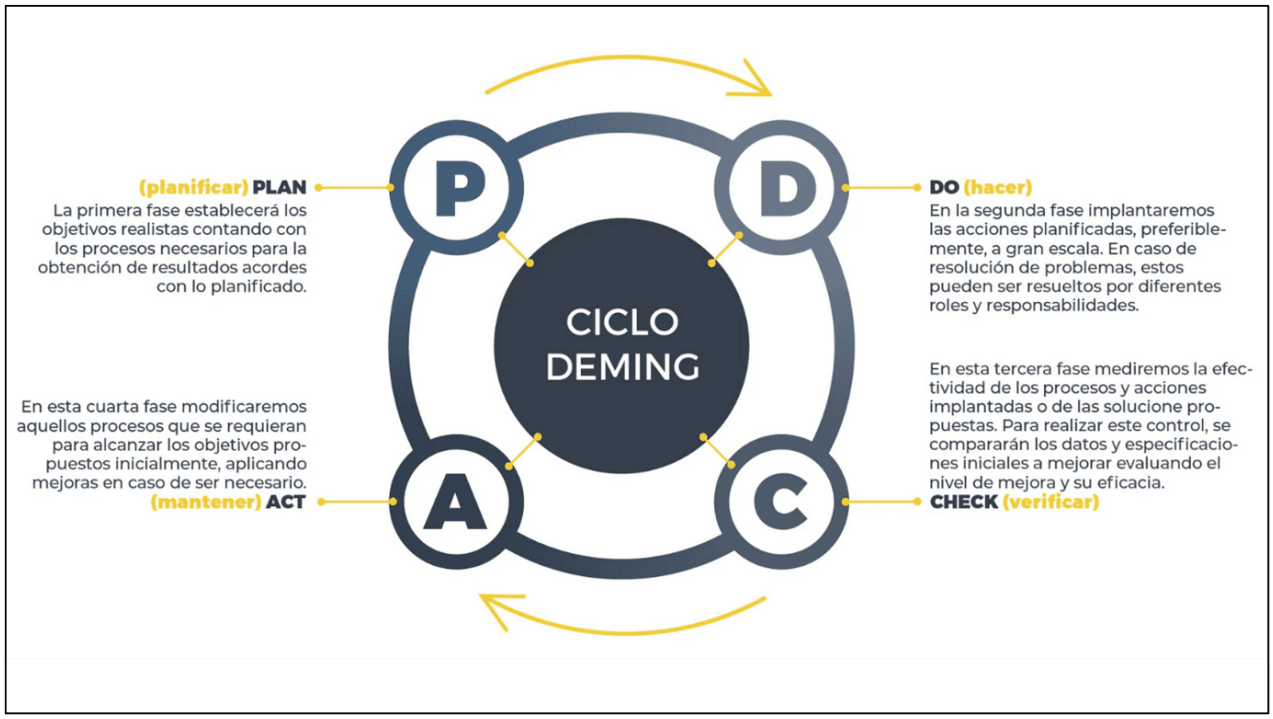


Fig. 11. Ciclo de Deming [44].

1.5.2.3. Sistema de Gestión de Seguridad de la Información

Según Citterio [45] un SGSI es “un conjunto de políticas, procedimientos, procesos y herramientas diseñados para proteger la confidencialidad, integridad y disponibilidad de la información dentro de una organización. El principal objetivo de un SGSI es identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información, mediante la implementación de medidas de seguridad adecuadas y el monitoreo continuo de las actividades pertinentes. Este sistema está diseñado para garantizar que la información sensible se maneje de manera segura y para adoptar las medidas necesarias para prevenir y mitigar las amenazas a la seguridad”.

La importancia radica en varias razones:

- Resguarda la información delicada: “Un SGSI protege los datos confidenciales y vitales de una organización, asegurando su integridad, privacidad y

disponibilidad. Esto es esencial para mantener la confianza de los clientes, colaboradores y otras partes involucradas" [45].

- Asegura el cumplimiento normativo: "Muchos sectores están sujetos a regulaciones que exigen medidas de seguridad de la información. Un SGSI facilita el cumplimiento de estos requerimientos legales y normativos, evitando posibles sanciones o multas por incumplimiento" [45].
- Manejo de riesgos: "Un SGSI ayuda a identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información de manera sistemática. Esto contribuye a mitigar amenazas y vulnerabilidades, reduciendo la probabilidad de incidentes de seguridad y sus impactos asociados" [45].
- Optimización de operaciones: "Al establecer procesos y controles claros para la gestión de la seguridad de la información, un SGSI puede mejorar la eficiencia operativa al minimizar interrupciones y tiempos de inactividad provocados por incidentes de seguridad" [45].
- Preserva la reputación: "Un SGSI sólido ayuda a mantener la buena imagen de una organización al prevenir la divulgación no autorizada de información sensible, los fallos de seguridad y otros incidentes que podrían afectar negativamente su reputación" [45].

1.5.2.4. Sistema de Gestión de Seguridad de la información de Servicios en la Nube

Según [46] "un SGSI adaptado a los servicios en la nube constituye un marco de trabajo meticulosamente estructurado para abordar los retos de seguridad inherentes al uso de estos servicios. Este enfoque se centra en salvaguardar la confidencialidad, integridad y disponibilidad de los datos alojados, procesados o transmitidos a través de la nube". Aspectos críticos de este SGSI abarcan:

- La evaluación de riesgos específicamente vinculados a la nube: Dicha valuación contempla la identificabilidad y el análisis de riesgos particulares derivados del empleo de servicios en entornos CC, verbigracia, la SI de informaciones durante su transmisión, su resguardo en reposo y la gerencia de los accesos y las identidades [28].
- La selección cuidadosa de proveedores de servicios CC: Implica un meticuloso análisis de los proveedores para asegurar su cumplimiento con los estándares de SI requeridos y garantizar la prestación de adecuadas pautas de salvaguarda de informaciones [28].
- La instauración de controles de seguridad pertinentes: Esto conlleva el diseño e implementación de controles específicos destinados a mitigar los riesgos identificados y resguardar las informaciones en entornos CC. Dichas medidas pueden incluir la encriptación de informaciones, la autentificación mediante análisis multi factorial y la administración de la totalidad de accesos [28].
- El seguimiento constante y la mejora continua: Se establecen procedimientos para monitorear y evaluar de manera constante Ia eficacia de Ios lineamientos de SI instaurados, así como para identificar y remediar nuevas amenazas y vulnerabilidades a medida que surjan [28].

En síntesis, un SGSI dirigido a los servicios CC resulta esencial para aseguramiento de la protección de las informaciones en contextos de nube, salvaguardando los datos contra Ias amenazas y los riesgos particulares asociados al uso de estos servicios.

1.5.2.5. Familia de normas lSO/lEC 27000 en la nube

Según Disterer [13], Ia familia de normas IS0/lEC 27000 se constituye de una (01)

norma de vocabulario, tres (03) normas de requisitos, once (11) normas de directrices, seis (06) normas de directrices específicas del sector y tres (03) normas de directrices específicas de control. A continuación, se muestra las normas de cada categoría relacionadas con la nube:

TABLA III.

ISO/IEC 27000 en la nube

Tipo	Denominación
Norma de vocabulario	"ISO/IEC 27000 - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario" [47].
Norma de requisitos	"ISO/IEC 27001 - Sistemas de gestión de la seguridad de la información - Definición de los requisitos del SGSI" [47].
Norma de orientación	"ISO/IEC 27002 - Código de prácticas para los controles de seguridad de la información" [47].
Normas de orientación sectoriales	"ISO/IEC 27017 - Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para los servicios en nube" [47]. ISO/IEC 27018 - Tecnología de la Información. Técnicas de seguridad. Código de práctica para la protección de identificación personal (PII) en nubes públicas que actúan como procesadores PII" [47].

Nota. Tomado de Arafat [43].

La IS0/IEC 27000 suministra una visión holística del SGSI, incluyendo terminologías y conceptualizaciones usualmente utilizados en el SGSI. Para asegurar la consistencia en la

terminología aceptada, toda la familia de normas IS0/IEC 27000 se basa en las terminologías y conceptualizaciones proporcionados en IS0/IEC 27000. Dicha norma suministra una base inicial integral por la que las organizaciones pueden empezar a introducir la familia IS0/IEC 27000 [43].

La norma IS0/IEC 27017 suministra pautas que apoyan la implantación de lineamientos de SI para los consumidores y proveedores de servicios CC. La selección de Ios controles apropiados y su implementación se basan en la evaluación de riesgos y otros requisitos para la usanza de los servicios CC. Cuando la norma IS0/lEC 27017, que se enfoca principalmente en la SI de los datos, se acompaña de la norma IS0/IEC 27018, que cubre la privacidad de los datos, se consiguen unos ángulos de SI de mayor amplitud de entornos CC [18].

La norma IS0/lEC 27017 proporciona una regulación mucho más aplicable al uso de los servicios en la nube [19]. Se proporcionan orientaciones específicas para treinta y siete (37) de los controles existentes de Ia norma IS0/lEC 27002; se establecen directrices separadas pero complementarias para las diversas clientelas de los servicios CC y el CSP. Se hace hincapié en la responsabilidad compartida de la SI de los servicios CC; haciendo que el cliente CC siga las políticas de usanza de los servicios CC y que el CSP proporcione informaciones al cliente.

La norma ISO/lEC 27017 incluye siete (07) controles adicionales que cuentan con gran relevancia para los servicios CC. Estos nuevos controles están numerados para que encajen con los correspondientes controles existentes de la norma IS0/lEC 27002; estos controles ampliados abarcan:

- Funciones y responsabilidades compartidas en entornos CC.
- Retirada y reintegro de los activos de los clientes de servicios CC.
- Segregación en entornos de computación virtual.

- Refuerzo de máquinas virtuales.
- Seguridad operativa del administrador.
- Monitorización de los servicios CC.
- Alineamiento de la gestión de la SI de las redes físico/virtuales.

La norma IS0/IEC 27018 se ha diseñado para todas las formas y tamaños de organizaciones de las organizaciones privadas y públicas que entregan servicios de procesamientos de informaciones a través de la nube como procesadores de PII [20]. Los controles de protección de la IIP de la norma IS0/IEC 27018 se establecieron teniendo en cuenta los requisitos ya contenidos en los controles de Ia norma IS0/lEC 27002. Aumenta Ia norma IS0/IEC 27002 complementando la guía de ejecución de los controles prescritos por la norma IS0/lEC 27002; y proporcionando controles adicionales ampliados y directrices asociadas que se adaptan para abordar los requisitos de protección de la IPI en la nube pública que no están cubiertos por Ios controles de Ia norma IS0/lEC 27002.

La IS0/IEC 27018 complementa la implantación de los siguientes once (11) controles de la IS0/IEC 27002:

- Políticas de SI.
- Organización de la SI.
- SI de los recursos humanos.
- Control de accesos.
- Criptografía.
- Seguridad ambiental y física.
- Seguridad de las operaciones.
- Seguridad de las comunicaciones.
- Gestión de incidencias de SI.
- Aspectos de la SI en la empresa.

- Gestión de la continuidad.
- Cumplimiento.

Por su parte, el anexo A de la norma IS0/IEC 27018 enumera once (11) controles ampliados para dar cumplimiento de los requisitos de protección de la IPS que se aplican a los CSP públicos que actúan como procesadores de IPS. Los controles ampliados que la norma IS0/lEC 27018 complementa a los controles de la norma IS0/IEC 27002 son:

- Consentimiento y elegibilidad.
- Legitimidad y especificación del propósito.
- Limitancia de la recogida.
- Minimización de los datos.
- Limitancia de la usanza, la conservación y la divulgación.
- Exactitud, precisión y calidad.
- Apertura, transparencia y notificación.
- Participación y acceso individuaI.
- Rendición de cuentas.
- Seguridad de la información.
- Cumplimiento de la privacidad

La familia de normas IS0/lEC 27000 tiene mucha flexibilidad y se desarrolla constantemente para mantenerse al día con las nuevas tendencias y tecnologías empresariales. El hecho de ser una norma internacional también ayuda a la conformidad de los CSP con políticas internacionales como el GDPR de la UE. Además, aumenta la confianza de los CSP desde la perspectiva de las organizaciones que pretenden migrar partes de su negocio a la nube. En general, esta estandarización es crucial para los CSP [18].

II. MATERIALES Y MÉTODO

2.1. Tipo y Diseño de investigación

2.1.1. Tipo de investigación

La presente investigación fue tecnológica aplicada pues, se construyó un SGSI considerando el contexto de servicios en la nube que existía en la institución pública, poniendo en práctica los conocimientos en SI que se obtuvieron a lo largo de la carrera y basándose asimismo en la normatividad propuesta por la ISO/IEC 27017, para posteriormente implementarla en una institución pública peruana, con lo que se logró mejorar la SI en dicha organización caso de estudio, considerando los indicadores previamente propuestos en la matriz de operacionalización de variables [48].

2.1.2. Diseño de investigación

Por su naturaleza, el estudio correspondió al diseño cuasi experimental, pues en el caso de los niveles de los indicadores de la variable independiente “SGSI de servicios en la nube”, sí se midieron dichos niveles, pero sin ser alterados, sino que fueron expuestos tal y según la apreciación de los expertos. Por el contrario, los niveles de Ia variable dependiente “SI en una institución pública peruana” fueron medidos, pero en el contexto posterior a la ejecución de la prueba piloto de dicho SGSI en la organización caso de estudio, por lo que dichos valores no fueron los inicialmente encontrados en dicha organización pública [48].

2.2. Variables, Operacionalización

2.2.1. Variables

Variable Independiente:

Sistema de gestión de seguridad de la información de servicios en la nube basado en la norma ISO/IEC 27017

Variable Dependiente:

Seguridad de la información en una institución pública peruana

2.2.2. Operacionalización

Se tuvieron las siguientes operacionalización de variables:

TABLA IV.

Operacionalización de la Variable Independiente

Variables	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos
VARIABLE INDEPENDIENTE: SGSI de servicios en la nube basado en la norma ISO/IEC 27017	Aceptación del SGSI	Nivel de Claridad	$N_{I01} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	T: Juicio de Expertos I: Ficha de Juicio de Expertos (Anexo 5)
		Nivel de Objetividad	$N_{I02} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	
		Nivel de Actualidad	$N_{I03} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	
		Nivel de Organización	$N_{I04} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	
		Nivel de Suficiencia	$N_{I05} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	
		Nivel de Intencionalidad	$N_{I06} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	
		Nivel de Consistencia	$N_{I07} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	
		Nivel de Coherencia	$N_{I08} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	
		Nivel de Metodología	$N_{I09} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	
		Nivel de Pertinencia	$N_{I10} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$	

TABLA V.

Operacionalización de la Variable Dependiente

Variables	Dimensión	Indicador	Ítem	Instrumentos de recolección de datos
VARIABLE DEPENDIENTE: Seguridad de la información en una institución pública peruana	Cumplimiento de Políticas de SI	C5. Políticas de seguridad de la información	$N_{C5} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	T: Observación I: Ficha de Análisis de Brechas (Anexo 6)
		C6. Organización de la seguridad de la información	$N_{C6} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C7. Seguridad de los recursos humanos	$N_{C7} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C8. Gestión de activos	$N_{C8} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C9. Control de acceso	$N_{C9} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C10. Criptografía	$N_{C10} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C11. Seguridad física y medioambiental	$N_{C11} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C12. Seguridad de las operaciones	$N_{C12} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C13. Seguridad de las comunicaciones	$N_{C13} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C14. Adquisición, desarrollo y mantenimiento de sistemas	$N_{14} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C15. Relaciones con los proveedores	$N_{15} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad	$N_{16} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad	$N_{C17} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	
		C18. Cumplimiento	$N_{C18} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$	

2.3. Población de estudio, muestra, muestreo y criterios de selección

Por una parte, en esta investigación, la población y muestra examinada fueron un caso de estudio, el Ministerio de Salud con sede en la Av. Salaverry N° 801, Jesús María, Lima, Lima, ya que, es una institución pública de salud peruana, que era justificadamente el contexto necesario que se pretendía, era una institución a la cual se tenía accesibilidad y consentimiento para el despliegue del estudio. Respecto a esto, y en cuanto al personal de la institución pública caso de estudio, se tuvo el apoyo de once (11) colaboradores quienes apoyaron en el levantamiento de informaciones, de manera directa o indirectamente mediante los permisos respectivos. Todos ellos son colaboradores que se encuentran involucrados relacionados a SI.

TABLA VI.

Población de estudio

N°	Estructura funcional de OGTI	Cantidad
1	Director General de OGTI	01
2	Director Ejecutivo de la Oficina de Gestión de la Información	01
3	Director Ejecutivo de la Oficina de Soporte e Infraestructura Tecnológica.	01
4	Director Ejecutivo de la Oficina de Innovación y Desarrollo Tecnológico.	01
5	Jefes de Equipo de la Oficina de Gestión de la Información	02
6	Jefes de Equipo de la Oficina de Soporte e Infraestructura Tecnológica	03
7	Jefes de Equipo de la Oficina de Innovación y Desarrollo Tecnológico	02

Por otra parte, existiendo varias normas con las que se pueden gestionar la SI, se tuvo en consideración aquella norma identificada por Disterer [49], la cual cumplió los criterios siguientes:

- Pertenecen a la familia ISO 27K
- Gestionan la SI
- Cuentan con el status de publicada por la ISO
- Enfocados en la computación en la nube
- Aborda acerca de controles de SI para los servicios en entornos CC.

TABLA VII.

Muestra de estudio

N°	Norma ISO	Denominación	Descripción	Última versión
1	lSO/lEC 27017	"Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para los servicios en la nube" [47]	"Aborda acerca de los controles de SI para los servicios en entornos CC. Se ocupa de proporcionar seguridad a los servicios de la nube, implementando controles a cada uno de los mencionados servicios" [47].	Publicada en 2015-12

Nota. Adaptado de [49].

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Concerniente a la **Variable Independiente**, se empleó el juicio de expertos ya que, cinco (05) expertos validaron el SGSI considerando los diez (10) indicadores mencionados en la TABLA IV. Fue preciso que los cinco (05) expertos en mención sean poseedores de

estas características:

- Poseer Grado Académico en Ingeniería en Ciberseguridad, Ingeniería de Sistemas o ingeniería de Software o Ingeniería Informática (excluyente).
- Poseer Postgrado acorde con Gestión de SI, Ciberseguridad, Gestión de la Información (excluyente).
- Poseer experiencia proba en gestión de SI en el sector público o privado (excluyente).
- Poseer experiencia académica y profesional >10 años en Iabores asociadas a Ia lngeniería de Sistemas (excluyente).
- Contar con publicaciones académicas relacionadas con la temática de la investigación (deseable).

Haciendo una búsqueda rápida de expertos se lograron contactar mediante correo electrónico a los siguientes cinco (05) expertos:

TABLA VIII.

Expertos para validación de Variable Independiente

N°	Apellidos y Nombres	Título Profesional	Grado Académico
1	Arias Moreno Franklin Jhino	Ingeniero de Sistemas	Maestro en Dirección de Sistemas y Tecnologías de Ia Información
2	Sosa Suarez Doris Elizabeth	Ingeniero de Sistemas	Maestro en Dirección de Sistemas y Tecnologías de Ia lnformación

3	Bocanegra Pinchi Yan Carlos	Ingeniero de Sistemas	Maestro (c) en Ingeniería de Sistemas con mención en Dirección Estratégica de Tecnologías de la Información
4	Meres Morales Evelyn Rosalía	Ingeniero de Sistemas	Maestro en Dirección de Sistemas y Tecnologías de la Información
5	Solano Lazo Úrsula Carola	Ingeniero de Sistemas	Maestra en Dirección de Sistemas y Tecnologías de la Información

Nota. Adaptado según información obtenida en [50].

Cabe mencionar, la ficha empleada para recopilar la opinión de dichos expertos se describe en el Anexo 5. Después de recibir las respuestas de los cinco expertos mencionados anteriormente, los resultados se registraron en una hoja de cálculo de MS-Excel para su análisis e interpretación. Estos resultados se presentaron en los hallazgos de la investigación y se pueden encontrar detallados en el Anexo 6.

Concerniente a la Variable Dependiente, se empleó una Ficha de Análisis de Brechas para valuar el nivel de madurez de las Políticas de SI en un nivel Pre Test y Post Test, considerando las catorce (14) cláusulas especificadas en la ISO/IEC 27017 y que se hallan especificadas en la TABLA V. El checklist fue elaborado con total análisis y contó con el visto bueno de colaboradores especificados en la TABLA VI. La evidencia de este instrumento de recolección se encuentra en el Anexo 6.

2.5. Procedimiento de análisis de datos

Por una parte, para evaluar SGSI en servicios CC fundamentado la norma lSO/lEC-27017 para instituciones públicas, se emplearon los indicadores para la **Variable Independiente** mostrados en la TABLA IV. Estos indicadores ayudaron a determinar el nivel de aceptación del SGSI previamente desarrollado, que se detallan a continuación:

Indicador	Técnica e instrumentos de recolección de datos
1.-Nivel de Claridad	T: Juicio de Expertos
2.-Nivel de Objetividad	I: Ficha de Juicio de Expertos
3.-Nivel de Actualidad	Anexo 5
4.-Nivel de Organización	
5.-Nivel de Suficiencia	
6.-Nivel de Intencionalidad	
7.-Nivel de Consistencia	
8.-Nivel de Coherencia	
9.-Nivel de Metodología	
10.-Nivel de Pertinencia	

Nota. Fuente, TABLA IV.

Para ello se empleó la siguiente fórmula estadística, la cual fue replicada indicador por indicador tal y como se evidenció en la TABLA IV:

$$N_{IJE} = \frac{(VE_1 + VE_2 + \cdots + VE_n)}{n}$$

Donde:

N_{IJE}: Nivel de Indicador según Juicio de Expertos

VE: Validación de Experto

n = Número TotaI de Expertos

Por otra parte, para la valoración de la **Variable Dependiente**, más específicamente, la SI en una institución pública peruana caso de estudio, se utilizaron catorce (14) indicadores que respondían específicamente a las cláusulas según la norma ISO/IEC 27017, siendo ellos los siguientes indicadores:

- C5. Políticas de seguridad de la información
- C6. Organización de la seguridad de la información
- C7. Seguridad de los recursos humanos
- C8. Gestión de activos
- C9. Control de acceso
- C10. Criptografía
- C11. Seguridad física y medioambiental
- C12. Seguridad de las operaciones
- C13. Seguridad de las comunicaciones
- C14. Adquisición, desarrollo y mantenimiento de sistemas
- C15. Relaciones con los proveedores
- C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad

- C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad
- C18. Cumplimiento

Para ello se empleó la siguiente fórmula estadística, la cual fue replicada indicador por indicador tal y como se evidenció en la TABLA V:

$$N_{Cn} = \frac{(\bar{x}_{P01} + \bar{x}_{P02} + \cdots + \bar{x}_{Pn})}{n}$$

Donde:

N_{Cn}: Nivel del indicador de cumplimiento de políticas de SI, que para este caso específico está asociado a una cláusula de la ISO/IEC 27017

$\bar{x}$: Promedio total del control según Ficha de Análisis de Brechas

n = Número Total de controles

2.6. Criterios éticos

Para esta investigación, se emplearon los siguientes criterios éticos:

a. Confidencialidad

"Se hizo uso de este criterio ya que, el investigador mantuvo en reserva las informaciones sensibles de la institución pública de salud peruana caso de estudio, de manera que se protejan dichas informaciones considerando las triada de la confidencialidad, integridad y disponibilidad, que es lo que tanto se requiere" [51].

b. Derechos de autor

"Se emplearon citas para referenciar a cada una de las fuentes académicas que

sirvieron de soporte para el conocimiento científico necesario en esta investigación, las mismas que, a posteriori, fueron localizadas en las referencias de este informe, más específicamente, en la sección ‘REFERENCIAS’” [51].

c. Búsqueda del bien

“Se hizo uso de este criterio ya que, se buscó el beneficio de la institución pública de salud peruana caso de estudio, percibiendo un mejoramiento en cuanto a los niveles de confidencialidad, integridad y disponibilidad de la información, logrando así el mejoramiento de la SI” [51].

3. RESULTADOS Y DISCUSIÓN

3.1. Resultados

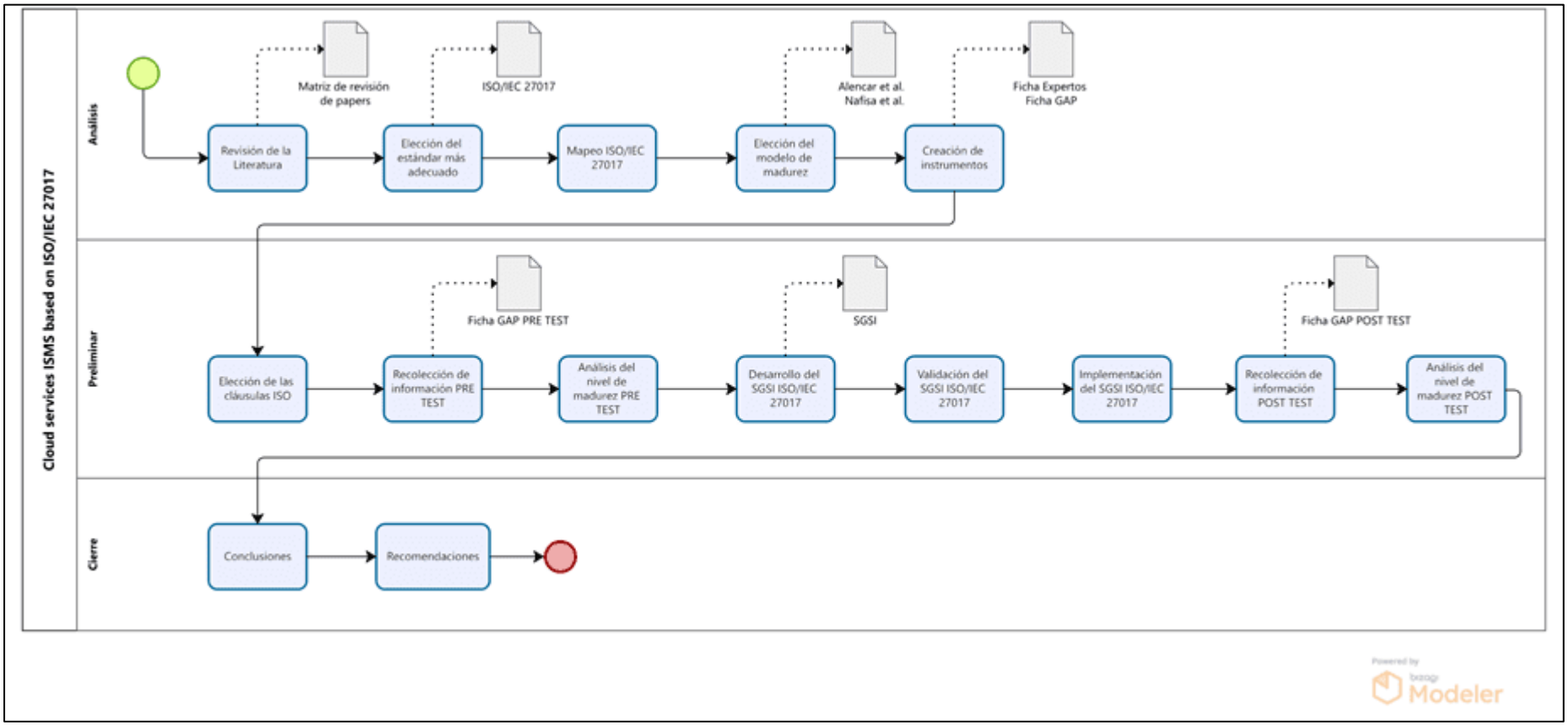


Fig. 12. Método propuesto.

3.1.1. Resultados de la Variable Independiente: SGSI de servicios en la nube basado en la norma ISO/IEC 27017

Para lograr determinar la “Aceptación del SGSI” que se desarrolló considerando la ISO/IEC 27017, se solicitó a los cinco (05) expertos mencionados en la TABLA VIII que dieran su apreciación crítica en base a los indicadores asignados a la Variable Independiente. Los expertos, que cumplieron previamente con ciertos requisitos para serlo, dieron su veredicto individual, los cuales fueron tabulados en hoja de cálculo de MS-Excel y cuyos resultados generales se muestran consolidados en la siguiente tabla:

TABLA IX.

Resultados de la Variable Independiente

Indicador	**Expertos**					**Promedio por indicador**
	Exp01	**Exp02**	**Exp03**	**Exp04**	**Exp05**	
Claridad	95	95	90	95	95	94.00
Objetividad	90	90	95	90	90	91.00
Actualidad	95	95	90	95	95	94.00
Organización	90	90	95	90	90	91.00
Suficiencia	95	95	90	95	95	94.00
Intencionalidad	90	90	95	90	90	91.00
Consistencia	95	95	90	95	95	94.00
Coherencia	90	90	95	90	90	91.00
Metodología	95	95	90	95	95	94.00
Pertinencia	95	95	95	95	95	95.00
Promedio por experto	93.00	93.00	92.50	93.00	93.00	N_{SGSI} = 92.90

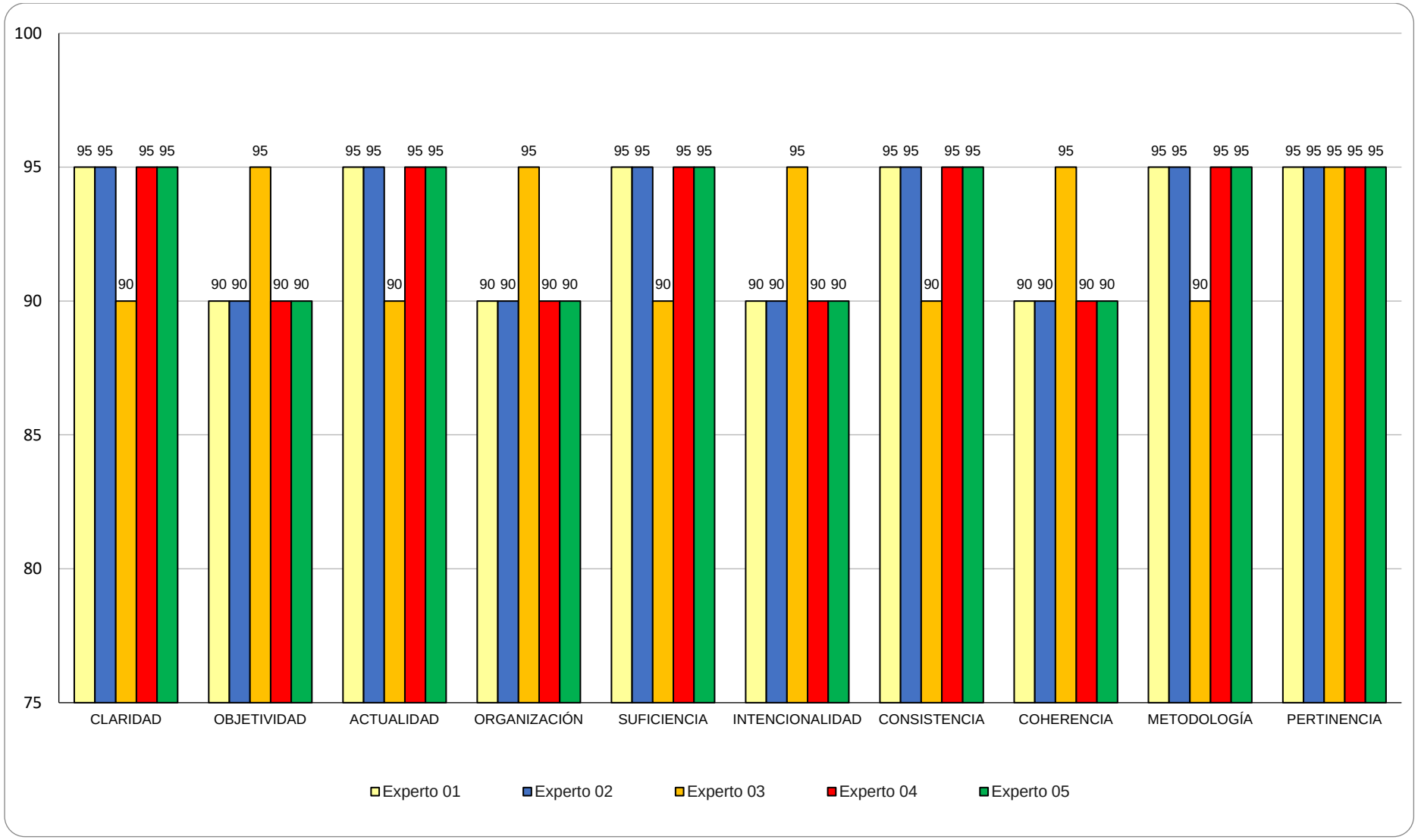


Fig. 13. Resultados de la Variable Independiente.

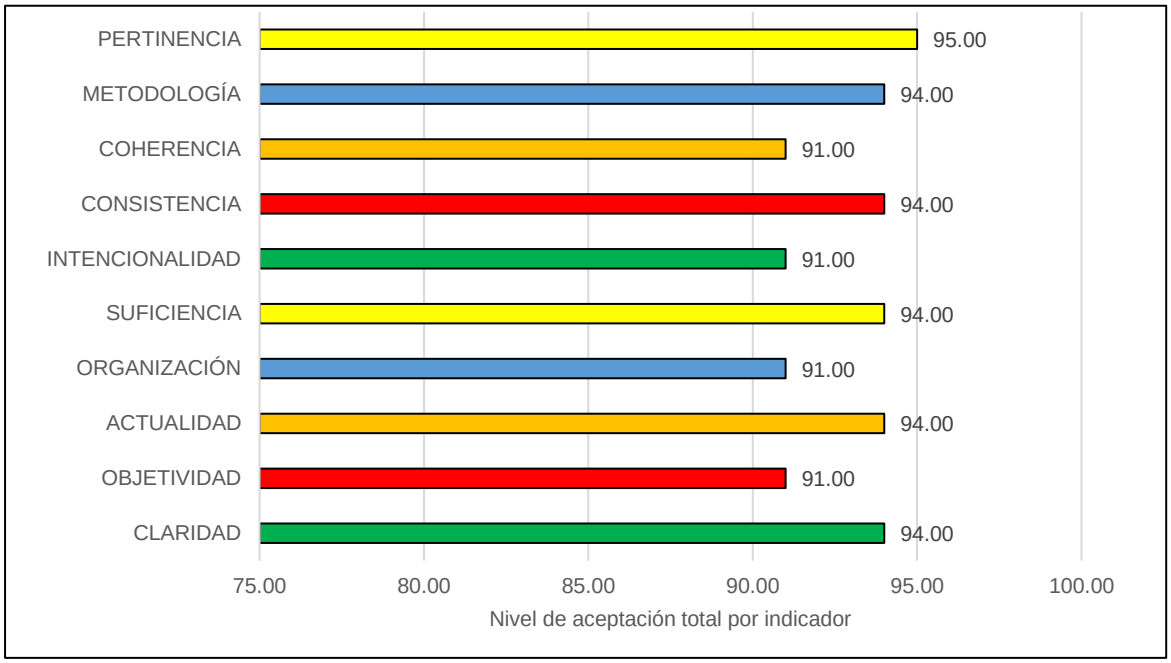


Fig. 14. Resultados generales de los indicadores de la Variable Independiente.

Respecto a la TABLA IX y Fig. 13, se pudo determinar que los diez (10) indicadores de la dimensión “Aceptación del SGSI” tuvieron una valoración promedio total de 92.90 considerando la totalidad de respuestas por parte de los cinco expertos, evidenciándose una valoración mínima de 91.00 (Objetividad, Organización, Intencionalidad y Coherencia) y una máxima de 95.00 (Pertinencia). lo cual en la escala de valoración diseñada y referenciada en la TABLA XXXV, obtuvo un Nivel “Excelente” considerándose como “Aplicable” por parte de los cinco (05) expertos, quienes expresaron que dicha propuesta era óptima para la realización de una prueba piloto en una institución pública caso de estudio.

3.1.2. Resultados de la Variable Dependiente: Seguridad de la información en una institución pública peruana

Si bien es cierto, la ISO/IEC 27017 no establece niveles de madurez de cumplimiento específicos, lo que sí hace es proporcionar directrices para la seguridad de la información en la nube acogidas bajo los lineamientos de la familia 27k, por tanto, ante esa carencia, se

diseñó el siguiente esquema general de niveles de madurez comúnmente utilizados en SGSI de la familia y que, bien pueden aplicarse en un contexto de cumplimiento de ISO/IEC 27017:

TABLA X.

Índice de criterios de evaluación del nivel de madurez

Índice de madurez	Nivel de madurez
0 - 0.49	0 - Inexistente
0.50 - 1.50	1 - Inicial
1.51 - 2.50	2 - Repetitivo
2.51 - 3.50	3 - Definido
3.51 - 4.50	4 - Gestionado
4.51 - 5.00	5 - Optimizado

Nota. Hecho considerando las escalas de [52, 17].

Los niveles de madurez fueron diseñados teniendo en consideración el Modelo de Madurez de las Capacidades de Ingeniería de Sistemas de Seguridad (denominado SSE-CMM) que fue desarrollado por el Software Engineering Institute (SEI) y quien, mediante estos niveles logra medir los procesos de una organización [53], en este caso específicamente de los niveles de seguridad de la información de servicios en la nube.

En cuanto a los criterios de evaluación, se asignaron puntuaciones en una escala de 0.00 a 5.00 para los promedios de cada una de las cláusulas, que en esta investigación hacen alusión a los indicadores de la Variable Dependiente, tal y como se muestra en la TABLA V. Estos niveles de madurez se realizan en forma de tamaños de rango nominal para ordenar la madurez. Las definiciones de cada nivel de madurez son especificadas a continuación:

TABLA XI.

Nivel de capacidad de la variable dependiente

Nivel	Definición
Nivel 0	En este nivel, la institución pública no tiene implementadas prácticas formales de seguridad de la información en la nube.
Nivel 1	La institución pública ha comenzado a tomar medidas para abordar la seguridad de la información en la nube, pero estas acciones son principalmente reactivas y no están formalizadas
Nivel 2	Se establecen procesos y procedimientos formales para gestionar la seguridad de la información en la nube, pero pueden ser inconsistentes y aún no están completamente integrados en la cultura de la institución pública.
Nivel 3	La organización tiene procesos y controles de seguridad de la información bien definidos y documentados, que se aplican de manera consistente en toda la institución pública.
Nivel 4	Se implementan mecanismos para medir y monitorear continuamente el desempeño de los controles de seguridad de la información en la nube, con el fin de mejorar su eficacia y eficiencia
Nivel 5	La institución pública tiene una cultura de mejora continua en la que se buscan constantemente oportunidades para optimizar y perfeccionar los controles de seguridad de la información en la nube, basándose en el análisis de datos y la retroalimentación del desempeño

Nota. Adaptado de [52].

Respecto a los resultados obtenidos y que permitieran evaluar el cumplimiento de Políticas de Seguridad de la Información de servicios en la nube, se emplearon métodos para la recopilación de información tales como observaciones de la mano con el personal de la institución caso de estudio. En concordancia con ello, el caso de estudio fue una institución

pública de salud peruana de la cual, se tuvo el apoyo de once (11) colaboradores quienes apoyaron en el levantamiento de informaciones, de manera directa o indirectamente mediante los permisos respectivos. Todos ellos fueron colaboradores que se encontraban involucrados relacionados a seguridad de la información.

TABLA XII.

Personal involucrado en le recolección de información

N°	Estructura funcional de OGTI	Cantidad
1	Director General de OGTI	01
2	Director Ejecutivo de la Oficina de Gestión de la Información	01
3	Director Ejecutivo de la Oficina de Soporte e Infraestructura Tecnológica.	01
4	Director Ejecutivo de la Oficina de Innovación y Desarrollo Tecnológico.	01
5	Jefes de Equipo de la Oficina de Gestión de la Información	02
6	Jefes de Equipo de la Oficina de Soporte e Infraestructura Tecnológica	03
7	Jefes de Equipo de la Oficina de Innovación y Desarrollo Tecnológico	02

El análisis fue llevado a cabo utilizando un análisis de brechas (GAP) para determinar el nivel de cumplimiento real de la institución pública en cuanto a la aplicación de las cláusulas y controles de la norma ISO/IEC 27017 y compararlo con el nivel de cumplimiento esperado, de manera que se pueda reconocer el nivel de madurez actual. A continuación, se muestra un ejemplo del análisis de brechas ejecutado, más específicamente respecto a la Cláusula 10: Criptografía:

TABLA XIII.

Ejemplo de análisis de brechas para C10

CLÁSULA	CONTROL	ESTADO	EVALUACIÓN	PROPIETARIO	RECOMENDACIONES	VALOR OBJETIVO DE CONTROL
10	CRIPTOGRAFÍA					
10.1	CONTROLES CRIPTOGRÁFICOS					
Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.						
10.1.1	Política de uso de los controles criptográficos CONTROL Debe elaborarse y aplicarse una política sobre el uso de controles criptográficos para la protección de la información.	CONDICIONES La institución pública no tiene una política formal específicamente relacionada con el uso de la criptografía, en su implementación la empresa no ha aplicado la criptografía al servicio. Actualmente, la referencia a la política se encuentra en la política de seguridad de la información. CAUSA La institución pública no aplica técnicas criptográficas para proteger los servicios o la información de la institución.	GAP Con base en el objetivo de control 10.1.1 del Anexo 10, se debe desarrollar e implementar una política relativa al uso de controles criptográficos para la protección de la información. Además, la institución pública debe proporcionar documentos relacionados con el uso de la criptografía que se entregan a los usuarios del servicio. IMPACTO Si posteriormente la institución pública utiliza la criptografía y no existe un control criptográfico que pueda tomar como referencia, entonces esta técnica no será utilizada de manera óptima para minimizar los riesgos derivados de incidentes de seguridad de la información.	Oficina General de Tecnologías de la Información	Si posteriormente la institución pública utiliza criptografía para proteger la información, será necesaria una política/procedimiento de control criptográfico. La empresa deberá proporcionar los controles criptográficos aplicados a los servicios prestados en cuanto a los servicios cloud.	0

Nota. Ejemplo del Análisis GAP para 1 de las 14 cláusulas totales. Adaptado de [17].

A continuación, a partir de los resultados recopilados, tal y como en el ejemplo de la tabla anterior, se ejecutó una evaluación utilizando el nivel de madurez tal y como se muestra en la siguiente imagen:

PERÚ
MINSA

PRE TEST

Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas

MATRIZ DE VALORACION ISO 27017

C10. Criptografía →	**0.00**

Item	ISO Ref	Requerimiento	Aplica (SI/NO)	Estado del cliente	Cumplimiento	Oportunidad de mejora	Observaciones
6.1	10.1	Controles criptográficos					
6.1.1	10.1.1	Política de uso de los controles criptográficos	SÍ	Dentro de la organización existen escasos controles criptográficos pero la Directiva de Seguridad en la nube establece ciertas particularidades que se están analizando respecto a los controles aplicados por el proveedor y su cumplimiento con la política interna. Adicionalmente, se está definiendo como conservar estas claves y manejar su ciclo de vida	0	Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debeestar alineado o incluído en el SGSI	
6.1.2	10.1.2	Gestión de claves	SÍ	Dentro de la organización existen escasos controles criptográficos pero la Directiva de Seguridad en la nube establece ciertas particularidades que se están analizando respecto a los controles aplicados por el proveedor y su cumplimiento con la política interna. Adicionalmente, se está definiendo como conservar estas claves y manejar su ciclo de vida	0	Los registros de control de cambios deben incluír los elementos de seguridad necesarios, la protección y revisión de los mismos y su inclusión en el SGSI	

CONFIDENCIALIDAD

SGSI de servicios en la nube basado en la ISO/IEC-27017
31/03/2024

Este documento contiene 1 pagina
Pagina 1 de 1

Referencia Interna para USS
TESIS-2022-02 V1 25/12/22
fev: DRDCH AFR: OGTI.

Fig. 15. Evaluación del nivel de madurez.

Vale mencionar que, el Análisis GAP y la evaluación del nivel de madurez se ejecutó para cada una de las 14 cláusulas según la ISO/IEC 27017. Sobre la base del análisis de brechas procesado en la hoja de datos de MS-Excel, el nivel de madurez de la seguridad de la información de servicios en la nube basado en la ISO/IEC 27017 se muestra en la siguiente tabla:

TABLA XIV.

Nivel de Madurez PRE TEST de la seguridad de información de servicios en la nube

Cláusulas	Nivel PRE TEST	Nivel de Madurez
C5. Políticas de seguridad de la información	0.50	Inicial
C6. Organización de la seguridad de la información	1.14	Inicial
C7. Seguridad de los recursos humanos	1.67	Repetitivo
C8. Gestión de activos	0.90	Inicial
C9. Control de acceso	1.43	Inicial
C10. Criptografía	0.00	Inexistente
C11. Seguridad física y medioambiental	0.60	Inicial
C12. Seguridad de las operaciones	1.36	Inicial
C13. Seguridad de las comunicaciones	1.71	Repetitivo
C14. Adquisición, desarrollo y mantenimiento de sistemas	1.62	Repetitivo
C15. Relaciones con los proveedores	1.00	Inicial
C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad	2.14	Repetitivo
C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad	1.75	Repetitivo
C18. Cumplimiento	0.25	Inexistente
PROMEDIO	**1.15**	**Inicial**

Nota. Obtenido del análisis ejecutado en un Nivel PRE TEST.

El resultado de los datos recolectados mediante la Ficha de Análisis de Brechas ya procesada muestra que, el valor promedio del control de la seguridad de la información de los servicios en la nube en la institución pública caso de estudio en un nivel PRE TEST es **1,15**. Este valor indica que la seguridad de la información de los servicios en la nube existe

en el primer nivel, es decir, Inicial.

Sobre la base de los resultados de la TABLA XIV, para cada una de las cláusulas de la norma ISO/IEC 27017:2015, puede verse un gráfico del nivel de madurez PRE TEST en la siguiente figura:

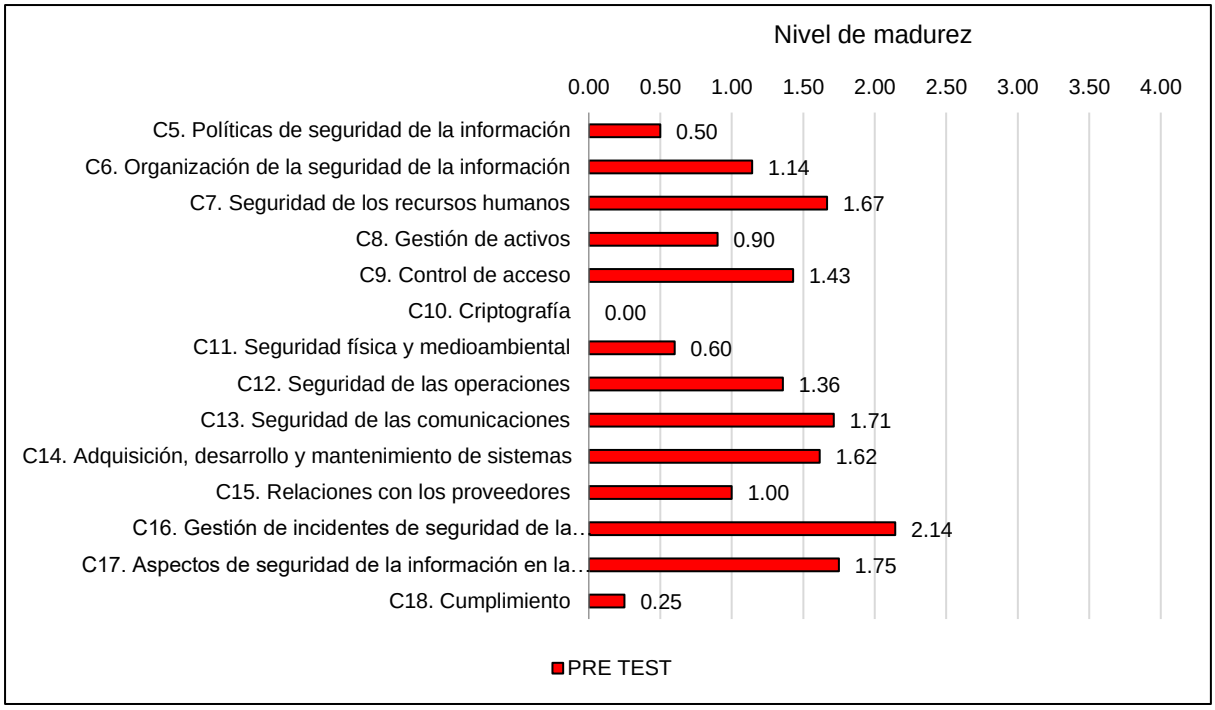


Fig. 16. Nivel de Madurez PRE TEST de la seguridad de información de servicios en la nube

Tras conocer que el nivel de madurez de la seguridad de la información de los servicios en la nube es de **1.15 (Inicial)**, el valor esperado del nivel de madurez es de **5 (Optimizado)** según la ISO/IEC 27017, sin embargo, para este estudio, el valor esperado es de **4 (Gestionado)**, el cual se justifica a) por la duración del uso de la computación en nube de la institución pública caso de estudio (>4 años), b) por la literatura científica encontrada respecto a niveles de madurez deseados [17] y c) las expectativas de las partes interesadas de dicha institución pública caso de estudio y del Director General de OGTI junto a su equipo de directores de las oficinas involucradas en esta investigación (OGI, OSIT y OIDT) que desean una buena gestión de seguridad de la información de los servicios en la nube.

TABLA XV.

Nivel de Madurez deseado según criterios

Criterios	Nivel deseado
Criterio 01: por la duración del uso de la computación en nube de la institución pública caso de estudio (>4 años)	4.00
Criterio 02: por la literatura científica encontrada respecto a niveles de madurez deseados [17]	4.00
Criterio 03: por las expectativas de las partes interesadas de dicha institución pública caso de estudio y del Director General de OGTI	4.00

Nota. Obtenido del análisis de brechas ejecutado en un Nivel PRE TEST.

En la siguiente tabla puede verse el Análisis GAP PRE TEST con respecto al nivel de madurez de cada una de las cláusulas:

TABLA XVI.

Nivel de Madurez Análisis GAP PRE TEST de la seguridad de información de servicios en la nube

Cláusulas	Nivel PRE TEST	Nivel Esperado	Brecha
C5. Políticas de seguridad de la información	0.50	4.00	3.50
C6. Organización de la seguridad de la información	1.14	4.00	2.86
C7. Seguridad de los recursos humanos	1.67	4.00	2.33
C8. Gestión de activos	0.90	4.00	3.10
C9. Control de acceso	1.43	4.00	2.57
C10. Criptografía	0.00	4.00	4.00
C11. Seguridad física y medioambiental	0.60	4.00	3.40

C12. Seguridad de las operaciones	1.36	4.00	2.64
C13. Seguridad de las comunicaciones	1.71	4.00	2.29
C14. Adquisición, desarrollo y mantenimiento de sistemas	1.62	4.00	2.38
C15. Relaciones con los proveedores	1.00	4.00	3.00
C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad	2.14	4.00	1.86
C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad	1.75	4.00	2.25
C18. Cumplimiento	0.25	4.00	3.75
		PROMEDIO	**2.85**

Nota. Obtenido del análisis de brechas ejecutado en un Nivel PRE TEST.

De la TABLA XVI se desprende que, la distancia de la brecha de seguridad de la información de servicios en la nube desde la condición actual PRE TEST a la condición esperada para cada cláusula es de 3.50 (C.5), 2.86 (C.6), 2.33 (C.7), 3.10 (C.8), 2.57 (C.9), 4.00 (C.10), 3.40 (C.11), 2.64 (C.12), 2.29 (C.13), 2.38 (C.14), 3.00 (C.15), 1.86 (C.16), 2.25 (C.17) y 3,75 (C.18).

Una vez conocida la brecha de cada cláusula, se sumaron y promediaron todos estos valores para calcular el valor de brecha global. Se sabe que el valor global de la brecha de seguridad de la información de servicios en la nube PRE TEST es de **2.85**, es decir, la brecha entre el nivel de madurez PRE TEST y el nivel de madurez esperado en la institución pública caso de estudio. Este valor estaba bastante alejado del nivel de madurez esperado, por lo que era necesario implementar los controles según la ISO/IEC 27017 existentes.

A continuación, se analizan el Nivel de Madurez PRE TEST vs Nivel de Madurez Esperado vs Nivel de Madurez ISO/IEC-27017, considerando para este caso de estudio un 4.00, según los criterios seleccionados previamente en la TABLA XV:

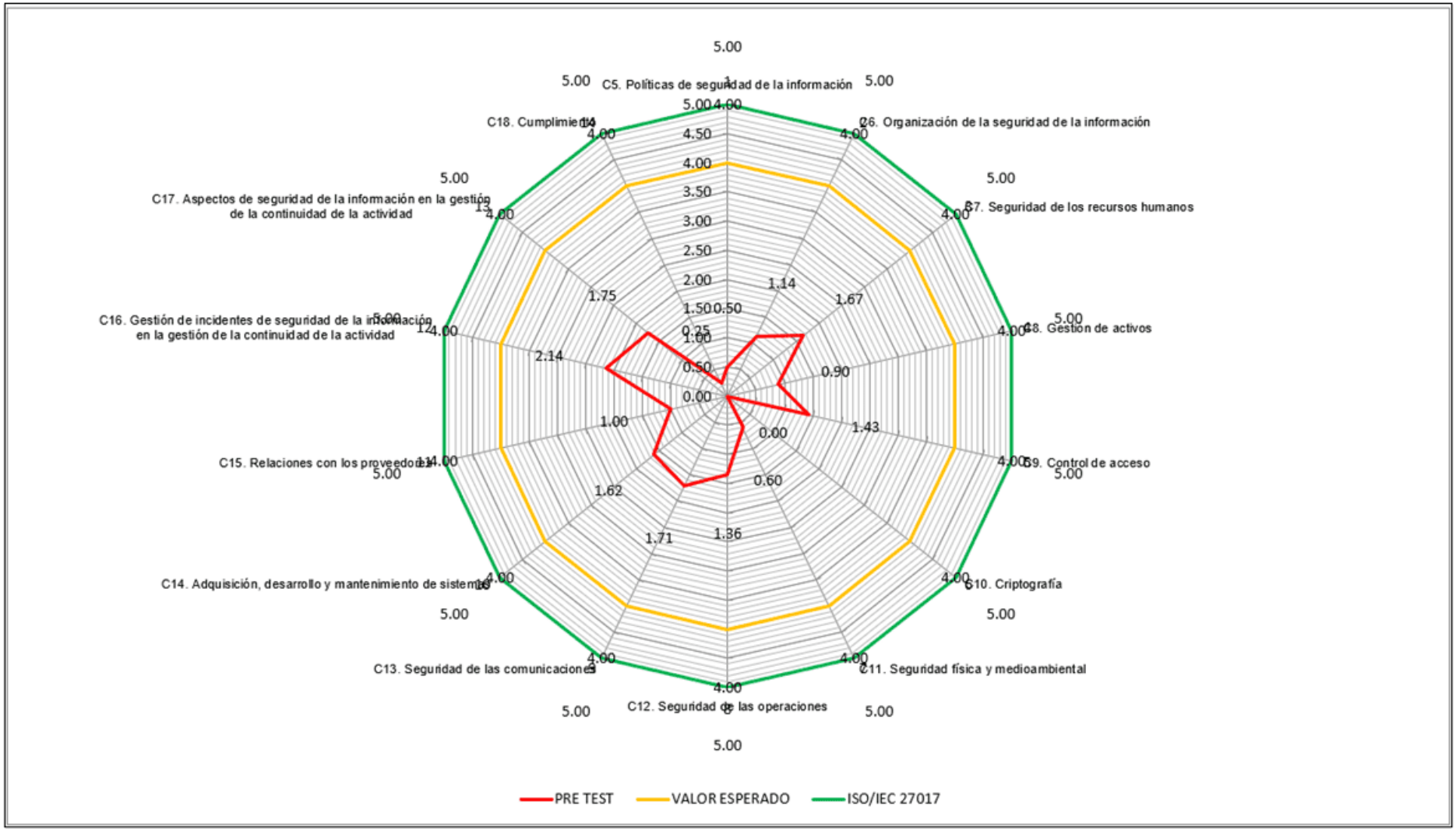


Fig. 17. Análisis de Nivel de Madurez PRE TEST vs Nivel de Madurez Esperado vs Nivel de Madurez ISO/IEC-27017

Por una parte, de la Fig. 17 se desprende que, que la cláusula C10 (Criptografía) tiene el valor más bajo, con un nivel de madurez y una brecha actuales de 0,00 y 4,00; seguido de la cláusula C18 (Cumplimiento) con un nivel de madurez y una brecha actuales de 0,25 y 3,75; y de la cláusula C5 (Políticas de seguridad de la información) con un nivel de madurez y una brecha actuales de 0,50 y 3,50, respectivamente. Estos resultados se resumen en la tabla siguiente:

TABLA XVII.

Análisis GAP PRE TEST de las brechas más altas según nivel esperado

Cláusulas	**Nivel PRE TEST**	**Nivel Esperado**	**Brecha**
C10. Criptografía	0.00	4.00	4.00
C18. Cumplimiento	0.25	4.00	3.75
C5. Políticas de seguridad de la información	0.50	4.00	3.50

Por otra parte, de la misma Fig. 17 se desprende que, que la cláusula C16 (Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad) tiene el valor más alto, con un nivel de madurez y una brecha actuales de 2,14 y 1,86; seguido de la cláusula C17 (Aspectos de seguridad de la información en la gestión de la continuidad de la actividad) con un nivel de madurez y una brecha actuales de 1,75 y 2,25; y de la cláusula C13 (Seguridad de las comunicaciones) con un nivel de madurez y una brecha actuales de 1,71 y 2,29, respectivamente. Estos resultados se resumen en la tabla siguiente:

TABLA XVIII.

Análisis GAP PRE TEST de las brechas más bajas según nivel esperado

Cláusulas	Nivel PRE TEST	Nivel Esperado	Brecha
C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad	2.14	4.00	1.86
C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad	1.75	4.00	2.25
C13. Seguridad de las comunicaciones	1.71	4.00	2.29

Este análisis PRE TEST mostró las debilidades de las políticas en la gestión de la seguridad de la información que ya han sido implementadas previamente por la institución pública peruana caso de estudio. Con esta auditoría preliminar y con el desarrollo de un sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 se esperaba que dicha institución refuerce las políticas dentro de los servicios en la nube, mejorando de esa manera la seguridad de la información.

Respecto a esto, se desarrolló el sistema de gestión de seguridad de la información de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas, el cual consideró el enfoque PDCA (Planificar, Hacer, Verificar, Actuar):

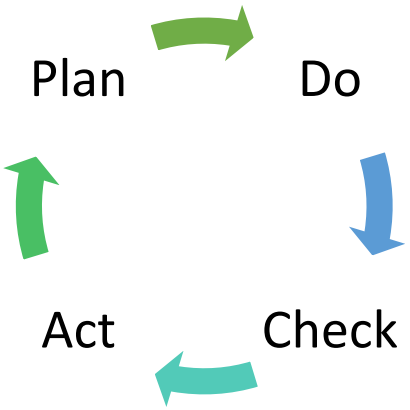


Fig. 18. Metodología PDCA empleada para el SGSI.

Posterior a ello, se implementó el SGSI durante un periodo de dieciocho (18) semanas, en las cuales se requirió una planificación cuidadosa para asegurar que cada etapa se complete de manera efectiva y eficiente.

Esta implementación se ejecutó durante, el lunes 01 de agosto del 2022 al domingo 04 de diciembre del 2022 considerando las cuatro etapas mencionadas previamente. A continuación, se muestra la distribución de tiempos para cada etapa del SGSI:

ETAPA	N°	TÍTULO DE LA TAREA	RESPONSABLE DE LA TAREA	FECHA INICIO	FECHA FIN	DURACIÓN (DÍAS)	% COMPLETITUD	CRONOGRAMA																		
								SEMANA																		
								1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
PLAN	1	SGSICC-F01: Planificar																								
	1.1	Análisis de activos y evaluación de riesgos	Bach. Dávila Chunga Dayán Ray	1/08/2022	14/08/2022	13	100%	x	x																	
	1.2	Establecimiento de políticas y procedimientos	Bach. Dávila Chunga Dayán Ray	1/08/2022	14/08/2022	13	100%	x	x																	
	1.3	Determinación de objetivos de seguridad	Bach. Dávila Chunga Dayán Ray	15/08/2022	28/08/2022	13	100%			x	x															
	1.4	Identificación de roles y responsabilidades	Bach. Dávila Chunga Dayán Ray	15/08/2022	20/08/2022	7	100%				x															
DO	2	SGSICC-F02: Hacer																								
	2.1	Implementación de Políticas y Procedimientos de SI	Bach. Dávila Chunga Dayán Ray	29/08/2022	25/09/2022	26	100%					x	x	x	x											
	2.2	Capacitación y Concientización	Bach. Dávila Chunga Dayán Ray	26/09/2022	9/10/2022	13	100%									x	x									
CHECK	3	SGSICC-F03: Verificar																								
	3.1	Auditoría Interna	Bach. Dávila Chunga Dayán Ray	10/10/2022	30/10/2022	20	100%											x	x	x						
	3.2	Revisión del desempeño	Bach. Dávila Chunga Dayán Ray	31/10/2022	6/11/2022	7	100%														x					
	3.3	Valoración del Riesgo Residual	Bach. Dávila Chunga Dayán Ray	7/11/2022	13/11/2022	7	100%															x				
ACT	4	SGSICC-F04: Actuar																								
	4.1	Mejora continua	Bach. Dávila Chunga Dayán Ray	14/11/2022	27/11/2022	13	100%																x	x		
	4.2	Revisión de la Dirección	Bach. Dávila Chunga Dayán Ray	28/11/2022	4/12/2022	6	100%																		X	

Fig. 19. Cronograma del desarrollo del sistema de gestión de seguridad basado en la ISO/IEC-27017.

Posteriormente a la evaluación del Nivel PRES TEST y habiendo ya puesto en marcha los controles del sistema de gestión de seguridad de la información para servicios en la nube basado en la ISO/IEC-27017 en la institución pública caso de estudio durante los meses presentados en el cronograma previo, se evaluó el nivel POST TEST, ejecutándose el mismo procedimiento con el que se evaluaron las 14 cláusulas en el nivel PRE TEST tal y como se explica en la Fig. 16. Sobre la base del análisis procesado en la hoja de datos de MS-Excel, el nivel de madurez POS TEST de la seguridad de la información de servicios en la nube basado en la ISO/IEC 27017 se muestra en la siguiente tabla:

TABLA XIX.

Nivel de Madurez POST TEST de la seguridad de información de servicios en la nube

Cláusulas	**Nivel POST TEST**	**Nivel de Madurez**
C5. Políticas de seguridad de la información	3.50	Definido
C6. Organización de la seguridad de la información	3.14	Definido
C7. Seguridad de los recursos humanos	3.67	Gestionado
C8. Gestión de activos	2.55	Definido
C9. Control de acceso	2.43	Repetitivo
C10. Criptografía	1.50	Inicial
C11. Seguridad física y medioambiental	1.87	Repetitivo
C12. Seguridad de las operaciones	2.36	Repetitivo
C13. Seguridad de las comunicaciones	2.57	Definido
C14. Adquisición, desarrollo y mantenimiento de sistemas	2.54	Definido
C15. Relaciones con los proveedores	1.80	Repetitivo
C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad	3.00	Definido
C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad	2.67	Definido
C18. Cumplimiento	1.88	Repetitivo
PROMEDIO	**2.53**	**Definido**

Nota. Obtenido del análisis ejecutado en un Nivel POST TEST.

El resultado de los datos recolectados mediante la Ficha de Análisis de Brechas ya procesada muestra que, el valor promedio del control de la seguridad de la información de los servicios en la nube en la institución pública caso de estudio en un nivel POST TEST es **2,53**. Este valor indica que la seguridad de la información de los servicios en la nube existe en el tercer nivel, es decir, **Definido**. Sobre la base de los resultados de la TABLA XIX, para cada una de las cláusulas de la norma ISO/IEC 27017:2015, puede verse un gráfico del nivel de madurez POST TEST en la siguiente figura:

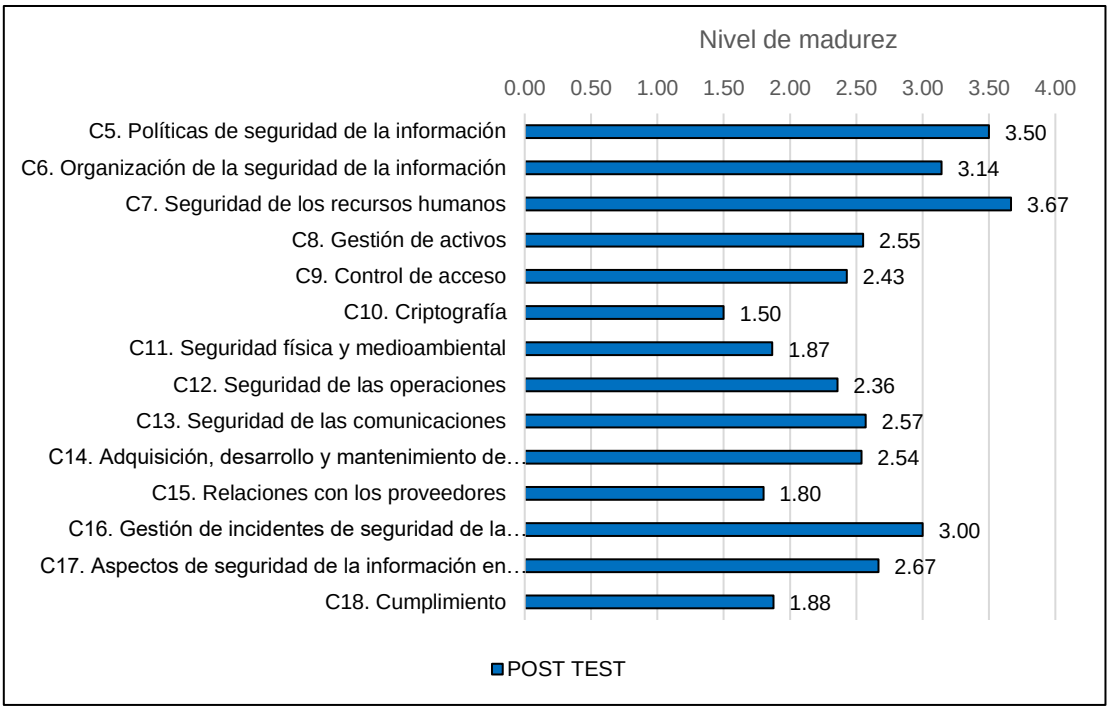


Fig. 20. Nivel de Madurez POST TEST de la seguridad de información de servicios en la nube

En la siguiente tabla puede verse el Análisis GAP POST TEST con respecto al nivel de madurez de cada una de las cláusulas:

TABLA XX.

Nivel de Madurez Análisis GAP POST TEST de la seguridad de información de servicios en la nube

Cláusulas	Nivel POST TEST	Nivel Esperado	Brecha
C5. Políticas de seguridad de la información	3.50	4.00	0.50
C6. Organización de la seguridad de la información	3.14	4.00	0.86
C7. Seguridad de los recursos humanos	3.67	4.00	0.33
C8. Gestión de activos	2.55	4.00	1.45
C9. Control de acceso	2.43	4.00	1.57
C10. Criptografía	1.50	4.00	2.50
C11. Seguridad física y medioambiental	1.87	4.00	2.13
C12. Seguridad de las operaciones	2.36	4.00	1.64
C13. Seguridad de las comunicaciones	2.57	4.00	1.43
C14. Adquisición, desarrollo y mantenimiento de sistemas	2.54	4.00	1.46
C15. Relaciones con los proveedores	1.80	4.00	2.20
C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad	3.00	4.00	1.00
C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad	2.67	4.00	1.33
C18. Cumplimiento	1.88	4.00	2.12
		PROMEDIO	**1.47**

Nota. Obtenido del análisis de brechas ejecutado en un Nivel PRE TEST.

De la

TABLA XX se desprende que, la distancia de la brecha de seguridad de la información de servicios en la nube desde la condición actual POST TEST a la condición esperada para cada cláusula es de 0.50 (C.5), 0.86 (C.6), 0.33 (C.7), 1.45 (C.8), 1.57 (C.9), 2.50 (C.10), 2.13 (C.11), 1.64 (C.12), 1.43 (C.13), 1.46 (C.14), 2.20 (C.15), 1.00 (C.16), 1.33 (C.17) y 2.12 (C.18).

Una vez conocida la brecha de cada cláusula, se sumaron y promediaron todos estos valores para calcular el valor de brecha global. Se sabe que el valor global de la brecha de seguridad de la información de servicios en la nube POST TEST es de **1.47**, es decir, la brecha entre el nivel de madurez POST TEST y el nivel de madurez esperado en la institución pública caso de estudio. Este valor estaba bastante aminorado en comparación con el nivel PRE TEST respecto al nivel de madurez esperado, por lo que la brecha se había acortado al implementar los controles según la ISO/IEC 27017.

A continuación, se analizan el Nivel de Madurez POST TEST vs Nivel de Madurez Esperado vs Nivel de Madurez ISO/IEC-27017, considerando para este caso de estudio un 4.00, según los criterios seleccionados previamente en la TABLA XV.

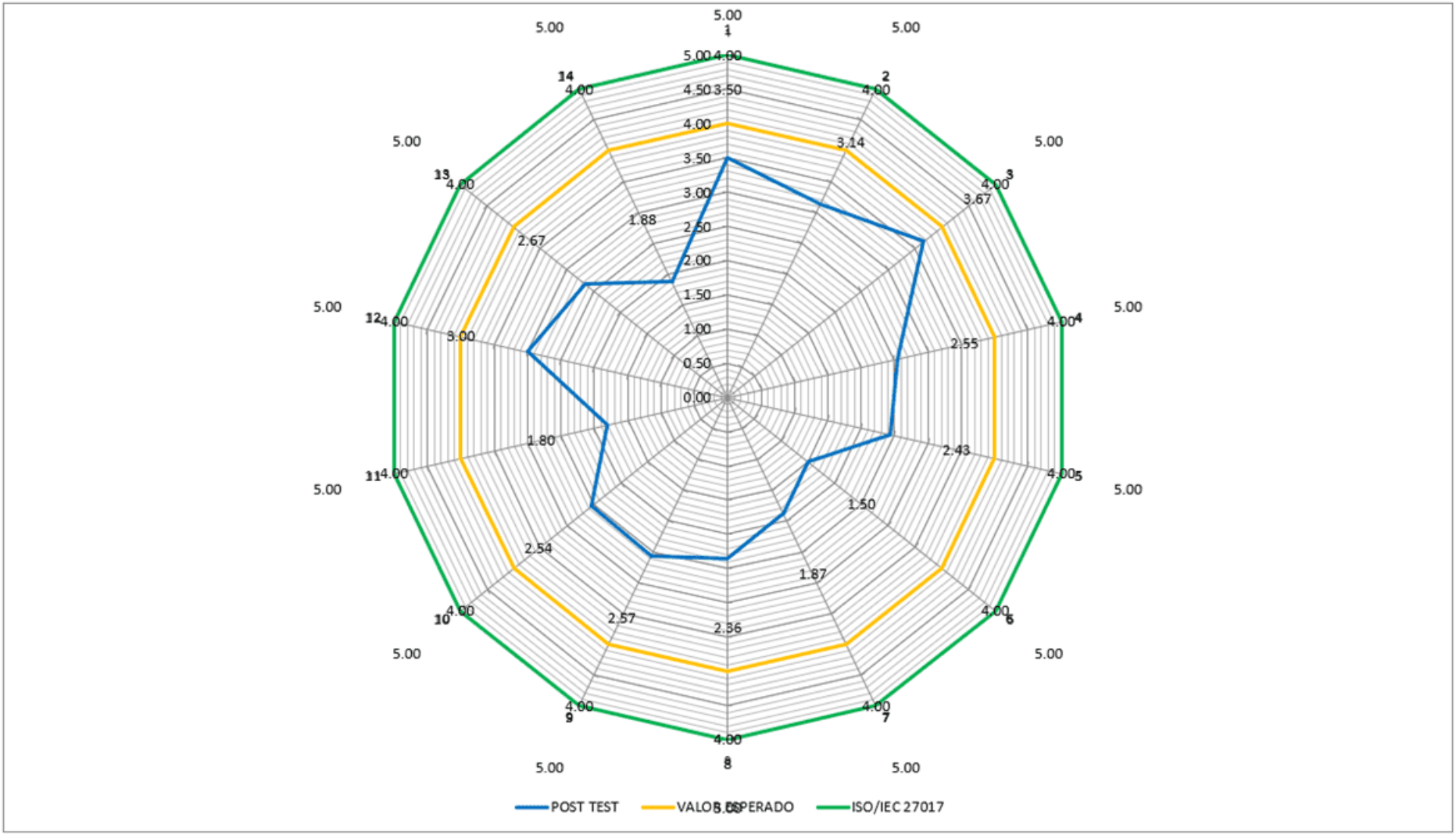


Fig. 21. Análisis de Nivel de Madurez POST TEST vs Nivel de Madurez Esperado vs Nivel de Madurez ISO/IEC-27017

A continuación, a partir de los resultados recopilados, se ejecutó una comparativa de los niveles de madurez PRE TEST y POST TEST tal y como se muestra en la siguiente tabla:

TABLA XXI.

Resultados del nivel de madurez PRE TEST vs POST TEST

CLÁUSULA	PRE TEST	POS TEST
C5	0.50	3.50
C6	1.14	3.14
C7	1.67	3.67
C8	0.90	2.55
C9	1.43	2.43
C10	0.00	1.50
C11	0.60	1.87
C12	1.36	2.36
C13	1.71	2.57
C14	1.62	2.54
C15	1.00	1.80
C16	2.14	3.00
C17	1.75	2.67
C18	0.25	1.88
PROMEDIO	**1.15**	**2.53**

La TABLA XXI y Fig. 22 explican la comparativa del nivel de madurez de PRE TEST, con el nivel de madurez de la norma ISO/IEC-27017, con el nivel de madurez esperado según la institución pública peruana caso de estudio y con el nivel de madurez POST TEST., evidenciándose mejorías que evolucionan de un valor promedio de **1,15 (INICIAL)** en un nivel PRE TEST hasta llegar a un valor promedio de 2.53 **(DEFINIDO)** en un nivel POST TEST. Este valor indica que la seguridad de la información de los servicios en la nube ha escalado dos (02) niveles de madurez.

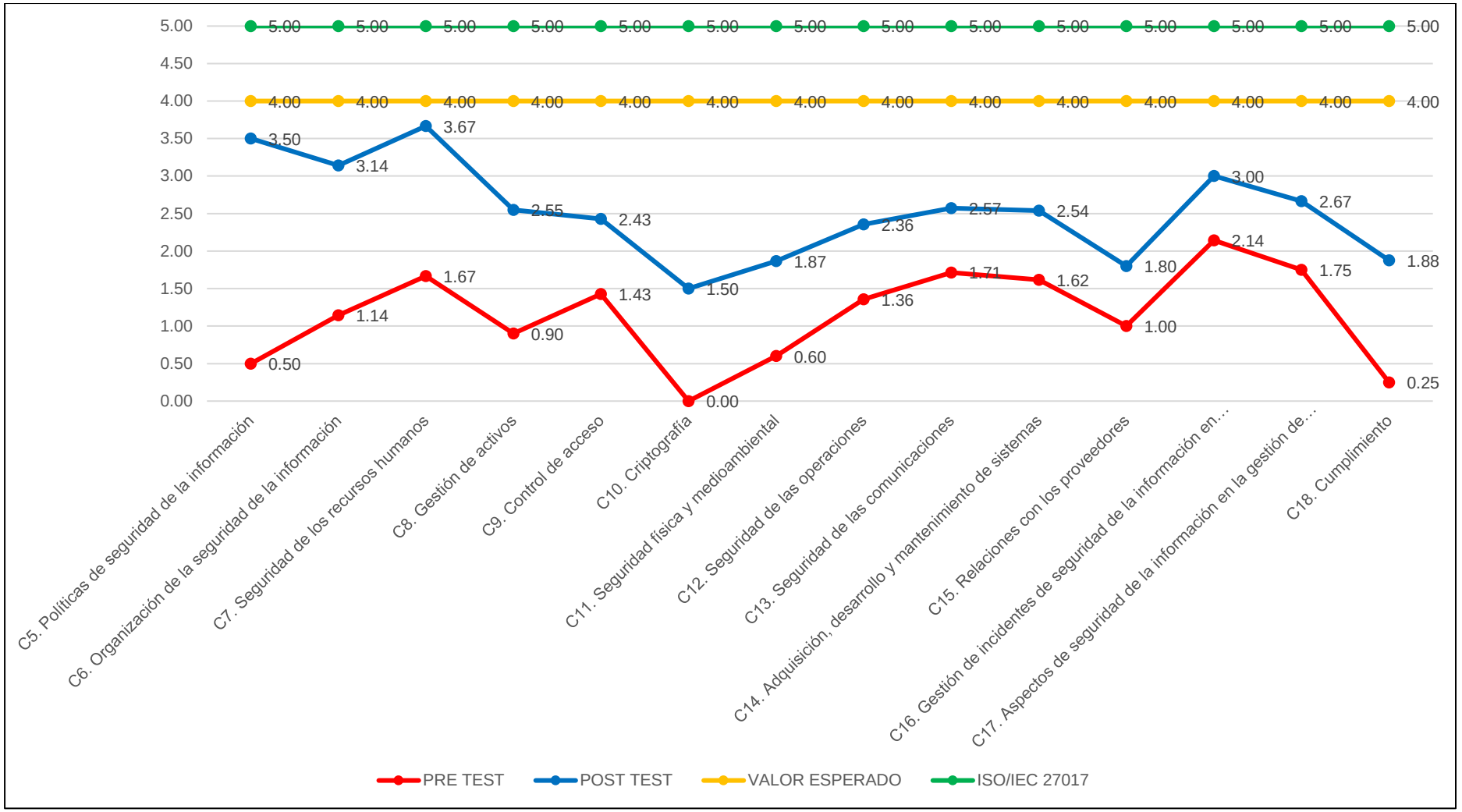


Fig. 22. Nivel de Madurez PRE TEST vs Nivel de Madurez POST TEST vs Nivel de Madurez Esperado vs Nivel de Madurez ISO/IEC-27017

TABLA XXII.

Detalle de niveles de madurez PRE TEST vs POST TEST

Cláusulas	Nivel PRE TEST	Nivel POST TEST
C5. Políticas de seguridad de la información	Inicial	Definido
C6. Organización de la seguridad de la información	Inicial	Definido
C7. Seguridad de los recursos humanos	Repetitivo	Gestionado
C8. Gestión de activos	Inicial	Definido
C9. Control de acceso	Inicial	Repetitivo
C10. Criptografía	Inexistente	Inicial
C11. Seguridad física y medioambiental	Inicial	Repetitivo
C12. Seguridad de las operaciones	Inicial	Repetitivo
C13. Seguridad de las comunicaciones	Repetitivo	Definido
C14. Adquisición, desarrollo y mantenimiento de sistemas	Repetitivo	Definido
C15. Relaciones con los proveedores	Inicial	Repetitivo
C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad	Repetitivo	Definido
C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad	Repetitivo	Definido
C18. Cumplimiento	Inexistente	Repetitivo

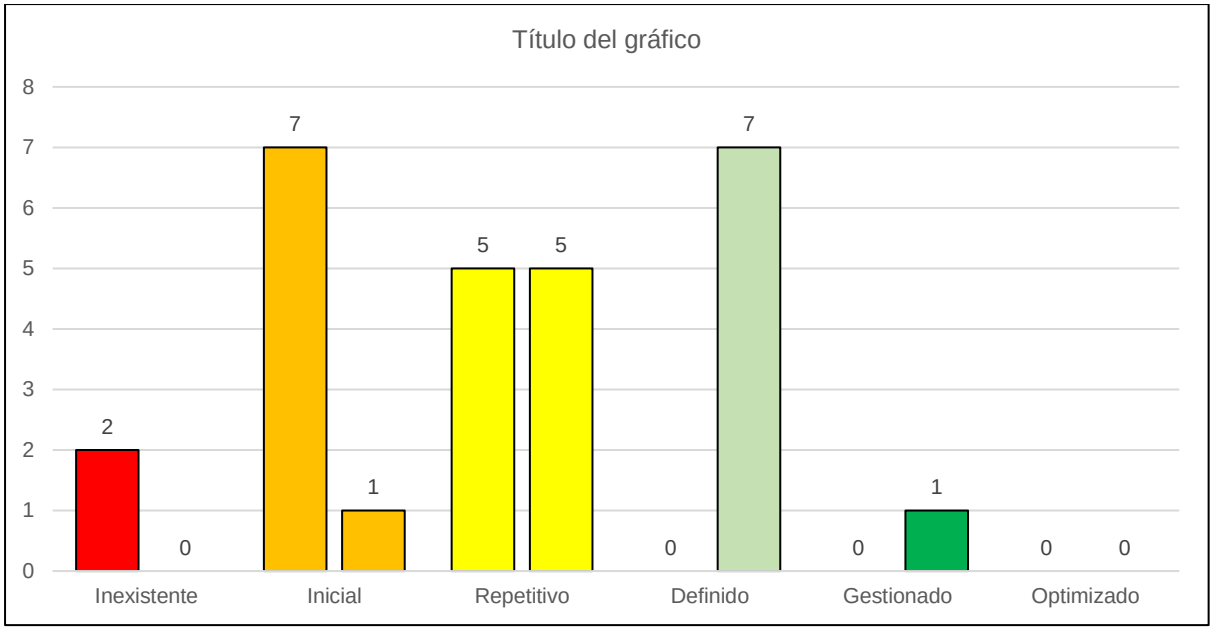


Fig. 23. Detalle de niveles de madurez PRE TEST vs POST TEST

Según la TABLA XXII y Fig. 23 puede evidenciarse que en el nivel POST TEST ya no existen cláusulas con nivel de madurez INEXISTENTE (de 2 cláusulas a 0 cláusulas). También se evidencia aminoramiento de cláusulas de con nivel de madurez INICIAL (de 7 cláusulas a 1 cláusulas). Asimismo, en el nivel REPETITIVO se mantienen los niveles de madurez (5 cláusulas). Respecto a los niveles DEFINIDO y GESTIONADO se evidencia un incremento en el nivel POST TEST (de 0 cláusulas a 7 cláusulas y de 0 cláusulas a 1 cláusulas respectivamente). Finalmente, en cuanto al nivel OPTIMIZADO, no se ha evidenciado ninguna cláusula con este nivel en ninguno de los dos momentos de la recolección de las informaciones.

3.2. Discusión

Respecto al objetivo, seleccionar el estándar más adecuado para la seguridad de la información para servicios en la nube, como lo que se pretendía era el desarrollo de un SGSI de servicios en la nube, era necesario que dicho SGSI se encuentre fundamentado en

estándares internacionales y que, en este caso concreto, ayude al propósito de la mejora de la seguridad de la información en instituciones públicas de salud peruanas, por lo que se optó por diseñar el SGSI fundamentado en la lSO/lEC 27017 para el caso de estudio. DISCUTE CON Estos resultados concuerdan con los obtenidos por Ruiz [21] quien realizó una investigación en donde primeramente, caracterizó los estándares de SI existentes en la literatura; luego, analizó la situación actual de dicha compañía en cuanto a infraestructura, niveles de seguridad, planes de contingencia, análisis de riesgos y vulnerabilidades, etcétera; posteriormente desarrolló el SGSI para servicios en la nube considerando la ISO/IEC 27017 y el apoyo del Ciclo PDCA y; finalmente validaron dicha propuesta por juicio de expertos en SI para llevarlo a la práctica en el caso de estudio, concluyendo que, dicho SGSI es un punto de partida para que dicha compañía pueda certificarse en la normativa ISO/IEC 27017 y así pueda seguir logrando el aminoramiento de los riesgos y vulnerabilidades de SI.

Respecto al objetivo, diagnosticar el nivel de cumplimiento actual de políticas de seguridad de la información en una institución pública de salud peruana caso de estudio, se diagnosticó que, el MINSA presentaba deficiencia en cuanto a la gestión de la SI reflejándose en el bajo nivel de seguridad de los equipos con los que se operaban, el poco conocimiento acerca de la preexistencia de políticas documentadas para la SI, los controles no aseguraban que solamente usuarios autorizados accedieran a ciertas funciones de los diversos sistemas, se carecían de procedimientos para la eliminación de accesos de usuarios a la finalización de vínculos laborales, no se venían firmando acuerdos de confidencialidad con empleados y proveedores, era defectuosos los procedimientos de destrucción de data en equipos sensibles, no se desplegaban programas de capacitación en temas de seguridad informática, ni mucho menos se concientizaban a los colaboradores con temas afines a los anteriormente mencionados. Estos resultados concuerdan con los obtenidos por Ayala [22] quien realizó una investigación en la que, primeramente, describieron la SI en cuanto a marcos existentes, tipos de cloud, etcétera; luego, caracterizaron la situación actual en cuanto a seguridad de la información de la compañía española caso de estudio; después, diseñaron el SGSI

fundamentado en la norma en IS0/IEC 27017 y considerando la metodología MAGERIT como soporte en la gestión de riesgos; posteriormente implementaron dicho SGSI, para; finalmente evaluar los resultados de dicha implantación, y en cuyos resultados evidenciaron que, el proceso de explotación CMS cloud poseía valores altos (3-Alto) en cuanto a DICAT con un valor de negocio de € 292.682.927; asimismo, la integridad y disponibilidad asumirían más riesgos con un 24% y 31% respectivamente, concluyendo que, el SGSI fundamentado en la IS0/IEC 27017 sí cumple con mejorar el nivel de SI en una compañía peruana de software que suministra software como PaaS.

Respecto al objetivo, diseñar un sistema de gestión de seguridad de la información para servicios en la nube basado en el estándar seleccionado previamente, se desarrolló dicho SGSI basada en dicha norma pues la lSO/IEC 27017 es una norma complementaria que se centra en los controles de SI que las organizaciones pueden optar por implementar. Asimismo, con el desarrollo de ISO/IEC 27017, las operaciones comúnmente llevadas a cabo, conceptualizadas como mejores praxis, se ofrecieron como procedimientos y métodos probados en la práctica, que podría ser adaptados a los requisitos determinados de las unidades organizacionales, tal y como fue el caso del MINSA. Estos resultados contrastan con los obtenidos por Peñafiel [26] quien diseñó un modelo de SGSI dentro de un ambiente Cloud Computing aplicando la Norma ISO 27001:2013 pero que no hizo una investigación a profundidad acerca de estándares en ambientes cloud dejando con ello un vacío teórico respecto a este tipo de revisiones previas. El diseño del modelo careció de detalles específicos sobre cómo implementar realmente el SGSI en un entorno de Cloud Computing dejando de lado desafíos técnicos específicos. Asimismo, el modelo propuesto careció de validación empírica o evidencia empírica de su eficacia, necesitando de evidencia de pruebas o casos de estudio que respalden la efectividad del modelo en situaciones reales. Asimismo, Estos resultados concuerdan con los obtenidos por Kamaruddin et al. [7] quienes desarrollaron la investigación, Cloud Security Pre-assessment Model For Cloud Service Provider Based On lSO/IEC 27017:2015 Additional Control, y en la que, primeramente,

realizaron una revisión de la literatura referente con la usanza de los servicios en la nube por parte de las organizaciones; luego, se evaluaron comparativamente cuatro (04) modelos existentes de preparación para la seguridad en la nube; después, seleccionaron mediante criterios de selección de dominios para el desarrollo de un modelo para la SI en la nube; posteriormente, diseñaron un modelo de siete (07) dominios y cuarenta y cuatro (44) controles considerando la ISO/IEC 27017 considerando tres fases: (i) desarrollo del modelo preliminar; (ii) verificación del modelo preliminar; y (iii) validación del modelo final y; finalmente validaron el modelo por expertos.

Respecto al objetivo, validar mediante juicio de expertos el SGSI para servicios en la nube propuesto, se validó dicho diseño mediante la técnica juicio de expertos con su instrumento ficha de juicio de expertos el cual se encuentra detallado en los anexos y que permitió darle el visto bueno a la que, en primera instancia fue la propuesta desarrollada por este investigador. Se pudo determinar que los diez (10) indicadores de la dimensión "Aceptación del SGSI" tuvieron una valoración promedio total de 92.90 considerando la totalidad de respuestas por parte de los cinco expertos, evidenciándose una valoración mínima de 91.00 (Objetividad, Organización, Intencionalidad y Coherencia) y una máxima de 95.00 (Pertinencia). lo cual en la escala de valoración diseñada y referenciada en la TABLA XXXV, obtuvo un Nivel "Excelente" considerándose como "Aplicable". Posterior e ello, se pudo implementar dicha propuesta en la institución caso de estudio con lo que se pudieron documentar los resultados obtenidos según las dimensiones previamente detalladas. Estos resultados concuerdan con los obtenidos por Tenelema [8] quien realizó una investigación en la que, primeramente, se caracterizaron las ISO/IEC 27017 y 27018; luego, se diseñó el SGSI considerando las ISO anteriormente mencionadas y fundamentado en Seguridad del Entorno, Conocer & Limite de Acceso, Detección y Respuesta; después, implementaron el modelo haciendo uso de herramientas tales como Mantis Bug Tracker, ClamAV, Aide, etcétera; finalmente, evaluaron los resultados de las pruebas obtenidas y en cuyops resultados posteriores a la validación por expertos, evidenciaron que, el modelo de SGSI ayudó en el

mejoramiento de los niveles de SI y en la mitigación de vulnerabilidades en un 75.0%, concluyendo que, el modelo de SGSI ayudó al mejoramiento de los niveles de SI en la nube en cuanto a cantidades de logs, riesgos mitigados y vulnerabilidades.

Respecto al objetivo, ejecutar una prueba piloto del SGSI para servicios en la nube en el caso de estudio, se ejecutó dicha prueba en el MINSA, para lo cual se requirió el permiso respectivo, con lo que posteriormente se procedió a realizar la aplicabilidad SOA, el diseño de los procedimientos y políticas internas en cuanto a seguridad de la información y, el plan de capacitación y concientización, conllevando a obtener la mejora en resultados de mejoramiento significativo en el 100% de las cláusulas, pasando de tener un nivel PRE TEST de madurez de la seguridad de la información de los servicios en la nube de 1.15 (Inicial) a un nivel PRE TEST de madurez de la seguridad de la información de los servicios en la nube de 2.53 (Definido). Estos resultados concuerdan con los obtenidos por Ahmad et al. [9] quienes desarrollaron la investigación en la que, primeramente, se caracterizó la coyuntura actual de la usanza de computación en la nube por organizaciones en dicho país asiático; luego, se diseñó un SGSI acorde a las necesidades de esta coyuntura local considerando la ISO/IEC 27017; posteriormente, se implementó dicho modelo en un caso de estudio local y; finalmente sus resultados evidenciaron que, se mejoraron los niveles de SI en dicho caso de estudio, evidenciándose mejoras en cuanto a la pérdida de control y gobernanza es especialmente porque los CSP anteriormente no eran fiables ni transparentes, concluyéndose que, este modelo sirve de soporte a los CSP malayos en el cumplimiento de las normas específicas de la nube para garantizar la SI de los datos de los clientes y que todos los recursos estén bien protegidos.

3.3. Aporte de la investigación

Con el objeto de seleccionar el estándar más adecuado para la seguridad de la información en entornos de servicios en la nube, la literatura propuestas por Kitchenham & Charters, se aplicaron las directrices para la verificación sistemática [21]. Estas directrices se

utilizan para obtener una visión general del área de investigación y complementarla mediante la revisión de las evidencias (artículos científicos-actas de conferencias), en temas específicos, como se pretende lograr en este informe. En este caso, el objetivo era analizar los resultados de la gestión de la seguridad de la información en servicios en la nube, así como comprender en qué medida se han implementado estos estándares en casos de estudio y, en algunos casos, identificar los resultados obtenidos por diversos autores. Proceso de revisión sistemática:

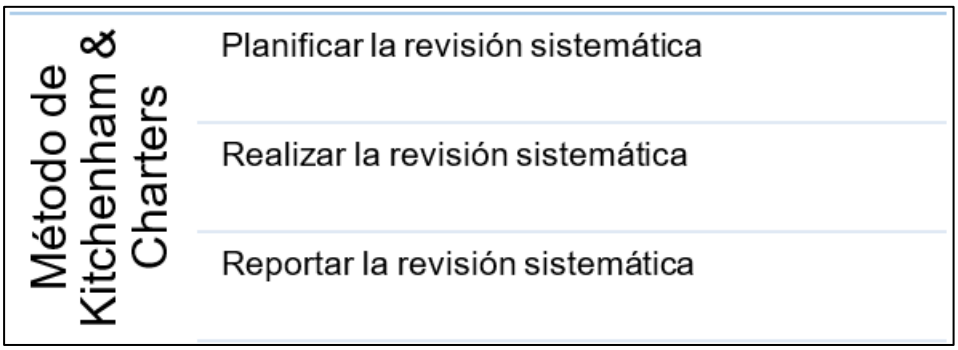


Fig. 24. Método de Sistemático de Revisión de Literatura [21].

Conociendo el referido la metodología a utilizar para la revisión de la literatura, se aproxima estándares más adecuados para la SI para servicios en la nube existente, para iniciar el proceso, se procedió a colocar en marcha el estudio. Para ello, se tuvo que seleccionar artículos vitales mediante la búsqueda en bases de datos-BD científicas utilizando un vínculo de búsqueda o palabras clave específicas. En esta búsqueda, se incluyeron cuatro bases de datos científicas, a saber:

Scopus	https://www.scopus.com
WoS	http://www.webofscience.com/
Science Direct	https://www.sciencedirect.com/
IEEE Xplore	https://ieeexplore.ieee.org/

Fig. 25. Bases de datos científicas empleadas.

Al elegir estas BD, el objetivo era recopilar únicamente artículos que hayan sido revisados por pares y publicados en fuentes reconocidas como revistas científicas, conferencias, talleres, libros o simposios. Para realizar la búsqueda en estas BD, se utilizó la siguiente cadena de búsqueda:

"Information security" OR "Information security management system" OR "information security management system for cloud services" OR "ISO/IEC 27017" OR "ISMS".

Fig. 26. Cadena de búsqueda para la revisión de artículos.

Se seleccionaron cuidadosamente estas bases de datos para garantizar que la recopilación de artículos incluyera solo aquellos sometidos a revisión por pares, publicados en fuentes académicas de prestigio como revistas especializadas, conferencias académicas, talleres temáticos, libros reconocidos y simposios de relevancia en el campo. Para explorar estas bases de datos de manera efectiva, se empleó una cadena de búsqueda específica:

La selección de la cadena de búsqueda fue diseñada a partir de búsquedas piloto en las que se probaron diversos términos y acrónimos relacionados con la gestión de la seguridad de la información. Estas pruebas iniciales permitieron identificar las palabras clave más efectivas para recuperar artículos relevantes. Cabe destacar que la revisión bibliográfica

se llevó a cabo bajo limitaciones de tiempo, enfocándose en literatura publicada entre los años 2018 y 2022. Este marco temporal fue elegido para asegurar que la información recopilada fuera contemporánea y relevante para los avances recientes en el campo.

Después de obtener método de búsqueda con artículos de las BDs, el siguiente paso fue examinar su notabilidad.

La fase inicial de este proceso consistió en evaluar la pertinencia de los artículos basándose en sus títulos. Aquellos artículos cuyos títulos indicaban claramente que no eran relevantes para el estudio fueron descartados de inmediato. Durante esta evaluación, se observó que algunos de los artículos recuperados mediante el protocolo de búsqueda no estaban relacionados con la gestión de la SI. En los casos donde la relevancia no podía determinarse fácilmente a partir del título, los artículos se trasladaban a la siguiente etapa para una selección más detallada. Este enfoque garantizaba que solo los artículos potencialmente valiosos avanzaran en el proceso de revisión, optimizando así el uso del tiempo y los recursos disponibles.

En la segunda fase del proceso de selección, se procedió a la lectura de los resúmenes de los artículos que superaron la fase previa. Se aplicaron criterios varios de exclusión para filtrar los artículos, descartando aquellos que: (1) no fueran revisados por pares, como entrevistas, anuncios de prensa o artículos de opinión, etcétera; (2) no tenían el texto completo en total disponibilidad; (3) no tenían un enfoque principal en la gestión de la SI; (4) eran duplicados de otros artículos científicos; (5) no estaban escritos en inglés; (6) habían sido retractados. Los artículos que superaron estos criterios de exclusión y que demostraron un enfoque claro en la gestión de la SI avanzaron a las siguientes etapas del proceso de revisión, garantizando así la relevancia y calidad de los estudios seleccionados. Esta metodología aseguraba que solo las investigaciones más pertinentes y rigurosas fueran consideradas para el análisis final, optimizando así la validez y utilidad de los resultados obtenidos.

La tercera fase del proceso consistió en organizar los artículos de investigación relevantes según la metodología descrita por Kitchenham y Charters. En esta etapa, se extrajeron palabras clave y conceptos de los resúmenes de los artículos que reflejaban sus aportaciones a la gestión de la seguridad de la información. Basándose en estas palabras clave, se agruparon los artículos en varias categorías temáticas. Una vez agrupados, se realizó una lectura detallada de cada artículo para confirmar su clasificación inicial. Si durante esta revisión más profunda se encontraba que un artículo se ajustaba mejor a una categoría diferente, se actualizaba su clasificación en consecuencia. Este enfoque no solo aseguraba una correcta categorización de los artículos, sino que también permitía identificar patrones y tendencias dentro de la literatura, facilitando una comprensión más estructurada y exhaustiva del campo de la gestión de la seguridad de la información. Además, este método riguroso garantizaba que cada artículo se ubicara en la categoría más adecuada, lo que ayudaba a destacar las áreas clave de investigación y las contribuciones más significativas dentro del dominio estudiado.

A veces, se estableció una nueva clase de observarse que, dicho artículo no se articula en ninguna de las clases preexistentes. En el proceso mapeado de los artículos el resultado es trascendental y relevante en varias categorías diversas.

Durante la etapa cuatro del proceso, se llevó a cabo una exhaustiva revisión de la información procedente de diversos estudios sistemáticos, abordando las preguntas de investigación planteadas. Se recopilaron siete aspectos clave de cada artículo investigado, incluyendo datos como autor, año de publicación, entre otros. Estos datos se presentan detalladamente en la siguiente tabla, proporcionando un resumen completo de la información extraída:

TABLA XXIII.

Elementos claves extraídos de los artículos científicos seleccionados

Nª	Elementos de datos	Detalle
1	Autor	Autor(es)
2	Año	Año de la publicación del artículo.
3	Título	Nombre de la publicación.
4	País	País de la publicación.
5	Fuente	Revista, Conferencia, Simposios.
6	Base de Datos	Base de Datos dende se encontró el artículo.
7	Procedencia	Universidad, institución, etcétera.

Nota. Fuente: elaboración propia.

Utilizando el protocolo de búsqueda, se recuperaron un total de 2216 artículos de bases de datos científicas. Tras una primera selección basada en los títulos, se excluyeron 1121 artículos anteriores al año 2018, quedando 412 para una nueva revisión. Posteriormente, se excluyeron los artículos no relacionados con la gestión de la seguridad de la información. Al final del proceso, se seleccionaron 15 artículos para su inclusión en el estudio, como se detalla en la siguiente figura:

El análisis de la información extraída de estos 15 artículos científicos permitió determinar la existencia de un estándar (01) para la gestión de la SI en entornos CC, el mismo que se encuentra identificado en la siguiente tabla:

TABLA XXIV.

Estándar internacional extraído de los artículos científicos

N°	Estándar	Denominación	Estatus	Fecha de Publicación
1	ISO/IEC 27017	“Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para los servicios en la nube” [47].	Publicada	2015-12

Nota. Fuente: elaboración propia.

Dicho lo anterior, lo que se pretendía era el desarrollo de un SGSI de servicios en la nube, por lo que era necesario que dicho SGSI se encuentre fundamentado en estándares internacionales y que, en este caso concreto, ayude al propósito de la mejora de la SI en instituciones públicas de salud peruanas, por lo que se optó por diseñar el SGSI fundamentado en la ISO/IEC 27017 para el caso de estudio.

Respecto a esta ISO, la ISO/IEC 27017:2015 suministra pautas para la SI aplicables a la gestión de seguridad en entornos CC, y su objetivo es ayudar a las organizaciones a proteger la confidencialidad, la integridad y la disponibilidad de las informaciones almacenada en la nube.

La norma ISO/IEC 27017:2015 no presenta controles nuevos en comparación con las normas anteriores de SI, sino que se centra en cómo aplicar esos controles específicamente en entornos CC. En lugar de introducir conceptos completamente nuevos en seguridad, ofrece recomendaciones y controles adicionales para el abordaje de los riesgos únicos ligados con la utilización de servicios CC.

Por lo tanto, no hay "controles nuevos" en la ISO/IEC 27017 en el sentido de que se introduzcan conceptos completamente nuevos en seguridad de la información, sino más bien una orientación sobre cómo aplicar los controles existentes en entornos CC.

Control N°	Descripción
CLD 6.3.1	“Este control se refiere a alguna medida específica relacionada con la gestión de accesos en la nube. Por ejemplo, podría abordar cómo se administran y controlan los accesos a los recursos en la nube, como las aplicaciones o los datos almacenados en ella. Es probable que el control incluya directrices sobre quién puede acceder a qué información, cómo se autentican los usuarios, cómo se gestionan los privilegios de acceso y cómo se monitorizan y auditan los accesos para detectar posibles amenazas o abusos” [54].
CLD 8.1.5	“Este control se refiere a la gestión de incidentes de seguridad en la nube. Podría establecer directrices sobre cómo detectar, reportar, investigar y responder a incidentes de seguridad que ocurran en un entorno de computación en la nube. Esto podría incluir la implementación de procedimientos de respuesta a incidentes, la designación de responsables de seguridad, la notificación de incidentes a las partes relevantes y la realización de análisis de causa raíz para prevenir futuros incidentes similares. En resumen, este control podría ayudar a garantizar una respuesta adecuada y eficaz ante posibles incidentes de seguridad en la nube, como lo especifica la norma ISO/IEC 27017” [54].
CLD 9.5.1	“Este control se refiere a la gestión de la seguridad de la información en la nube en relación con la auditoría y el monitoreo. Podría establecer directrices sobre cómo realizar auditorías regulares de seguridad en la nube, así como sobre cómo monitorear continuamente los sistemas y datos en la nube para detectar posibles brechas de seguridad o actividades sospechosas. Esto podría incluir la implementación de herramientas de monitoreo, la revisión periódica de registros de actividad, la generación de informes de auditoría y la respuesta adecuada a las alertas de seguridad. En resumen, este control podría ayudar a garantizar que la seguridad en la nube se mantenga constantemente vigilada y actualizada según lo establecido por la norma ISO/IEC 27017” [54].
CLD 9.5.2	“Este control se refiere la respuesta ante incidentes de seguridad en la nube. Podría establecer directrices sobre cómo gestionar y responder a incidentes de seguridad

cuando ocurren en un entorno de computación en la nube. Esto podría incluir la implementación de procedimientos de respuesta a incidentes específicos para la nube, la designación de un equipo de respuesta a incidentes, la realización de simulacros de incidentes, la comunicación con proveedores de servicios en la nube y otras partes interesadas, y la revisión posterior a los incidentes para mejorar los procesos de respuesta en el futuro. En resumen, este control podría ayudar a garantizar que las organizaciones estén preparadas para manejar eficazmente los incidentes de seguridad en la nube, según lo establecido por la norma ISO/IEC 27017" [54].

CLD 12.1.5 "Este control se refiere a la gestión de cambios en el entorno de la nube. Puede establecer directrices sobre cómo gestionar y controlar los cambios en los servicios, sistemas y configuraciones en la nube de manera segura. Esto podría incluir procedimientos para evaluar el impacto de los cambios, obtener autorización antes de implementar cambios significativos, llevar registros de cambios realizados, realizar pruebas de seguridad antes y después de los cambios, y garantizar que los cambios no introduzcan vulnerabilidades en el entorno de la nube. En resumen, este control ayudaría a garantizar que los cambios en la nube se realicen de manera segura y controlada, según lo establecido por la norma ISO/IEC 27017" [54].

CLD 12.4.5 "Este control se refiere a la seguridad de los datos en tránsito en la nube. Podría establecer directrices sobre cómo proteger la información mientras se mueve de un lugar a otro dentro de la infraestructura de la nube. Esto podría incluir la encriptación de datos durante la transferencia, el uso de conexiones seguras como SSL/TLS, el uso de redes privadas virtuales (VPN) para comunicaciones seguras, y la implementación de medidas para prevenir la interceptación no autorizada de datos en tránsito. En resumen, este control se centra en garantizar la seguridad de los datos mientras se transmiten entre diferentes componentes de la infraestructura de la nube, como lo especifica la norma ISO/IEC 27017" [54].

CLD 13.1.4 "Este control se refiere a la gestión de incidentes de seguridad en la nube. Podría establecer directrices sobre cómo detectar, notificar, investigar y responder a incidentes de seguridad en la nube. Esto podría incluir la implementación de procedimientos de respuesta a incidentes, la designación de responsables de seguridad, la realización de análisis de causa raíz para prevenir futuros incidentes similares y la mejora continua de los procesos de respuesta a incidentes. En resumen, este control podría ayudar a garantizar que las organizaciones estén preparadas para manejar de manera eficaz y adecuada los incidentes de seguridad en la nube, como lo especifica la norma ISO/IEC 27017" [54].

Nota. Adaptado de [54].

En esta investigación, se tomó como caso de estudio al Ministerio de Salud ya que, es una institución pública de salud peruana, que era justamente el contexto de estudio que se requería, era una institución a la que se tenía acceso y permiso para desarrollar la investigación. A continuación, se muestra info relevante de dicha organización:

Nombre: Ministerio de Salud

Nombre Comercial: MINSA

RUC: 20131373237

Dirección: Av. Salaverry N° 801, Jesús María, Lima, Lima

Fecha de inicio de actividades: 05/10/1935

Actividades Económicas:

- Principal - 8411 – "Actividades de la administración pública en general" (SUNAT, 2022).

- Secundaria 1 - 4772 – "Venta al por menor de productos farmacéuticos y médicos, cosméticos y artículos de tocador en comercios especializados" (SUNAT, 2022).

- Secundaria 2 - 8690 – "Otras actividades de atención de la salud humana" (SUNAT, 2022).

Fig. 27. Logo MINSA.

Acerca del Negocio: "Conducir eficientemente e íntegramente el Sistema Nacional Coordinado y Descentralizado de Salud basado en Redes Integradas de Salud, las políticas para asegurar universalmente a los peruanos en salud, y las acciones y políticas intersectoriales acerca de determinantes de naturaleza social; todo ello en beneplácito de la de todos los peruanos, más específicamente, a favor de su bienestar y salud" [55].

Misión: "Que el acceso al cuidado y la atención integral en salud individual y colectiva de las personas sea universal, independientemente de su condición socioeconómica y de su ubicación geográfica" [55].

Visión: "Nuestra visión es que en el año 2023 el acceso al cuidado y la atención integral en salud individual y colectiva de las personas sea universal, independientemente de su condición socioeconómica y de su ubicación geográfica" [55].

- Valores:
- Integridad
- Vocación de servicio
- Compromiso
- Imparcialidad
- Transparencia
- Innovación

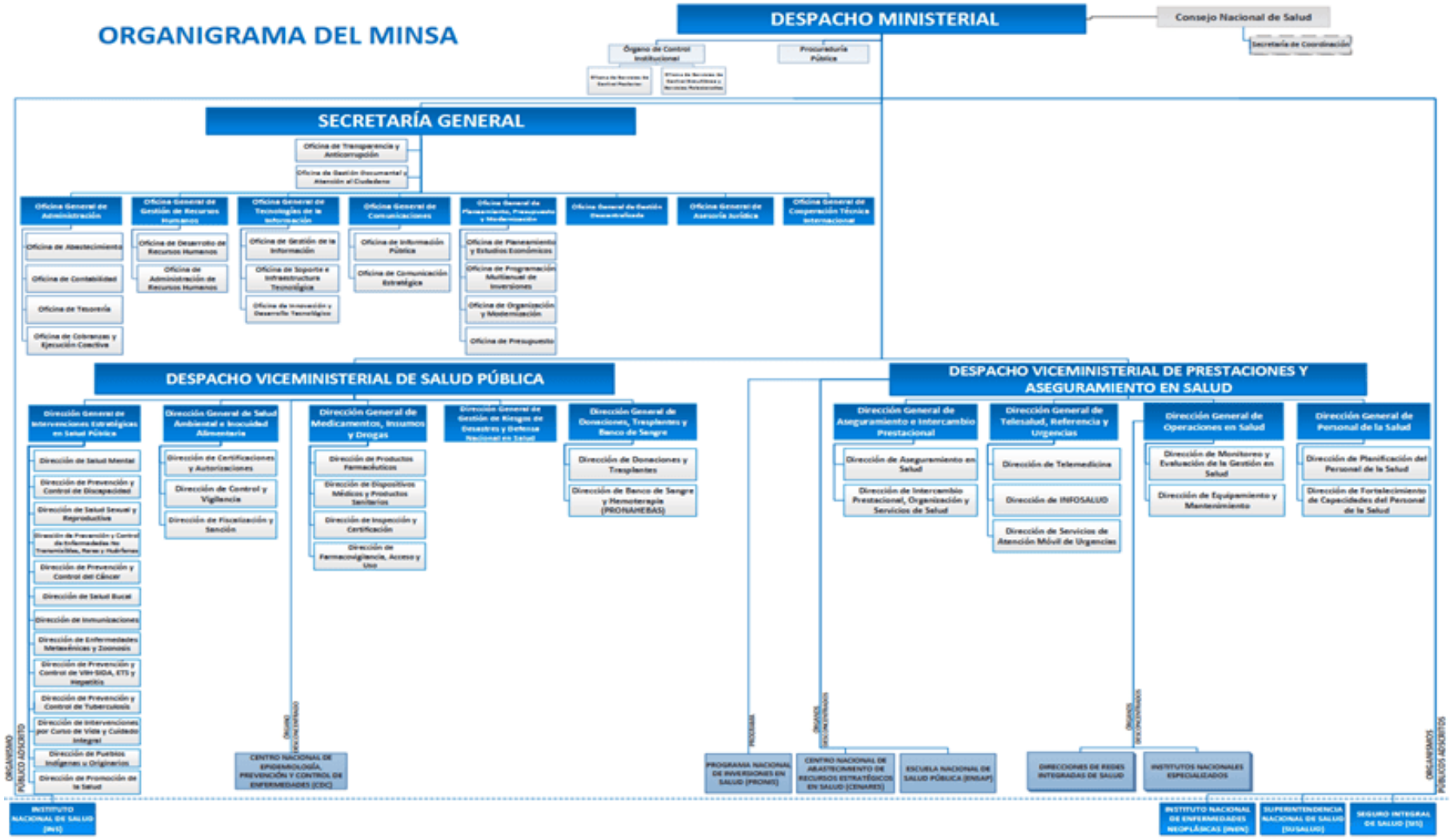


Fig. 28. Organigrama MINSA.

La alta dirección cuenta con tales órganos:

a. Despacho Ministerial

"Está a cargo del ministro de Salud, quien es la más alta autoridad política y ejecutiva del sector. Es el titular del pliego presupuestario y representa al Ministerio de Salud" [55]. A su vez cuenta con los siguientes órganos:

1. Consejo Nacional de Salud
2. Órgano de Control Institucional
3. Procuraduría Pública

b. Despacho Viceministerial de Salud Pública

"Está a cargo del viceministro de Salud Pública. Es el órgano de la Alta Dirección, responsable de proponer y conducir la implementación, la evaluación y la supervisión de la política sectorial de salud pública, así como las intervenciones de promoción y protección de la salud de la población" [55]. A su vez cuenta con los siguientes órganos:

1. "Dirección General de Intervenciones Estratégicas en Salud Pública (DIGIESP).
2. Dirección General de Salud Ambiental e Inocuidad Alimentaria (DIGESA).
3. Dirección General de Medicamentos, Insumos y Drogas (DIGEMID).
4. Dirección General de Gestión del Riesgo de Desastres y Defensa Nacional en Salud (DIGERD).

5. Dirección General de Donaciones, Trasplantes y Banco de Sangre (DIGDOT).

6. Órgano desconcentrado

7. Centro Nacional de Epidemiología, Prevención y Control de Enfermedades (CDC)" (MEF, 2022)

c. Despacho Viceministerial de Prestaciones y Aseguramiento en Salud

"Está a cargo del viceministro de Prestaciones y Aseguramiento en Salud. Es el órgano de la Alta Dirección, responsable de formular, proponer, coordinar, conducir, evaluar y supervisar la implementación de la política sectorial relacionada a la organización, gestión y funcionamiento de la prestación de servicios de salud, así como al acceso a la atención, al aseguramiento, a la infraestructura, a las tecnologías sanitarias y al desarrollo de los recursos humanos en salud" [55]. A su vez cuenta con los siguientes órganos:

1. "Dirección General de Aseguramiento e Intercambio Prestacional.

2. Dirección General de Telesalud, Referencia y Urgencias.

3. Dirección General de Operaciones en Salud.

4. Dirección General de Personal de la Salud.

5. Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud (CENARES).

6. Escuela Nacional de Salud Pública (ENSAP).

7. Escuela Nacional de Inversiones en Salud (PRONIS).

8. Unidad Funcional de Gestión de la Calidad” (MEF, 2022)

d. Secretaría General

“Es el órgano de la Alta Dirección, responsable de la coordinación y supervisión de la gestión de los sistemas administrativos en el Ministerio de Salud y de los órganos de administración interna bajo su competencia” (MINSA, 2020). A su vez cuenta con los siguientes órganos:

1. “Oficina de Transparencia y Anticorrupción (OTRANS).
2. Oficina de Gestión Documental y Atención al Ciudadano.
3. Oficina General de Planeamiento, Presupuesto y Modernización.
4. Oficina General de Gestión Descentralizada.
5. Oficina General de Asesoría Jurídica.
6. Oficina General de Cooperación Técnica Internacional.
7. Oficina General de Administración.
8. Oficina General de Gestión de Recursos Humanos.
9. Oficina General de Tecnologías de la Información.
10. Oficina General de Comunicaciones.
11. Unidad Funcional de Gestión de Dialogo Laboral” (MEF, 2022)

Asimismo, en cuanto a personal, el MINSA, según Resolución Secretarial N° 187-2021-MINSA cuenta con 1637 colaboradores (CAS y nombrados) distribuidos en los diversos órganos anteriormente mencionados.

Por otra parte, se identificaron los procesos del MINSA, los cuales se visualizan aquí:

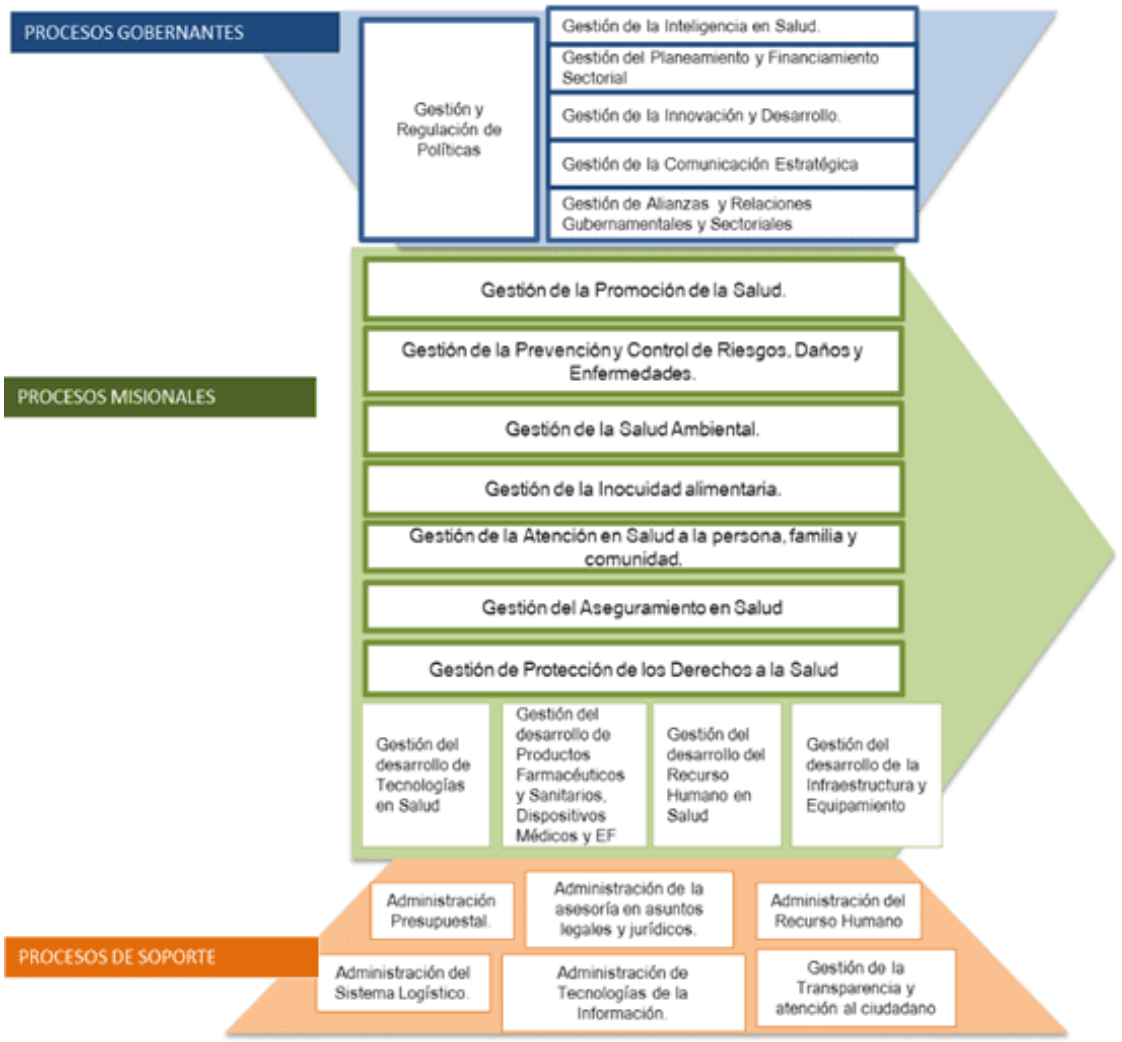


Fig. 29. Mapa de procesos del MINSA.

A. GOBERNANTES

“Los procesos gobernantes del MINSA son los procedimientos y mecanismos establecidos por el Ministerio de Salud (MINSA) para supervisar, regular y dirigir las actividades relacionadas con la salud pública y la prestación de servicios de salud en un país. Estos procesos incluyen la formulación de políticas de salud, la planificación estratégica, la asignación de recursos, la supervisión de la calidad de los servicios de salud y la coordinación entre diferentes instituciones y actores del sector salud. En resumen, son las acciones organizativas y de control que el Ministerio de Salud utiliza para asegurar que se cumplan los objetivos y estándares en el ámbito de la salud pública y la atención médica” [56]. Estos son:

- Gestión y regulación de políticas
- Gestión de la inteligencia en salud
- Gestión del planeamiento y financiamiento sectorial
- Gestión de innovación y desarrollo
- Gestión de la comunicación estratégica
- Gestión de alianzas y relaciones gubernamentales y sectoriales

B. MISIONALES

“Los procesos misionales del Ministerio de Salud (MINSA) constituyen el conjunto de actividades centrales y fundamentales destinadas a cumplir con la misión principal y los objetivos estratégicos de la institución en el ámbito de la salud pública y la atención médica. Estas actividades representan la esencia de la labor del MINSA y están dirigidas a promover, proteger y mejorar la salud de la población, así como a garantizar la disponibilidad y calidad

de los servicios de salud. Incluyen la planificación y ejecución de programas de prevención de enfermedades, la supervisión de la calidad y seguridad de los servicios de salud, la promoción de estilos de vida saludables, la respuesta a emergencias sanitarias, entre otras acciones clave. En resumen, los procesos misionales del MINSA son los pilares fundamentales que sustentan su contribución a la salud y el bienestar de la sociedad" [56]. Estos son:

- "Gestión de la promoción de la salud
- Gestión de la prevención y control de riesgos, daños y enfermedades
- Gestión de la salud ambiental
- Gestión de la inocuidad alimentaria
- Gestión de la atención en salud a la persona, familia y comunidad
- Gestión del aseguramiento en salud
- Gestión de protección de los derechos a la salud
- Gestión del desarrollo de tecnologías en salud
- Gestión del desarrollo de productos farmacéuticos y sanitarios, dispositivos médicos y EF
- Gestión del desarrollo del recurso humano en salud
- Gestión del desarrollo de la infraestructura y equipamiento" [56].

C. SOPORTE

“Los procesos de soporte del Ministerio de Salud (MINSA) abarcan una serie de actividades y funciones que actúan como cimientos fundamentales para respaldar y facilitar la ejecución eficiente de las operaciones y objetivos centrales de la institución en el campo de la salud pública y la prestación de servicios de salud. Estos procesos proporcionan los recursos, la infraestructura y el respaldo necesarios para asegurar que las actividades principales del MINSA puedan llevarse a cabo de manera óptima. Engloban áreas como la gestión de recursos humanos, la administración financiera, la adquisición de suministros y equipos médicos, la tecnología de la información, así como la comunicación institucional, todas esenciales para el desarrollo efectivo de las funciones ministeriales. En síntesis, los procesos de soporte son los pilares sobre los cuales descansa y se sustenta la labor esencial del MINSA en la promoción y salvaguarda de la salud pública” [56]. Estos son:

- “Administración presupuestal
- Administración de la asesoría en asuntos legales y jurídicos
- Administración del Recurso Humano
- Administración del Sistema Logístico
- Administración de Tecnologías de la Información
- Gestión de la Transparencia y atención al ciudadano” [56].

Luego, se establecieron parámetros de evaluación conforme a los estándares establecidos en la normativa correspondiente, con el objetivo de identificar los procesos más significativos dentro del ámbito del MINSA. A continuación, se detallan los criterios de evaluación utilizados en este proceso de selección:

TABLA XXV.

Criterios de evaluación de los procesos

Nª	Elementos de datos	Detalle
C1	Valor estratégico del proceso	Es una valoración acerca del proceso que genere un impacto importante en la institución.
C2	Criticidad de los activos	Es una valoración acerca de los activos de información involucrados.
C3	Importancia operatividad y comercial	Es una valoración de la confidencialidad, integridad y disponibilidad operativa y comercial de los procesos.
C4	Expectativas y percepciones	Es una valoración sobre las expectativas y percepciones de las partes interesadas y voluntad y la reputación de la institución.

Nota. Fuente: elaboración propia

Tras establecer los parámetros para evaluar la importancia, se ejecutó la evaluación de los procesos del MINSA. Se aplicó una escala de evaluación para identificar los procesos más relevantes dentro del MINSA mostrada a continuación:

- 1 = Débil
- 2 = Leve
- 3 = Normal
- 4 = Moderado
- 5 = Fuerte

Se continua con la muestra las valoraciones creadas a dada uno de los procesos del MINSA:

TABLA XXVI.

Resultados de la evaluación de los procesos gobernantes del MINSA

Código	Proceso	C01	C02	C03	C04	Sumatoria
(PG-01)	Gestión y regulación de políticas	3	3	3	3	12
(PG-02)	Gestión de la inteligencia en salud	3	4	4	3	14
(PG-03)	Gestión del planeamiento y financiamiento sectorial	3	4	4	3	14
(PG-04)	Gestión de innovación y desarrollo	5	5	5	5	20
(PG-05)	Gestión de la comunicación estratégica	3	4	4	3	14
(PG-06)	Gestión de alianzas y relaciones gubernamentales y sectoriales	3	4	4	3	14
(PA-06)	Gestión de la transparencia y atención al ciudadano	3	4	4	3	14

La tabla previa retrata los resultados de una evaluación de los procesos gubernamentales del MINSA, empleando criterios de criticidad. Cada proceso fue evaluado en cuatro criterios, identificados como C01, C02, C03 y C04, con calificaciones que varían del 1 al 5, siendo 5 la puntuación más alta. La suma total de estas calificaciones se presenta en la columna "Sumatoria".

El PG-01 recibió calificaciones de 3 en todos los criterios, con una sumatoria de 12; el PG-02 obtuvo calificaciones de 3, 4, 4 y 3 en los criterios C01 a C04, respectivamente, sumando un total de 14; el PG-03, similar a PG-02, con calificaciones de 3, 4, 4 y 3, también sumando 14; el PG-04, destaca con las calificaciones más altas, obteniendo 5 en todos los

criterios, logrando la mayor sumatoria de 20; el PG-05, calificada con 3, 4, 4 y 3, respectivamente, alcanzando una sumatoria de 14 y; finalmente, PG-06, evaluado con calificaciones de 3, 4, 4 y 3, también con una sumatoria de 14.

De esta evaluación, se destaca que el proceso de "Gestión de innovación y desarrollo" (PG-04) es considerado el más crítico y mejor gestionado, dado que obtuvo la puntuación máxima en todos los criterios evaluados. Los otros procesos, aunque también críticos, presentan áreas de mejora según los criterios evaluados.

TABLA XXVII.

Resultados de la evaluación de los procesos misionales del MINSA

Código	Proceso	C01	C02	C03	C04	Sumatoria
(PM-01)	Gestión de la promoción de la salud	3	2	4	2	11
(PM-02)	Gestión de la prevención y control de riesgos, daños y enfermedades	3	4	4	3	14
(PM-03)	Gestión de la salud ambiental	3	4	4	3	14
(PM-04)	Gestión de la inocuidad alimentaria	3	4	4	3	14
(PM-05)	Gestión de la atención en salud a la persona, familia y comunidad	3	4	4	3	14
(PM-06)	Gestión del aseguramiento en salud	3	4	4	3	14
(PM-07)	Gestión de protección de los derechos a la salud	3	4	4	3	14
(PM-08)	Gestión del desarrollo de tecnologías en salud	5	5	5	5	20

(PM-09)	Gestión del desarrollo de productos farmacéuticos y sanitarios, dispositivos médicos y EF	3	4	4	3	14
(PM-10)	Gestión del desarrollo del recurso humano en salud	3	4	4	3	14
(PM-11)	Gestión del desarrollo de la infraestructura y equipamiento	3	4	4	3	14

La tabla previa retrata los resultados de la evaluación de los procesos misionales del MINSA, empleando criterios de criticidad. Cada proceso fue evaluado cuatro (04) criterios diferentes, identificados como C01, C02, C03 y C04, con calificaciones que varían del 1 al 5, siendo 5 la puntuación más alta La suma total de estas calificaciones se presenta en la columna "Sumatoria".

El PM-01 obtuvo calificaciones de 3, 2, 4 y 2 en los criterios evaluados, con una sumatoria total de 11, la más baja entre todos los procesos evaluados; el PM-02, recibió puntuaciones de 3, 4, 4 y 3, sumando un total de 14; PM-03, obtuvo calificaciones de 3, 4, 4 y 3, alcanzando una sumatoria de 14; el PM-04, fue evaluada con puntuaciones de 3, 4, 4 y 3, sumando 14 en total; el PM-05, recibió 3, 4, 4 y 3 en los criterios, sumando 14; el PM-06, obtuvo calificaciones de 3, 4, 4 y 3, alcanzando una sumatoria de 14; el PM-07, evaluado con 3, 4, 4 y 3, alcanzando una sumatoria de 14; el PM-08, destaca con las calificaciones máximas de 5 en todos los criterios evaluados, logrando una sumatoria perfecta de 20, lo que indica una alta criticidad y buen desempeño; el PM-09, obtuvo puntuaciones de 3, 4, 4 y 3, sumando un total de 14; el PM-10, recibió calificaciones de 3, 4, 4 y 3, alcanzando una sumatoria de 14 y; el PM-11, evaluado con 3, 4, 4 y 3, sumando 14 en total.

De esta evaluación, se puede observar que el proceso de "Gestión del desarrollo de tecnologías en salud" (PM-08) es el más crítico y mejor gestionado, dado que obtuvo la puntuación máxima en todos los criterios. Los demás procesos, aunque también críticos, presentan áreas de mejora según los criterios evaluados.

TABLA XXVIII.

Resultados de la evaluación de los procesos de soporte del MINSA

Código	Proceso	C01	C02	C03	C04	Sumatoria
(PS-01)	Administración presupuestal	3	4	4	3	14
(PS-02)	Administración de la asesoría en asuntos legales y jurídicos	3	2	4	2	11
(PS-03)	Administración del recurso humano	3	4	4	3	14
(PS-04)	Administración del sistema logístico	3	4	4	3	14
(PS-05)	Administración de tecnologías de la información	5	5	5	5	20
(PA-06)	Gestión de la transparencia y atención al ciudadano	3	4	4	3	14

La tabla previa retrata los resultados de la evaluación de los procesos de soporte del MINSA, empleando criterios de criticidad. Cada proceso fue evaluado cuatro (04) criterios diferentes, identificados como C01, C02, C03 y C04, con calificaciones que varían del 1 al 5, siendo 5 la puntuación más alta La suma total de estas calificaciones se presenta en la columna "Sumatoria".

El PS-01 recibió puntuaciones de 3, 4, 4 y 3 en los criterios, sumando un total de 14 puntos; el PS-02 obtuvo calificaciones de 3, 2, 4 y 2, alcanzando una sumatoria de 11, la más baja entre los procesos evaluados; el PS-03 fue evaluado con puntuaciones de 3, 4, 4 y 3, sumando un total de 14 puntos; el PS-04 recibió calificaciones de 3, 4, 4 y 3 en los criterios, alcanzando una sumatoria de 14 puntos; el PS-05 destacó con las puntuaciones máximas de 5 en todos los criterios evaluados, logrando una sumatoria perfecta de 20 puntos, lo que indica una alta criticidad y buen desempeño en este proceso y; el PS-06 obtuvo calificaciones de 3, 4, 4 y 3, sumando un total de 14 puntos.

De esta evaluación, se puede observar que el proceso de "Administración de tecnologías de la información" (PS-05) es considerado el más crítico y mejor gestionado, dado que obtuvo la puntuación máxima en todos los criterios. Los otros procesos, aunque también críticos, presentan áreas de mejora según los criterios evaluados.

Después de la valoración de la importancia de dichos procesos del MINSA, se decidió elegir los tres (03) procesos más destacados considerando la suma de la criticidad según criterios anticipadamente establecidos, como se detalla en la tabla siguiente:

TABLA XXIX.

Resultados generales de criticidad de los procesos del MINSA

Código	Proceso	Total
(PG-04)	Gestión de innovación y desarrollo	20
(PM-08)	Gestión del desarrollo de tecnologías en salud	20
(PS-05)	Administración de tecnologías de la información	20

Posterior a la selección de los tres (03) procesos de mayor criticidad según el análisis realizado en esta investigación, se procedió con la especificación de cada uno de ellos:

a. Proceso Gobernante: Gestión de innovación y desarrollo (PG-04)

Se refiere a “la estructura y conjunto de actividades establecidas por el Ministerio de Salud para dirigir y fomentar la innovación y el progreso en el ámbito de la salud pública y la atención médica. Este proceso implica la creación de políticas, estrategias y programas destinados a promover la innovación en el sector de la salud, así como a impulsar el desarrollo de nuevas tecnologías, métodos de tratamiento, políticas de prevención y modelos de atención médica. En términos más simples, este proceso se encarga de impulsar nuevas ideas y enfoques en el campo de la salud para mejorar la calidad de los servicios y la atención a la población” [56].

b. Proceso Misional: Gestión del desarrollo de tecnologías en salud (PM-08)

Se refiere a “la estructura y conjunto de actividades implementadas por el Ministerio de Salud para supervisar y fomentar el avance tecnológico en el ámbito de la salud. Este proceso implica la planificación, evaluación y coordinación de iniciativas relacionadas con la creación y aplicación de nuevas tecnologías médicas, equipos y sistemas de información destinados a mejorar la atención médica y el manejo de enfermedades. Esencialmente, este proceso busca facilitar la introducción y el uso efectivo de innovaciones tecnológicas para mejorar la salud y el bienestar de la población” [56].

c. Proceso de Soporte: Administración de tecnologías de la información (PS-05)

Se refiere a “la organización y las acciones establecidas por el Ministerio de Salud para supervisar y gestionar los recursos informáticos. Esto incluye la planificación, implementación, mantenimiento y seguridad de sistemas, redes y software utilizados para

respaldar las actividades del MINSA en salud pública y atención médica. Básicamente, este proceso se encarga de asegurar el correcto funcionamiento de las tecnologías de la información que utiliza el Ministerio de Salud en su día a día” [56].

A continuación, se muestran las fichas técnicas del Proceso Nivel 0 de cada uno de los tres (03) procesos seleccionados:

FICHA TÉCNICA DEL PROCESO NIVEL 0: GESTIÓN DE LA INNOVACIÓN Y DESARROLLO			
1) Nombre	Gestión de la Innovación y Desarrollo.	**4) Responsable**	Órgano de asesoramiento
2) Objetivo	Lograr innovaciones institucionales y mejoras organizacionales en la gestión sectorial que favorezcan la modernización de las instituciones del Sector para la consecución de sus resultados.	**5) Requisitos**	• DS Nº 004-2013-PCM – PNMGP • Ley Nº26842, Ley General de Salud.
3) Alcance	Comprende la implantación de modelos institucionales, organizacionales, modelos de innovación de procesos y gestión de la calidad de los procesos organizacionales del Sector, la investigación e identificación de mejoras y la certificación de procesos bajo estándares de calidad.	**6) Clasificación**	Gobernante

DESCRIPCIÓN DEL PROCESO				
7) Proveedores	**8) Entradas**	**9) Procesos nivel 1**	**10) Salidas**	**11) Ciudadano o Destinatario de los bienes y servicios**
• MINSA (Proceso Planeamiento Estratégico) • MINSA (todos los procesos gobernantes y misionales) • Gobiernos Regionales – DIRESAS • PCM	• Políticas Públicas sectoriales e institucionales aprobadas • Visión y Misión Sectorial e institucional • Planes de Largo, Mediano y Corto Plazo en Salud. • Reporte de cumplimiento de los objetivos de los planes. • Proyectos y programas priorizados, elaborados y viables • Resultados de los indicadores de impacto de las políticas en la población. • Resultados de la eficiencia del MINSA • Identificación de necesidades de mejora en regiones • Lineamientos del sistema de modernización de la gestión pública de PCM	• Diseño e implementación de modelos organizacionales del sector y la institución • Innovación y mejora de la gestión de procesos sectoriales e institucionales	• Modelos organizacionales • Mapas y manuales de procesos sectoriales e institucionales • Propuestas de procesos de mejora, simplificación e innovación • Procesos sectoriales certificados • Instrumentos de gestión actualizados • Lineamientos y estrategias de modernización institucional y sectorial • Normas técnicas y acciones de asistencia técnica	• MINSA (todos los procesos gobernantes y misionales) • Gobiernos Regionales – DIRESAS

EVIDENCIAS E INDICADORES DEL PROCESO
12) Indicadores
• Número de proyectos de mejora de procesos priorizados e implementados en la cadena de valor sectorial. • Impacto de las mejoras organizacionales implementadas en la eficiencia del MINSA y el cumplimiento de objetivos.

Fig. 30. Ficha técnica del proceso gobernante “Gestión de la Innovación y Desarrollo”.

FICHA TÉCNICA DEL PROCESO NIVEL 0: GESTIÓN DEL DESARROLLO DE TECNOLOGÍAS EN SALUD.					
1) Nombre	Gestión del desarrollo de Tecnologías en Salud	**4) Responsable**	Viceministerio de Salud Pública / Instituto Nacional de Salud		
2) Objetivo	Lograr la incorporación de tecnologías sanitarias adecuadas, de calidad y actualizadas para la mejora de los servicios de salud	**5) Requisitos**	• Ley Nº26842, Ley General de Salud, Título XV. • Ley N°29973, Ley General de la Persona con Discapacidad, Art. 34° • Decreto Legislativo 1161, Art. 3°, núm. 9 • Decreto Legislativo 1168, Art. 5°		
3) Alcance	Comprende la conducción de la política nacional y sectorial referente al desarrollo de tecnologías en salud (bancos de sangre, donación de órganos, tejidos y células, sistemas de diagnósticos por imágenes, medicamentos y vacunas) que asegure su innovación, evaluación y transferencia, el establecimiento de la regulación, la definición de estándares, la supervisión del cumplimiento de la política, y la fiscalización de laboratorios de salud pública a nivel nacional. *La implementación de algunos procesos de nivel 1 del MINSA se vinculan a los procesos del INS.			**6) Clasificación**	Misional

DESCRIPCIÓN DEL PROCESO				
7) Proveedores	**8) Entradas**	**9) Procesos nivel 1**	**10) Salidas**	**11) Ciudadano o Destinatario de los bienes y servicios**
• MINSA (Proceso Planeamiento Estratégico) • MINSA (Proceso Inteligencia en Salud) • MINSA (Gestión de la Atención en Salud) • IGSS • INS • Gobiernos Regionales – DIRESAS • CONCYTEC	• Políticas Públicas sectoriales e institucionales aprobadas • Planes de Largo, Mediano y Corto Plazo en Salud. • Sistemas de información articulados y confiables. • Propuestas de política y regulación en tecnologías en salud • Informes de necesidades en tecnologías en los servicios de salud • Propuesta de Plan Multianual de Desarrollo y Transferencia Tecnológica desde el INS • Políticas y regulación en materia de transferencia tecnológica de CONCYTEC	• Implementación y supervisión de Laboratorios de Salud. • Desarrollo de Bancos de Sangre • Desarrollo de la Donación de Órganos, Tejidos y Células. • Desarrollo de Sistemas de Diagnóstico por Imágenes. • Desarrollo de Medicamentos y Vacunas • Investigación en desarrollo de Tecnologías en Salud.	• Propuesta de política en materia de tecnologías en salud del INS revisada • Lineamientos y normas técnicas de desarrollo de tecnologías en salud • Plan Multianual de Desarrollo y Transferencia Tecnológica • Estándares de calidad • Informe situacional en tecnologías en salud • Acciones de comunicación social en materia de donación de órganos, tejidos y células. • Autorizaciones y acreditaciones para el funcionamiento de bancos de sangre y para la donación de tejidos, órganos y células. • Informes del desempeño del INS	• MINSA (Proceso Gestión de Políticas y Regulación) • Gobiernos Regionales – DIRESAS • IGSS • SUSALUD • INS • MINSA (Proceso Gestión de Inteligencia en Salud)

EVIDENCIAS E INDICADORES DEL PROCESO
12) Indicadores
• Incremento del porcentaje de tecnologías sanitarias de calidad incorporadas a los servicios de salud.

Fig. 31. Ficha técnica del proceso misional “Gestión del Desarrollo de Tecnologías en Salud”.

FICHA TÉCNICA DEL PROCESO NIVEL 0: ADMINISTRACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN					
1) Nombre	Administración de Tecnologías de la Información.	**4) Responsable**	Secretaria General.		
2) Objetivo	Garantiza la calidad, oportunidad y seguridad de los recursos tecnológicos del MINSA.	**5) Requisitos**	• Ley Nº29158, Ley Orgánica del Poder Ejecutivo. • D.S. N° 004-2013-PCM		
3) Alcance	Comprende las acciones de soporte para el diseño, implementación, mantenimiento del recurso tecnológico de la institución, asegurando su suficiencia, relevancia, calidad, oportunidad y seguridad de los software y plataformas.	**6) Clasificación**	Soporte.		
DESCRIPCIÓN DEL PROCESO					
7) Proveedores	**8) Entradas**	**9) Procesos nivel 1**	**10) Salidas**	**11) Ciudadano o Destinatario de los bienes y servicios**	
• Direcciones, oficinas y unidades del MINSA • DISA Lima Metropolitana	• Plan Estratégico de Tecnologías de Información (PETI). • Requerimiento TIC de las unidades orgánicas. • Requerimientos de información de las unidades orgánicas. • Propuesta de solución TIC aprobada. • Matriz de requerimientos • Prototipos de alto nivel • Arquitectura de TI a alto nivel • Pacto colectivo • Estímulos, beneficios y servicios dictaminados y/o gestionados. • Reporte trimestral de pago de primas (gastos médicos y de vida)	• Diseñar y regular el uso de tecnologías. • Formular propuesta de soluciones tecnológicas • Desarrollar Soluciones Tecnológicas • Controlar la operatividad de las TIC.	• TIC • Propuesta de solución TIC. • Solución Tics • Requerimientos técnicos • Especificación de Casos de Uso del Sistema • Diseño Detallado de Software • Arquitectura de Software • Arquitectura de Tecnologías de Información • Manuales • Plan de Capacitación Técnica • Modelamiento de Negocio. • Requerimiento atendido • Informe de monitoreo y control • Acta de conformidad del usuario • Manual de Usuario • Manual del Sistema • Manual de Operaciones • Informe de mantenimiento	• Direcciones, oficinas y unidades del MINSA • DISA Lima Metropolitana	
EVIDENCIAS E INDICADORES DEL PROCESO					
12) Indicadores					
• % de los Órganos del MINSA con sistemas tecnológicos en operación y respondiendo a las demandas.					

Fig. 32. Ficha técnica del proceso de soporte “Administración de Tecnologías de la Información”.

Tras la identificabilidad de aquellos procesos más críticos dentro del ámbito del MINSA, se llevó a cabo un re-levamiento de inventario de activos por área, con el propósito de efectuar un diagnóstico más exhaustivo de los recursos disponibles en esta institución estatal

Después de completar el diagnóstico inicial, quedó claro que el principal obstáculo en materia de SI en el MINSA es la ausencia de una gestión efectiva de medidas preventivas, especialmente en lo que respecta a los servicios en la nube. Por consiguiente, resulta crucial implementar un SGSI fundamentado en la normativa ISO/IEC-27017 con propósitos de elevar el nivel de SI en esta institución pública peruana, la cual se considera como un caso de estudio.

TABLA XXX.

Causas y efectos de la deficiente gestión de la seguridad de la información en el MINSA

Problemática	**Causas**	**Consecuencias**
Deficiente gestión de la seguridad de la información en el MINSA	Desconocimiento de la peligrosidad de los ataques a la seguridad de la información en la nube	Infiltración de software maliciosos como Ransomware, Pishing, etcétera.
	No se codifica las cuentas de acceso	Pérdida de información valiosa
	Falta de sensibilización en cuanto a los riesgos a la SI en la nube	No se forman hábitos de preservación de la seguridad de la información
	Falta de un plan de renovación de equipos para la continuidad operativa de la organización	Deficiente gestión de activos informáticos
	Carencia de acuerdos basados en la confidencialidad	Pérdidas de información por la nula regulación de la confidencialidad

Para desarrollar el SGSI, se requirió utilizar una metodología para la gestión de riesgos de información. Por ende, se desplegó una RSL para identificar metodologías disponibles en esta área. Esto condujo a la búsqueda de investigaciones sobre estas metodologías, lo que resultó en la identificación de los estudios mencionados a continuación:

TABLA XXXII.

Estudios acerca de metodologías para la gestión de riesgos de la seguridad de la información

N°	Autor	Año	Metodologías identificadas
1	Gritzalis et al.	2021	“EBIOS, MEHARI, OCTAVE, IT-Grundschutz, MAGERIT, CRAMM, HTRA, NIST SP800, RiskSafe, CORAS, COBIT” (Gritzalis et al., 2021).
2	Acevedo & Satizábal	2016	“OCTAVE, CORAS, Australian ST, NTC-ISO/IEC 27005, CRAMM, MAGERIT, NIST Risk Management Methodology for IT systems, IDB Methodology, NIST Malware Incident Prevention Methodology” (Acevedo & Satizábal, 2016).
3	Macedo & Da Silva	2012	“OCTAVE, MEHARI, MAGERIT, IT-Grundschutz, EBIOS, IRAM, SARA, SPRINT, ISO 27005, NIST SP800-30, CRAMM, MIGRA, MAR, ISAMM, GAO/AIMD-00-33, IT System Security Assessment, MG-2 and MG-3, Security Risk Management Guide, Dutch A&K Analysis, MARION, Austrian IT Security Handbook, Microsoft's security risk management guide, RiskIT” (Macedo & Da Silva, 2012)
4	Syalim et al.	2009	“MEHARI, MAGERIT, NIST800-30, Microsoft's Security Management Guide” (Syalim et al., 2009)

Nota. Fuente: elaboración propia.

Como se pudo revelar en la tabla anterior, sí existen evidencias de metodologías que gestionen los riesgos de la información.

TABLA XXXIIII.

Comparación de metodologías para la gestión de riesgos de seguridad de la información existentes en la literatura

Metodología	Enfoque	Desarrollado por	Principales características	Identifica Riesgos	Tipo
MAGERIT	Basado en análisis de riesgos y evaluación de impacto	Centro Cristológico Nacional (CCN)	Proporciona un enfoque para la gestión de riesgos de seguridad de la información que incluye la identificación de activos, amenazas y vulnerabilidades, así como la evaluación de impacto y la selección de medidas de seguridad adecuadas.	Sí	Metodología
NIST SP 800-30	Basado en la gestión de riesgos	National Institute of Standards and Technology (NIST)	Ofrece pautas detalladas para la evaluación de riesgos de seguridad de la información, con un enfoque en la identificación, evaluación y mitigación de riesgos.	Sí	Metodología
OCTAVE	Participativo y centrado en activos críticos	Carnegie Mellon University	Se enfoca en la identificación de activos críticos, amenazas y vulnerabilidades, involucrando a las partes interesadas clave en el proceso de evaluación de riesgos.	Sí	Metodología

MEHARI	Estructurado y basado en análisis de riesgos	Club de la Seguridad de la Información Francesa (CLUSIF)	Utiliza un enfoque estructurado que abarca la identificación de activos, amenazas, vulnerabilidades y la evaluación de riesgos asociados, desarrollado por el CLUSIF.	Sí	Metodología
CRAMM	Detallado y centrado en sistemas de TI	CCTA Risk Analysis and Management Method	Se centra en la evaluación de riesgos de seguridad de la información en sistemas de tecnología de la información, utilizando un enfoque detallado que incluye la identificación de activos, amenazas, vulnerabilidades y controles de seguridad.	Sí	Metodología
FAIR	Cuantitativo y basado en análisis de factores	Factor Analysis of Information Risk (FAIR)	Permite cuantificar y gestionar riesgos de seguridad de la información de manera objetiva, evaluando factores como la frecuencia y el impacto de los eventos de riesgo para determinar la exposición al riesgo y las medidas de mitigación adecuadas.	Sí	Metodología
CORAS	Orientado a objetos y análisis de sistemas	SINTEF	Se centra en la identificación y análisis de riesgos en sistemas complejos de información, utilizando un enfoque orientado a objetos para modelar activos, amenazas y vulnerabilidades, y evaluar los riesgos asociados.	Sí	Metodología

Nota. Fuente, Adaptado de [23].

Tabla comparativa de Metodologías para la Implementación de un SGSI en Servicios en la Nube

CRITERIO	MARGERIT	NIST SP 800-30	OCTAVE	MEHARI	CRAMM	FAIR	CORAS
Enfoque	Gestión de riesgos	Gestión de riesgos	Gestión de riesgos	Gestión de riesgos	Gestión de riesgos	Gestión de riesgos	Gestión de riesgos
Compatibilidad con la nube	Adaptable a la nube	Adaptable a la nube	Adaptable a la nube	Adaptable a la nube	Adaptable a la nube	Adaptable a la nube	Adaptable a la nube
Código abierto	Si	No	No	No	No	No	No
Actualización	Baja	Media	Media	Media	Media	Alta	Alta
Curva de aprendizaje	Alta	Media	Media	Media	Media	Alta	Alta
Compatibilidad con herramientas EAR	Alta	Media	Media	Media	Media	Alta	Alta
Aplicabilidad en el contexto peruano	Alta	Media	Media	Media	Media	Media	Media
Facilidad de implementación	Alta	Media	Media	Media	Media	Media	Media
Enfoque en riesgos específicos	Si	Si	Si	Si	Si	Si	Si

Nota. Fuente: elaboración propia.

Tabla Comparativa con Puntajes

CRITERIO	MARGERIT	NIST SP 800-30	OCTAVE	MEHARI	CRAMM	FAIR	CORAS
Enfoque	9	8	8	8	7	8	8
Compatibilidad con la nube	8	8	8	8	8	8	8
Código abierto	10	6	6	6	6	6	6
Actualización	8	8	8	8	8	8	8
Curva de aprendizaje	8	7	6	6	6	5	5
Compatibilidad con herramientas EAR	8	7	7	7	7	8	8
Aplicabilidad en el contexto peruano	9	7	7	7	7	7	7
Facilidad de implementación	8	7	6	6	6	6	6
Enfoque en riesgos específicos	9	8	8	8	7	8	8
Puntaje promedio (total/9)	9	7	7	7	7	7	7

Nota. Fuente: elaboración propia.

Descripción de los Puntajes:

9-10=>Excelente

7-8=>Bueno

5-6=>Aceptable

1-4=>Necesita mejoras

De acuerdo a la tabla comparativa, MAGERIT se estableció la metodología más apropiada para desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) para servicios en la nube, siguiendo la norma ISO/IEC-27017. Su puntaje promedio de nueve (9) siendo su capacidad para identificar riesgos de seguridad, ser de código abierto, estar actualizada, ser compatible con herramientas de “Entorno de Análisis de Riesgos” (EAR), y su adaptabilidad al contexto peruano. Comparado con otras metodologías, MAGERIT ofrece una mejor combinación de estas características clave, lo que lo hace especialmente idóneo para fortalecer la seguridad en las instituciones de salud pública en el Perú

En relación con MAGERIT (por su acrónimo de “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”), esta metodología, originada en España, goza de un amplio uso y es de código abierto para la gestión de riesgos en concordancia activa con las normativas de la familia ISO/IEC-27k. Primariamente divulgada en 1997, MAGERIT se destaca por su facilidad de uso y aplicabilidad, lo que suele traducirse en resultados positivos en la gestión de riesgos. Además, puede emplearse como una herramienta de apoyo para mejoramiento de toma de decisiones.

MAGERIT tiene como propósitos:

a. “Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de tratarlos a tiempo” [57].

b. “Ofrecer un método sistemático para el análisis de estos riesgos.

c. Ayudar a describir y planificar las medidas adecuadas para mantener los riesgos bajo control" [57].

d. "Indirectamente, preparar a la organización para los procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso" [57].

Actualmente existen tres (3) versiones de MAGERIT, las cuales se pueden encontrar en tres (03) libros, como se muestra en la siguiente imagen:

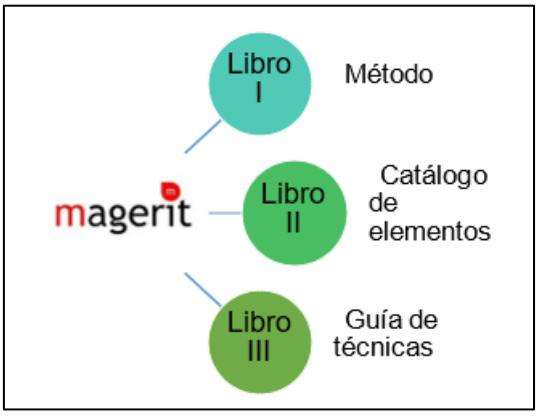


Fig. 33. Documentación disponible en MAGERIT v.3.

De la imagen previa se desprende que:

a. Libro I: Método. "Describe los pasos centrales y las tareas básicas para llevar a cabo un proyecto de análisis y gestión de riesgos; la descripción formal del proyecto; la aplicación al desarrollo de sistemas de información y proporciona un gran número de pistas prácticas, así como los fundamentos teóricos, junto con alguna otra información complementaria" [58].

b. Libro II: Catálogo de elementos. "Proporciona elementos y criterios estándar para los sistemas de información y el modelado de riesgos: clases de activos, dimensiones de valoración, criterios de valoración, amenazas típicas y salvaguardas a considerar; también describe los informes que contienen los

hallazgos y conclusiones (modelo de valor, mapa de riesgos, evaluación de salvaguardas, estado de riesgos, informe de deficiencias y plan de seguridad), contribuyendo así a lograr uniformidad" [58].

c. Libro III: Guía de Técnicas. "Describe técnicas utilizadas frecuentemente para llevar a cabo proyectos de análisis y gestión de riesgos tales como: análisis tabular y algorítmico; árboles de amenazas, análisis de costo-beneficio, diagramas de flujo de datos, diagramas de proceso, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones, presentaciones) y análisis Delphi. La aplicación de la metodología puede apoyarse en el software PILAR/EAR, que explota y aumenta sus potencialidades y eficacia (PILAR está limitado a la Administración Pública Española. EAR es un producto comercial)" [58].

Como bien se ha podido observar anteriormente, MAGERIT brinda el soporte para la gestión de los riesgos asociados a la seguridad informática, que es justamente lo que se pretendía proponer mediante la puesta en marcha del SGSI. Acerca de esto, el SGSI propuesto para el MINSA se encuentra basado en el Ciclo propuesto por el norteamericano William Edwards Deming, el mismo que permite relacionar sus cuatro (04) fases con la estructura de la norma ISO/IEC 27017. "El Ciclo de Deming, es un modelo de mejora continua de la calidad que consta de una secuencia lógica de cuatro etapas claves: planificar, hacer, verificar y actuar" [58]. Para esta investigación, el ciclo de Deming permitió específicamente:

a. Iniciar el nuevo proyecto de mejora de la SI.

b. Desarrollar un nuevo diseño para el proceso de la SI.

c. Puntualizar un proceso de trabajo repetitivo

d. Proyectar la compilación y el análisis de datos para verificar y priorizar los inconvenientes o los principios esenciales que afectan la SI en entornos CC.

e. Implementar cambios en factor de SI en entornos CC.

f. Trabajar hacia la mejora continua de la organización haciendo énfasis en la SI en entornos CC.

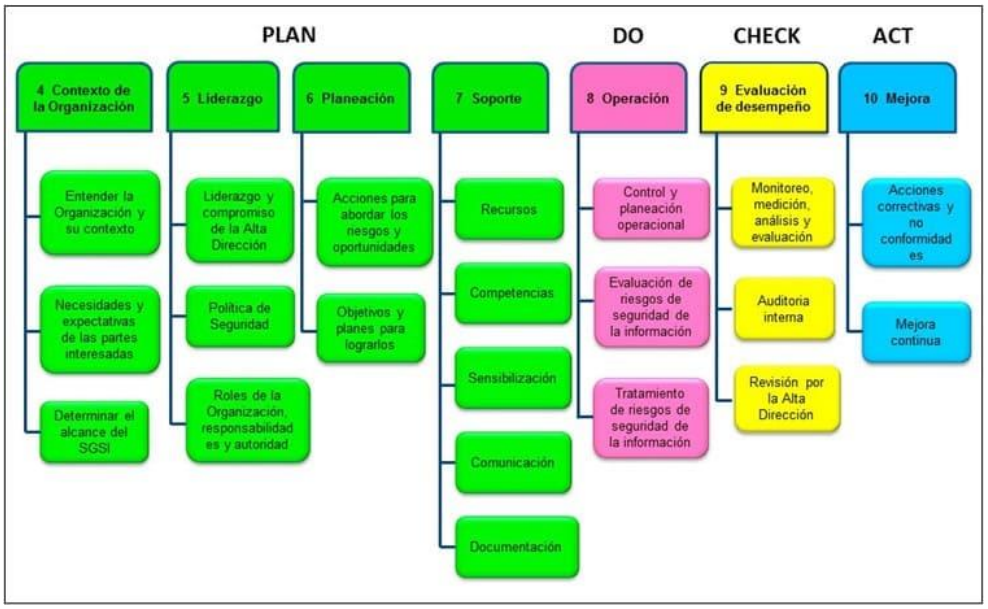


Fig. 34. Ciclo de Deming aplicado a un SGSI.

Posterior al diseño del SGSI para los servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones púbicas de salud peruanas, se necesitó validar dicho SGSI por expertos:

ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy buena			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	El SGSI está formulado con lenguaje apropiado																				
OBJETIVIDAD	El SGSI está expresado en conductas observables																				
ACTUALIDAD	El SGSI es adecuado al avance de la gestión de la seguridad de la información de servicios en la nube																				
ORGANIZACIÓN	El SGSI muestra una organización lógica																				
SUFICIENCIA	El SGSI comprende los aspectos en cantidad y calidad																				
INTENCIONALIDAD	El SGSI es adecuado para valorar la gestión de la seguridad de la información de servicios en la nube																				
CONSISTENCIA	El SGSI está basado en aspectos teóricos científicos de la seguridad de la información de servicios en la nube																				
COHERENCIA	El SGSI muestra coherencia entre cada una de sus actividades																				
METODOLOGÍA	El SGSI en cuanto a su estrategia responde al propósito de la investigación																				
PERTINENCIA	El SGSI es útil y adecuado para la investigación																				

VALORACIÓN: _____

OPINIÓN DE APLICABILIDAD: _____

Lugar y fecha: Chiclayo, ____ junio del 2022.

_____

Fig. 35. Indicadores considerados en la Ficha de Juicio de Expertos.

Luego de tener el instrumento, se procedió a solicitar la apreciación crítica de cinco (05) expertos para que validen el SGSI de servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones púbicas de salud peruanas, el mismo que fue desarrollado por el investigador. Para ello, fue necesario que dichos expertos posean las siguientes características:

- Poseer Grado Académico en Ingeniería de Sistemas o Ingeniería de Software o Ingeniería Informática

- Poseer postgrado acorde con la Gestión de TI, Gestión de la Seguridad de la Información

- Poseer experiencia proba en procesos de seguridad de la información y/o seguridad informática en la gestión pública o privada

- Poseer experiencia profesional mayor a 10 años en labores asociadas a la Ingeniería de Sistemas.

Los expertos que validaron dicho SGSI fueron:

TABLA XXXIII.

Expertos para validación del método propuesto

N°	Apellidos y Nombres	Título Profesional	Grado Académico
1	Arias Moreno Franklin Jhino	Ingeniero de Sistemas	Maestro en Dirección de Sistemas y Tecnologías de la Información
2	Sosa Suarez Doris Elizabeth	Ingeniero de Sistemas	Maestro en Dirección de Sistemas y Tecnologías de la Información
3	Bocanegra Pinchi Yan Carlos	Ingeniero de Sistemas	Maestro (c) en Ingeniería de Sistemas con mención en Dirección Estratégica de Tecnologías de la Información
4	Meres Morales Evelyn Rosalía	Ingeniero de Sistemas	Maestro en Dirección de Sistemas y Tecnologías de la Información
5	Solano Lazo Úrsula Carola	Ingeniero de Sistemas	Maestra en Dirección de Sistemas y Tecnologías de la Información

Posterior a la selección de los expertos, ellos validaron consiguiendo los siguientes resultados:

TABLA XXXIV.

Valoración de los expertos acerca del método propuesto

Indicador	Expertos					Promedio por indicador
	Exp01	Exp02	Exp03	Exp04	Exp05	
Claridad	95	95	90	95	95	94.00
Objetividad	90	90	95	90	90	91.00
Actualidad	95	95	90	95	95	94.00
Organización	90	90	95	90	90	91.00
Suficiencia	95	95	90	95	95	94.00
intencionalidad	90	90	95	90	90	91.00
Consistencia	95	95	90	95	95	94.00
Coherencia	90	90	95	90	90	91.00
Metodología	95	95	90	95	95	94.00
Pertinencia	95	95	95	95	95	95.00
Promedio por experto	93.00	93.00	92.50	93.00	93.00	N_{SGSI} = 92.90

Respecto a la TABLA IX y Fig. 13, se pudo determinar que los diez (10) indicadores de la dimensión “Aceptación del SGSI” tuvieron una valoración promedio total de 92.90 considerando la totalidad de respuestas por parte de los cinco expertos, evidenciándose una valoración mínima de 91.00 (Objetividad, Organización, Intencionalidad y Coherencia) y una máxima de 95.00 (Pertinencia). lo cual en la escala de valoración diseñada y referenciada en la TABLA XXXV, obtuvo un Nivel “Excelente” considerándose como “Aplicable” por parte de

los cinco (05) expertos, quienes expresaron que dicha propuesta era óptima para Ia realización de una prueba piloto en una institución pública caso de estudio.

TABLA XXXV.

Escala de valoración para nivel de aceptación del SGSI

Puntaje	**Nivel**	**Interpretación**
84.0-100.0	Excelente	Aplicable
68.0-83.0	Alto	Aplicable
53.0-67.0	Mediano	Aplicable
36.0-52.0	Bajo	No Aplicable
0.00-35.0	Muy Bajo	No Aplicable

Fuente, adaptado de [59].

A continuación, se muestra al detalle el desarrollo del SGSI para servicios en la nube para el entorno CC del MINSA:

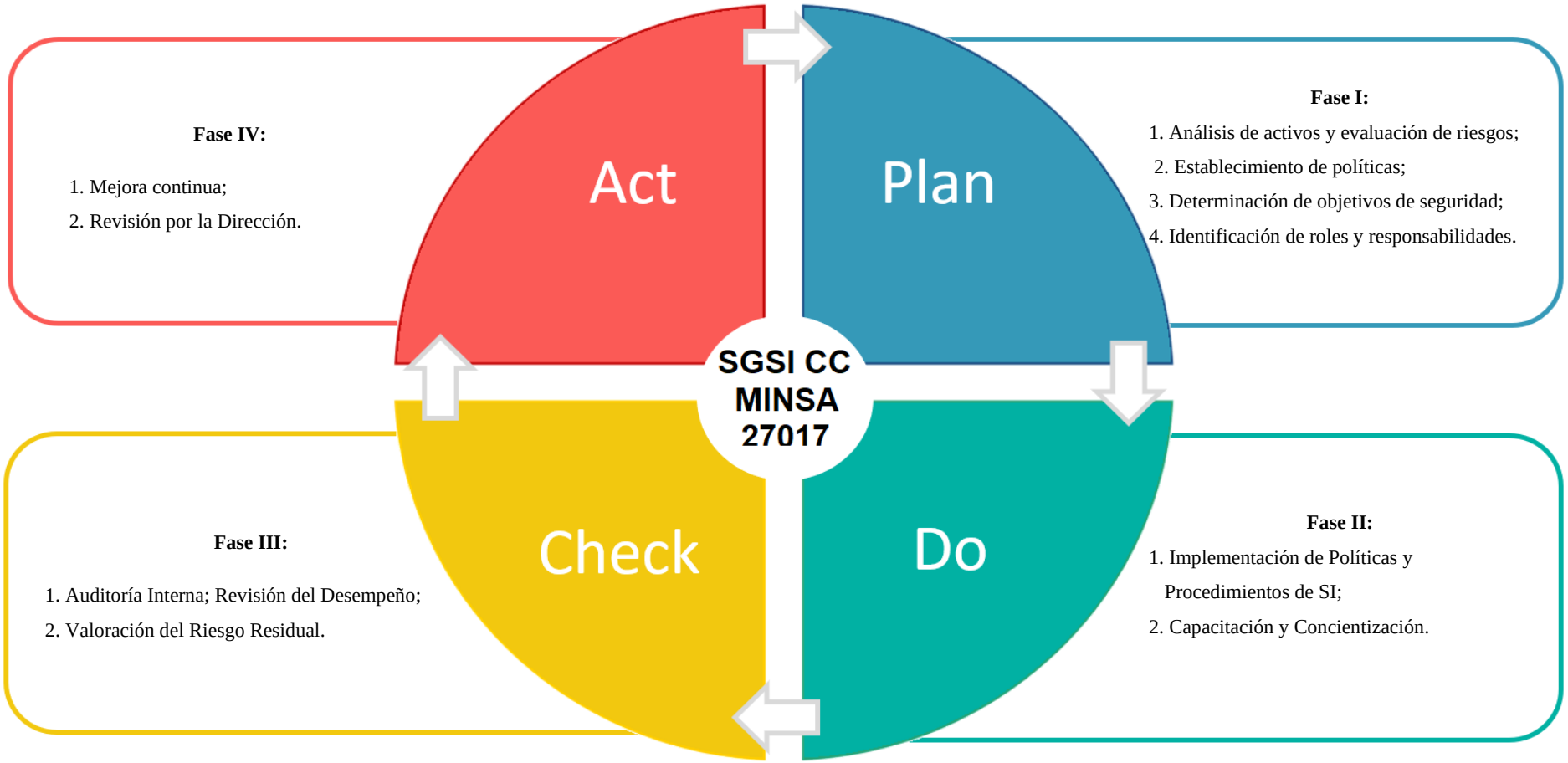


Fig. 36. SGSI de servicios en la nube propuesto para el MINSA.

A continuación, se especifican al detalle cada una de las fases del SGSI de servicios en la nube propuesto para el MINSA:

FASE 01: SGSICC-01 Planificar (PLAN)

"Describe la planificación aplicada al MINSA y el desarrollo de los lineamientos para cada procedimiento" [47].

SGSICC-F01.01: Análisis de activos y evaluación de riesgos:

En esta fase, se ejecutó un análisis exhaustivo de los activos del MINSA, identificando aquellos que eran críticos para sus operaciones, considerando para ello un inventario de activos al cual se tuvo acceso mediante un permiso otorgado por la institución. Esto implicó no solamente los activos físicos, como servidores y dispositivos de almacenamiento, sino también aquellos usuarios que tenían acceso al uso de activos informáticos, y que, por ende, a través de ellos, tenían acceso a datos de pacientes, informes médicos y documentos administrativos.

Se completó el inventario de activos en cada una de las áreas del MINSA, se procedió a evaluar los activos informáticos. Dado que estos activos tienen un valor para la institución pública, es imperativo protegerlos. En este proceso, se consideraron tres (03) características que los activos deben tener para ser valorados, según Chopra & Chaudhary [10], las cuales se detallan en la siguiente figura:

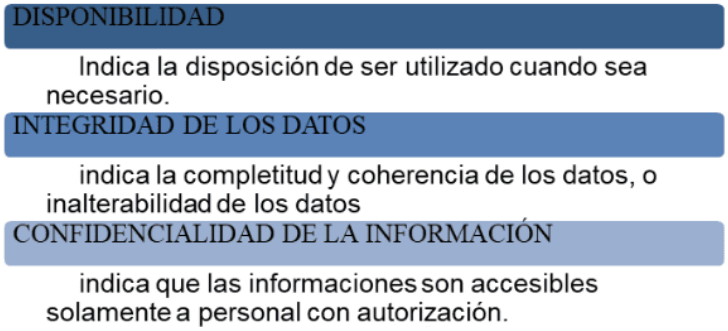


Fig. 37. Características de los activos para ser valorados.

Asimismo, fue necesario establecer la escala de valores para los activos, lo cual quedó establecido de la siguiente manera:

TABLA XXXVI.

Escala y cuadro de valores para activos

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6 – 8	Alto	Daño grave
3 - 5	Medio	Daño importante
1 – 2	Bajo	Daño menor
0	Despreciable	Daño insignificante

Fuente, Elaboración propia.

Por tanto, luego de especificar las características de los activos informáticos a valorar y la escala para obtener dicha valoración, se procedió a realizar este procedimiento el cual quedó establecido en la siguiente tabla:

TABLA XXXVII.

Valoración de activos

Código	Categoría	Activo	Confidencialidad	Integridad	Disponibilidad
VAMINSA01	Hardware	Computador Desktop	10	10	10
VAMINSA-02	Hardware	Computador Portátil	10	10	10
VAMINSA-03	Hardware	Computador iMac	10	10	10
VAMINSA-04	Hardware	iPad Pro	10	10	10
VAMINSA-05	Hardware	Televisores Led FHD	05	05	05
VAMINSA-06	Hardware	Celulares	10	10	10
VAMINSA-07	Hardware	Impresora	06	06	06
VAMINSA-08	Hardware	Proyector	06	06	06
VAMINSA-09	Hardware	Cámaras IP	10	10	10
VAMINSA-10	Hardware	Router Alámbrico	10	10	10
VAMINSA-11	Hardware	Repetidor Wifi	10	10	10
VAMINSA-12	Hardware	Switch	10	10	10
VAMINSA-13	Hardware	Teléfonos IP	07	07	07
VAMINSA-14	Hardware	Kit De Seguridad De Cámaras	10	10	10
VAMINSA-15	Hardware	Estabilizadores	05	05	05
VAMINSA-16	Hardware	Ups	06	06	06
VAMINSA-17	Software	Servidor Sistema X3250 M6	10	10	10

VAMINSA-18	Software	Antivirus Kaspersky Corporativo	06	06	06
VAMINSA-19	Software	SQL Server 2014	08	08	08
VAMINSA-20	Software	Software Licencia Sistema Operativo	10	10	10
VAMINSA-21	Software	Software De Edición De Videos	04	04	04
VAMINSA-22	Software	Software De Edición De Imágenes	04	04	04
VAMINSA-23	Software	Software SAP ERP	09	09	09
VAMINSA-24	Software	Software VPN	08	08	08
VAMINSA-25	Software	Software de Desarrollo Propio	07	07	07
VAMINSA-26	Software	Software De Ofimática	06	06	06
VAMINSA-27	Software	Software De Gestión	10	10	10

Nota. Fuente, inventario de activos.

Utilizando la metodología MAGERIT, has evaluado los riesgos asociados a estos activos, considerando su disponibilidad, integridad y confidencialidad. Esta evaluación te permite priorizar los recursos y controles de seguridad donde más se necesitan, mitigando así los riesgos más significativos para la organización.

Como se puede apreciar en la tabla previa, las calificaciones promedio para los Activos Esenciales y los Datos son notablemente ELEVADAS. Esto se atribuye a su vital importancia y su influencia en el proceso de registro de datos en línea. Por consiguiente, es fundamental reducir al mínimo los errores o, en su caso, asegurar que cualquier error sea lo menos relevante posible.

A continuación, muestro el catálogo de amenazas según el tipo de origen:

TABLA XXXVIII.

Identificación de amenazas potenciales

Identificador	Descripción	Listado
N	Desastre natural	Fuego Inundación Terremoto Rayo
I	De origen industrial	Fuego Inundación Descarga eléctrica Polvo Vibración Fallas en los equipos Corte de energía Temperatura inadecuada Corte de suministros Degradación en almacenamiento
E	Errores no intencionados	Errores de usuario Errores de administrador Error de configuración Presencia de virus Sobrecalentamiento Borrado de información Ingeniería Social Software vulnerable Error de actualización de software

		Error de mantenimiento e hardware Falta de recursos de hardware Pérdida de equipos Exceso de confianza Desecho de activos
A	Ataques intencionados	Manipulaciones de configuraciones Suplantaciones de identidades Abuso en acceso privilegiado Presencia de virus Mal uso de recursos Acceso sin autorización Negación de compromisos Interceptaciones en la comunicación Destrucción de información Borrado de información Mal uso del software Mal uso del hardware Denegación de servicio Hurto Terrorismo Personal indispuesto Ingeniería Social Extorción

Topología de amenazas

TABLA XXXIX.

Tabla de amenazas y vulnerabilidades

Amenaza	Activo	Dimensión	Descripción de los Riesgos	Vulnerabilidad
Siniestro	HW SI AUX	D	Peligro de incendio por corto circuito	Sensores de humo no hace sonar la alarma. Contiene sustancias inflamables. No hay procedimiento para el manejo de incendios. Personal sin conocimiento ante un siniestro.
Inundación	HW SI	D	Daño en los servidores	Sensores de aniegos no son analizados o examinados para comprobar su operatividad.
Corte de energía	HW SI AUX	D	Falta de energía para su funcionalidad	Falta de procedimiento ante corte en el fluido eléctrico. UPS no refieren con buena separación. Falta de procedimiento para comprobar y probar frecuentemente su operatividad.

Degradación en almacenamiento	SI	D	Falta de capacidad	Insuficiente soporte del software en los servidores. Falta de aprovisionamiento de cintas de almacenamiento (backup).
Manipulación de configuración	D SW HW COM	I C D A	La configuración de un activo sea inadecuada	Falta de detección de intrusos en tiempo real. La política aplicada en la seguridad tiene un nivel muy alto (usuarios olvidan sus contraseñas.
Suplantación de identidad	SW	C A I	Acceso privilegiado a personal no autorizado	Falta de auditoría con acceso no permitido. Las políticas aplicadas con las contraseñas no son revisadas constantemente. El proceso de altas y bajas no es controlado en tiempo real.
Sabotaje digital	SW	D C I	Acceso privilegiado a los servicios en línea.	Son limitados los sistemas de seguridad ante la protección de ataques cibernético. Inexperiencia de herramientas de control y bloqueos. Falta de conocimiento en relación de la protección de las informaciones de programas (Web Site).
Arbitrariedad de acceso privilegiado	SW	C	Manipulación de la data para uso personal	Falta de revisión constante de derechos y permisos de usuario en la Base de datos - BD.

	HW	I		No existe software de alerta cuando ocurre modificación inapropiada en la BD.
Exceso de confianza	HW SW	D I C	Uso de claves por terceros	El personal cede sus acceso al personal de su confianza. Las claves son anotadas facilitando los datos sensibles en pos-its a la vista de cualquier personal.
Denegación del servicio	HW SW	D	Falta de algún recurso	Falta de noción en el uso al momento de aplicar cortafuegos. Conocer las políticas ante los riesgos. Demora de asignar permisos al usuario. Sin conexión a red externa e interna.
Hurto o robo	HW SW	D	Mal utilización de claves en beneficio ajeno Sustracción de información	Falta vigilancia con los dispositivos de almacenamiento. Falta de sistematización con los equipos inventariados.
	AUX COM	C		Control impropio de personal con acceso a equipos de cómputos. Falta de aviso de las alarmas de intrusos no son revisados para verificar su operatividad.

Desecho de activos	HW C SI	C	Facilidad de entregar de activos con información sensible	Falta de conocimiento de las políticas de desecho o proceso de baja de activos. Falta de procedimiento de destrucción de información de activos incinerados.

SGSICC-F01.02: Establecimiento de políticas y procedimientos:

En esta sub fase se desarrollaron políticas y procedimientos detallados para la gestión de la SI en servicios en la nube, tomando como base los requisitos de la norma ISO/IEC 27017 y adaptándolos a las necesidades específicas del MINSA. Estas políticas y procedimientos abarcan todas las áreas relevantes de seguridad, desde el acceso y autenticación hasta la gestión de incidentes y la continuidad del negocio y se encuentra localizados en el Anexo 12.

Asimismo, se emplearon fichas de análisis de brechas de brechas para los niveles pre y post test, de manera que permitan evaluar el cumplimiento de las 14 cláusulas de la ISO/IEC 27017, asegurando una implementación integral y efectiva de las políticas y procedimientos establecidos.

FICHA DE ANÁLISIS DE BRECHAS - ISO 27017

CLÁUSULA	CONTROL	ESTADO	EVALUACIÓN	PROPIETARIO	¿SE CUMPLE?	¿NO SE CUMPLE?	RECOMENDACIONES	VALOR DEL OBJETIVO DE CONTROL
A. 5. Políticas de seguridad de la información								
5.1. Política de Seguridad de la información								
5.1.1	Políticas para la seguridad de la información				☐	☐		
5.1.2	Revisión de las políticas de seguridad de la información				☐	☐		
A. 6. Organización de la seguridad de la información								
6.1. Organización interna								
6.1.1	Roles y responsabilidades en seguridad de la información				☐	☐		
6.1.2	Asignación de responsabilidades				☐	☐		
6.1.3	Contacto con las autoridades				☐	☐		
6.1.4	Contacto con grupos de especial interés				☐	☐		
6.1.5	Segregation of duties				☐	☐		
6.2. Dispositivos móviles y teletrabajo								
6.2.1	Política de dispositivos móviles				☐	☐		
6.2.2	Teletrabajo				☐	☐		

Fig. 38. Ficha de Análisis de Brechas empleada en el PLAN SF2.

La ficha empleada para dicho análisis GAP se encuentra en el Anexo 6 y fue revisada por el jefe de equipo. Vale mencionar que en esta etapa se trabajó de la mano con el equipo que se encuentra especificado en la TABLA VI quienes, en conjunto con el investigador, fueron ejecutando el análisis de cada una de las cláusulas, haciendo uso de dicha ficha GAP.

SGSICC-F01.03: Determinación de objetivos de seguridad:

Se definieron objetivos de seguridad claros y medibles que se alineen con las políticas establecidas y los requisitos de la ISO/IEC 27017. En conjunto con los jefes y responsable de oficina, se establecieron los siguiente tres (03) objetivos que se buscaba alcanzar con el SGSI para servicios en la nube propuesto:

a. Objetivo de Integridad: Garantizar la exactitud y consistencia de la información almacenada en la nube, mediante la implementación de controles de acceso y auditoría y otros controles adicionales, para prevenir la alteración no autorizada de la información.
b. Objetivo de Confidencialidad: Proteger la privacidad de las informaciones que se encuentran almacenadas en la nube, asegurando que solo el personal autorizado tenga acceso a la información confidencial y aplicando políticas y procedimientos para proteger dichas informaciones.
c. Objetivo de Disponibilidad: Garantizar la disponibilidad continua de los servicios en la nube del MINSA, mediante la implementación de políticas y procedimientos para mitigar el riesgo de interrupciones no planificadas para garantizar tiempos de actividad óptimos.

SGSICC-F01.04: Identificación de roles y responsabilidades:

Se asignaron roles y responsabilidades específicos a directores y jefes de área del MINSA, asegurando que todas las partes interesadas estén involucradas en la implementación y mantenimiento del SGSI. Esto incluyó responsabilidades como la supervisión de la seguridad de los activos asignados, la ejecución de controles de seguridad y la participación en auditorías internas y revisiones de cumplimiento. A continuación, se muestran los roles y responsabilidades en una tabla:

TABLA XL.

Roles y responsabilidades en el desarrollo del SGSI

N°	Rol	Responsabilidades
1	Director General de OGTI	Supervisa y da su aprobación a la implementación del SGSI en el MINSA. Asegura la asignación adecuada de recursos para garantizar la SI en servicios en la nube.
2	Director Ejecutivo de la OGI	Coordina la identificación y protección de los activos de información vitales. Supervisa la aplicación de controles de SI en los servicios en la nube.
3	Director Ejecutivo de la OSIT	Garantiza la disponibilidad y la fiabilidad de la infraestructura para la SI de servicios en la nube. Coordina la implementación de medidas de respaldo y recuperación ante desastres.
4	Director Ejecutivo de la OIDT	Evalúa y propone nuevas tecnologías y soluciones para mejorar la SI en la nube. Coordina la capacitación y concienciación del personal sobre las políticas de SI en la nube.
5	Jefes de Equipo de la OGI	Implementan y supervisan los controles de SI en los sistemas y datos de la nube. Realizan auditorías internas periódicas para evaluar el cumplimiento de las políticas de SI.
6	Jefes de Equipo de la OSIT	Gestionan la disponibilidad y el rendimiento de los servicios en la nube. Coordinan la respuesta a incidentes de SI y la recuperación ante desastres.
7	Jefes de Equipo de la OIDT	Investigan y proponen mejoras en los procesos y tecnologías de SI en la nube. Colaboran con otros departamentos para garantizar la implementación efectiva del SGSI
8	Bach. Dayan Ray Davila Chunga	Contribuye a identificar nuevas amenazas y vulnerabilidades en los servicios en la nube. Participa en la investigación de incidentes de SI y en la aplicación de medidas correctivas.

En resumen, la fase de Planificar (Plan) del SGSI para el MINSA fue integral para establecer una base sólida para la gestión de la SI en el entorno CC con el que contaba dicha institución. Desde el análisis de activos y evaluación de riesgos hasta el establecimiento de políticas y procedimientos, esta fase ha sentado las bases necesarias para un enfoque efectivo y proactivo hacia la SI en la institución.

FASE 02: SGSICC-02 Hacer (DO)

"Establece los requisitos para medir el funcionamiento del SGSI, las expectativas de la alta dirección y su retroalimentación sobre las mismas. Igual que los procesos necesarios para cumplir con los objetivos y requisitos de seguridad, y para llevar a cabo la evaluación y tratamiento de los riesgos de seguridad de la información" [47].

SGSICC-F02.01: Implementación de Políticas y Procedimientos de SI

En la sub fase de Implementación de Políticas y Procedimientos de SI en el contexto del MINSA, se llevó a cabo un despliegue efectivo de las políticas de seguridad de la información (SI) diseñadas para abordar los riesgos específicos asociados con el uso de servicios en entornos CC. Estas políticas, detalladas en el Anexo 12 de este informe, abarcaron aspectos críticos como la gestión de accesos, la gestión de datos, la continuidad del negocio, la privacidad de la información y el cumplimiento normativo.

La estructuración de estas políticas se basó en los estándares y directrices proporcionados por la norma ISO/IEC 27017, la cual define un conjunto de 14 cláusulas que sirvieron como marco de referencia para el desarrollo de las políticas específicas aplicadas en el entorno del MINSA, institución caso de estudio. Esta metodología aseguró una cobertura integral de los aspectos fundamentales de SI en el contexto CC.

Es importante destacar que este proceso de implementación se realizó en estrecha colaboración con los directores y jefes de TI del MINSA, quienes proporcionaron valiosa información y apoyo durante todo el proceso, tal y como se comentó previamente en el TABLA XL. Gracias al permiso otorgado por la institución caso de estudio, se pudo comunicar de manera efectiva las políticas de SI a todo el personal relevante del MINSA que utilizaba o tenía acceso a los servicios en la nube. Para este caso específico, se detalla en párrafos más adelante una tabla resumen dicho personal capacitado.

Para asegurar la comprensibilidad y el cumplimiento de estas políticas por parte de los usuarios, se desarrollaron materiales visuales y de capacitación. Entre estos, se destacó el uso de presentaciones en PowerPoint, las cuales permitieron presentar de manera clara y concisa los principios y procedimientos fundamentales de SI en el contexto CC del MINSA.

En resumen, la implementación de políticas y procedimientos de SI en el MINSA se llevó a cabo de manera integral, siguiendo las mejores prácticas y estándares reconocidos en el campo de la SI y CC, más específicamente, haciendo uso de la ISO/IEC 27017. La colaboración entre los responsables de TI y el investigador garantizó una implementación efectiva y una concientización adecuada sobre la importancia de la SI en este tipo de entornos en la nube.

SGSICC-F02.02: Capacitación y Concientización

En esta sub fase, se consideró una etapa de diseño del cronograma de capacitación y concientización sobre SI en la nube para el personal del MINSA, se tomaron en consideración varios factores clave para garantizar la efectividad y relevancia del programa de formación. Entre estos factores, se incluyó el número de empleados, sus roles y responsabilidades dentro de la organización, así como el nivel de conocimiento previo en seguridad de la información y hasta sus funciones en cuanto al uso de informaciones que se

emplean en los servicios CC.

Inicialmente, se identificaron a aquellos colaboradores que tenían acceso a información sensible dentro del MINSA. Estos colaboradores, aunque contaban con un nivel de conocimiento previo en SI, aún presentaban brechas en cuanto a la comprensibilidad y aplicación de los principios de SI en entornos CC. Para garantizar una capacitación efectiva, se llevó a cabo un proceso de selección cuidadoso, priorizando a aquellos empleados cuyas responsabilidades implicaban un manejo directo de datos sensibles o críticos para la institución pública caso de estudio.

El personal seleccionado correspondió a tres (03) grupos principales, pertenecientes a las diferentes áreas funcionales dentro del MINSA: la OGTI, la OSIT y la OIDT. Cada uno de estos grupos representaba un conjunto específico de roles y responsabilidades relacionadas con la gestión y protección de la información en la nube.

En la tabla siguiente proporcionada, se detalla el número de empleados seleccionados en cada una de estas áreas, lo que permitió tener una visión clara del alcance y la distribución del programa de capacitación. Este enfoque dirigido y segmentado aseguró que la formación se adaptara adecuadamente a las necesidades y contextos laborales de cada grupo de empleados, maximizando así su relevancia y utilidad práctica:

TABLA XLI.

Personal capacitado

N°	Oficina de Gestión TI	Cantidad
1	Oficina de Gestión de la Información	08
2	Oficina de Soporte e Infraestructura Tecnológica	12
3	Oficina de Innovación y Desarrollo Tecnológico	15

Basándose en los resultados de la evaluación de necesidades de capacitación, se diseñó un programa exhaustivo que abordaba los temas clave relacionados con la SI en el entorno CC del MINSA. Este programa buscaba llenar las brechas de conocimiento identificadas y proporcionar a los empleados las habilidades y competencias necesarias para enfrentar los desafíos específicos asociados con la SI en el uso de servicios CC.

El programa de capacitación incluyó una variedad de métodos y recursos de aprendizaje para adaptarse a los estilos de aprendizaje y necesidades individuales de los empleados. Se programaron sesiones presenciales para brindar una experiencia interactiva y participativa, cursos en línea para facilitar el acceso a contenido educativo en cualquier momento y lugar, y sesiones en grupo para fomentar la discusión y el intercambio de ideas entre los participantes.

El cronograma de capacitación, detallado en la tabla presentada, mostró cómo se distribuirían las actividades a lo largo de un período de dos (02) semanas. La semana inicial estuvo dedicada a la introducción del programa y la impartición de un curso en línea sobre los fundamentos de la nube de Google Cloud, proporcionado por Talento Digital del Gobierno de Perú el cual se encuentra alojado en [60]. Esta capacitación proporcionó una comprensión básica de los conceptos clave de la computación en la nube y sentó las bases para el resto del programa.

En la segunda semana, se llevaron a cabo talleres prácticos presenciales sobre el uso seguro de los servicios CC, seguidos de otro curso en línea sobre conceptos clave de la computación en la nube [61]. Finalmente, se realizó una sesión en grupo para discutir y aclarar las políticas y procedimientos de SI propuestos para el MINSA.

Es importante destacar que este cronograma se diseñó para complementar y reforzar los temas presentados en el diagrama de GANTT, que se incluyó en los resultados del informe. Juntos, estos elementos proporcionaron una visión completa y detallada del

programa de capacitación en SI en la nube para el personal del MINSA. A continuación, se detalla el cronograma de capacitación seguido:

TABLA XLII.

Cronograma de capacitación

Semana	Actividad de capacitación	Duración	Método
Semana 1	Sesión Inaugural: Presentación del Programa de Capacitación y la Importancia de la Seguridad de la Información en la Nube	1 día	Sesión Presencial
Semana 1	Curso en Línea: Fundamentos en la Nube de Google Cloud - Talento Digital - Gobierno de Perú	5 días	Curso en Línea
Semana 2	Sesión Presencial: Talleres Prácticos sobre Uso alineados a la SI de Servicios en la Nube	1 día	Sesión Presencial
Semana 2	Curso en Línea: Aprende computación en la nube: Conceptos clave	1 día	Curso en Línea
Semana 2	Sesión en Grupo: Discusión y Clarificación de Políticas y Procedimientos de Seguridad de la Información en la Nube propuesto	1 día	Sesión en Grupo

Fuente, Elaboración propia

FASE 03: SGSICC-03 Verificar (CHECK)

SGSICC-F03.01: Auditoría Interna

En esta sub fase, era esencial ejecutar auditorías por varias razones cruciales. En primer lugar, permitió identificar las áreas prioritarias que necesitaban ser auditadas con mayor urgencia, lo que garantizaba que los recursos se asignaran de manera eficiente y se enfocaran en las áreas de mayor riesgo o importancia para la organización. Además, facilitó la asignación adecuada de recursos necesarios para llevar a cabo las auditorías de manera efectiva, incluida la selección del equipo auditor, la programación de tiempo y la asignación de presupuesto para realizar las auditorías planificadas. Respecto ello, las auditorías fueron diseñadas considerando aquellas cláusulas con las brechas más altas según el nivel esperado, las cuales se encuentran en la TABLA XVII.

Además, la planificación definió la frecuencia con la que se llevarían a cabo las auditorías internas, lo que permitió establecer un programa de auditoría regular y sistemático. Esto garantizó una cobertura continua de los controles de SI y la identificación oportuna de cualquier desviación o incumplimiento.

Asimismo, facilitó la alineación de las auditorías internas con los objetivos estratégicos del MINSA y con los requisitos de cumplimiento normativo, asegurando que las auditorías abordaran áreas críticas que respaldaran los objetivos y la misión de dicha institución pública peruana. Además, permitió asegurar el cumplimiento con los requisitos normativos y regulatorios aplicables, incluyendo la identificación de estándares de SI, como ISO/IEC 27017, y la programación de auditorías para evaluar el cumplimiento con estos estándares.

En resumen, la planificación de auditorías era esencial para garantizar la efectividad y eficiencia del proceso de auditoría interna, asegurando que se llevaran a cabo de manera sistemática, enfocada y en línea con los objetivos y requisitos de la organización. A continuación, se muestra la tabla resumen con el calendario de auditorías ejecutado:

TABLA XLIII.

Calendario de auditorías

Fecha Inicio	Fecha Fin	Área de Auditoría	Detalle
10/10/22	16/10/22	C10. Criptografía	Se evaluó la implementación y gestión de criptografía.
17/10/22	23/10/22		Se revisó la política de gestión de claves criptográficas.
24/10/22	30/10/22	C18. Cumplimiento	Se realizó una evaluación del cumplimiento con leyes y regulaciones de protección de datos.
31/10/22	06/11/22		Se llevó a cabo una revisión del cumplimiento con requisitos contractuales de seguridad de la información.
07/11/22	13/11/22	C5. Políticas de SI	Se auditó las políticas de clasificación de la información.
14/11/22	20/11/22		Se evaluó la implementación de políticas de gestión de accesos.

Fuente, Elaboración propia

Respeto al detalle de las frecuencias, se optó por realizar dos (02) auditorías para cada cláusula que obtuvo un nivel de brecha más alto, distribuidas a lo largo del período de tiempo disponible. Las áreas de enfoque fueron las C10, C18 y C5.

La planificación detallada de las auditorías para las cláusulas C10, C18 y C5 permitió identificar y abordar las brechas de SI de manera efectiva, asegurando la protección de la información y el cumplimiento de las normativas aplicables. Un enfoque estructurado y sistemático en la revisión de estas áreas críticas contribuyó a fortalecer el SGSI CC y a mitigar los riesgos asociados con la SI.

Para el desarrollo de las auditorías se hizo uso de la ficha alojada en el Anexo 6. En base a ello, se realizó una revisión exhaustiva de la documentación existente, que incluyó políticas, procedimientos, registros de seguridad y cualquier otro documento relevante relacionado con la SI. Esto permitió evaluar la conformidad con los requisitos establecidos en la norma ISO/IEC 27017, que era justamente la norma internacional en la que se basó el SGSI propuesto. Se llevaron a cabo entrevistas con el director y los jefes, los cuales son actores claves de la institución pública caso de estudio, para comprender cómo se implementan y gestionan los controles de SI en la práctica. Estas entrevistas proporcionaron información valiosa sobre la efectividad de los controles y la cultura de SI en la institución.

SGSICC-F03.02: Revisión del Desempeño

Para revisar el desempeño PRE TEST de la institución pública caso de estudio, se tuvo primero que identificar la misión y visión de la OGTI del MINSA ya que es esa área la que, establece claramente su compromiso con la SI en dicha institución pública peruana, especialmente en el ámbito de la salud. Estos principios fundamentales son la base sobre la cual se construye y opera el SGSI en la institución y son los siguientes:

TABLA XLIV.

Misión y visión OGTI

Misión	**Visión**
“Velar por la seguridad de la información en las instituciones públicas, especialmente en el ámbito de la salud, garantizando la integridad, confidencialidad y disponibilidad de los datos relacionados con la salud pública. Nuestra misión es aplicar	“Convertirnos en referentes en seguridad de la información para las instituciones públicas en Perú, liderando la adopción de tecnologías y prácticas que aseguren la protección de los datos sensibles de la población. Aspiramos a ser reconocidos por

tecnologías avanzadas y mejores prácticas en gestión de información para fortalecer la seguridad y protección de los datos”.	nuestra excelencia en la gestión de la información, contribuyendo a un entorno donde la seguridad de los datos sea un pilar fundamental para un sistema de salud pública más seguro y eficiente”.

Fuente, Elaboración propia

Respecto a la tabla anterior, dichas declaraciones establecen claramente su compromiso con la SI en la institución pública peruana, especialmente en el ámbito de la salud. La Oficina General de Tecnología de la Información - OGTI se compromete a garantizar la integridad, confidencialidad y disponibilidad de los datos relacionados con la salud pública, aplicando TI avanzadas y mejores prácticas en gestión de información para fortalecer la seguridad y protección de los datos.

En el proceso de evaluación del nivel de madurez del SGSI, se utilizó un modelo de madurez que constó de seis (06) niveles, el cual permitió evaluar el nivel actual de SI. Los niveles fueron desde "Inexistente", donde no existía evidencia de un enfoque sistemático para la SI, hasta "Optimizado", donde las prácticas eran mejoradas continuamente para maximizar la protección de los datos. La evaluación del nivel de madurez fue fundamental para identificar áreas de mejora y establecer un camino claro hacia la excelencia en la gestión de la SI. Alineando los resultados de esta evaluación con la misión y visión de la Oficina General de Tecnología de la Información - OGTI, asegurándose que, el SGSI esté en sintonía con los objetivos estratégicos de la organización y contribuya a la realización de su compromiso con la SI, no solamente en el MINSA, sino que, también en las instituciones públicas. Los niveles de madurez en mención fueron:

TABLA XLV.

Niveles de madurez para revisión del desempeño

Nivel	Definición
Nivel 0	En este nivel, la institución pública no tiene implementadas prácticas formales de seguridad de la información en la nube.
Nivel 1	La institución pública ha comenzado a tomar medidas para abordar la seguridad de la información en la nube, pero estas acciones son principalmente reactivas y no están formalizadas
Nivel 2	Se establecen procesos y procedimientos formales para gestionar la seguridad de la información en la nube, pero pueden ser inconsistentes y aún no están completamente integrados en la cultura de la institución pública.
Nivel 3	La organización tiene procesos y controles de seguridad de la información bien definidos y documentados, que se aplican de manera consistente en toda la institución pública.
Nivel 4	Se implementan mecanismos para medir y monitorear continuamente el desempeño de los controles de seguridad de la información en la nube, con el fin de mejorar su eficacia y eficiencia
Nivel 5	La institución pública tiene una cultura de mejora continua en la que se buscan constantemente oportunidades para optimizar y perfeccionar los controles de seguridad de la información en la nube, basándose en el análisis de datos y la retroalimentación del desempeño

Nota. Adaptado de [52].

Con estos niveles de madurez, se lograron identificar los niveles de cada una de las cláusulas según la ISO/IEC 27017, identificando que existían las siguientes cláusulas con las brechas más altas:

TABLA XLVI.

Brechas más altas según nivel esperado

Cláusulas	Nivel PRE TEST	Nivel Esperado	Brecha
C10. Criptografía	0.00	4.00	4.00
C18. Cumplimiento	0.25	4.00	3.75
C5. Políticas de seguridad de la información	0.50	4.00	3.50

Fuente, Elaboración propia

SGSICC-F03.03: Valoración del Riesgo Residual

Basado en el análisis GAP y los resultados de los niveles de madurez, identificamos los riesgos residuales en las cláusulas con mayores brechas:

A. Cláusula C10 (Criptografía):

- Nivel PRE TEST: 0.00
- Nivel POST TEST: 1.50
- Brecha Actual: 2.50
- Descripción: Inicialmente no había implementación de criptografía, aunque se han logrado avances, la criptografía sigue siendo insuficiente.
- Riesgo Residual: Exposición de datos sensibles y acceso no autorizado.

B. Cláusula C18 (Cumplimiento):

- Nivel PRE TEST: 0.25
- Nivel POST TEST: 1.88
- Brecha Actual: 2.12
- Descripción: El cumplimiento normativo era casi inexistente, y aunque ha

mejorado, sigue siendo deficiente.

- Riesgo Residual: Sanciones legales, pérdida de confianza y reputación.

C. Cláusula C5 (Políticas de Seguridad de la Información):

- Nivel PRE TEST: 0.50
- Nivel POST TEST: 3.50
- Brecha Actual: 0.50
- Descripción: Las políticas de seguridad han mejorado significativamente pero aún necesitan perfeccionarse.
- Riesgo Residual: Aplicación inconsistente de las políticas, posibles vulnerabilidades.

TABLA XLVII.

Probabilidad de amenazas

Probabilidad de amenaza				
100	S	Siempre	Seguro	Diario
90	MF	Muy frecuente	Casi seguro	Semanal
70-80	F	Frecuente	Muy probable	Mensual
40-60	N	Normal	Posible	Trimestral
20-30	P	Poco frecuente	Poco probable	Semestral
10	MP	Muy poco frecuente	Muy raro	Anual
0	N	Nunca	nunca	Nunca

TABLA XLVIII.

Impacto del nivel de riesgos

VALOR	IMPACTO	DESCRIPCIÓN
1	Insignificante	Impacta Levemente en la operatividad del proceso
2	Menor	Impacta en la operatividad del proceso
3	Medio	Impacta Levemente en la operatividad del macro proceso
4	Crítico	Impacta Levemente en la operatividad de los procesos
5	Catastrófico	Impacta fuertemente en la operatividad de los procesos

La Tabla XLIX proporciona una clasificación del nivel de riesgo en función de un sistema de puntuación. Esta clasificación es crucial para evaluar la gravedad de los riesgos residuales identificados en el proceso de valoración del SGSI.

TABLA XLIX.

Nivel de riesgo

Nivel de riesgo	
1,2,3	Bajo
4,5	Medio
6,7,8	Alto
9,10,11	critico

La Tabla XXXVIII es una matriz de evaluación de riesgos que relaciona el impacto de un riesgo con la probabilidad de que ocurra. Esta matriz es fundamental para la valoración de los riesgos residuales en el SGSI. A continuación, se explica cómo utilizar esta matriz para clasificar y priorizar los riesgos. Ejes de la Matriz:

A. Impacto (Eje Horizontal):

Categorías:

- Insignificante: Daño mínimo o sin consecuencias.
- Menor: Daño pequeño, interrupciones menores.
- Medio: Daño moderado, interrupciones significativas.
- Crítico: Daño grave, interrupciones mayores.
- Catastrófico: Daño extremadamente grave, interrupciones severas y prolongadas.

B. Probabilidad (Eje Vertical):

Categorías:

- Siempre: El riesgo se materializa constantemente.
- Muy frecuente: El riesgo ocurre con alta frecuencia.
- Frecuente: El riesgo ocurre regularmente.
- Normal: El riesgo ocurre ocasionalmente.
- Poco frecuente: El riesgo ocurre raramente.
- Muy poco frecuente: El riesgo ocurre en contadas ocasiones.
- Nunca: El riesgo no se ha materializado.

TABLA L.

Impacto vs Probabilidad

Probabilidad \ Impacto	Insignificante	Menor	Medio	Critico	Catastrófico
Siempre	7	8	9	10	11
Muy frecuente	6	7	8	9	10
Frecuente	5	6	7	8	9
Normal	4	5	6	7	8
Poco frecuente	3	4	5	6	7
Muy poco frecuente	2	3	4	5	6
Nunca	1	2	3	4	5

Fuente, Elaboración propia.

TABLA LI.

Matriz de gestión de riesgos

Cód.	Riesgo	Descripción	Causas	Consecuencias	ANALISIS DE RIESGOS				
					Valor	Probabilidad	(10) VALOR	Impacto	Severidad
1	Compra de equipos sin las características mínimas requeridas para el tratamiento de la información.	1. Comprar software que no cumple los requerimientos mínimos requeridos por el MINSA. 2. Comprar activos de comunicación (sw, router, etc) inadecuados a las necesidades del MINSA.	1. Desconocimiento de características actuales de los equipos. 2. Falta de revisión de las características solicitadas.	Pérdidas económicas. Denegación del sistema. Inestabilidad de los procesos.	20	Poco frecuente	2	Menor	40
2	Uso indebido de la información	Posibilidad de que se acceda, manipule y/o divulgue sin autorización la información privilegiada. de reserva que se origine, suministre o custodie en los sistemas de información.	1. Bajo nivel de seguridad para el acceso a la información. 2. Desconocimiento de las políticas de manejo de información. 3. Actos mal intencionados de terceros. 4. Acceso no autorizado a información. 5. Fraude interno.	Desconfianza del público usuario. Mala imagen, Toma de decisiones no adecuadas.	70	Frecuente	3	Medio	210
3	Vulnerabilidad del sistema de información	Posibilidad que un tercero ingrese de forma indebida al sistema de información del MINSA, para alterar, robar o dañar la información.	1. Nivel bajo de seguridad para el acceso a la información. 2. Seguridad perimetral inestable 3. Bugs en los sistemas de información. 4. Desconocimiento de los estándares	Pérdidas económicas. Inestabilidad de los procesos. Fuga de información	20	Poco frecuente	4	Critico	80

			para la implementación del aseguramiento de la información.						
4	Daños, deterioro o pérdida de los equipos informáticos	Posibilidad de que se presenten daños, fallas o pérdidas de los recursos tecnológicos, en su uso, y/o almacenamiento.	1. Falta y/o inadecuado mantenimiento de los equipos informáticos. 2. Baja calidad de los equipos informáticos. 3. Inadecuado uso de los equipos informáticos. 4. Falta de capacitación sobre el adecuado uso de los equipos informáticos. 5. Falta de protección de los equipos informáticos. 6. Terrorismo 7. Factores ambientales	Equipos averiados. Mal uso de los recursos informáticos.	70	Frecuente	2	Menor	140
5	Ausencia y/o deficiencia en los software y sistemas de información	Baja calidad en los resultados y/o estadísticas en los aplicativos que intervienen en el sistema.	1. Trámite engorroso para adquisición de activos. 2. Falta y/o inadecuado mantenimiento de los recursos tecnológicos 3. Baja calidad de los recursos tecnológicos	Elevación de las tasas en los servicios.	20	Poco frecuente	3	Medio	40
6	Inadecuada utilización de los recursos Web	Hace referencia a la inadecuada utilización de la página Web del MINSA.	1. Falta de cultura tecnológica 2. Falta de capacitación en el uso del sistema y los aplicativos que intervienen en el proceso.	Desinformación de los usuarios. Proceso de inscripción tradicional con la lentitud y	80	Frecuente	2	Menor	160

				riegos tradicionales.					
7	Fallas en las comunicaciones	Posible denegación de los servicios de networking (internet, redes, intranet, servicio telefónico).	1. Falta de disponibilidad del servicio por parte del proveedor 2. Falta de mantenimiento de los equipos y redes 3. Deterioro de las redes 4. Falla en las comunicaciones.	Acceso inoportuno a los servicios de inscripción y publicidad:	40	Normal	3	Critico	120
8	Fallas en el fluido eléctrico	Posible denegación de los servicios eléctricos	1. Fluctuaciones en el fluido eléctrico. 2. Falta de protección ante pico de voltajes y/o interrupción del fluido eléctrico no planificado (Redundancia de Energía). 3. Inadecuada solución de sistema ininterrumpido de energía (UPS)	No prestar atención oportuna a los usuarios. Perjuicio económico para la institución	30	Poco frecuente	3	Crítico	90
9	Fracaso de eventos programados	Suspensión de actividades o eventos	1. Poca o nula divulgación. 2. Desinterés de los usuarios respecto a temas de seguridad de la información.	Personal no capacitado. Frustración de los Gerentes ante incumplimiento de las metas.	90	Muy frecuente	3	Crítico	270

10	Humedad producida por sistemas de refrigeración inadecuados y/o filtraciones de agua	Daños en la infraestructura física (Servidores y demás activos dentro del datacenter).	1. Mal funcionamiento de los sistemas de aire de acondicionado. 2. Inadecuada protección del ambiente del datacenter frente a las amenazas ambientales.	Inestabilidad en los servicios registrales. Posible pérdida de información. Interrupción de procesos, daños físicos en los activos dependientes.	10	Muy poco frecuente	3	Crítico	30
11	Accesos no autorizados a las instalaciones del Área de Sistemas.	Ingreso de personas no autorizadas para la manipulación de equipos informáticos	1. Inadecuado control de acceso a las instalaciones 2.Puertas no aptas para la seguridad informática y de la información.	Pérdida de activos. Daños, manipulación, robos en la infraestructura Informática	50	Normal	3	Medio	150

TABLA LII.

Matriz de tratamiento de riesgos

Código	Riesgo	EVALUACIÓN DE RIESGOS							
		Control	Descripción del Control	Tipo de Control	Está Documentado	Tipo de documento	Aplicación	Eficacia del control	Frecuencia del control
1	Compra de equipos sin las características mínimas requeridas para el tratamiento de la información.	Evolución de experto	Diagnóstico sobre ventajas y desventajas de las compras	Preventivo	SI	Procedimientos establecidos	SI	Alta	Cuando se presenta
2	Uso indebido de la información	Mejoramiento de la jerarquía de usuarios. Divulgación de las políticas de manejo de la información. Monitoreo a los sistemas de información. Procedimientos para asignación de roles y accesos a los sistemas de información.	Establecimiento de roles en el sistema. Optimización de los controles en los sistemas de información	Preventivo	SI	Procedimiento de altas y bajas de acceso	SI	Alta	Mensual
3	Vulnerabilidad del sistema de información	Fortalecimiento de los equipos de seguridad perimetral. Procedimientos de control para la detección de vulnerabilidades en los sistemas de información. Aplicación de buenas prácticas para implementación de sistemas de información seguros.	Verificar que las políticas de Aseguramiento de la información estén funcionando adecuadamente de acuerdo a las normas internacionales ISO	Preventivo	SI	Normas de políticas de aseguramiento de la información	SI	Alta	Semanal
4	Daños, deterioro o pérdida de equipos informáticos	Mantener el material y los equipos asignados para el cumplimiento de las funciones	Inventarios frecuentes con reporte del estado actual de los equipos informáticos.	Preventivo	SI	Políticas de control de equipos.	SI	Alta	Semanal
5	Ausencia y/o deficiencia en los software y sistemas de información	Determinar las características adecuadas	Brindar asesoría en la adquisición adecuada a los requerimientos del MINSA	Preventivo	NO		SI	Alta	Cuando se presenta

6	Inadecuada utilización de los recursos Web	Capacitación y concientización	A través de la red de capacitadores, cursos y/o manuales de usuario	Preventivo	SI	Políticas de capacitación y concientización	SI	Alta	Cuando se presenta
7	Fallas en las comunicaciones	Verificación de las conectividades entre los activos comprendidos en el sistema	Monitoreo de performance de las redes de comunicaciones	Preventivo	NO		SI	Alta	Semanal
8	Fallas en el fluido eléctrico	Verificación de toma eléctrica, para establecer que el voltaje sea el apropiado para la instalación de los equipos. Verificación de operatividad de UPS.	Verificación de puntos eléctricos, para detectar fallas en el fluido que pueda afectar el funcionamiento de los equipos informáticos.	Preventivo	SI	Directivas de protección de equipos informáticos	SI	Alta	Cuando se presenta
9	Fracaso de eventos programados	Diseñar programa de eventos, Diseño adecuado de la logística, manejar plan de medios	Divulgación de responsabilidades y tareas	Preventivo	SI	Plan de capacitación y concientización	SI	Media	Cuando se presenta
10	Humedad producida por sistemas de refrigeración inadecuados y/o filtraciones de agua	Evolución de experto. Mantenimiento preventivo	Diagnóstico del sistema de refrigeración y mantenimiento	Correctivo	SI	Plan de mantenimiento de equipos	SI	Baja	Programado
11	Accesos no autorizados a las instalaciones del Área de Sistemas.	Reforzar el acceso físico a las instalaciones del Área de Sistemas.	Instalación de nuevas cerraduras biométricas, y monitorización de ingresos a las instalaciones del Área de Sistemas.	Preventivo	NO		SI	Alta	Semanal

Nota. Fuente, [62].

TABLA LIII.

Escala por tipo de control

APLICACIÓN		**PERIODICIDAD**		**PRODUCTO**		
PREVENTIVO	4	PERIODICO	3	12	ALTA	4
PREVENTIVO	4	PERMANENTE	2	8	MEDIA	3
PREVENTIVO	4	OCASIONAL	1	4	BAJA	2
CORRECTIVO	3	PERIODICO	3	9	ALTA	4
CORRECTIVO	3	PERMANENTE	2	6	MEDIA	3
CORRECTIVO	3	OCASIONAL	1	3	BAJA	2
DETECTIVO	2	PERIODICO	3	6	ALTA	3
DETECTIVO	2	PERMANENTE	2	4	MEDIA	2
DETECTIVO	2	OCASIONAL	1	2	BAJA	2
INEXISTENTE	1			1	INEXISTENTE	1

Eficacia del Control	
ALTO	4
MEDIO	3
BAJO	2
ENEXISTENTE	1

“El riesgo residual es el nivel resultante del riesgo después de aplicar controles. La fórmula para determinar el nivel de exposición del riesgo es la división entre el nivel del riesgo dividido entre el nivel de eficacia del control que se encuentra asociado al riesgo” [47].

$$Riesgo\ residual = \frac{Nivel\ de\ Riesgo\ Inherente}{Control\ (eficacia)}$$

TABLA LIV.

Valoración del riesgo residual

Valoración de riesgo (residual)		
Descripción	Nª de Nivel	Calificación
INACEPTABLE	1	> 30
IMPORTANTE	2	20 a 30
MODERADO	3	10 a 20
TOLERABLE	4	5 a 9.9
ACEPTABLE	5	< 5

Fuente, Elaboración propia

3.3.1.1. Fase para el tratamiento del riesgo

Acción: Actividad a realizar.

a. Opciones de Posibles Tratamientos: acciones a tomar en respuesta.

b. Resultado del Costo/Beneficio.

Tipo de Tratamiento:

a. Prevenir: Evitar iniciar o continuar la actividad que generó el riesgo.

b. Aceptar: Tolerar o aumentar el riesgo para aprovechar una oportunidad.

c. Evitar: Eliminar la fuente de riesgo.

d. Mitigar: Modificar la probabilidad y/o las consecuencias.

e. Transferir: Compartir el riesgo con otra parte.

f. Retener: Mantener el riesgo mediante una decisión consciente.

Responsable: Encargado de la actividad o tarea a realizar.

Fecha de Acción: Fecha en que se conceptualiza la acción.

FASE 04: SGSICC-04 Actuar (ACT)

"Establece el proceso de mejora del SGSI, a partir de las no conformidades identificadas en el MINSA. Se deben establecer acciones para solucionarlos o para deshacerse de ellos" [47].

SGSICC-F04.01: Mejora continua

En el proceso de evaluación del SGSI del MINSA, se analizaron los niveles de madurez de diversas cláusulas antes y después de la implementación de mejoras. Los resultados mostraron un avance significativo en varias áreas clave de la seguridad de la información. Los niveles de madurez fueron evaluados y ajustados para garantizar la mejora continua del SGSI:

TABLA LV.

Detalle PRE TEST vs POST TEST de los niveles de madurez

Cláusulas	Nivel PRE TEST	Nivel POST TEST
C5. Políticas de seguridad de la información	Inicial	Definido
C6. Organización de la seguridad de la información	Inicial	Definido
C7. Seguridad de los recursos humanos	Repetitivo	Gestionado
C8. Gestión de activos	Inicial	Definido
C9. Control de acceso	Inicial	Repetitivo
C10. Criptografía	Inexistente	Inicial
C11. Seguridad física y medioambiental	Inicial	Repetitivo
C12. Seguridad de las operaciones	Inicial	Repetitivo
C13. Seguridad de las comunicaciones	Repetitivo	Definido
C14. Adquisición, desarrollo y mantenimiento de sistemas	Repetitivo	Definido
C15. Relaciones con los proveedores	Inicial	Repetitivo
C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad	Repetitivo	Definido
C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad	Repetitivo	Definido
C18. Cumplimiento	Inexistente	Repetitivo

Con base en la evaluación detallada de los niveles de madurez, se identificaron varias áreas que requerían ajustes y mejoras. Estas revisiones sirvieron como base para implementar cambios y actualizaciones en las políticas y procedimientos del SGSI de servicios en la nube del MINSA. Por ejemplo:

- En la C5, se procedió al desarrollo y formalización de políticas de SI, las cuales establecieron directrices claras y procedimientos estandarizados. Este esfuerzo permitió una evolución desde un nivel inicial hasta alcanzar un nivel definido de madurez en esta área.
- En la C6, se implementaron estructuras organizacionales específicas y se asignaron roles claros para la gestión de la SI. Estas acciones mejoraron la coordinación y la responsabilidad dentro de la organización, logrando así un nivel definido de madurez.
- En la C7, se introdujeron programas de capacitación y concienciación dirigidos al personal, destacando la importancia de la SI. Esta iniciativa permitió alcanzar un nivel gestionado en la madurez de la seguridad de los recursos humanos.
- En la C8, se estableció un inventario completo de activos y se desarrollaron procedimientos para su gestión y protección. Estas medidas mejoraron significativamente el nivel de madurez, elevándolo a definido.
- En la C9, se implementaron controles de acceso más estrictos, los cuales se revisaron periódicamente para asegurar su eficacia. Estas acciones elevaron el nivel de madurez a repetitivo.
- En la C10, se introdujeron prácticas básicas de criptografía y se promovió su uso en todas las comunicaciones y almacenamiento de datos. Esta progresión permitió avanzar desde un nivel inexistente hasta un nivel inicial.
- En la C11, se mejoraron las medidas de seguridad física y ambiental dentro de las instalaciones. Estas mejoras permitieron alcanzar un nivel repetitivo en la madurez de esta área.
- En la C12, se revisaron y mejoraron las operaciones diarias relacionadas con la SI. Gracias a estos esfuerzos, se logró avanzar a un nivel repetitivo en la madurez.
- En la C13, se implementaron controles de seguridad robustos para las

comunicaciones, lo cual permitió alcanzar un nivel definido de madurez.

- En la C14, se establecieron procedimientos para asegurar que los sistemas adquiridos y desarrollados cumplan con los requisitos de SI. Estas acciones llevaron el nivel de madurez a definido.
- En la C15, se mejoraron los acuerdos de seguridad con los proveedores, asegurando que cumplan con los estándares del SGSI. Estas mejoras lograron elevar el nivel de madurez a repetitivo.
- En la C16, se desarrollaron procedimientos específicos para la gestión de incidentes de SI, asegurando una respuesta rápida y eficaz. Esta iniciativa permitió alcanzar un nivel definido de madurez.
- En la C17, se integraron aspectos de SI en los planes de continuidad del negocio, mejorando así la preparación y la respuesta ante incidentes. Estas acciones llevaron el nivel de madurez a definido.
- En la C18, se mejoraron los procesos para asegurar el cumplimiento de las normativas y estándares de SI. Gracias a estas mejoras, se logró avanzar desde un nivel inexistente hasta un nivel repetitivo en la madurez de cumplimiento.

Las evaluaciones realizadas permitieron identificar áreas específicas que requerían ajustes y mejoras. Con base en estas evaluaciones, se implementaron cambios y actualizaciones en las políticas y procedimientos del SGSI de servicios en la nube del MINSA. Estos cambios fueron esenciales para asegurar la mejora continua del SGSI, permitiendo así una evolución significativa en los niveles de madurez y fortaleciendo la postura de SI dentro de la institución pública peruana caso de estudio.

SGSICC-F04.02: Revisión por la Dirección

Durante la fase de cierre del SGSI para servicios en la nube del MINSA, se llevó a

cabo una reunión de revisión por parte de la dirección para evaluar los resultados de las auditorías y las propuestas de mejora. En esta etapa, se presentaron los hallazgos clave y las recomendaciones a la alta dirección en una sesión informativa diseñada para resaltar los aspectos críticos del SGSI. Se proporcionaron ejemplos concretos y casos prácticos para ilustrar los puntos discutidos y facilitar la comprensión de los temas técnicos por parte de los líderes de la organización.

Durante la presentación, se enfatizó la importancia estratégica de la SI y se destacaron los riesgos asociados con la falta de medidas de seguridad adecuadas. Se alentó un diálogo abierto y constructivo, permitiendo que los miembros de la alta dirección expresaran sus preocupaciones y comentarios sobre los resultados presentados. Se hizo hincapié en la necesidad de un compromiso activo de la dirección para implementar las mejoras propuestas en el SGSI.

Como resultado de la revisión por la dirección, se obtuvo el respaldo y el compromiso de la alta dirección para la mejora continua del SGSI. Se acordaron medidas específicas para abordar las áreas de mejora identificadas, incluyendo la asignación de recursos adicionales, ajustes en políticas y procedimientos, y la implementación de iniciativas de capacitación y concienciación del personal. Se establecieron métricas y objetivos claros para medir el progreso en la implementación de las mejoras acordadas, garantizando así un enfoque continuo en la seguridad de la información a largo plazo.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Se seleccionó el estándar más adecuado para la seguridad de la información para servicios en la nube, ya que pretendía era el desarrollo de un SGSI de servicios en la nube, y que, en este caso concreto, ayude al propósito de la mejora de la seguridad de la

información en instituciones públicas de salud peruanas, por lo que se optó por la ISO/IEC 27017 para el caso de estudio.

Se diagnosticó el estado actual de la gestión de los servicios en la nube del MINSA, evidenciándose, poco conocimiento en políticas de seguridad, no aseguramiento del acceso de personal autorizado, carencia de procedimientos para la eliminación de accesos de usuarios, no se venían firmando acuerdos de confidencialidad, eran defectuosos los procedimientos de destrucción de data en equipos sensibles, no desarrollaba capacitación y concientización en seguridad de la información.

Se diseñó el SGSI para servicios en la nube basado en el estándar lSO/lEC 27017 para el MINSA, para lo cual se realizó un ranking de metodologías existentes para la gestión de los riesgos llegando a determinar a MAGERIT como la de mejores prestaciones, y sumada con, el soporte del Ciclo de Deming, pudo establecer un sistema de cuatro fases bien definidas.

Se validó mediante juicio de expertos el SGSI para servicios en la nube para el MINSA mediante dicha técnica, de modo que los expertos emitieron su veredicto favorable con un promedio de 92.83 de aprobación, determinándose que dicho SGSI poseía los requerimientos necesarios de la gestión de la información d ellos servicios en la nube

Se ejecutó una prueba piloto del SGSI para servicios en la nube en el MINSA, obteniéndose mejoras significativas en el 100% de los indicadores para cada una de las cuatro (04) dimensiones de la seguridad de la información.

4.2. Recomendaciones

Se recomienda al MINSA minimizar los riesgos ante las amenazas que se muestra en aumento en los distintos aspectos del avance tecnológico, implementando para ese fin, el

presente SGSI para servicios en la nube que se ha desplegado en esta investigación pues se encuentra enmarcado en un estándar de rigor internacional.

Se recomienda a futuros investigadores en seguridad de Ia información, hacer usanza de Ios indicadores elaborados en esta investigación pues se encuentra fundamentada en las dimensiones de la gestión de Ia seguridad de Ia información de servicios en Ia nube y en Ias características propias de la ISO/IEC 27017.

Se recomienda a los directivos de las diversas instituciones públicas que, aprovechando el alto nivel de validez por parte de Ios expertos acerca del SGSI para servicios en la nube propuesto en esta investigación, se implemente en su totalidad en sus representadas para comprobar de forma práctica la total efectividad de Ias políticas de seguridad definidas.

Se recomienda la aplicabilidad de mantenimiento periódico a las políticas diseñadas en esta investigación ya que nos encontramos en un contexto de total cambio en el que se vienen introduciendo amenazas de manera perenne en los servicios en la nube.

REFERENCIAS

[1] A. Sunyaev, «Cloud computing,» de *Internet computing: Principles of distributed systems and emerging internet-based technologies*, Karlsruhe, Springer, 2020, pp. 195-236.

[2] Facts & Factors, «Cloud Computing Market Size, Share Global Analysis Report, 2022-2028,» Facts & Factors Research, Nueva York, 2022.

[3] eHealth, «La adopción del Cloud Computing en el sector salud en América Latina,» eHealth Reporter, 2022. [En línea]. Available: https://es.slideshare.net/ehCOS/la-adopcin-del-cloud-computing-en-el-sector-salud-en-amrica-latina.

[4] ANDINA, «Crece adopción de la nube en el sector público y estos son los retos pendientes,» Agencia Peruana de Noticias, 3 Diciembre 2022. [En línea]. Available: https://andina.pe/agencia/noticia-crece-adopcion-de-nube-el-sector-publico-y-estos-son-los-retos-pendientes-919953.aspx.

[5] DIario El Peruano, «Crecimiento de los servicios de nube pública representará más de 2.300 millones de dólares al 2027,» 22 Octubre 2023. [En línea]. Available: https://www.elperuano.pe/noticia/225942-crecimiento-de-los-servicios-de-nube-publica-representara-mas-de-2300-millones-de-dolares-al-2027.

[6] D. Rosales, «Los servicios en la nube ganan fuerza y continúan como la principal tendencia de TI para 2023,» Revista Summa, 22 Noviembre 2022. [En línea]. Available: https://revistasumma.com/los-servicios-en-la-nube-ganan-fuerza-y-continuan-como-la-principal-tendencia-de-ti-para-2023/.

[7] K. De Abrew y R. Wickramarachchi, «Organizational Factors Affecting the ISMS Effectiveness in Sri Lankan IT Organizations: A Systematic Review,» de *International Conference on Industrial Engineering and Operations Management Monterrey*, Ciudad de México, 2021.

[8] PYME TV, «Impacto económico de la adopción de la nube en Perú,» PyME TV, 21 Febrero 2024. [En línea]. Available: https://pymetv.pe/impacto-economico-de-la-adopcion-de-la-nube-en-peru.

[9] Quint, «La tecnología cloud sigue siendo un negocio al alza en nuestro país,» Revista Cloud Computing, 12 Julio 2022. [En línea]. Available: https://www.revistacloudcomputing.com/2022/07/la-tecnologia-cloud-sigue-siendo-un-negocio-al-alza-en-nuestro-pais/.

[10] Oracle, «Oracle and KPMG Cloud Threat Report 2020,» ESG, Nueva York, 2020.

[11] R. Clarke y T. Youngstein, «Cyberattack on Britain's National Health Service - A Wake-up Call for Modern Medicine,» *The New England Journal of Medicine and Surgery and the Collateral Branches of Science*, vol. 377, nº 5, pp. 409-411, 2017.

[12] H. Solomon, «LifeLabs faulted by Ontario, B.C. privacy commissioners for huge data breach,» IT World Canada, 26 Junio 2020. [En línea]. Available: https://www.itworldcanada.com/article/lifelabs-faulted-for-huge-data-breach-by-ontario-b-c-privacy-commissioners/432525.

[13] PWC, «Conti cyber attack on the HSE,» HSE Board, Dublín, 2021.

[14] IT Seller, «Próximos ciberataques al sector salud podrían tener graves consecuencias,» IT Seller, 20 Febrero 2023. [En línea]. Available:

https://itseller.pe/2023/02/20/proximos-ciberataques-al-sector-salud-podrian-tener-graves-consecuencias/.

[15] L. Arcila, «Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información,» Universidad Católica de Colombia, Bogotá, 2019.

[16] J. Cuervo, «Resolución Ministerial nº 187-2010-PCM de 15 de junio de 2010, autorizan ejecución de la "Encuesta de Seguridad de la Información en la Administración Pública-2010",» Informática Jurídica, 1 Enero 2014. [En línea]. Available: https://www.informatica-juridica.com/anexos/resolucion-ministerial-no-187-2010-pcm-de-15-de-junio-de-2010-autorizan-ejecucion-de-la-quot-encuesta-de-seguridad-de-la-informacion-en-la-administracion-publica-2010-quot/.

[17] F. Nafisa, R. Yasirandi y R. Utomo, «Information Security Audit Analysis on Cloud Providers Using ISO/IEC 27017: 2015 at PT. XYZ,» *eProceedings of Engineering,* vol. 10, nº 3, pp. 3671-3676, 2023.

[18] N. Kamaruddin, I. Mohamed, A. Jarno y M. Daud, «Cloud Security Pre-assessment Model For Cloud Service Provider Based On ISO/IEC 27017: 2015 Additional Control,» *Revolution,* vol. 2, nº 5, pp. 1-17, 2020.

[19] W. Wendy y W. Gunawan, «Measuring information security and cybersecurity on private cloud computing,» *Journal of Theoretical and Applied Information Technology,* vol. 97, nº 1, pp. 156-168, 2019.

[20] N. Ahmad, I. Mohamed, M. Daud, A. Jarno y N. Hamid, «Cloud Service Provider Security Readiness Model: The Malaysian Perspective,» de *2019 International Conference on Electrical Engineering and Informatics (ICEEI)*, Bandung, 2019.

[21] G. Ruiz, «Sistema de gestión de seguridad de la información de servicios en la nube para la empresa "Masiva" de la ciudad de Quito, con base en la norma ISO/IEC 27017,» Universidad Técnica del Norte, Quito, 2021.

[22] J. Ayala, «Diseño del sistema de gestión de seguridad de la información para una compañía de software que provee servicios PAAS,» Universidad de Alcalá, Alcalá de Henares, 2021.

[23] E. Tenelema, «Implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube con base en las normas ISO 27017 y 27018,» Escuela Superior Politécnica de Chimborazo, Riobamba, 2020.

[24] M. Alcántara, «Estrategia de adaptación de un sistema de gestión de la seguridad de la información universitario a computación en la nube,» Universidad Nacional del Callao, Callao, 2019.

[25] A. Fernández, L. García y A. Garófalo, «Propuesta de controles de seguridad para nubes privadas y centros de datos virtualizados,» *Telemática*, vol. 17, nº 1, pp. 56-72, 2018.

[26] C. Peñafiel, «Diseño de un modelo para establecer un sistema de gestión de la seguridad de la información dentro de un ambiente Cloud Computing, aplicando la Norma ISO 27001:2013,» Pontificia Universidad Católica del Ecuador, Quito, 2019.

[27] O. Schluga, E. Bauer, A. Bicaku, S. Maksuti, M. Tauber y A. Wöhler, «Operations security evaluation of IaaS-cloud backend for industry 4.0,» de *International Conference on Cloud Computing and Services Science CLOSER 2018*, Madeira, 2018.

[28] N. Tissir, S. El Kafhali y N. Aboutabit, «Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal,» *Journal of Reliable Intelligent Environments*, vol. 7, nº 2, pp. 69-84, 2021.

[29] H. Haro, «Guía de implementación de normas de autenticación y seguridad en entornos cloud computing para pymes,» Pontificia Universidad Católica del Ecuador, Quito, 2021.

[30] M. Tajammul y R. Parveen, «Comparative analysis of big ten ISMS standards and their effect on cloud computing,» de *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, Gurgaon, 2017.

[31] Y. Wei y M. Blake, «Service-oriented computing and cloud computing: Challenges and opportunities,» *IEEE Internet Computing*, vol. 14, nº 6, pp. 72-75, 2010.

[32] A. Rashid y A. Chaturvedi, «Cloud computing characteristics and services: a brief review,» *International Journal of Computer Sciences and Engineering*, vol. 7, nº 2, pp. 421-426, 2019.

[33] S. Kim, «ISMS Implementation and Maintenance in Compliance with Finland's National Cybersecurity Requirements,» Haaga-Helia University of Applied Sciences, 2022, 2022.

[34] J. Gallego, «Conceptos fundamentales de Azure,» Medium, 22 Noviembre 2022. [En línea]. Available: https://medium.com/@0xCamiX/conceptos-fundamentales-de-azure-e9c73b2e1189.

[35] J. Condori, «Ventajas y desventajas de cloud computing,» *Revista de información, tecnología y sociedad,* vol. 86, nº 1, pp. 86-87, 2012.

[36] V. Rai, K. Bagoria, K. Mehta, V. Sood, K. Gupta, L. Sharma y M. Chauhan, «Cloud computing in healthcare industries: Opportunities and challenges,» de *Recent Innovations in Computing: Proceedings of ICRIC 2021*, Singapur, 2022.

[37] M. Bamiah, S. Brohi y S. Chuprat, «A study on significance of adopting cloud computing paradigm in healthcare sector,» de *International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*, Dubai, 2012.

[38] T. McGuinness, «Microsoft Cloud for Healthcare, la nube ad hoc que acelera la digitalización del sector sanitario,» Microsoft, 23 Septiembre 2020. [En línea]. Available: https://news.microsoft.com/es-es/2020/09/23/microsoft-cloud-for-healthcare-la-nube-ad-hoc-que-acelera-la-digitalizacion-del-sector-sanitario/.

[39] A. Gillies, «Improving the quality of information security management systems with ISO27000,» *The TQM Journal,* vol. 23, nº 4, pp. 367-376, 2011.

[40] I. Tøndel, M. Line y M. Jaatun, «Information security incident management: Current practice as reported in the literature,» *Computers & Security*, vol. 45, nº 1, pp. 42-57, 2014.

[41] J. Llanos, F. Albeiro y M. Mejía, «Implementación de un sistema de seguridad de la información en empresa del sector salud,» *SUMMA*, vol. 5, nº 2, p. 114, 2023.

[42] J. Tang, «The implementation of Deming's system model to improve security management: A case study,» *International Journal of Management*, vol. 25, nº 1, pp. 54-60, 2008.

[43] M. Arafat, «Information security management system challenges within a cloud computing environment,» de *ICFNDS '18: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, Nueva York, 2018.

[44] T. Lean, «¿Qué es el Ciclo de Deming?,» Tienda Lean, 2020. [En línea]. Available: https://www.tiendalean.com/pages/que-es-el-ciclo-de-deming.

[45] A. Citterio, «Sistema di gestione della sicurezza delle informazioni (SGSI), cos'è, perché è importante averlo,» Bigdata 4 Innovation, 17 Diciembre 2020. [En línea]. Available: https://www.bigdata4innovation.it/sicurezza-e-privacy/sistema-di-gestione-della-sicurezza-delle-informazioni-sgsi-cose-perche-e-importante-averlo/.

[46] L. Tot, G. Grubor y T. Marta, «Introducing the information security management system in cloud computing environment,» *Acta Polytechnica Hungarica*, vol. 12, nº 3, pp. 147-166, 2015.

[47] ISO, «ISO/IEC 27017:2015 Information technology: Security techniques, Code of practice for information security controls based on ISO/IEC 27002 for cloud services,» 1 Diciembre 2015. [En línea]. Available: https://www.iso.org/standard/43757.html.

[48] C. Espinoza, Metodología de la Investigación Tecnológica: Pensando en Sistemas, Segunda ed., Huancayo: Universidad Nacional del Centro, 2014.

[49] G. Disterer, «ISO/IEC 27000, 27001 and 27002 for information security management,» *Journal of Information Security,* vol. 4, nº 2, pp. 92-100, 2013.

[50] SUNEDU, «Registro Nacional de Grados Académicos y Títulos Profesionales,» 2024. [En línea]. Available: https://enlinea.sunedu.gob.pe/.

[51] A. Noreña, N. Alcaraz, J. Rojas y D. Rebolledo, «Aplicabilidad de los criterios de rigor y éticos en la investigación cualitativa,» *Aquichan,* vol. 12, nº 3, pp. 263-274, 2012.

[52] R. Alencar, C. Merkle, D. dos Santos y C. Becker, «A cyclical evaluation model of information security maturity,» *Information Management & Computer Security,* vol. 22, nº 3, pp. 265-278, 2014.

[53] A. Dávila, «El modelo SEI/CMM y el proceso de desarrollo de Software,» Pontificia Universidad Católica del Perú, Lima, 2002.

[54] Sysprove, «ISO 27017 - Security Controls for Cloud Services,» Sysprove Consulting, 2021. [En línea]. Available: https://sysprove.com/iso-27017-security-controls-for-cloud-services/.

[55] MINSA, «Información institucional,» Ministerio de Salud, 2024. [En línea]. Available: https://www.gob.pe/institucion/minsa/institucional.

[56] MINSA, «Mapa de Procesos del Ministerio de Salud,» Ministerio de Salud, Lima, 2014.

[57] A. Fernández y D. Garcia, «Complex vs. simple asset modeling approaches for information security risk assessment: Evaluation with MAGERIT methodology,» de *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, Dublín, 2016.

[58] ENISA, «Magerit,» The European Union Agency for Cybersecurity, 2024. [En línea]. Available: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html.

[59] H. Limson, «Online Academic Information System,» *Academic Journal of Science*, vol. 5, nº 1, pp. 353-364, 2016.

[60] PCM, «Aprende los fundamentos de la nube con Google Cloud,» Presidencia del Consejo de Ministros, 10 Diciembre 2023. [En línea]. Available: https://www.gob.pe/institucion/pcm/campa%C3%B1as/37638-aprende-los-fundamentos-de-la-nube-con-google-cloud.

[61] D. Linthicum, «Aprende computación en la nube: Conceptos clave,» LinkedIn Learning, 31 Marzo 2022. [En línea]. Available: https://es.linkedin.com/learning/aprende-computacion-en-la-nube-conceptos-clave?trk=learning-serp_learning-search-card_search-card&upsellOrderOrigin=default_guest_learning.

[62] K. Moron, «Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C.,» Universidad Señor de Sipán, Pimentel, 2023.

ANEXOS.

Anexo 1. Resolución de aprobación del proyecto de investigación

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0526-2024/FIAU-USS

Pimentel, 09 de julio de 2024

VISTO:
El Acta de reunión N° 02 - 07 - 2024 del Comité de investigación de la INGENIERÍA DE SISTEMASremitida mediante vía oficio N° 0129-2024/FIAU-IS-USS de fecha 04 de julio de 2024, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico *y tesis* son *aprobados por el Comité de Investigación* y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de laresolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, *el* Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis esun estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C".

Que, mediante documentos de vistos, el Comité de investigación de la referida Escuela profesional acordó aprobar título de proyecto de investigación, de la línea de investigación de CIENCIAS DE LA INFORMACIÓN COMO HERRAMIENTAS MULTIDISCIPLINARES Y ESTRATÉGICAS EN EL CONTEXTO INDUSTRIAL Y DE ORGANIZACIONES, a cargo de los estudiantes y /o egresados del Programa de estudios INGENIERÍA DE SISTEMAS, hasta la fecha que indica la presente resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normasy reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1: APROBAR, TITULO DE PROYECTO DE INVESTIGACIÓN a cargo de los estudiantes y /o egresados del Programa de estudios de **INGENIERÍA DE SISTEMAS que** se detallan en el anexo de la presente Resolución

ARTÍCULO 2: DEJAR SIN **EFECTO**, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

Facultad de Ingeniería Arquitectura y Urbanismo
USS UNIVERSIDAD SEÑOR DE SIPÁN SAC

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0526-2024/FIAU-USS

Pimentel, 09 de julio de 2024

ANEXO

APROBACION TITULO DE PROYECTO DE INVESTIGACIÓN

APELLIDOS NOMBRES	TITULO DEL PROYECTO DE INVESTIGACIÓN
DAVILA CHUNGA DAYAN RAY	Sistema de gestión de seguridad de la información de servicios en la nube basado en ISO/IEC-27017 para instituciones públicas
CAMPOS CLAVO BILELMO	Modelo de adquisición de tecnologías de la información para mejorar la gestión de las adquisiciones en entidades públicas del Perú

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Facultad de Ingeniería Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Dr. Victor Alexci Tuesta Monteza
Decano (E) / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Dr. Halyn Alvarez Vasquez
Secretario Académico Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Cc: Interesado, Archivo

Anexo 2. Resolución de asesor de proyecto de tesis

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0471-2024/FIAU-USS

Pimentel, 30 de mayo de 2024

VISTO:
El Acta de reunión N° 28 - 05 - 2024 del Comité de investigación de la INGENIERÍA DE SISTEMAS remitida mediante vía oficio N° 0109-2024/FIAU-IS-USS de fecha 30 de mayo de 2024, y:

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48º que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y *tesis* son *aprobados por el Comité de Investigacióny* derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de laresolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24º señala: La tesis esun estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado: *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.

Que, mediante documentos de vistos, el Comité de investigación de la referida Escuela profesional acordó aprobar la designación de asesor de tesis, de la línea de investigación de CIENCIAS DE LA INFORMACIÓN COMO HERRAMIENTAS MULTIDISCIPLINARES Y ESTRATÉGICAS EN EL CONTEXTO INDUSTRIAL Y DE
ORGANIZACIONES, a cargo de los estudiantes y /o egresados del Programa de estudios INGENIERÍA DE SISTEMAS, hasta la fecha que indica la presente resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normasy reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1: APROBAR, designación de asesor de tesis a cargo de los estudiantes y /o egresados del Programa deestudios de **INGENIERÍA DE SISTEMAS que** se detallan en el anexo de la presente Resolución.

ARTÍCULO 2: DEJAR SIN **EFECTO**, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0471-2024/FIAU-USS

Pimentel, 30 de mayo de 2024

ANEXO

APROBACION DESIGNACION DE ASESOR DE TESIS

APELLIDOS	TITULO DEL PROYECTO DE INVESTIGACIÓN	NOMBRE DEL NUEVO ASESOR
DAVILA CHUNGA, DAYAN RAY	Aprobación de proyecto 0468-2024/FIAU-USS Sistema de gestión de servicios en la nube basado en la ISO/IEC27017 para seguridad de la información en instituciones pública	Mg. Mejia Cabrera Ivan Heber

Dr. Victor Alexci Tuesta Monteza
Decano (E) / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Dr. Halyn Alvarez Vásquez
Secretario Académico Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Cc: Interesado, Archivo

Anexo 3. Carta de presentación del estudiante para realizar caso de estudio

UNIVERSIDAD SEÑOR DE SIPÁN

"Año del Fortalecimiento de la Soberanía Nacional"

Pimentel, 06 de julio de 2022

Señor(a):
Ing. Nieves Vanessa Gonzalez Escobedo
Ministerio de Salud
Ciudad.-

ASUNTO:
Presentación de estudiante para realizar caso de estudio.

Es grato dirigirme a usted para expresarle el saludo institucional a nombre de la Escuela Profesional de Ingeniería de Sistemas, perteneciente a la Facultad de Ingeniería, Arquitectura y Urbanismo, de la Universidad Señor de Sipán, a la vez presentar al estudiante del IX ciclo, Davila Chunga Dayan Ray con código universitario 2110818926, e identificado con DNI 10467519, quién recogerá información relevante en la institución que usted representa, como parte de su proyecto de INVESTIGACIÓN, cuyo tema de investigación aprobado con resolución N°0443-2022/FIAU-USS, titulado "Desarrollo de un sistema de gestión de seguridad de la información de servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones públicas peruanas".

Para ello, solicitamos su autorización, esperando que el estudiante cumpla con todos los requerimientos necesarios.

En espera de su atención a la presente, aprovecho la oportunidad para expresarle mi consideración y estima personal.

Cordialmente,

Mag. Ing. Heber Ivan Mejia Cabrera
Director (e) de la Escuela Profesional de Ingeniería de Sistemas
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.

ADMISIÓN E INFORMES
074 481610 - 074 481632
CAMPUS USS
Km. 5, carretera a Pimentel
Chiclayo, Perú

www.uss.edu.pe

Anexo 4. Carta de aceptación de la institución para la recolección de datos

PERÚ | Ministerio de Salud | Secretaría General | Oficina General de Tecnologías de la Información

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

Lima 11 de julio del 2022

CARTA DE ACEPTACIÓN

Señor(a):
Ing. MEJIA CABRERA HEBER IVAN
Escuela Profesional de Ingeniería de Sistemas
Universidad Señor de Sipán S.A.C.

ASUNTO: **Aceptación de Proyecto de Investigación**

Es grato dirigirme a usted para comunicarle que el Señor: **DAYAN RAY DAVILA CHUNGA**, con el código universitario Nº 2110818926, identificado con el DNI 10467519, estudiante del IX ciclo Escuela Profesional de Ingeniería de Sistema, ha sido aceptado para realizar su **PROYECTO DE INVESTIGACIÓN "***Desarrollo de un sistema de gestión de seguridad de la información de servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones públicas peruanas***"** en la oficina de Redes y Telecomunicaciones de la OSIT/OGTI de la Sede Central del Ministerio de Salud, de acuerdo a los recursos y el asesoramiento requerido para el cumplimiento de las actividades que le sean asignadas.

Sin otro particular me suscribo de Usted, reiterando las nuestra de mi especial consideración y estima.

Atentamente,

MINISTERIO DE SALUD
Oficina General de Tecnologías de la Información
ING. NIEVES VANESSA GONZALEZ ESCOBEDO
Jefe de Equipo Redes y Telecomunicaciones
Oficina de Soporte e Infraestructura Tecnológica

Siempre con el pueblo

Anexo 5. Instrumento de recolección de datos - Ficha de Juicio de Expertos

VALIDACIÓN POR JUICIO DE EXPERTOS
INSTRUMENTO DE RECOLECCIÓN

Título de la investigación:

DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS

Autor:

Dávila Chunga Dayán Ray

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente sistema de gestión de seguridad de la información de servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones públicas de salud peruanas.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: _____

1.2. Grado Académico y Profesión: _____

1.3. Áreas de Experiencia Profesional: _____

1.4. Institución donde labora: _____

1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS.**

II. VALIDACIÓN

Se utilizarán los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - **[250-400]**, Regular - **[450-600]**, Buena: **[650-800]**, Muy Buena - **[850-1000]**

ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy buena			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	El SGSI está formulado con lenguaje apropiado																				
OBJETIVIDAD	El SGSI está expresado en conductas observables																				
ACTUALIDAD	El SGSI es adecuado al avance de la gestión de la seguridad de la información de servicios en la nube																				
ORGANIZACIÓN	El SGSI muestra una organización lógica																				
SUFICIENCIA	El SGSI comprende los aspectos en cantidad y calidad																				
INTENCIONALIDAD	El SGSI es adecuado para valorar la gestión de la seguridad de la información de servicios en la nube																				
CONSISTENCIA	El SGSI está basado en aspectos teóricos científicos de la seguridad de la información de servicios en la nube																				
COHERENCIA	El SGSI muestra coherencia entre cada una de sus actividades																				
METODOLOGÌA	El SGSI en cuanto a su estrategia responde al propósito de la investigación																				
PERTINENCIA	El SGSI es útil y adecuado para la investigación																				

VALORACIÓN: _____

OPINIÓN DE APLICABILIDAD: _____

Lugar y fecha: Chiclayo, ____ junio del 2022.

_____

Anexo 6. Instrumento de recolección de datos - Ficha de Análisis de Brechas

FICHA DE ANÁLISIS DE BRECHAS - ISO 27017

CLÁUSULA	CONTROL	ESTADO	EVALUACIÓN	PROPIETARIO	¿SE CUMPLE?	¿NO SE CUMPLE?	RECOMENDACIONES	VALOR DEL OBJETIVO DE CONTROL
A. 5. Políticas de seguridad de la información								
5.1. Política de Seguridad de la información								
5.1.1	Políticas para la seguridad de la información				☐	☐		
5.1.2	Revisión de las políticas de seguridad de la información				☐	☐		
A. 6. Organización de la seguridad de la información								
6.1. Organización interna								
6.1.1	Roles y responsabilidades en seguridad de la información				☐	☐		
6.1.2	Asignación de responsabilidades				☐	☐		
6.1.3	Contacto con las autoridades				☐	☐		
6.1.4	Contacto con grupos de especial interés				☐	☐		
6.1.5	Segregation of duties				☐	☐		
6.2. Dispositivos móviles y teletrabajo								
6.2.1	Política de dispositivos móviles				☐	☐		
6.2.2	Teletrabajo				☐	☐		
A. 7. Seguridad de los recursos humanos								
7.1. Antes del empleo								
7.1.1	Investigación de antecedentes				☐	☐		
7.1.2	Términos y condiciones del empleo				☐	☐		
7.2. Durante el empleo								
7.2.1	Responsabilidades de gestión				☐	☐		
7.2.2	Concienciación, educación y capacitación en seguridad de la información				☐	☐		
7.2.3	Proceso disciplinario				☐	☐		
7.3. Finalización del empleo o cambio en el puesto de trabajo								
7.3.1	Responsabilidades ante la finalización o cambio				☐	☐		
A. 8. Gestión de activos								
8.1. Responsabilidad sobre los activos								
8.1.1	Inventario de activos				☐	☐		
8.1.2	Propiedad de los activos				☐	☐		
8.1.3	Uso aceptable de los activos				☐	☐		
8.1.4	Devolución de activos				☐	☐		
8.2. Clasificación de la información								
8.2.1	Clasificación de la información				☐	☐		
8.2.2	Etiquetado de la información				☐	☐		
8.2.3	Manipulado de la información				☐	☐		
8.3. Manipulación de los soportes								
8.2.1	Gestión de soportes extraíbles				☐	☐		
8.2.2	Eliminación de soportes				☐	☐		
8.2.3	Soportes físicos en tránsito				☐	☐		

A. 9. Control de accesos								
9.1. Requisitos de negocio para el control de acceso								
9.1.1	Política de control de acceso				☐	☐		
9.1.2	Acceso a las redes y a los servicios de red				☐	☐		
9.2. Gestión de acceso de usuario								
9.2.1	Registro y baja de usuario				☐	☐		
9.2.2	Provisión de acceso de usuario				☐	☐		
9.2.3	Gestión de privilegios de acceso				☐	☐		
9.2.4	Gestión de la información secreta de autenticación de los usuarios				☐	☐		
9.2.5	Revisión de los derechos de acceso de usuario				☐	☐		
9.2.6	Retirada o reasignación de los derechos de acceso				☐	☐		
9.3. Responsabilidades del usuario								
9.3.1	Uso de la información secreta de autenticación				☐	☐		
9.4. Control de acceso a sistemas y aplicaciones								
9.4.1	Restricción del acceso a la información				☐	☐		
9.4.2	Procedimientos seguros de inicio de sesión				☐	☐		
9.4.3	Sistema de gestión de contraseñas				☐	☐		
9.4.4	Uso de utilidades con privilegios del sistema				☐	☐		
9.4.5	Control de acceso al código fuente de los programas				☐	☐		
A. 10. Criptografía								
10.1. Controles criptográficos								
10.1.1	Política de uso de los controles criptográficos				☐	☐		
10.1.2	Gestión de claves				☐	☐		
A. 11. Seguridad física y ambiental								
11.1. Áreas seguras								
11.1.1	Perímetro de seguridad físico				☐	☐		
11.1.2	Controles físicos de entrada				☐	☐		
11.1.3	Seguridad de oficinas, despachos y recursos				☐	☐		
11.1.4	Protección contra las amenazas externas y ambientales				☐	☐		
11.1.5	El trabajo en áreas seguras				☐	☐		
11.1.6	Áreas de carga y descarga				☐	☐		
11.2. Seguridad de los equipos								
11.2.1	Ubicación y protección de equipos				☐	☐		
11.2.2	Instalaciones de suministro				☐	☐		
11.2.3	Seguridad del cableado				☐	☐		
11.2.4	Mantenimiento de los equipos				☐	☐		
11.2.5	Retirada de materiales propiedad de la empresa				☐	☐		
11.2.6	Seguridad de los equipos fuera de las instalaciones				☐	☐		
11.2.7	Reutilización o eliminación segura de equipos				☐	☐		
11.2.8	Equipo de usuario desatendido				☐	☐		
11.2.9	Política de puesto de trabajo despejado y pantalla limpia				☐	☐		
A. 12. Seguridad de las operaciones								
12.1 Procedimientos y responsabilidades operacionales								
12.1.1	Análisis y especificaciones de los requerimientos de seguridad				☐	☐		
12.1.2	Gestión de cambios				☐	☐		

12.1.3	Gestión de capacidades				☐	☐		
12.1.4	Separación de los recursos de desarrollo, prueba y operación				☐	☐		
12.2. Protección contra el software malicioso (malware)								
12.2.1	Controles contra el código malicioso				☐	☐		
12.3. Copias de seguridad								
12.3.1	Copias de seguridad de la información				☐	☐		
12.4. Registros y supervisión								
12.4.1	Registro de eventos				☐	☐		
12.4.2	Protección de la información del registro				☐	☐		
12.4.3	Registros de administración y operación				☐	☐		
12.4.4	Sincronización del reloj				☐	☐		
12.5. Control del software en explotación								
12.5.1	Instalación del software en explotación				☐	☐		
12.6. Gestión de la vulnerabilidad técnica								
12.6.1	Gestión de las vulnerabilidades técnicas				☐	☐		
12.6.2	Restricción en la instalación de software				☐	☐		
12.7. Consideraciones sobre la auditoría de sistemas de información								
12.7.1	Controles de auditoría de sistemas de información				☐	☐		
A. 13. Seguridad de las comunicaciones								
13.1. Gestión de la seguridad de las redes								
13.1.1	Controles de red				☐	☐		
13.1.2	Seguridad de los servicios de red				☐	☐		
13.1.3	Segregación en redes				☐	☐		
13.2. Intercambio de información								
13.2.1	Políticas y procedimientos de intercambio de información				☐	☐		
13.2.2	Acuerdos de intercambio de información				☐	☐		
13.2.3	Mensajería electrónica				☐	☐		
13.2.4	Acuerdos de confidencialidad o no revelación				☐	☐		
A. 14. Adquisición, desarrollo y mantenimiento de sistemas								
14.1. Requisitos de seguridad en los sistemas de información								
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información				☐	☐		
14.1.2	Asegurar los servicios de aplicaciones en redes públicas				☐	☐		
14.1.3	Protección de las transacciones de servicios de aplicaciones				☐	☐		
14.2. Seguridad en el desarrollo y en los procesos de soporte								
14.2.1	Política de desarrollo seguro				☐	☐		
14.2.2	Procedimiento de control de cambios en sistemas				☐	☐		
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo				☐	☐		
14.2.4	Restricciones a los cambios en los paquetes de software				☐	☐		
14.2.5	Principios de ingeniería de sistemas seguros				☐	☐		
14.2.6	Entorno de desarrollo seguro				☐	☐		
14.2.7	Externalización del desarrollo de software				☐	☐		
14.2.8	Pruebas funcionales de seguridad de sistemas				☐	☐		
14.2.9	Pruebas de aceptación de sistemas				☐	☐		
14.3. Datos de prueba								
14.3.1	Protección de los datos de prueba				☐	☐		
A. 15. Relaciones con los proveedores								
15.1. Seguridad en las relaciones con proveedores								

15.1.1	Política de seguridad de la información en las relaciones con los proveedores				☐	☐		
15.1.2	Requisitos de seguridad en contratos con terceros				☐	☐		
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones				☐	☐		
15.2. Gestión de la provisión de servicios del proveedor								
15.2.1	Control y revisión de la provisión de servicios del proveedor				☐	☐		
15.2.2	Gestión de cambios en la provisión del servicio del proveedor				☐	☐		
A. 16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad								
16.1. Gestión de incidentes de seguridad de la información y mejoras								
16.1.1	Responsabilidades y procedimientos				☐	☐		
16.2.1	Notificación de los eventos de seguridad de la información				☐	☐		
16.3.1	Notificación de puntos débiles de la seguridad				☐	☐		
16.4.1	Evaluación y decisión sobre los eventos de seguridad de información				☐	☐		
16.5.1	Respuesta a incidentes de seguridad de la información				☐	☐		
16.6.1	Aprendizaje de los incidentes de seguridad de la información				☐	☐		
16.7.1	Recopilación de evidencias				☐	☐		
A. 17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad								
17.1. Continuidad de la seguridad de la información								
17.1.1	Planificación de la continuidad de la seguridad de la información				☐	☐		
17.1.2	Implementar la continuidad de la seguridad de la información				☐	☐		
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información				☐	☐		
17.2. Redundancias								
17.2.1	Disponibilidad de los recursos de tratamiento de la información				☐	☐		
A. 18. Cumplimiento								
18.1. Cumplimiento de los requisitos legales y contractuales								
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales				☐	☐		
18.1.2	Derechos de Propiedad Intelectual (DPI)				☐	☐		
18.1.3	Protección de los registros de la organización				☐	☐		
18.1.4	Protección y privacidad de la información de carácter personal				☐	☐		
18.1.5	Regulación de los controles criptográficos				☐	☐		
18.2. Revisiones de la seguridad de la información								
18.2.1	Revisión independiente de la seguridad de la información				☐	☐		

Anexo 7. Validez del SGSI de servicios en la nube

EXPERTO 01: Mg. Arias Moreno Franklin Jhino

VALIDACIÓN POR JUICIO DE EXPERTOS
INSTRUMENTO DE RECOLECCIÓN

Título de la investigación:

DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS

Autor:

Dávila Chunga Dayán Ray

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente sistema de gestión de seguridad de la información de servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones públicas de salud peruanas.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: ARIAS MORENO FRANKLIN JHINO
1.2. Grado Académico y Profesión: MG. DIRECCIÓN DE SISTEMAS Y T.I.
1.3. Áreas de Experiencia Profesional: ÁREA DE SISTEMAS
1.4. Institución donde labora: MINISTERIO DE SALUD – MINSA
1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS.**

II. VALIDACIÓN

Se utilizarán los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - **[250-400],** Regular - **[450-600],** Buena: **[650-800],** Muy Buena - **[850-1000]**

ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy buena			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	El SGSI está formulado con lenguaje apropiado																			X	
OBJETIVIDAD	El SGSI está expresado en conductas observables																		X		
ACTUALIDAD	El SGSI es adecuado al avance de la gestión de la seguridad de la información de servicios en la nube																			X	
ORGANIZACIÓN	El SGSI muestra una organización lógica																		X		
SUFICIENCIA	El SGSI comprende los aspectos en cantidad y calidad																			X	
INTENCIONALIDAD	El SGSI es adecuado para valorar la gestión de la seguridad de la información de servicios en la nube																		X		
CONSISTENCIA	El SGSI está basado en aspectos teóricos científicos de la seguridad de la información de servicios en la nube																			X	
COHERENCIA	El SGSI muestra coherencia entre cada una de sus actividades																		X		
METODOLOGÍA	El SGSI en cuanto a su estrategia responde al propósito de la investigación																			X	
PERTINENCIA	El SGSI es útil y adecuado para la investigación																			X	

VALORACIÓN: _____930_____

OPINIÓN DE APLICABILIDAD: _____ **MUY BUENA PROPUESTA**_____

Lugar y fecha: Chiclayo, __07__ noviembre del 2022.

EXPERTO 02: Mg. Sosa Suarez Doris Elizabeth

VALIDACIÓN POR JUICIO DE EXPERTOS
INSTRUMENTO DE RECOLECCIÓN

Título de la investigación:

DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS

Autor:

Dávila Chunga Dayán Ray

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente sistema de gestión de seguridad de la información de servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones públicas de salud peruanas.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: SOSA SUAREZ DORIS ELIZABETH

1.2. Grado Académico y Profesión: MG. DIRECCIÓN DE SISTEMAS Y T.I.

1.3. Áreas de Experiencia Profesional: ÁREA DE SISTEMAS

1.4. Institución donde labora: INSTITUTO NACIONAL DE SALUD - INS

1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS.**

II. VALIDACIÓN

Se utilizarán los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - **[250-400],** Regular - **[450-600],** Buena: **[650-800],** Muy Buena - **[850-1000]**

ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy buena			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	El SGSI está formulado con lenguaje apropiado																			X	
OBJETIVIDAD	El SGSI está expresado en conductas observables																		X		
ACTUALIDAD	El SGSI es adecuado al avance de la gestión de la seguridad de la información de servicios en la nube																			X	
ORGANIZACIÓN	El SGSI muestra una organización lógica																		X		
SUFICIENCIA	El SGSI comprende los aspectos en cantidad y calidad																			X	
INTENCIONALIDAD	El SGSI es adecuado para valorar la gestión de la seguridad de la información de servicios en la nube																		X		
CONSISTENCIA	El SGSI está basado en aspectos teóricos científicos de la seguridad de la información de servicios en la nube																			X	
COHERENCIA	El SGSI muestra coherencia entre cada una de sus actividades																		X		
METODOLOGÌA	El SGSI en cuanto a su estrategia responde al propósito de la investigación																			X	
PERTINENCIA	El SGSI es útil y adecuado para la investigación																			X	

VALORACIÓN: _____930_____

OPINIÓN DE APLICABILIDAD: _____ **MUY BUENA PROPUESTA**_____

Lugar y fecha: Chiclayo, __07__ noviembre del 2022.

DSosa

EXPERTO 03: Mg. (c) Bocanegra Pinchi Yan Carlos

VALIDACIÓN POR JUICIO DE EXPERTOS
INSTRUMENTO DE RECOLECCIÓN

Título de la investigación:

DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS

Autor:

Dávila Chunga Dayán Ray

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente sistema de gestión de seguridad de la información de servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones públicas de salud peruanas.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: BOCANEGRA PINCHI YAN CARLOS

1.2. Grado Académico y Profesión: Mg. (c) INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

1.3. Áreas de Experiencia Profesional: INGENIERÍA DE SISTEMAS

1.4. Institución donde labora: BLACKTECH CONSULTING SRL

1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS.**

II. VALIDACIÓN

Se utilizarán los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - **[250-400]**, Regular - **[450-600]**, Buena: **[650-800]**, Muy Buena - **[850-1000]**

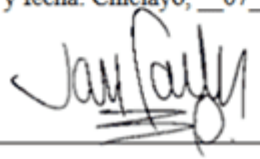
ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy buena			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	El SGSI está formulado con lenguaje apropiado																		X		
OBJETIVIDAD	El SGSI está expresado en conductas observables																			X	
ACTUALIDAD	El SGSI es adecuado al avance de la gestión de la seguridad de la información de servicios en la nube																		X		
ORGANIZACIÓN	El SGSI muestra una organización lógica																			X	
SUFICIENCIA	El SGSI comprende los aspectos en cantidad y calidad																		X		
INTENCIONALIDAD	El SGSI es adecuado para valorar la gestión de la seguridad de la información de servicios en la nube																			X	
CONSISTENCIA	El SGSI está basado en aspectos teóricos científicos de la seguridad de la información de servicios en la nube																		X		
COHERENCIA	El SGSI muestra coherencia entre cada una de sus actividades																			X	
METODOLOGÌA	El SGSI en cuanto a su estrategia responde al propósito de la investigación																		X		
PERTINENCIA	El SGSI es útil y adecuado para la investigación																			X	

VALORACIÓN: _____925_____

OPINIÓN DE APLICABILIDAD: _____ MUY BUENA PROPUESTA_____

Lugar y fecha: Chiclayo, __07__ noviembre del 2022.



EXPERTO 04: Mg. Meres Morales Evelyn Rosalía

VALIDACIÓN POR JUICIO DE EXPERTOS
INSTRUMENTO DE RECOLECCIÓN

Título de la investigación:

DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS

Autor:

Dávila Chunga Dayán Ray

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente sistema de gestión de seguridad de la información de servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones públicas de salud peruanas.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: MERES MORALES EVELYN ROSALIA

1.2. Grado Académico y Profesión: Mg. EN DIRECCIÓN DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN

1.3. Áreas de Experiencia Profesional: INGENIERÍA DE SISTEMAS

1.4. Institución donde labora: CANVIA "Servicios y tecnologías de la información"

1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS.**

II. VALIDACIÓN

Se utilizarán los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - **[250-400]**, Regular - **[450-600]**, Buena: **[650-800]**, Muy Buena - **[850-1000]**

ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy buena			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	El SGSI está formulado con lenguaje apropiado																			X	
OBJETIVIDAD	El SGSI está expresado en conductas observables																		X		
ACTUALIDAD	El SGSI es adecuado al avance de la gestión de la seguridad de la información de servicios en la nube																			X	
ORGANIZACIÓN	El SGSI muestra una organización lógica																		X		
SUFICIENCIA	El SGSI comprende los aspectos en cantidad y calidad																			X	
INTENCIONALIDAD	El SGSI es adecuado para valorar la gestión de la seguridad de la información de servicios en la nube																		X		
CONSISTENCIA	El SGSI está basado en aspectos teóricos científicos de la seguridad de la información de servicios en la nube																			X	
COHERENCIA	El SGSI muestra coherencia entre cada una de sus actividades																		X		
METODOLOGÌA	El SGSI en cuanto a su estrategia responde al propósito de la investigación																			X	
PERTINENCIA	El SGSI es útil y adecuado para la investigación																			X	

VALORACIÓN: _____930_____

OPINIÓN DE APLICABILIDAD: _____ MUY BUENA PROPUESTA_____

Lugar y fecha: Chiclayo, __07__ noviembre del 2022.

EXPERTO 05: Mg. Solano Lazo Úrsula Carola

VALIDACIÓN POR JUICIO DE EXPERTOS
INSTRUMENTO DE RECOLECCIÓN

Título de la investigación:

DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS

Autor:

Dávila Chunga Dayán Ray

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente sistema de gestión de seguridad de la información de servicios en la nube basado en la norma ISO/IEC 27017 para mejorar la seguridad de la información en instituciones públicas de salud peruanas.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: SOLANO LAZO URSULA CAROLA

1.2. Grado Académico y Profesión: Mg. DIRECCIÓN DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN

1.3. Áreas de Experiencia Profesional: INGENIERÍA DE SISTEMAS

1.4. Institución donde labora: **CANVIA** "Servicios y tecnologías de la información"

1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SERVICIOS EN LA NUBE BASADO EN LA NORMA ISO/IEC 27017 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS PERUANAS.**

II. VALIDACIÓN

Se utilizarán los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - **[250-400]**, Regular - **[450-600]**, Buena: **[650-800]**, Muy Buena - **[850-1000]**

ASPECTOS DE VALIDACIÓN

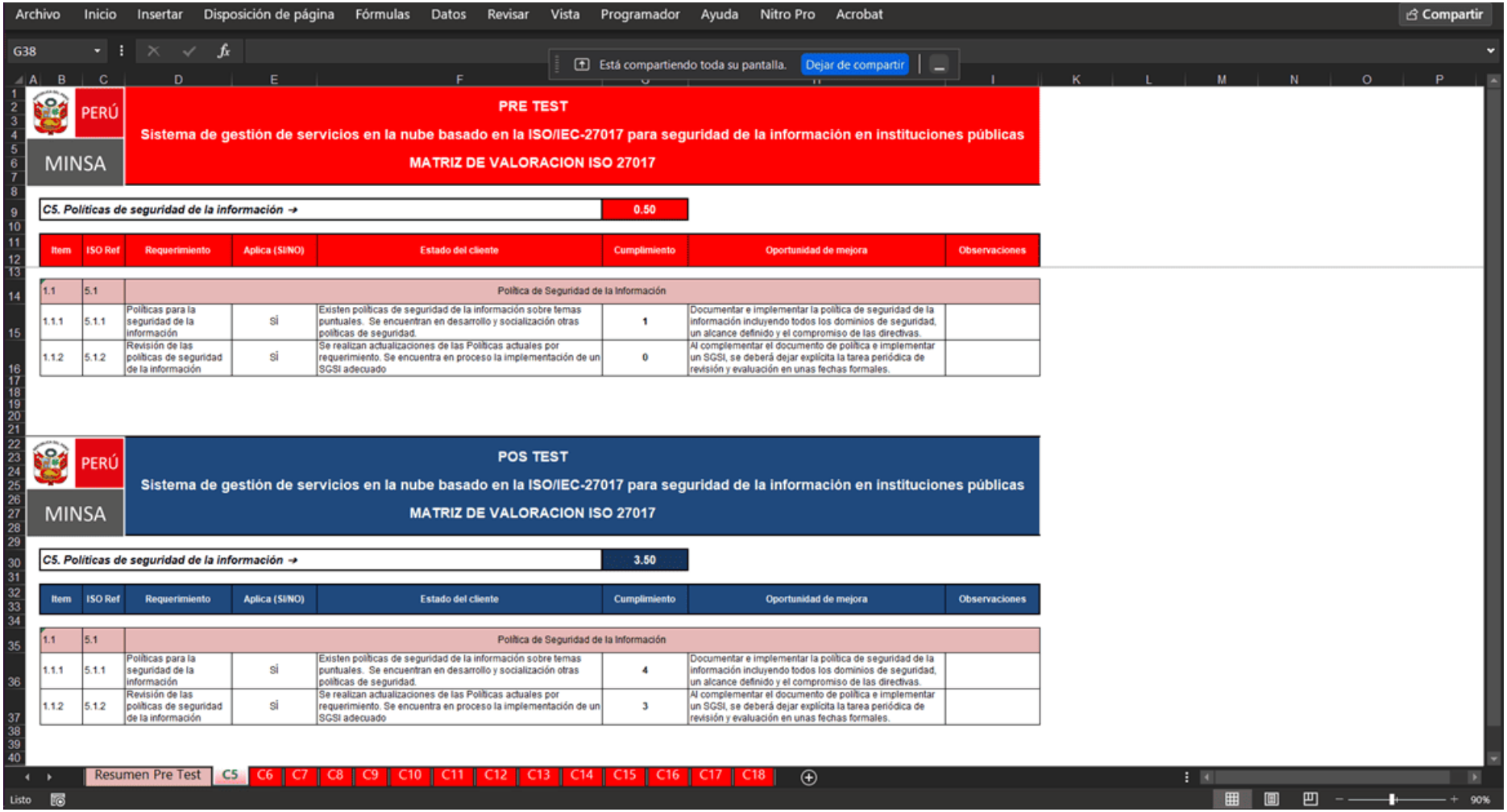
Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy buena			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	El SGSI está formulado con lenguaje apropiado																			X	
OBJETIVIDAD	El SGSI está expresado en conductas observables																		X		
ACTUALIDAD	El SGSI es adecuado al avance de la gestión de la seguridad de la información de servicios en la nube																			X	
ORGANIZACIÓN	El SGSI muestra una organización lógica																		X		
SUFICIENCIA	El SGSI comprende los aspectos en cantidad y calidad																			X	
INTENCIONALIDAD	El SGSI es adecuado para valorar la gestión de la seguridad de la información de servicios en la nube																		X		
CONSISTENCIA	El SGSI está basado en aspectos teóricos científicos de la seguridad de la información de servicios en la nube																			X	
COHERENCIA	El SGSI muestra coherencia entre cada una de sus actividades																		X		
METODOLOGÌA	El SGSI en cuanto a su estrategia responde al propósito de la investigación																			X	
PERTINENCIA	El SGSI es útil y adecuado para la investigación																			X	

VALORACIÓN: _____930_____

OPINIÓN DE APLICABILIDAD: _____ MUY BUENA PROPUESTA_____

Lugar y fecha: Chiclayo, __07__ noviembre del 2022.

Anexo 8. Análisis de brechas en cuanto a cumplimiento ISO/IEC 27017



PERÚ
MINSA

PRE TEST

Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas

MATRIZ DE VALORACION ISO 27017

C5. Políticas de seguridad de la información →	0.50

Item	ISO Ref	Requerimiento	Aplica (SI/NO)	Estado del cliente	Cumplimiento	Oportunidad de mejora	Observaciones
1.1	5.1	Política de Seguridad de la Información					
1.1.1	5.1.1	Políticas para la seguridad de la información	SÍ	Existen políticas de seguridad de la información sobre temas puntuales. Se encuentran en desarrollo y socialización otras políticas de seguridad.	1	Documentar e implementar la política de seguridad de la información incluyendo todos los dominios de seguridad, un alcance definido y el compromiso de las directivas.	
1.1.2	5.1.2	Revisión de las políticas de seguridad de la información	SÍ	Se realizan actualizaciones de las Políticas actuales por requerimiento. Se encuentra en proceso la implementación de un SGSI adecuado	0	Al complementar el documento de política e implementar un SGSI, se deberá dejar explícita la tarea periódica de revisión y evaluación en unas fechas formales.	

PERÚ
MINSA

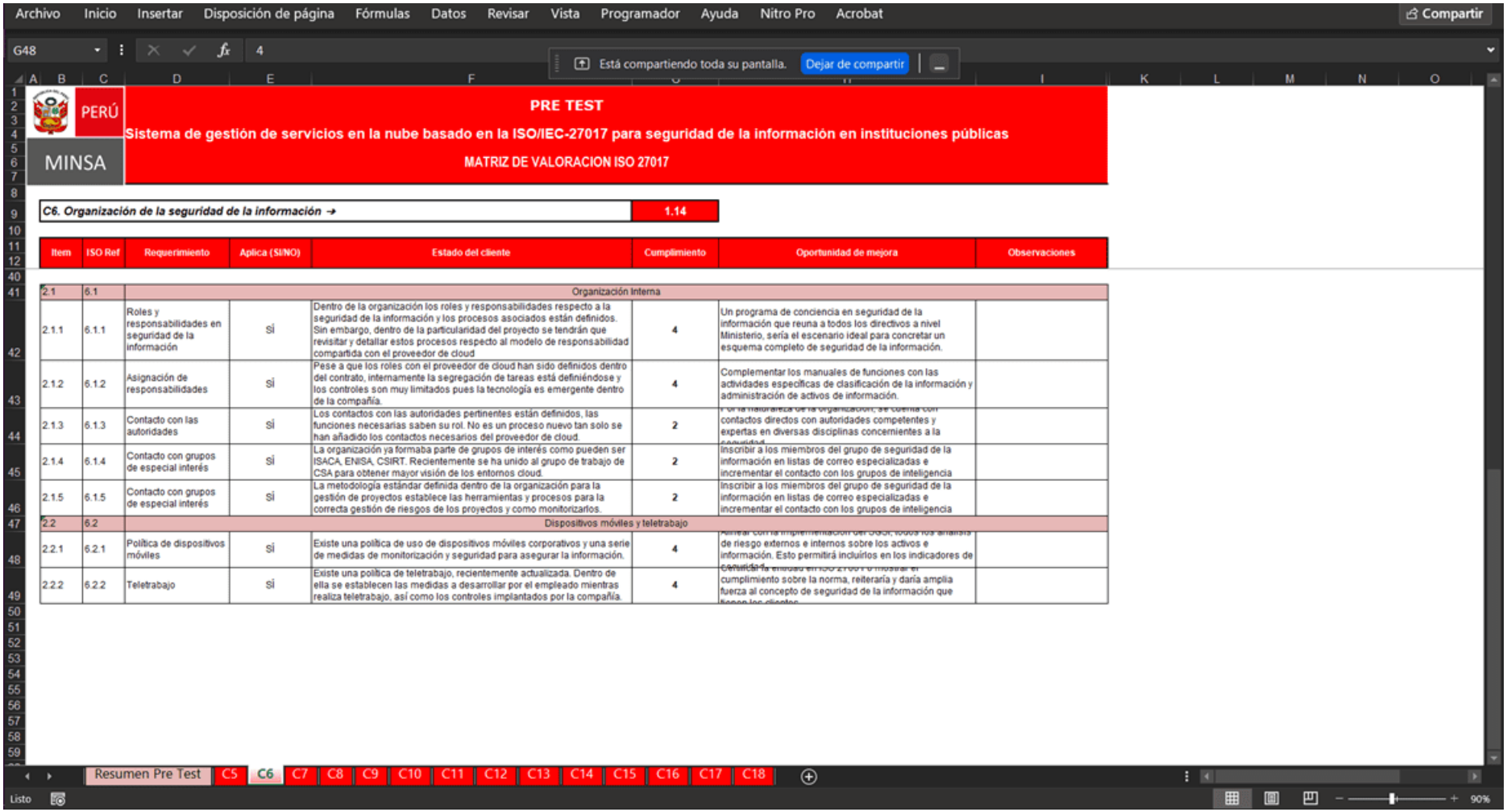
POS TEST

Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas

MATRIZ DE VALORACION ISO 27017

C5. Políticas de seguridad de la información →	3.50

Item	ISO Ref	Requerimiento	Aplica (SI/NO)	Estado del cliente	Cumplimiento	Oportunidad de mejora	Observaciones
1.1	5.1	Política de Seguridad de la Información					
1.1.1	5.1.1	Políticas para la seguridad de la información	SÍ	Existen políticas de seguridad de la información sobre temas puntuales. Se encuentran en desarrollo y socialización otras políticas de seguridad.	4	Documentar e implementar la política de seguridad de la información incluyendo todos los dominios de seguridad, un alcance definido y el compromiso de las directivas.	
1.1.2	5.1.2	Revisión de las políticas de seguridad de la información	SÍ	Se realizan actualizaciones de las Políticas actuales por requerimiento. Se encuentra en proceso la implementación de un SGSI adecuado	3	Al complementar el documento de política e implementar un SGSI, se deberá dejar explícita la tarea periódica de revisión y evaluación en unas fechas formales.	



PERÚ

MINSA

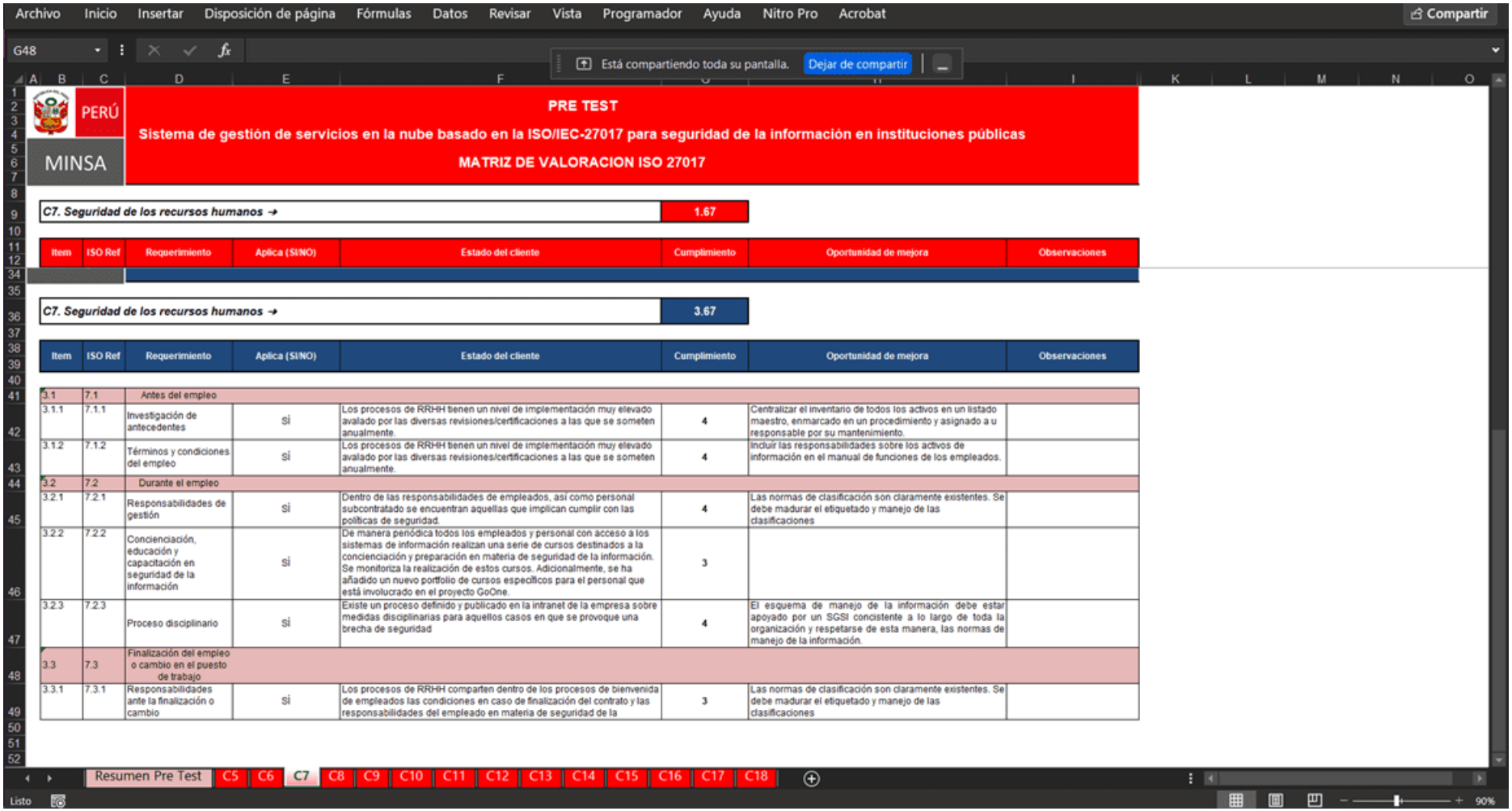
PRE TEST

Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas

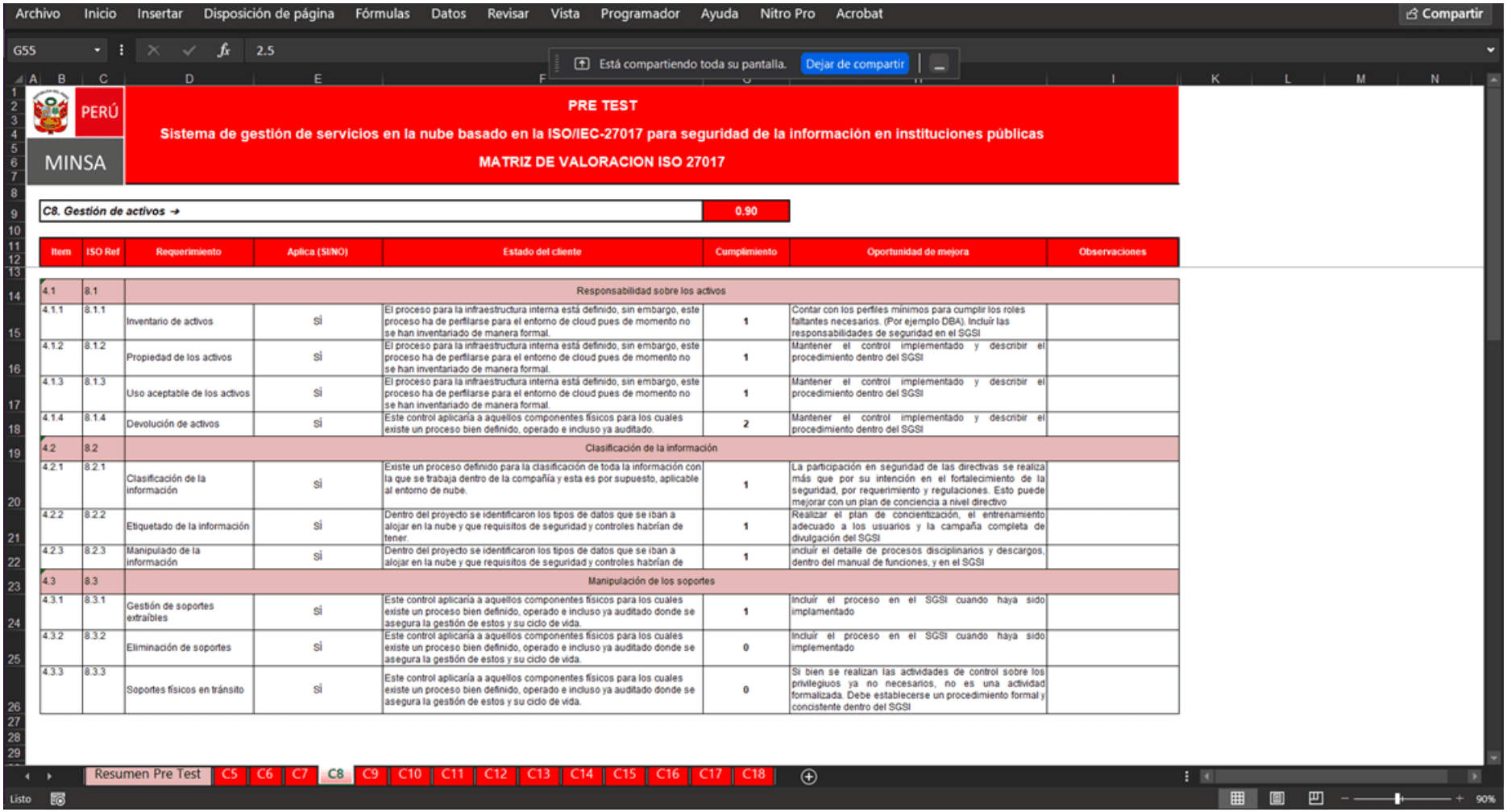
MATRIZ DE VALORACION ISO 27017

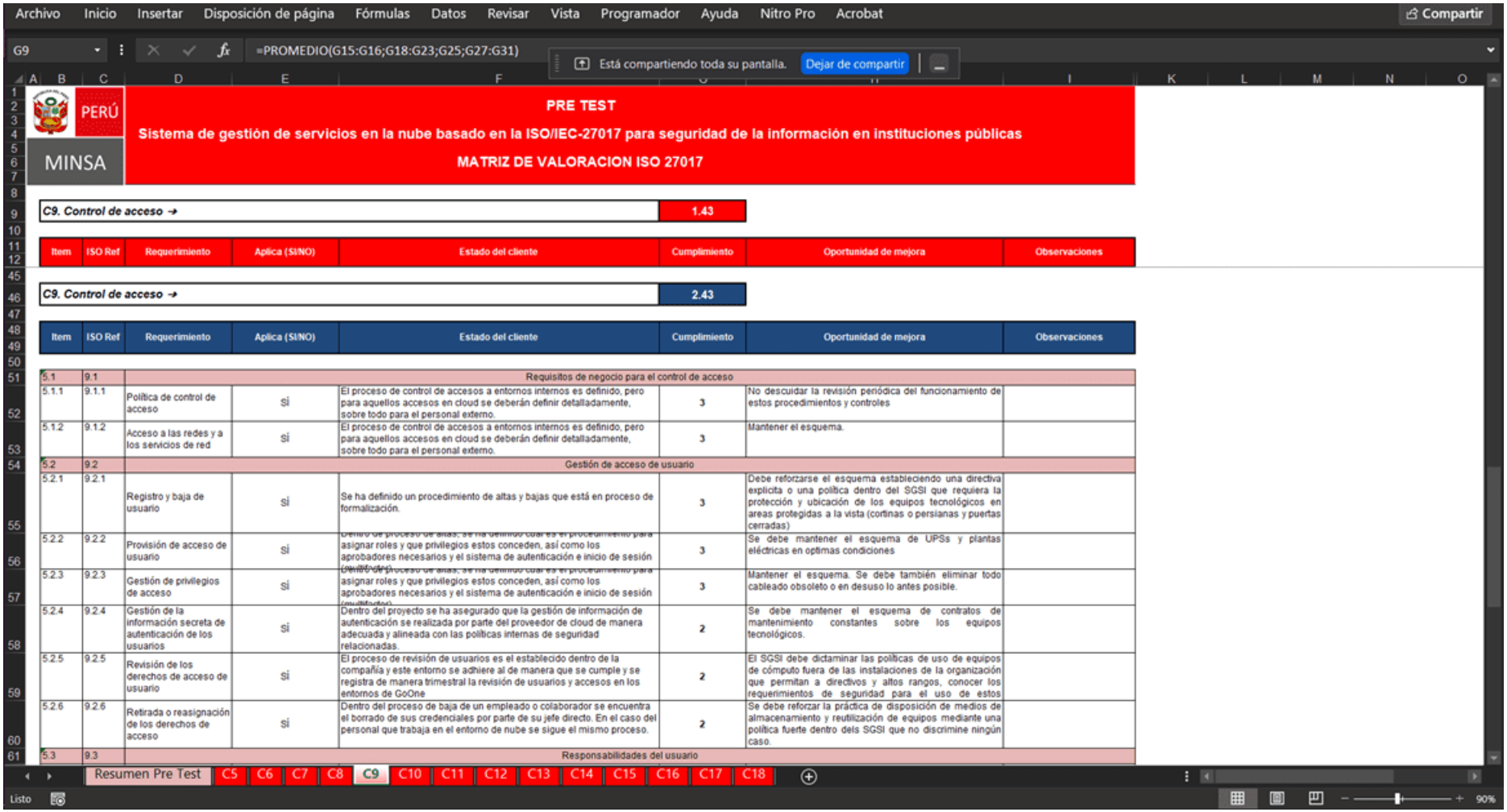
C6. Organización de la seguridad de la información →	1.14

Item	ISO Ref	Requerimiento	Aplica (SI/NO)	Estado del cliente	Cumplimiento	Oportunidad de mejora	Observaciones
2.1	6.1	Organización Interna					
2.1.1	6.1.1	Roles y responsabilidades en seguridad de la información	Sí	Dentro de la organización los roles y responsabilidades respecto a la seguridad de la información y los procesos asociados están definidos. Sin embargo, dentro de la particularidad del proyecto se tendrán que revisitar y detallar estos procesos respecto al modelo de responsabilidad compartida con el proveedor de cloud	4	Un programa de conciencia en seguridad de la información que reuna a todos los directivos a nivel Ministerio, sería el escenario ideal para concretar un esquema completo de seguridad de la información.	
2.1.2	6.1.2	Asignación de responsabilidades	Sí	Pese a que los roles con el proveedor de cloud han sido definidos dentro del contrato, internamente la segregación de tareas está definiéndose y los controles son muy limitados pues la tecnología es emergente dentro de la compañía.	4	Complementar los manuales de funciones con las actividades especificas de clasificación de la información y administración de activos de información.	
2.1.3	6.1.3	Contacto con las autoridades	Sí	Los contactos con las autoridades pertinentes están definidos, las funciones necesarias saben su rol. No es un proceso nuevo tan solo se han añadido los contactos necesarios del proveedor de cloud.	2	Por la naturaleza de la organización, se cuenta con contactos directos con autoridades competentes y expertas en diversas disciplinas concernientes a la seguridad	
2.1.4	6.1.4	Contacto con grupos de especial interés	Sí	La organización ya formaba parte de grupos de interés como pueden ser ISACA, ENISA, CSIRT. Recientemente se ha unido al grupo de trabajo de CSA para obtener mayor visión de los entornos cloud.	2	Inscribir a los miembros del grupo de seguridad de la información en listas de correo especializadas e incrementar el contacto con los grupos de inteligencia	
2.1.5	6.1.5	Contacto con grupos de especial interés	Sí	La metodología estándar definida dentro de la organización para la gestión de proyectos establece las herramientas y procesos para la correcta gestión de riesgos de los proyectos y como monitorizarlos.	2	Inscribir a los miembros del grupo de seguridad de la información en listas de correo especializadas e incrementar el contacto con los grupos de inteligencia	
2.2	6.2	Dispositivos móviles y teletrabajo					
2.2.1	6.2.1	Política de dispositivos móviles	Sí	Existe una política de uso de dispositivos móviles corporativos y una serie de medidas de monitorización y seguridad para asegurar la información.	4	Alinear con la implementación del SGSI, todos los análisis de riesgo externos e internos sobre los activos e información. Esto permitirá incluirlos en los indicadores de seguridad	
2.2.2	6.2.2	Teletrabajo	Sí	Existe una política de teletrabajo, recientemente actualizada. Dentro de ella se establecen las medidas a desarrollar por el empleado mientras realiza teletrabajo, así como los controles implantados por la compañía.	4	definidas en ISO 27001 o mostrar el cumplimiento sobre la norma, reiteraría y daría amplia fuerza al concepto de seguridad de la información que hacen los clientes	



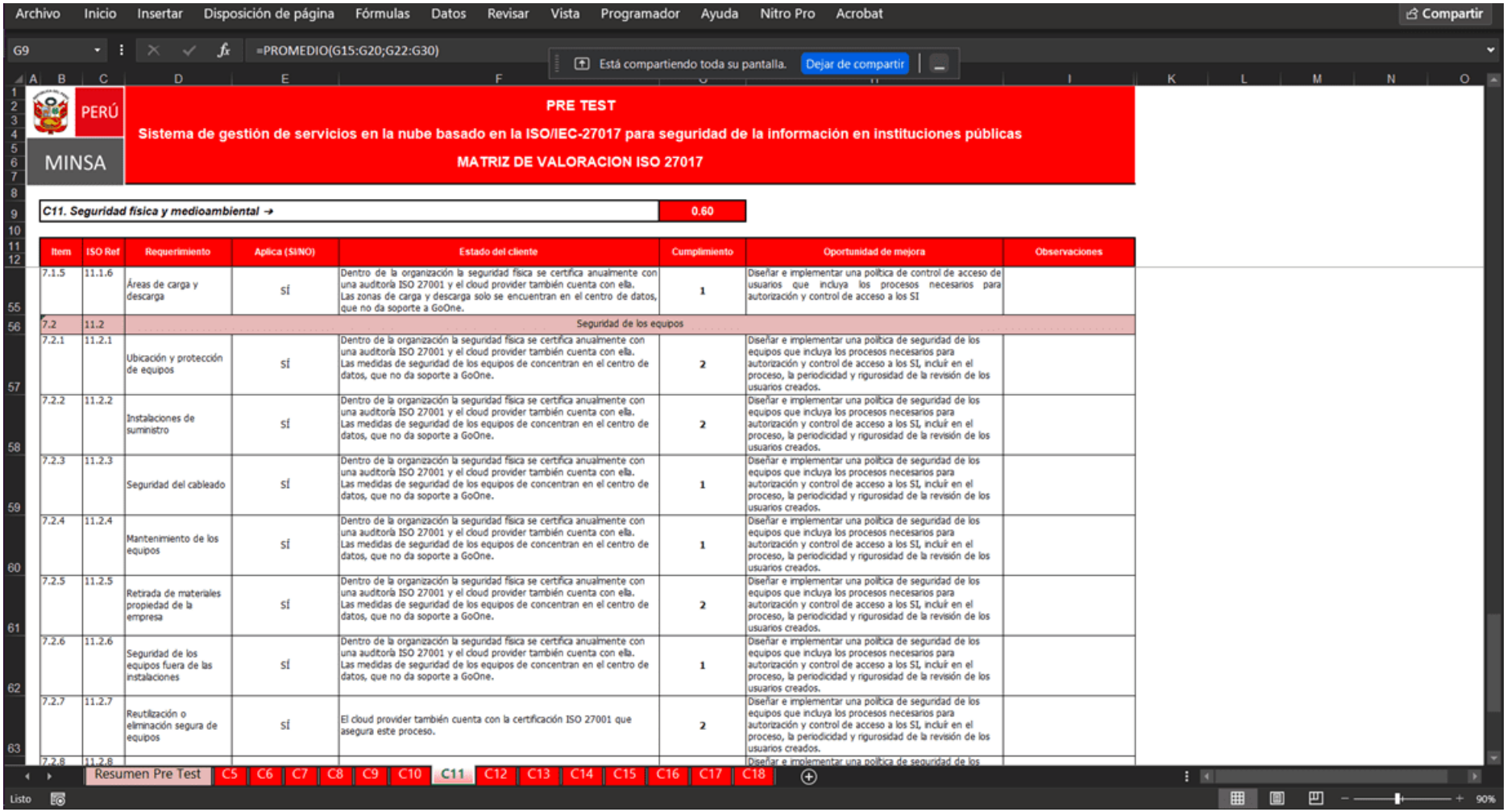
Item	ISO Ref	Requerimiento	Aplica (SI/NO)	Estado del cliente	Cumplimiento	Oportunidad de mejora	Observaciones
3.1	7.1	Antes del empleo					
3.1.1	7.1.1	Investigación de antecedentes	Sí	Los procesos de RRHH tienen un nivel de implementación muy elevado avalado por las diversas revisiones/certificaciones a las que se someten anualmente.	4	Centralizar el inventario de todos los activos en un listado maestro, enmarcado en un procedimiento y asignado a u responsable por su mantenimiento.	
3.1.2	7.1.2	Términos y condiciones del empleo	Sí	Los procesos de RRHH tienen un nivel de implementación muy elevado avalado por las diversas revisiones/certificaciones a las que se someten anualmente.	4	Incluir las responsabilidades sobre los activos de información en el manual de funciones de los empleados.	
3.2	7.2	Durante el empleo					
3.2.1	7.2.1	Responsabilidades de gestión	Sí	Dentro de las responsabilidades de empleados, así como personal subcontratado se encuentran aquellas que implican cumplir con las políticas de seguridad.	4	Las normas de clasificación son claramente existentes. Se debe madurar el etiquetado y manejo de las clasificaciones	
3.2.2	7.2.2	Concienciación, educación y capacitación en seguridad de la información	Sí	De manera periódica todos los empleados y personal con acceso a los sistemas de información realizan una serie de cursos destinados a la concienciación y preparación en materia de seguridad de la información. Se monitoriza la realización de estos cursos. Adicionalmente, se ha añadido un nuevo portfolio de cursos específicos para el personal que está involucrado en el proyecto GoOne.	3		
3.2.3	7.2.3	Proceso disciplinario	Sí	Existe un proceso definido y publicado en la intranet de la empresa sobre medidas disciplinarias para aquellos casos en que se provoque una brecha de seguridad	4	El esquema de manejo de la información debe estar apoyado por un SGSI concistente a lo largo de toda la organización y respetarse de esta manera, las normas de manejo de la información.	
3.3	7.3	Finalización del empleo o cambio en el puesto de trabajo					
3.3.1	7.3.1	Responsabilidades ante la finalización o cambio	Sí	Los procesos de RRHH comparten dentro de los procesos de bienvenida de empleados las condiciones en caso de finalización del contrato y las responsabilidades del empleado en materia de seguridad de la	3	Las normas de clasificación son claramente existentes. Se debe madurar el etiquetado y manejo de las clasificaciones	


Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Programador Ayuda Nitro Pro Acrobat
Compartir
G55
2.5
Está compartiendo toda su pantalla.
Dejar de compartir
PERÚ
MINSA
PRE TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C8. Gestión de activos →
0.90
Item
ISO Ref
Requerimiento
Aplica (SI/NO)
Estado del cliente
Cumplimiento
Oportunidad de mejora
Observaciones
4.1
8.1
Responsabilidad sobre los activos
4.1.1
8.1.1
Inventario de activos
SÍ
El proceso para la infraestructura interna está definido, sin embargo, este proceso ha de perfilarse para el entorno de cloud pues de momento no se han inventariado de manera formal.
1
Contar con los perfiles mínimos para cumplir los roles faltantes necesarios. (Por ejemplo DBA). Incluir las responsabilidades de seguridad en el SGSI
4.1.2
8.1.2
Propiedad de los activos
SÍ
El proceso para la infraestructura interna está definido, sin embargo, este proceso ha de perfilarse para el entorno de cloud pues de momento no se han inventariado de manera formal.
1
Mantener el control implementado y describir el procedimiento dentro del SGSI
4.1.3
8.1.3
Uso aceptable de los activos
SÍ
El proceso para la infraestructura interna está definido, sin embargo, este proceso ha de perfilarse para el entorno de cloud pues de momento no se han inventariado de manera formal.
1
Mantener el control implementado y describir el procedimiento dentro del SGSI
4.1.4
8.1.4
Devolución de activos
SÍ
Este control aplicaría a aquellos componentes físicos para los cuales existe un proceso bien definido, operado e incluso ya auditado.
2
Mantener el control implementado y describir el procedimiento dentro del SGSI
4.2
8.2
Clasificación de la información
4.2.1
8.2.1
Clasificación de la información
SÍ
Existe un proceso definido para la clasificación de toda la información con la que se trabaja dentro de la compañía y esta es por supuesto, aplicable al entorno de nube.
1
La participación en seguridad de las directivas se realiza más que por su intención en el fortalecimiento de la seguridad, por requerimiento y regulaciones. Esto puede mejorar con un plan de conciencia a nivel directivo
4.2.2
8.2.2
Etiquetado de la información
SÍ
Dentro del proyecto se identificaron los tipos de datos que se iban a alojar en la nube y que requisitos de seguridad y controles habrían de tener.
1
Realizar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI
4.2.3
8.2.3
Manipulado de la información
SÍ
Dentro del proyecto se identificaron los tipos de datos que se iban a alojar en la nube y que requisitos de seguridad y controles habrían de
1
incluir el detalle de procesos disciplinarios y descargos, dentro del manual de funciones, y en el SGSI
4.3
8.3
Manipulación de los soportes
4.3.1
8.3.1
Gestión de soportes extraíbles
SÍ
Este control aplicaría a aquellos componentes físicos para los cuales existe un proceso bien definido, operado e incluso ya auditado donde se asegura la gestión de estos y su ciclo de vida.
1
Incluir el proceso en el SGSI cuando haya sido implamentado
4.3.2
8.3.2
Eliminación de soportes
SÍ
Este control aplicaría a aquellos componentes físicos para los cuales existe un proceso bien definido, operado e incluso ya auditado donde se asegura la gestión de estos y su ciclo de vida.
0
Incluir el proceso en el SGSI cuando haya sido implementado
4.3.3
8.3.3
Soportes físicos en tránsito
SÍ
Este control aplicaría a aquellos componentes físicos para los cuales existe un proceso bien definido, operado e incluso ya auditado donde se asegura la gestión de estos y su ciclo de vida.
0
Si bien se realizan las actividades de control sobre los privilegiuos ya no necesarios, no es una actividad formalizada. Debe establecerse un procedimiento formal y concistente dentro del SGSI
Resumen Pre Test
C5
C6
C7
C8
C9
C10
C11
C12
C13
C14
C15
C16
C17
C18
Listo
90%

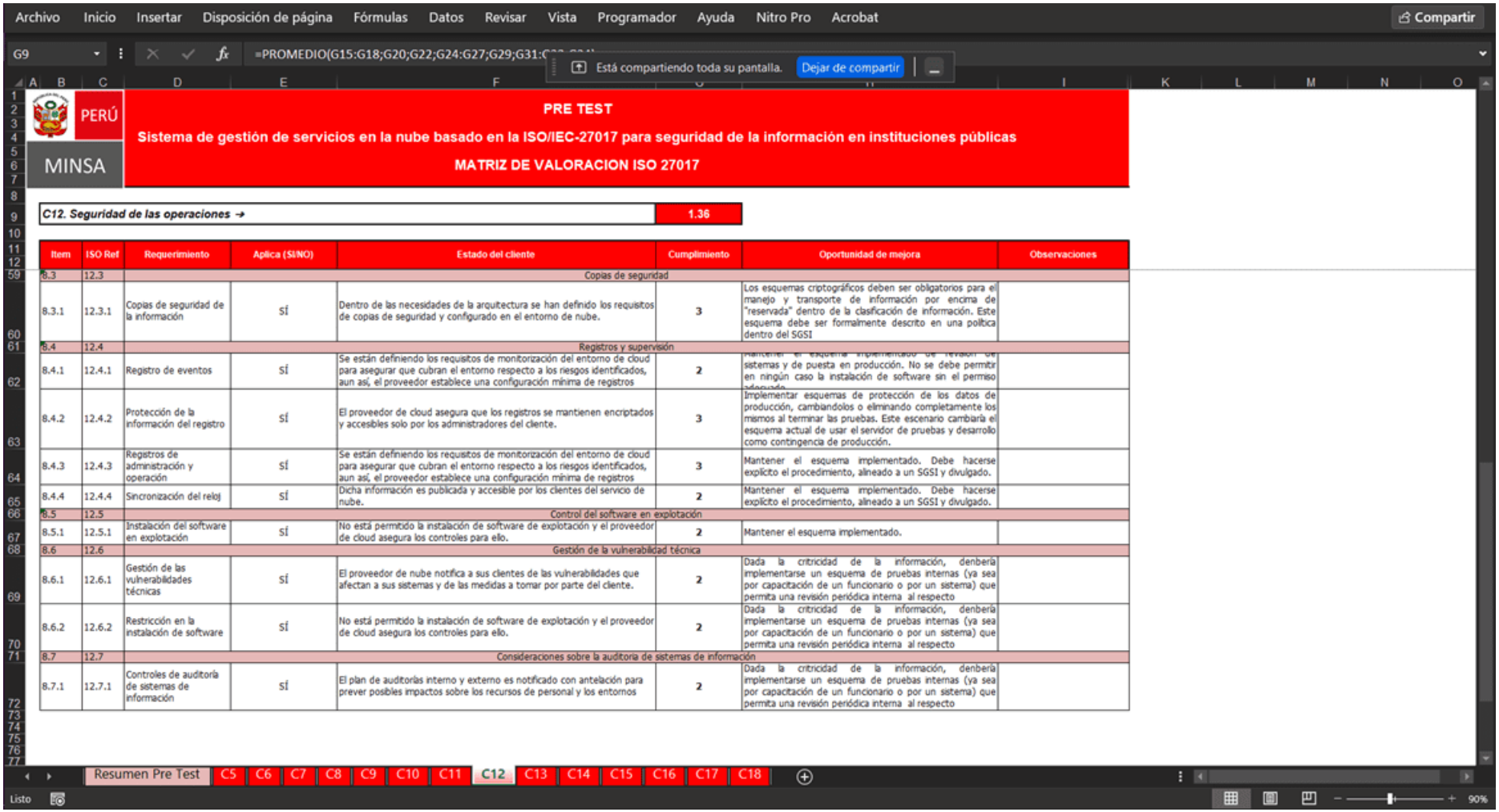


Item	ISO Ref	Requerimiento	Aplica (SI/NO)	Estado del cliente	Cumplimiento	Oportunidad de mejora	Observaciones
5.1	9.1	Requisitos de negocio para el control de acceso					
5.1.1	9.1.1	Política de control de acceso	Sí	El proceso de control de accesos a entornos internos es definido, pero para aquellos accesos en cloud se deberán definir detalladamente, sobre todo para el personal externo.	3	No descuidar la revisión periódica del funcionamiento de estos procedimientos y controles	
5.1.2	9.1.2	Acceso a las redes y a los servicios de red	Sí	El proceso de control de accesos a entornos internos es definido, pero para aquellos accesos en cloud se deberán definir detalladamente, sobre todo para el personal externo.	3	Mantener el esquema.	
5.2	9.2	Gestión de acceso de usuario					
5.2.1	9.2.1	Registro y baja de usuario	Sí	Se ha definido un procedimiento de altas y bajas que está en proceso de formalización.	3	Debe reforzarse el esquema estableciendo una directiva explicita o una política dentro del SGSI que requiera la protección y ubicación de los equipos tecnológicos en areas protegidas a la vista (cortinas o persianas y puertas cerradas)	
5.2.2	9.2.2	Provisión de acceso de usuario	Sí	Dentro de proceso de altas, se ha definido cual es el procedimiento para asignar roles y que privilegios estos conceden, así como los aprobadores necesarios y el sistema de autenticación e inicio de sesión (auditorías)	3	Se debe mantener el esquema de UPSs y plantas eléctricas en optimas condiciones	
5.2.3	9.2.3	Gestión de privilegios de acceso	Sí	Dentro de proceso de altas, se ha definido cual es el procedimiento para asignar roles y que privilegios estos conceden, así como los aprobadores necesarios y el sistema de autenticación e inicio de sesión (auditorías)	3	Mantener el esquema. Se debe también eliminar todo cableado obsoleto o en desuso lo antes posible.	
5.2.4	9.2.4	Gestión de la información secreta de autenticación de los usuarios	Sí	Dentro del proyecto se ha asegurado que la gestión de información de autenticación se realizada por parte del proveedor de cloud de manera adecuada y alineada con las políticas internas de seguridad relacionadas.	2	Se debe mantener el esquema de contratos de mantenimiento constantes sobre los equipos tecnológicos.	
5.2.5	9.2.5	Revisión de los derechos de acceso de usuario	Sí	El proceso de revisión de usuarios es el establecido dentro de la compañía y este entorno se adhiere al de manera que se cumple y se registra de manera trimestral la revisión de usuarios y accesos en los entornos de GoOne	2	El SGSI debe dictaminar las políticas de uso de equipos de cómputo fuera de las instalaciones de la organización que permitan a directivos y altos rangos, conocer los requerimientos de seguridad para el uso de estos	
5.2.6	9.2.6	Retirada o reasignación de los derechos de acceso	Sí	Dentro del proceso de baja de un empleado o colaborador se encuentra el borrado de sus credenciales por parte de su jefe directo. En el caso del personal que trabaja en el entorno de nube se sigue el mismo proceso.	2	Se debe reforzar la práctica de disposición de medios de almacenamiento y reutilización de equipos mediante una política fuerte dentro dels SGSI que no discrimine ningún caso.	
5.3	9.3	Responsabilidades del usuario					

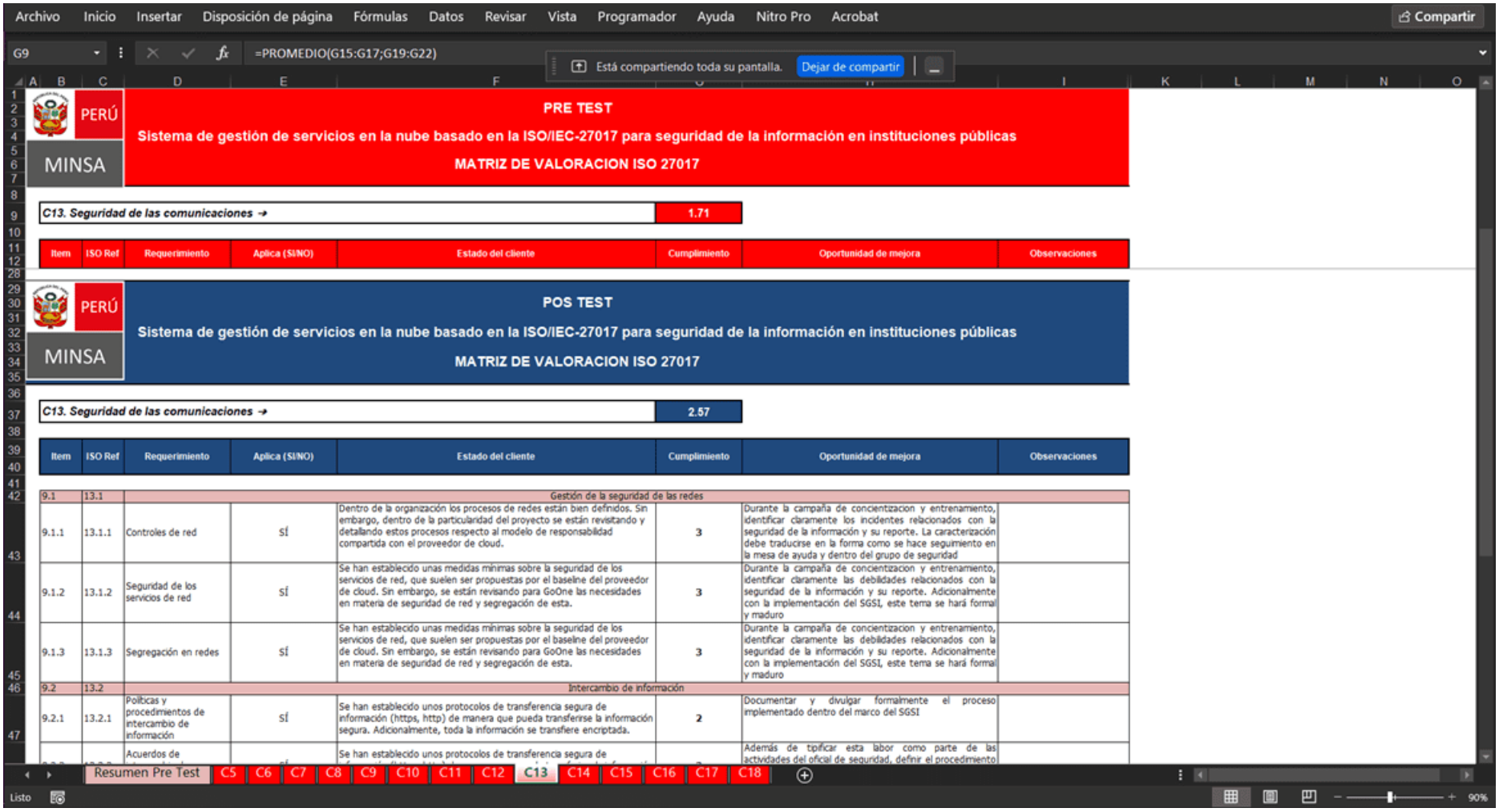

Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Programador Ayuda Nitro Pro Acrobat
Compartir
G9
=PROMEDIO(G15:G16)
Está compartiendo toda su pantalla.
Dejar de compartir
PERÚ
MINSA
PRE TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C10. Criptografía →
0.00
Item | ISO Ref | Requerimiento | Aplica (SI/NO) | Estado del cliente | Cumplimiento | Oportunidad de mejora | Observaciones
6.1 | 10.1 | Controles criptográficos
6.1.1 | 10.1.1 | Política de uso de los controles criptográficos | SI | Dentro de la organización existen escasos controles criptográficos, prácticamente nulos pero la Directiva de Seguridad en la nube establece ciertas particularidades que se están analizando respecto a los controles aplicados por el proveedor y su cumplimiento con la política interna. Adicionalmente, se está definiendo como conservar estas claves y manejar su ciclo de vida | 0 | Los manuales deben incluir procedimientos contingentes del área, así como las actividades en casos de emergencia. Todo debeestar alineado o incluido en el SGSI
6.1.2 | 10.1.2 | Gestión de claves | SI | Dentro de la organización existen escasos controles criptográficos pero la Directiva de Seguridad en la nube establece ciertas particularidades que se están analizando respecto a los controles aplicados por el proveedor y su cumplimiento con la política interna. Adicionalmente, se está definiendo como conservar estas claves y manejar su ciclo de vida | 0 | Los registros de control de cambios deben incluir los elementos de seguridad necesarios, la protección y revisión de los mismos y su inclusión en el SGSI
Página 1
PERÚ
MINSA
POS TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C10. Criptografía →
1.50
Item | ISO Ref | Requerimiento | Aplica (SI/NO) | Estado del cliente | Cumplimiento | Oportunidad de mejora | Observaciones
6.1 | 10.1 | Controles criptográficos
6.1.1 | 10.1.1 | Política de uso de los controles criptográficos | SI | Dentro de la organización existen escasos controles criptográficos pero la Directiva de Seguridad en la nube establece ciertas particularidades que se están analizando respecto a los controles aplicados por el proveedor y su cumplimiento con la política interna. Adicionalmente, se está | 2 | Los manuales deben incluir procedimientos contingentes del área, así como las actividades en casos de emergencia. Todo debeestar alineado o incluido en el SGSI
Resumen Pre Test C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18
Listo
80%

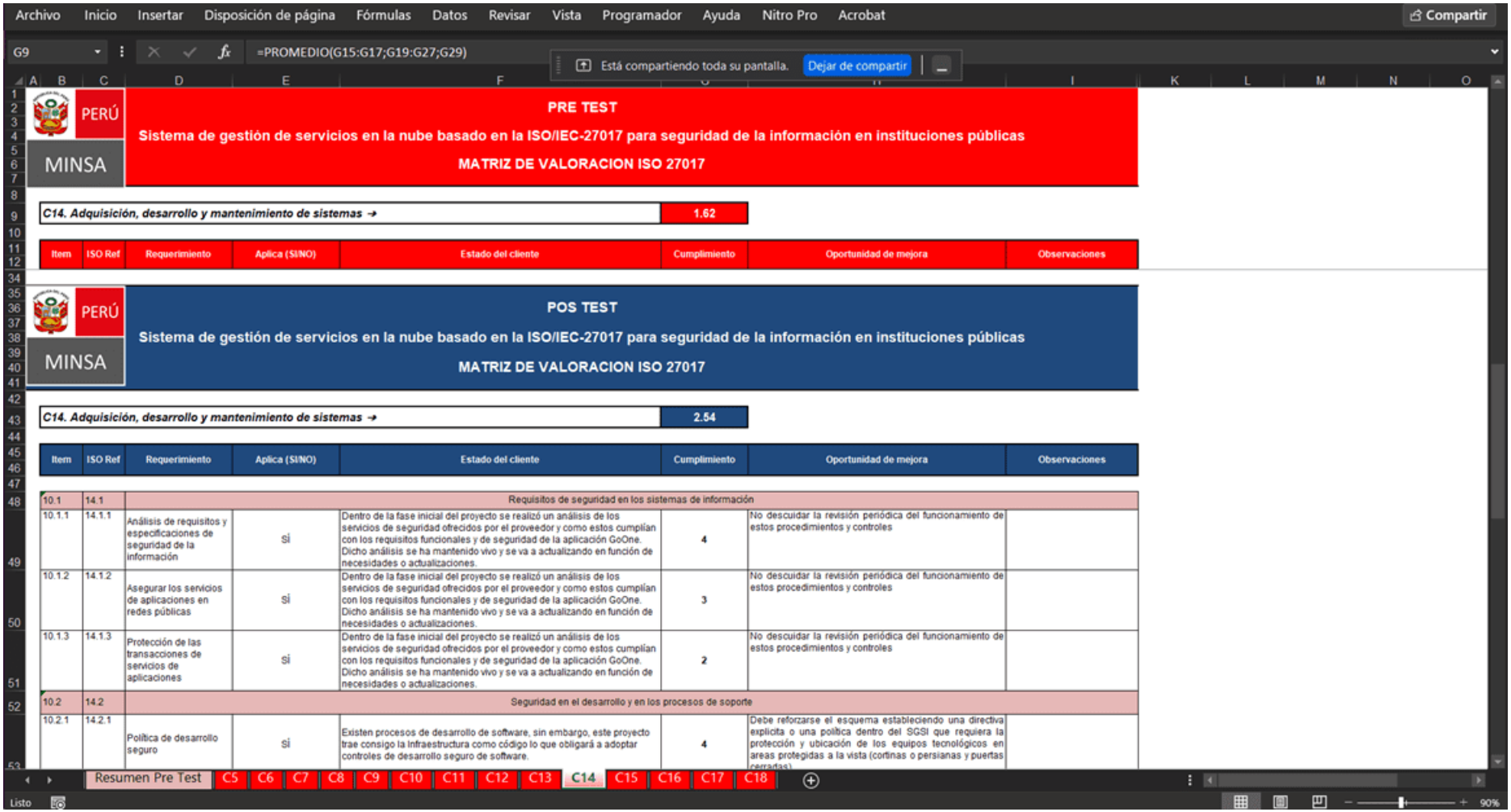


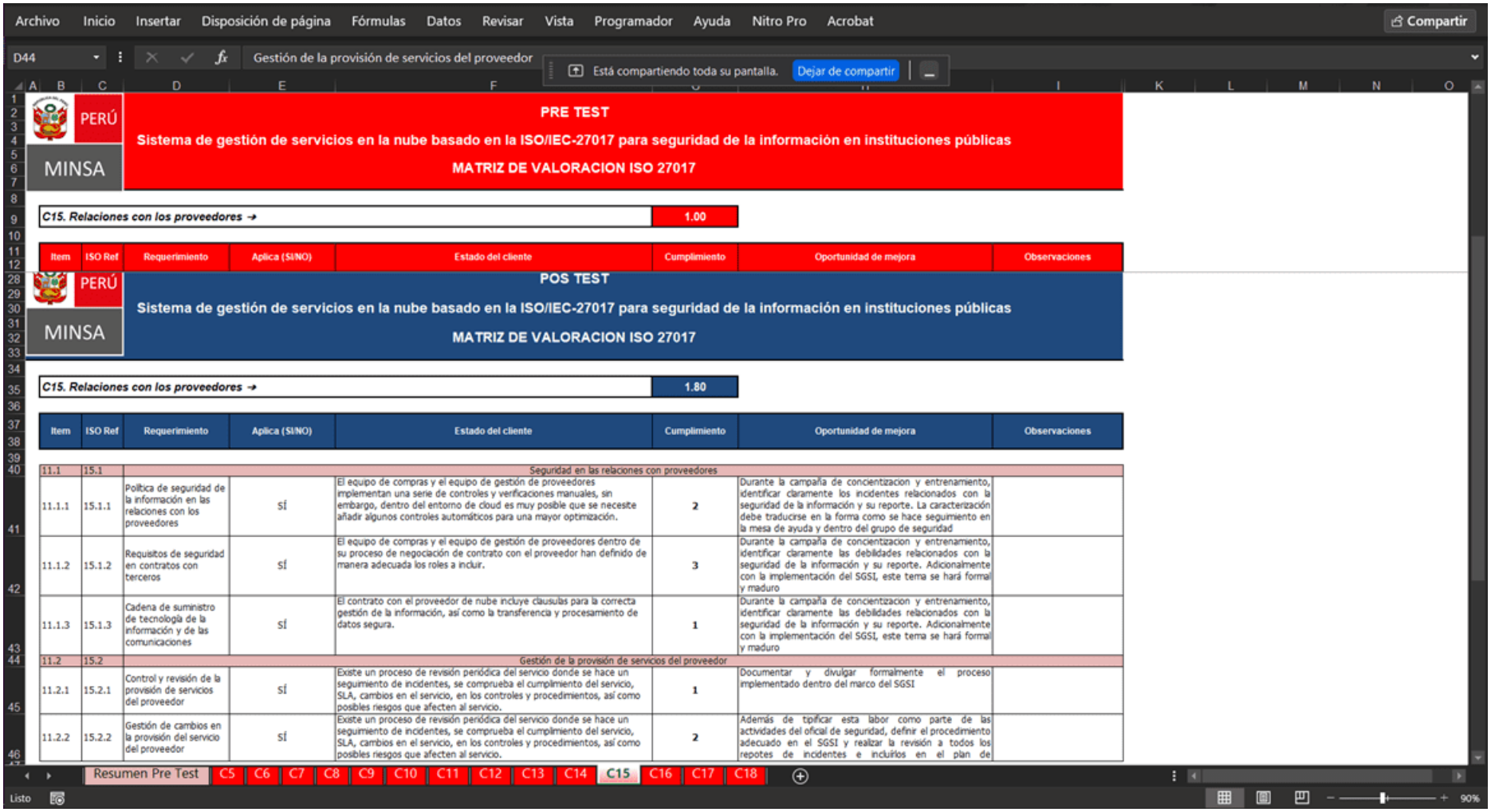
Item	ISO Ref	Requerimiento	Aplica (SI/NO)	Estado del cliente	Cumplimiento	Oportunidad de mejora	Observaciones
7.1.5	11.1.6	Áreas de carga y descarga	SÍ	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las zonas de carga y descarga solo se encuentran en el centro de datos, que no da soporte a GoOne.	1	Diseñar e implementar una política de control de acceso de usuarios que incluya los procesos necesarios para autorización y control de acceso a los SI	
7.2	11.2	Seguridad de los equipos					
7.2.1	11.2.1	Ubicación y protección de equipos	SÍ	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las medidas de seguridad de los equipos de concentran en el centro de datos, que no da soporte a GoOne.	2	Diseñar e implementar una política de seguridad de los equipos que incluya los procesos necesarios para autorización y control de acceso a los SI, incluir en el proceso, la periodicidad y rigurosidad de la revisión de los usuarios creados.	
7.2.2	11.2.2	Instalaciones de suministro	SÍ	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las medidas de seguridad de los equipos de concentran en el centro de datos, que no da soporte a GoOne.	2	Diseñar e implementar una política de seguridad de los equipos que incluya los procesos necesarios para autorización y control de acceso a los SI, incluir en el proceso, la periodicidad y rigurosidad de la revisión de los usuarios creados.	
7.2.3	11.2.3	Seguridad del cableado	SÍ	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las medidas de seguridad de los equipos de concentran en el centro de datos, que no da soporte a GoOne.	1	Diseñar e implementar una política de seguridad de los equipos que incluya los procesos necesarios para autorización y control de acceso a los SI, incluir en el proceso, la periodicidad y rigurosidad de la revisión de los usuarios creados.	
7.2.4	11.2.4	Mantenimiento de los equipos	SÍ	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las medidas de seguridad de los equipos de concentran en el centro de datos, que no da soporte a GoOne.	1	Diseñar e implementar una política de seguridad de los equipos que incluya los procesos necesarios para autorización y control de acceso a los SI, incluir en el proceso, la periodicidad y rigurosidad de la revisión de los usuarios creados.	
7.2.5	11.2.5	Retirada de materiales propiedad de la empresa	SÍ	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las medidas de seguridad de los equipos de concentran en el centro de datos, que no da soporte a GoOne.	2	Diseñar e implementar una política de seguridad de los equipos que incluya los procesos necesarios para autorización y control de acceso a los SI, incluir en el proceso, la periodicidad y rigurosidad de la revisión de los usuarios creados.	
7.2.6	11.2.6	Seguridad de los equipos fuera de las instalaciones	SÍ	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las medidas de seguridad de los equipos de concentran en el centro de datos, que no da soporte a GoOne.	1	Diseñar e implementar una política de seguridad de los equipos que incluya los procesos necesarios para autorización y control de acceso a los SI, incluir en el proceso, la periodicidad y rigurosidad de la revisión de los usuarios creados.	
7.2.7	11.2.7	Reutilización o eliminación segura de equipos	SÍ	El cloud provider también cuenta con la certificación ISO 27001 que asegura este proceso.	2	Diseñar e implementar una política de seguridad de los equipos que incluya los procesos necesarios para autorización y control de acceso a los SI, incluir en el proceso, la periodicidad y rigurosidad de la revisión de los usuarios creados.	
7.2.8	11.2.8					Diseñar e implementar una política de seguridad de los	

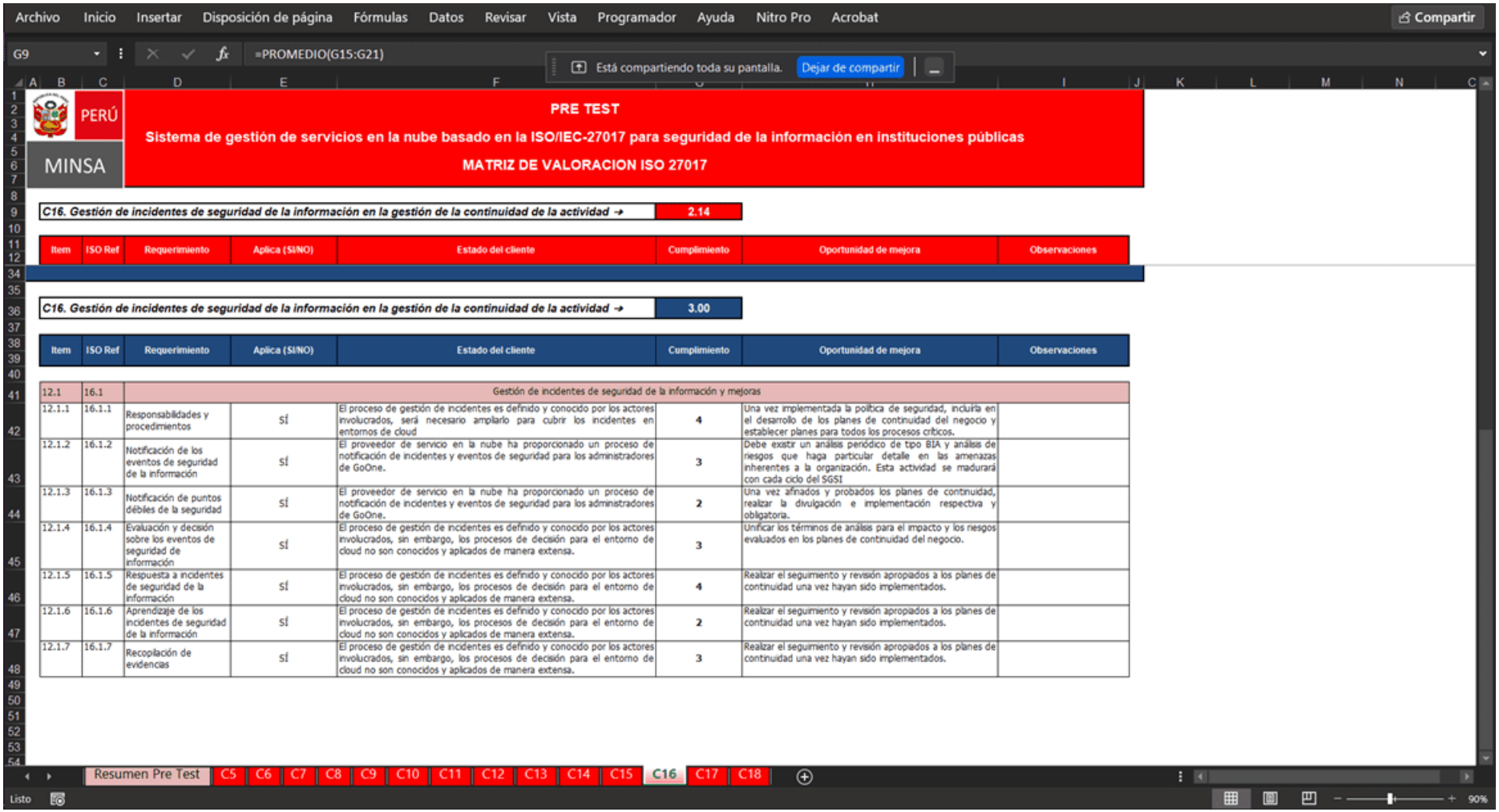


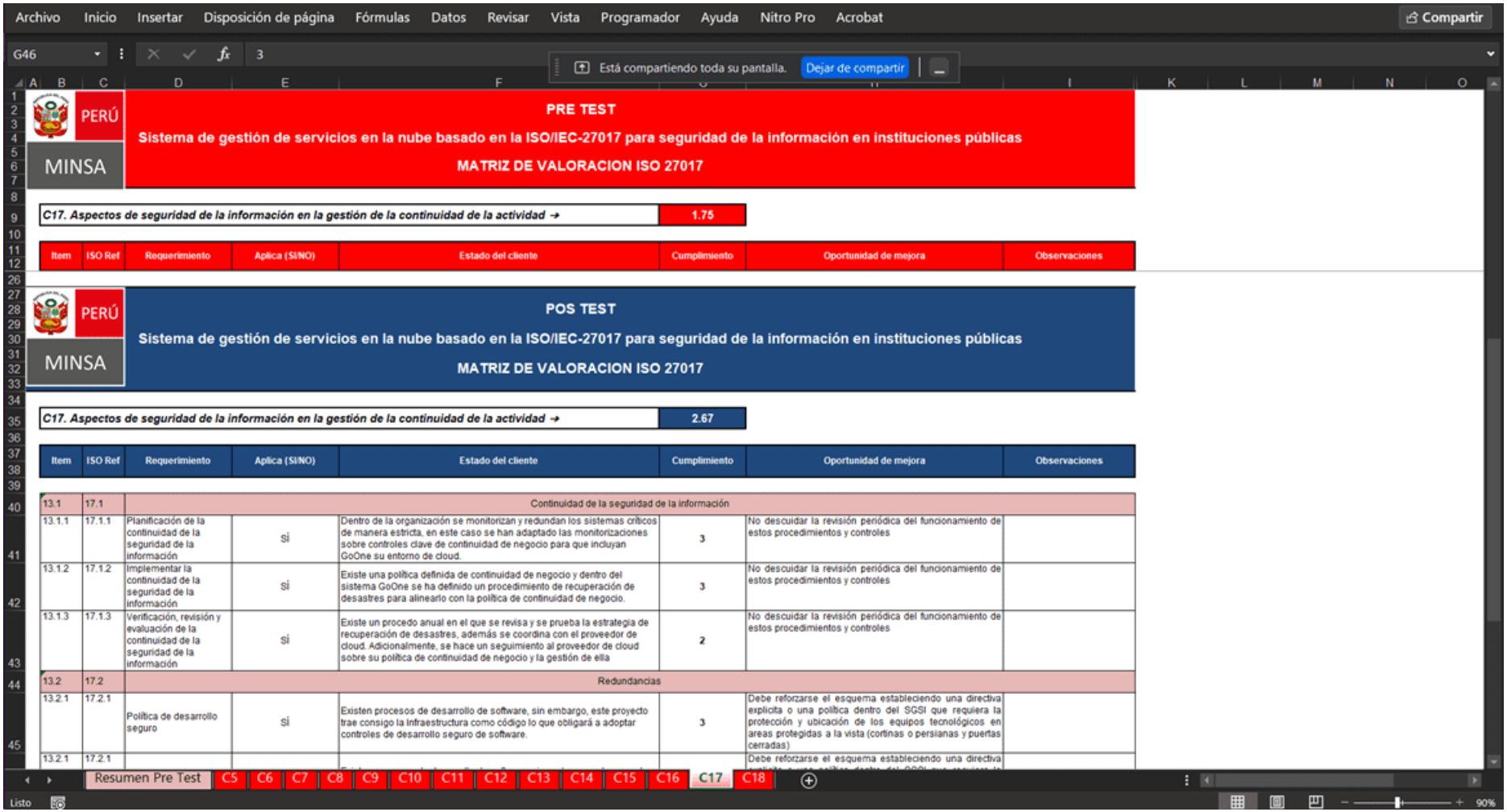
Item	ISO Ref	Requerimiento	Aplica (SI/NO)	Estado del cliente	Cumplimiento	Oportunidad de mejora	Observaciones
8.3	12.3			Copias de seguridad			
8.3.1	12.3.1	Copias de seguridad de la información	SÍ	Dentro de las necesidades de la arquitectura se han definido los requisitos de copias de seguridad y configurado en el entorno de nube.	3	Los esquemas criptográficos deben ser obligatorios para el manejo y transporte de información por encima de "reservada" dentro de la clasificación de información. Este esquema debe ser formalmente descrito en una política dentro del SGSI	
8.4	12.4			Registros y supervisión			
8.4.1	12.4.1	Registro de eventos	SÍ	Se están definiendo los requisitos de monitorización del entorno de cloud para asegurar que cubran el entorno respecto a los riesgos identificados, aun así, el proveedor establece una configuración mínima de registros	2	[illegible] sistemas y de puesta en producción. No se debe permitir en ningún caso la instalación de software sin el permiso	
8.4.2	12.4.2	Protección de la información del registro	SÍ	El proveedor de cloud asegura que los registros se mantienen encriptados y accesibles solo por los administradores del cliente.	3	Implementar esquemas de protección de los datos de producción, cambiandolos o eliminando completamente los mismos al terminar las pruebas. Este escenario cambiaría el esquema actual de usar el servidor de pruebas y desarrollo como contingencia de producción.	
8.4.3	12.4.3	Registros de administración y operación	SÍ	Se están definiendo los requisitos de monitorización del entorno de cloud para asegurar que cubran el entorno respecto a los riesgos identificados, aun así, el proveedor establece una configuración mínima de registros	3	Mantener el esquema implementado. Debe hacerse explícito el procedimiento, alineado a un SGSI y divulgado.	
8.4.4	12.4.4	Sincronización del reloj	SÍ	Dicha información es publicada y accesible por los clientes del servicio de nube.	2	Mantener el esquema implementado. Debe hacerse explícito el procedimiento, alineado a un SGSI y divulgado.	
8.5	12.5			Control del software en explotación			
8.5.1	12.5.1	Instalación del software en explotación	SÍ	No está permitido la instalación de software de explotación y el proveedor de cloud asegura los controles para ello.	2	Mantener el esquema implementado.	
8.6	12.6			Gestión de la vulnerabilidad técnica			
8.6.1	12.6.1	Gestión de las vulnerabilidades técnicas	SÍ	El proveedor de nube notifica a sus clientes de las vulnerabilidades que afectan a sus sistemas y de las medidas a tomar por parte del cliente.	2	Dada la criticidad de la información, denbería implementarse un esquema de pruebas internas (ya sea por capacitación de un funcionario o por un sistema) que permita una revisión periódica interna al respecto	
8.6.2	12.6.2	Restricción en la instalación de software	SÍ	No está permitido la instalación de software de explotación y el proveedor de cloud asegura los controles para ello.	2	Dada la criticidad de la información, denbería implementarse un esquema de pruebas internas (ya sea por capacitación de un funcionario o por un sistema) que permita una revisión periódica interna al respecto	
8.7	12.7			Consideraciones sobre la auditoría de sistemas de información			
8.7.1	12.7.1	Controles de auditoría de sistemas de información	SÍ	El plan de auditorías interno y externo es notificado con antelación para prever posibles impactos sobre los recursos de personal y los entornos	2	Dada la criticidad de la información, denbería implementarse un esquema de pruebas internas (ya sea por capacitación de un funcionario o por un sistema) que permita una revisión periódica interna al respecto	

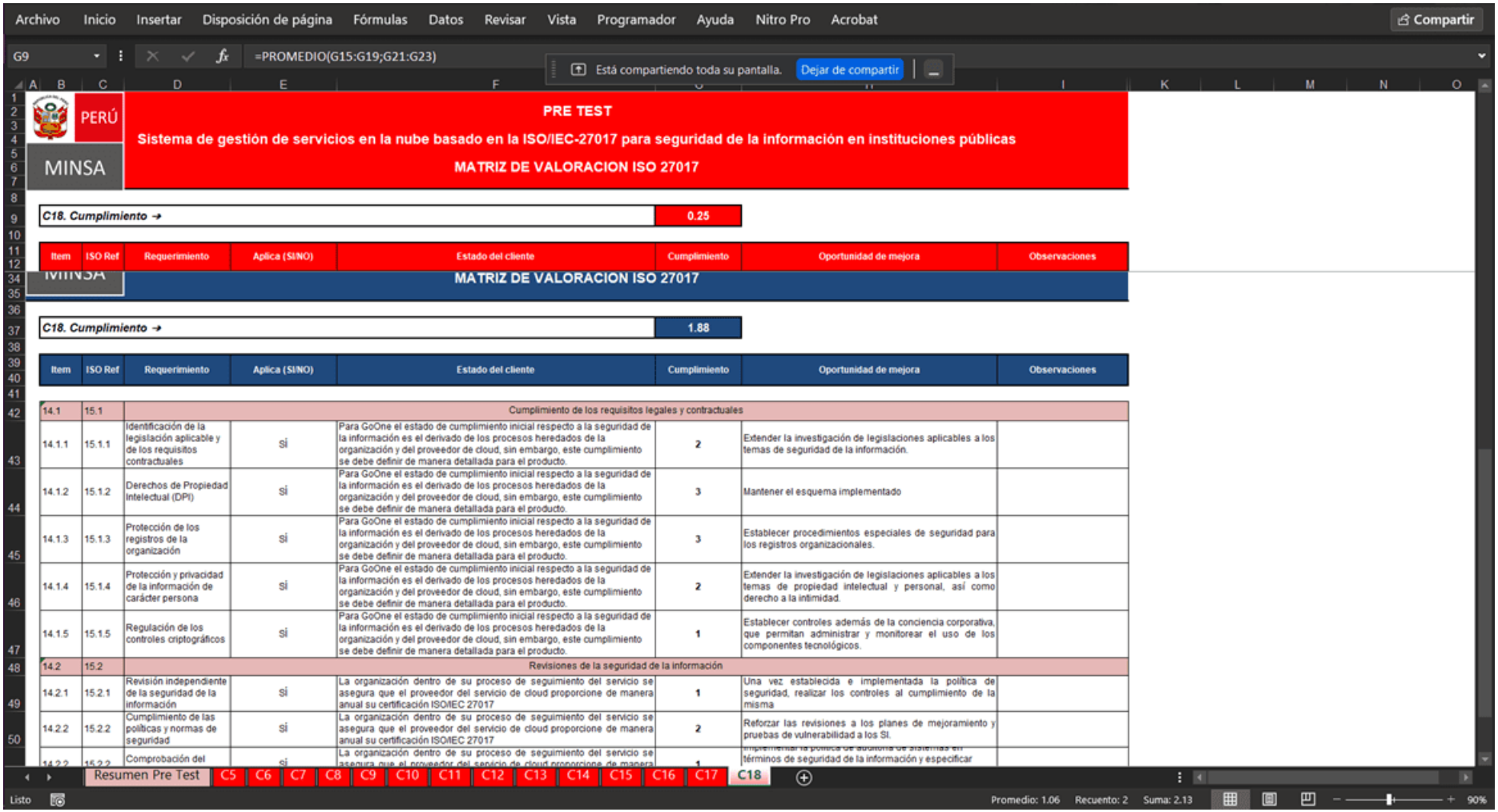

Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Programador Ayuda Nitro Pro Acrobat
Compartir
G9
=PROMEDIO(G15:G17;G19:G22)
Está compartiendo toda su pantalla.
Dejar de compartir
PERÚ
MINSA
PRE TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C13. Seguridad de las comunicaciones →
1.71
Item
ISO Ref
Requerimiento
Aplica (SI/NO)
Estado del cliente
Cumplimiento
Oportunidad de mejora
Observaciones
PERÚ
MINSA
POS TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C13. Seguridad de las comunicaciones →
2.57
Item
ISO Ref
Requerimiento
Aplica (SI/NO)
Estado del cliente
Cumplimiento
Oportunidad de mejora
Observaciones
9.1 13.1 Gestión de la seguridad de las redes
9.1.1 13.1.1 Controles de red SÍ Dentro de la organización los procesos de redes están bien definidos. Sin embargo, dentro de la particularidad del proyecto se están revisitando y detallando estos procesos respecto al modelo de responsabilidad compartida con el proveedor de cloud. 3 Durante la campaña de concientizacion y entrenamiento, identificar claramente los incidentes relacionados con la seguridad de la información y su reporte. La caracterización debe traducirse en la forma como se hace seguimiento en la mesa de ayuda y dentro del grupo de seguridad
9.1.2 13.1.2 Seguridad de los servicios de red SÍ Se han establecido unas medidas mínimas sobre la seguridad de los servicios de red, que suelen ser propuestas por el baseline del proveedor de cloud. Sin embargo, se están revisando para GoOne las necesidades en materia de seguridad de red y segregación de esta. 3 Durante la campaña de concientizacion y entrenamiento, identificar claramente las debilidades relacionados con la seguridad de la información y su reporte. Adicionalmente con la implementación del SGSI, este tema se hará formal y maduro
9.1.3 13.1.3 Segregación en redes SÍ Se han establecido unas medidas mínimas sobre la seguridad de los servicios de red, que suelen ser propuestas por el baseline del proveedor de cloud. Sin embargo, se están revisando para GoOne las necesidades en materia de seguridad de red y segregación de esta. 3 Durante la campaña de concientizacion y entrenamiento, identificar claramente las debilidades relacionados con la seguridad de la información y su reporte. Adicionalmente con la implementación del SGSI, este tema se hará formal y maduro
9.2 13.2 Intercambio de información
9.2.1 13.2.1 Políticas y procedimientos de intercambio de información SÍ Se han establecido unos protocolos de transferencia segura de información (https, http) de manera que pueda transferirse la información segura. Adicionalmente, toda la información se transfiere encriptada. 2 Documentar y divulgar formalmente el proceso implementado dentro del marco del SGSI
Acuerdos de
Además de tipificar esta labor como parte de las actividades del oficial de seguridad, definir el procedimiento
Resumen Pre Test C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18
Listo
90%


Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Programador Ayuda Nitro Pro Acrobat
Compartir
G9
=PROMEDIO(G15:G17;G19:G27;G29)
Está compartiendo toda su pantalla.
Dejar de compartir
PERÚ
MINSA
PRE TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C14. Adquisición, desarrollo y mantenimiento de sistemas →
1.62
Item
ISO Ref
Requerimiento
Aplica (SI/NO)
Estado del cliente
Cumplimiento
Oportunidad de mejora
Observaciones
PERÚ
MINSA
POS TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C14. Adquisición, desarrollo y mantenimiento de sistemas →
2.54
Item
ISO Ref
Requerimiento
Aplica (SI/NO)
Estado del cliente
Cumplimiento
Oportunidad de mejora
Observaciones
10.1
14.1
Requisitos de seguridad en los sistemas de información
10.1.1
14.1.1
Análisis de requisitos y especificaciones de seguridad de la información
Sí
Dentro de la fase inicial del proyecto se realizó un análisis de los servicios de seguridad ofrecidos por el proveedor y como estos cumplían con los requisitos funcionales y de seguridad de la aplicación GoOne. Dicho análisis se ha mantenido vivo y se va a actualizando en función de necesidades o actualizaciones.
4
No descuidar la revisión periódica del funcionamiento de estos procedimientos y controles
10.1.2
14.1.2
Asegurar los servicios de aplicaciones en redes públicas
Sí
Dentro de la fase inicial del proyecto se realizó un análisis de los servicios de seguridad ofrecidos por el proveedor y como estos cumplían con los requisitos funcionales y de seguridad de la aplicación GoOne. Dicho análisis se ha mantenido vivo y se va a actualizando en función de necesidades o actualizaciones.
3
No descuidar la revisión periódica del funcionamiento de estos procedimientos y controles
10.1.3
14.1.3
Protección de las transacciones de servicios de aplicaciones
Sí
Dentro de la fase inicial del proyecto se realizó un análisis de los servicios de seguridad ofrecidos por el proveedor y como estos cumplían con los requisitos funcionales y de seguridad de la aplicación GoOne. Dicho análisis se ha mantenido vivo y se va a actualizando en función de necesidades o actualizaciones.
2
No descuidar la revisión periódica del funcionamiento de estos procedimientos y controles
10.2
14.2
Seguridad en el desarrollo y en los procesos de soporte
10.2.1
14.2.1
Política de desarrollo seguro
Sí
Existen procesos de desarrollo de software, sin embargo, este proyecto trae consigo la Infraestructura como código lo que obligará a adoptar controles de desarrollo seguro de software.
4
Debe reforzarse el esquema estableciendo una directiva explícita o una política dentro del SGSI que requiera la protección y ubicación de los equipos tecnológicos en areas protegidas a la vista (cortinas o persianas y puertas cerradas)
Resumen Pre Test
C5
C6
C7
C8
C9
C10
C11
C12
C13
C14
C15
C16
C17
C18
Listo
90%

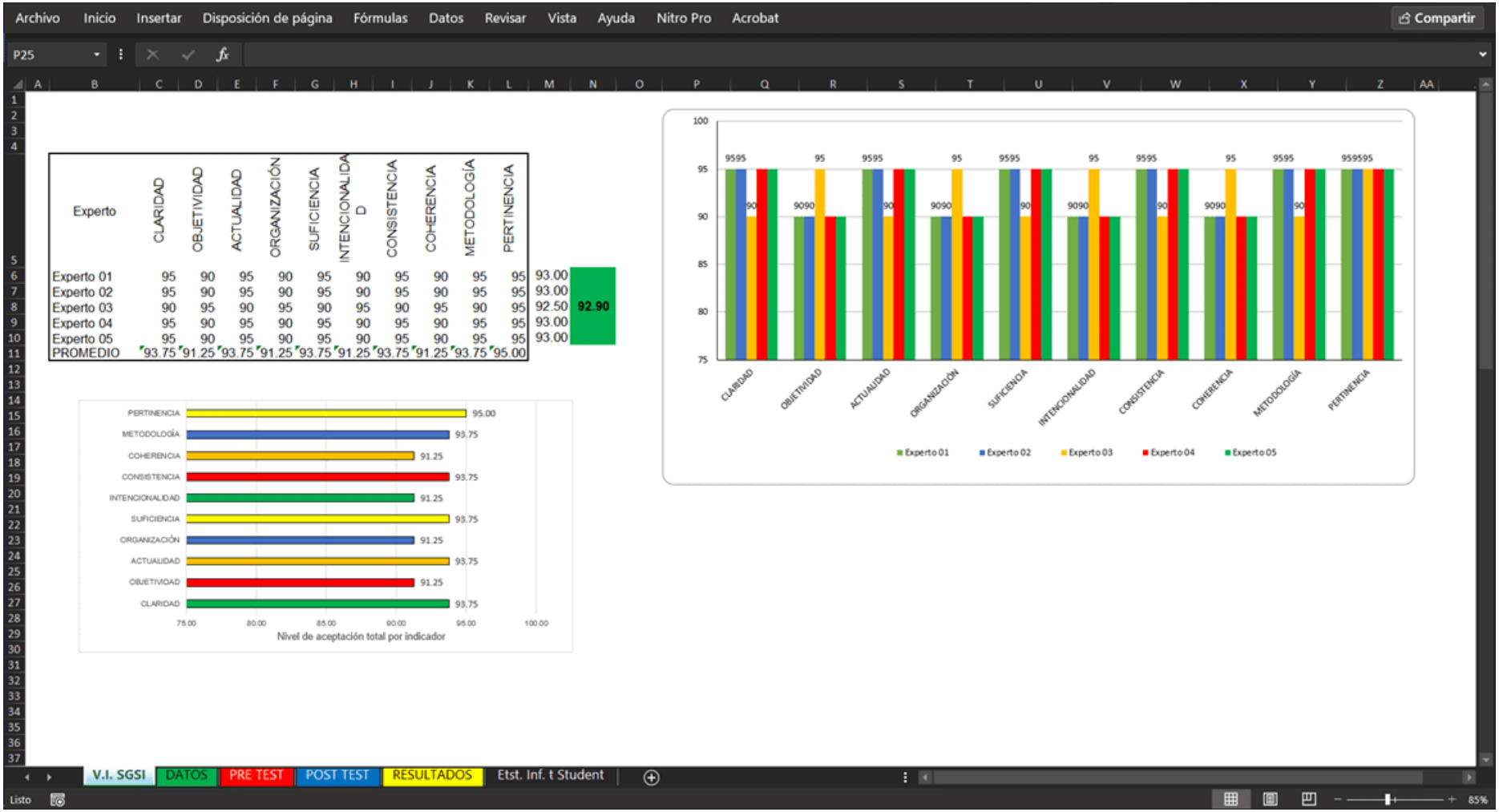

Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Programador Ayuda Nitro Pro Acrobat
Compartir
D44
Gestión de la provisión de servicios del proveedor
Está compartiendo toda su pantalla.
Dejar de compartir
PERÚ
MINSA
PRE TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C15. Relaciones con los proveedores →
1.00
Item
ISO Ref
Requerimiento
Aplica (SI/NO)
Estado del cliente
Cumplimiento
Oportunidad de mejora
Observaciones
PERÚ
MINSA
POS TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C15. Relaciones con los proveedores →
1.80
Item
ISO Ref
Requerimiento
Aplica (SI/NO)
Estado del cliente
Cumplimiento
Oportunidad de mejora
Observaciones
11.1
15.1
Seguridad en las relaciones con proveedores
11.1.1
15.1.1
Política de seguridad de la información en las relaciones con los proveedores
SÍ
El equipo de compras y el equipo de gestión de proveedores implementan una serie de controles y verificaciones manuales, sin embargo, dentro del entorno de cloud es muy posible que se necesite añadir algunos controles automáticos para una mayor optimización.
2
Durante la campaña de concientizacion y entrenamiento, identificar claramente los incidentes relacionados con la seguridad de la información y su reporte. La caracterización debe traducirse en la forma como se hace seguimiento en la mesa de ayuda y dentro del grupo de seguridad
11.1.2
15.1.2
Requisitos de seguridad en contratos con terceros
SÍ
El equipo de compras y el equipo de gestión de proveedores dentro de su proceso de negociación de contrato con el proveedor han definido de manera adecuada los roles a incluir.
3
Durante la campaña de concientizacion y entrenamiento, identificar claramente las debilidades relacionados con la seguridad de la información y su reporte. Adicionalmente con la implementación del SGSI, este tema se hará formal y maduro
11.1.3
15.1.3
Cadena de suministro de tecnología de la información y de las comunicaciones
SÍ
El contrato con el proveedor de nube incluye clausulas para la correcta gestión de la información, así como la transferencia y procesamiento de datos segura.
1
Durante la campaña de concientizacion y entrenamiento, identificar claramente las debilidades relacionados con la seguridad de la información y su reporte. Adicionalmente con la implementación del SGSI, este tema se hará formal y maduro
11.2
15.2
Gestión de la provisión de servicios del proveedor
11.2.1
15.2.1
Control y revisión de la provisión de servicios del proveedor
SÍ
Existe un proceso de revisión periódica del servicio donde se hace un seguimiento de incidentes, se comprueba el cumplimiento del servicio, SLA, cambios en el servicio, en los controles y procedimientos, así como posibles riesgos que afecten al servicio.
1
Documentar y divulgar formalmente el proceso implementado dentro del marco del SGSI
11.2.2
15.2.2
Gestión de cambios en la provisión del servicio del proveedor
SÍ
Existe un proceso de revisión periódica del servicio donde se hace un seguimiento de incidentes, se comprueba el cumplimiento del servicio, SLA, cambios en el servicio, en los controles y procedimientos, así como posibles riesgos que afecten al servicio.
2
Además de tipificar esta labor como parte de las actividades del oficial de seguridad, definir el procedimiento adecuado en el SGSI y realizar la revisión a todos los repotes de incidentes e incluirlos en el plan de
Resumen Pre Test
C5
C6
C7
C8
C9
C10
C11
C12
C13
C14
C15
C16
C17
C18
Listo
90%


Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Programador Ayuda Nitro Pro Acrobat
Compartir
G9
=PROMEDIO(G15:G21)
Está compartiendo toda su pantalla.
Dejar de compartir
PERÚ
MINSA
PRE TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad → 2.14
Item | ISO Ref | Requerimiento | Aplica (SI/NO) | Estado del cliente | Cumplimiento | Oportunidad de mejora | Observaciones
C16. Gestión de incidentes de seguridad de la información en la gestión de la continuidad de la actividad → 3.00
Item | ISO Ref | Requerimiento | Aplica (SI/NO) | Estado del cliente | Cumplimiento | Oportunidad de mejora | Observaciones
12.1 | 16.1 | Gestión de incidentes de seguridad de la información y mejoras
12.1.1 | 16.1.1 | Responsabilidades y procedimientos | SÍ | El proceso de gestión de incidentes es definido y conocido por los actores involucrados, será necesario ampliarlo para cubrir los incidentes en entornos de cloud | 4 | Una vez implementada la política de seguridad, incluirla en el desarrollo de los planes de continuidad del negocio y establecer planes para todos los procesos críticos.
12.1.2 | 16.1.2 | Notificación de los eventos de seguridad de la información | SÍ | El proveedor de servicio en la nube ha proporcionado un proceso de notificación de incidentes y eventos de seguridad para los administradores de GoOne. | 3 | Debe existir un análisis periódico de tipo BIA y análisis de riesgos que haga particular detalle en las amenazas inherentes a la organización. Esta actividad se madurará con cada ciclo del SGSI
12.1.3 | 16.1.3 | Notificación de puntos débiles de la seguridad | SÍ | El proveedor de servicio en la nube ha proporcionado un proceso de notificación de incidentes y eventos de seguridad para los administradores de GoOne. | 2 | Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria.
12.1.4 | 16.1.4 | Evaluación y decisión sobre los eventos de seguridad de información | SÍ | El proceso de gestión de incidentes es definido y conocido por los actores involucrados, sin embargo, los procesos de decisión para el entorno de cloud no son conocidos y aplicados de manera extensa. | 3 | Unificar los términos de análisis para el impacto y los riesgos evaluados en los planes de continuidad del negocio.
12.1.5 | 16.1.5 | Respuesta a incidentes de seguridad de la información | SÍ | El proceso de gestión de incidentes es definido y conocido por los actores involucrados, sin embargo, los procesos de decisión para el entorno de cloud no son conocidos y aplicados de manera extensa. | 4 | Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados.
12.1.6 | 16.1.6 | Aprendizaje de los incidentes de seguridad de la información | SÍ | El proceso de gestión de incidentes es definido y conocido por los actores involucrados, sin embargo, los procesos de decisión para el entorno de cloud no son conocidos y aplicados de manera extensa. | 2 | Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados.
12.1.7 | 16.1.7 | Recopilación de evidencias | SÍ | El proceso de gestión de incidentes es definido y conocido por los actores involucrados, sin embargo, los procesos de decisión para el entorno de cloud no son conocidos y aplicados de manera extensa. | 3 | Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados.
Resumen Pre Test C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18
Listo
90%

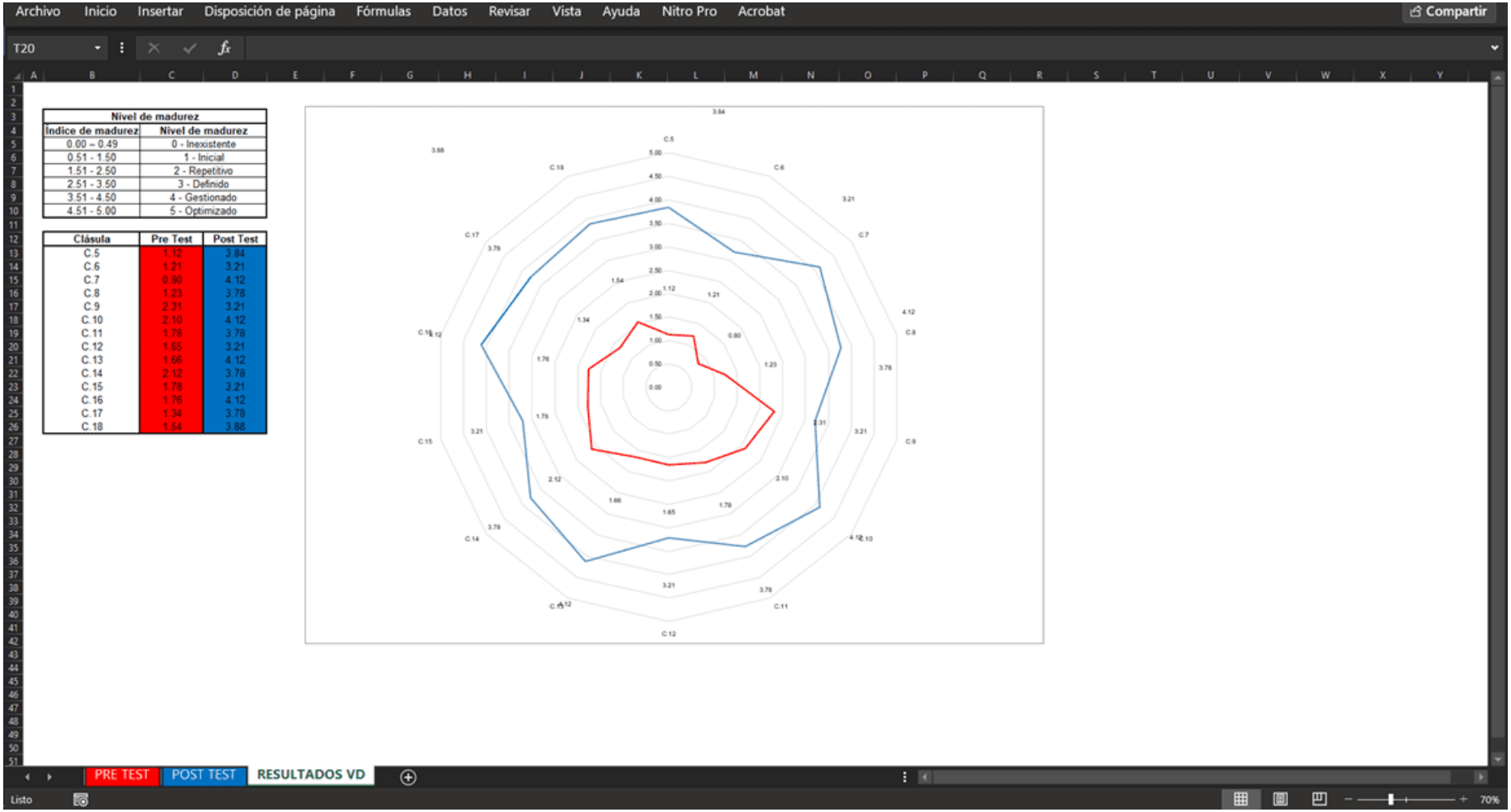

Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Programador Ayuda Nitro Pro Acrobat
Compartir
Está compartiendo toda su pantalla.
Dejar de compartir
PERÚ
MINSA
PRE TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad → 1.75
Item | ISO Ref | Requerimiento | Aplica (SI/NO) | Estado del cliente | Cumplimiento | Oportunidad de mejora | Observaciones
PERÚ
MINSA
POS TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C17. Aspectos de seguridad de la información en la gestión de la continuidad de la actividad → 2.67
Item | ISO Ref | Requerimiento | Aplica (SI/NO) | Estado del cliente | Cumplimiento | Oportunidad de mejora | Observaciones
13.1 | 17.1 | Continuidad de la seguridad de la información
13.1.1 | 17.1.1 | Planificación de la continuidad de la seguridad de la información | Sí | Dentro de la organización se monitorizan y redundan los sistemas críticos de manera estricta, en este caso se han adaptado las monitorizaciones sobre controles clave de continuidad de negocio para que incluyan GoOne su entorno de cloud. | 3 | No descuidar la revisión periódica del funcionamiento de estos procedimientos y controles
13.1.2 | 17.1.2 | Implementar la continuidad de la seguridad de la información | Sí | Existe una política definida de continuidad de negocio y dentro del sistema GoOne se ha definido un procedimiento de recuperación de desastres para alinearlo con la política de continuidad de negocio. | 3 | No descuidar la revisión periódica del funcionamiento de estos procedimientos y controles
13.1.3 | 17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Sí | Existe un procedo anual en el que se revisa y se prueba la estrategia de recuperación de desastres, además se coordina con el proveedor de cloud. Adicionalmente, se hace un seguimiento al proveedor de cloud sobre su política de continuidad de negocio y la gestión de ella | 2 | No descuidar la revisión periódica del funcionamiento de estos procedimientos y controles
13.2 | 17.2 | Redundancias
13.2.1 | 17.2.1 | Política de desarrollo seguro | Sí | Existen procesos de desarrollo de software, sin embargo, este proyecto trae consigo la Infraestructura como código lo que obligará a adoptar controles de desarrollo seguro de software. | 3 | Debe reforzarse el esquema estableciendo una directiva explícita o una política dentro del SGSI que requiera la protección y ubicación de los equipos tecnológicos en areas protegidas a la vista (cortinas o persianas y puertas cerradas)
13.2.1 | 17.2.1 | Debe reforzarse el esquema estableciendo una directiva
Resumen Pre Test | C5 | C6 | C7 | C8 | C9 | C10 | C11 | C12 | C13 | C14 | C15 | C16 | C17 | C18
Listo
90%


Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Programador Ayuda Nitro Pro Acrobat
Compartir
G9
=PROMEDIO(G15:G19;G21:G23)
Está compartiendo toda su pantalla.
Dejar de compartir
PERÚ
MINSA
PRE TEST
Sistema de gestión de servicios en la nube basado en la ISO/IEC-27017 para seguridad de la información en instituciones públicas
MATRIZ DE VALORACION ISO 27017
C18. Cumplimiento →
0.25
Item
ISO Ref
Requerimiento
Aplica (SI/NO)
Estado del cliente
Cumplimiento
Oportunidad de mejora
Observaciones
MINSA
MATRIZ DE VALORACION ISO 27017
C18. Cumplimiento →
1.88
Item
ISO Ref
Requerimiento
Aplica (SI/NO)
Estado del cliente
Cumplimiento
Oportunidad de mejora
Observaciones
14.1
15.1
Cumplimiento de los requisitos legales y contractuales
14.1.1
15.1.1
Identificación de la legislación aplicable y de los requisitos contractuales
Sí
Para GoOne el estado de cumplimiento inicial respecto a la seguridad de la información es el derivado de los procesos heredados de la organización y del proveedor de cloud, sin embargo, este cumplimiento se debe definir de manera detallada para el producto.
2
Extender la investigación de legislaciones aplicables a los temas de seguridad de la información.
14.1.2
15.1.2
Derechos de Propiedad Intelectual (DPI)
Sí
Para GoOne el estado de cumplimiento inicial respecto a la seguridad de la información es el derivado de los procesos heredados de la organización y del proveedor de cloud, sin embargo, este cumplimiento se debe definir de manera detallada para el producto.
3
Mantener el esquema implementado
14.1.3
15.1.3
Protección de los registros de la organización
Sí
Para GoOne el estado de cumplimiento inicial respecto a la seguridad de la información es el derivado de los procesos heredados de la organización y del proveedor de cloud, sin embargo, este cumplimiento se debe definir de manera detallada para el producto.
3
Establecer procedimientos especiales de seguridad para los registros organizacionales.
14.1.4
15.1.4
Protección y privacidad de la información de carácter persona
Sí
Para GoOne el estado de cumplimiento inicial respecto a la seguridad de la información es el derivado de los procesos heredados de la organización y del proveedor de cloud, sin embargo, este cumplimiento se debe definir de manera detallada para el producto.
2
Extender la investigación de legislaciones aplicables a los temas de propiedad intelectual y personal, así como derecho a la intimidad.
14.1.5
15.1.5
Regulación de los controles criptográficos
Sí
Para GoOne el estado de cumplimiento inicial respecto a la seguridad de la información es el derivado de los procesos heredados de la organización y del proveedor de cloud, sin embargo, este cumplimiento se debe definir de manera detallada para el producto.
1
Establecer controles además de la conciencia corporativa, que permitan administrar y monitorear el uso de los componentes tecnológicos.
14.2
15.2
Revisiones de la seguridad de la información
14.2.1
15.2.1
Revisión independiente de la seguridad de la información
Sí
La organización dentro de su proceso de seguimiento del servicio se asegura que el proveedor del servicio de cloud proporcione de manera anual su certificación ISO/IEC 27017
1
Una vez establecida e implementada la política de seguridad, realizar los controles al cumplimiento de la misma
14.2.2
15.2.2
Cumplimiento de las políticas y normas de seguridad
Sí
La organización dentro de su proceso de seguimiento del servicio se asegura que el proveedor del servicio de cloud proporcione de manera anual su certificación ISO/IEC 27017
2
Reforzar las revisiones a los planes de mejoramiento y pruebas de vulnerabilidad a los SI.
Comprobación del
Sí
La organización dentro de su proceso de seguimiento del servicio se asegura que el proveedor del servicio de cloud proporcione de manera
1
términos de seguridad de la información y especificar
Resumen Pre Test
C5
C6
C7
C8
C9
C10
C11
C12
C13
C14
C15
C16
C17
C18
Listo
Promedio: 1.06
Recuento: 2
Suma: 2.13
90%

Anexo 9. Tabulación de resultados de la Variable Independiente



Anexo 10. Tabulación de resultados de la Variable Dependiente



Nivel de madurez	
Índice de madurez	Nivel de madurez
0.00 – 0.49	0 - Inexistente
0.51 - 1.50	1 - Inicial
1.51 - 2.50	2 - Repetitivo
2.51 - 3.50	3 - Definido
3.51 - 4.50	4 - Gestionado
4.51 - 5.00	5 - Optimizado

Clásula	Pre Test	Post Test
C.5	1.12	3.84
C.6	1.21	3.21
C.7	0.80	4.12
C.8	1.23	3.78
C.9	2.31	3.21
C.10	2.10	4.12
C.11	1.78	3.78
C.12	1.65	3.21
C.13	1.66	4.12
C.14	2.12	3.78
C.15	1.78	3.21
C.16	1.76	4.12
C.17	1.34	3.78
C.18	1.54	3.88

Anexo 11. Declaración de aplicabilidad

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción al MINSA
				LR	CO	BR/BP	RRA	SI/NO	
5	**Políticas de seguridad de la información**								
5.1	**Directrices establecidas por la dirección para la seguridad de la información**								
5.1.1	**Políticas para la seguridad de la información**	Hay existencia de políticas de seguridad de la información sin documentación, se debe redactar un documento de políticas para que sea distribuido y conocido por todo el personal incluido en el proceso del SGSI				X		Si	Se diseñó e implementó el documento de Política de Seguridad de la Información.
5.1.2	**Revisión de las políticas para seguridad de la información**	Se debe establecer un procedimiento que permita la revisión periódica de las políticas de la seguridad de la información por lo menos cada año				X		Si	Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determina el periodo de revisión de la política. Control C002.

6	**Organización de la seguridad de la información**								
6.1	**Organización interna.**								
6.1.1	**Roles y responsabilidades para la seguridad de información**	Se deben definir roles y responsabilidades de acuerdo a las políticas de seguridad de la información a todos los que interactúen con el SGSI				x		si	Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determinan los roles y responsabilidades respecto a la seguridad de la información. Control C003.
6.1.2	**Separación de deberes**	Se deben separar las ares consideradas de gran importancia para que así los deberes y responsabilidades asignadas sean separadas, de esta forma se evita el uso indebido de los activos de la organización			x	x		si	Los procesos del MINSA se han determinado considerando segregación en los procesos. Control C004.
6.1.3	**Contacto con las autoridades**	En el documento de políticas de la seguridad de la información se debe contemplar un procedimiento que permita gestionar el contacto permanente con autoridades reguladoras de seguridad de la información	La organización no tiene contacto con autoridades reguladoras de los procesos de negocio.					no	

6.1.4	**Contacto con grupos de interés especial**	Es importante que la persona encargada de la seguridad informática gestione el contacto permanente con grupos de interés, estos pueden ser foros, chats, wiki, comunidades relacionadas con la seguridad informática, con la intención de estar actualizados en aspectos relacionados a la seguridad	Las ejecuciones en seguridad de la información no están a cargo de personal operativo de la empresa.					no	
6.1.5	**Seguridad de la información en la gestión de proyectos**	La seguridad de la información se debe tratar en cualquier proyecto.	No representa un riesgo crítico para la empresa.					no	
6.2	**Dispositivos móviles y teletrabajo.**								
6.2.1	**Política para dispositivos móviles**	Se deben aplicar políticas para el uso adecuado de dispositivos móviles, su uso inadecuado representa grandes riesgos	Los procesos del MINSA no tienen participación de dispositivos móviles.					no	
6.2.2	**Teletrabajo**	La institución no posee empleos bajo la modalidad de teletrabajo en este momento	El MINSA no posee este tipo de trabajadores.					no	

7	**Seguridad de los recursos humanos**								
7.1	**Antes de asumir el empleo.**								
7.1.1	**Selección**	Se deben realizar una exhaustiva comprobación de los antecedentes del personal como empleados, contratistas, terceros, con el fin de saber su procedencia, referencias personales, judiciales entre otras				x		si	
7.1.2	**Términos y condiciones del empleo**	Se debe diseñar un documento que permita a los empleados, contratistas y terceros firmar cláusulas de confidencialidad con la organización, manejo adecuado de recursos tecnológicos		x	x			si	Se diseñó el documento Acuerdo de Confidencialidad el cual estipula que la información que corresponde a los procesos internos del MINSA, así como la información de los pacientes atendidos por la clínica, son de carácter confidencial y la divulgación de estos conlleva castigos penales, así como la ruptura de la relación con el MINSA. Control C005.

7.2	**Durante la ejecución del empleo.**								
7.2.1	**Responsabilidades de la dirección**	Se debe exigir a los empleados, contratistas y terceros el cumplimiento a cabalidad de las políticas de seguridad de la información implementadas por la institución				x		si	
7.2.2	**Toma de conciencia, educación y formación en la seguridad de la información**	Se debe capacitar a todo el personal en aspectos relacionados con la seguridad de la información				x		si	El personal del MINSA es sensibilizado respecto a temas de seguridad de la información. Control C006.
7.2.3	**Proceso disciplinario**	Se deben establecer políticas sobre sanciones que se aplicarán a quienes incumplan con lo descrito en las políticas de seguridad				x		si	Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determinan las penalidades sobre el incumplimiento de la política. Control C007.

7.3	**Terminación o cambio de empleo**								
7.3.1	**Terminación o cambio de responsabilidades de empleo**	Se debe informar a los empleados en los casos donde las responsabilidades y deberes que les fueron asignados durante el empleo, los cobijan aun cuando se realice una				x		si	
8	**Gestión de activos**								
8.1	**Responsabilidad por los activos**								
8.1.1	**Inventario de activos**	Se debe contar con un inventario detallado de los activos que posee la Cía				x	x	si	Se identificó y clasificó los activos de los procesos relevantes de la organización teniendo como resultado el Inventario de Activos de Información. Control C008.
8.1.2	**Propiedad de los activos**	Además de la implementación del control anterior, se debe identificar en custodia de quien se encuentra actualmente el activo				x	x	si	El inventario de activos diseñado tiene información actualizada del propietario (responsable) del activo de información. Control C009.

8.1.3	**Uso aceptable de los activos**	Debe existir una clausula donde los empleados se comprometan a realizar un uso aceptable de los activos de la organización				x			Se diseñó e implementó la política específica de Gestión de Activos en la que se establece el uso que los empleados le deben dar a los activos de información. Control C010.
8.1.4	**Devolución de activos**	Se debe establecer un proceso para la devolución de los activos para cuando los empleados cambien de puesto o cuando se termine su contrato							
8.2	**Clasificación de la información**								
8.2.1	**Clasificación de la información**	Se debe establecer un procedimiento que permita clasificar la información de acuerdo a su valor							
8.2.2	**Etiquetado de la información**	La información debe estar debidamente rotulada, además esta rotulación se debe clasificar de acuerdo al valor que representa la información para la empresa							
8.2.3	**Manejo de activos**	Se debe contar con procedimientos que ayuden en el adecuado manejo que se le debe dar a un activo							

8.3	**Manejo de medios**								
8.3.1	**Gestión de medios removibles**	Se deben establecer políticas sobre el correcto manejo que se le deben dar a los medios removibles, puesto que estos son necesarios en el desarrollo de las labores diarias. dar a un activo				x	x	si	Se diseñó e implementó la política específica de Gestión de Activos en la que se establece que los medios removibles deben ser inhabilitados en todas las computadoras de la clínica. Control C012.
8.3.2	**Disposición de los medios**	Protección de la información cuando los medios sean destinados a labores diferentes a las actuales, se podría hablar de un procedimiento de eliminación de información en estos casos.							
8.3.3	**Transferencia de medios físicos**	Definir procedimientos que permitan que la información almacenada en estos no sea divulgada, modificada o eliminada.		x		x	x	si	Se tiene como regla en el proceso de Procesamiento que el medico ocupacional del cliente puede decepcionar los resultados de los exámenes. Control C013.

9	**Control de acceso**								
9.1	**Requisitos del negocio para control de acceso**								
9.1.1	**Política de control de acceso**	Establecer políticas que permitan el acceso a la información de acuerdo a privilegios establecidos según sus funciones				x		si	Se diseñó e implementó la Política Específica de Gestión de Accesos. Control C014.
9.1.2	**Política sobre el uso de los servicios de red**	Definir el acceso a la red para el desarrollo de funciones que les fueron asignadas.							
9.2	**Gestión de acceso de usuarios**								
9.2.1	**Registro y cancelación del registro de usuarios**	Todos los usuarios con acceso a sistema de información deben estar debidamente registrados, adicionalmente se debe dar de baja a los que ya no hagan parte de la organización o no hagan uso del sistema.		x	x	x	x	si	El personal que cesa de la empresa se le debe retirar los accesos a los sistemas de información en un periodo oportuno. Control C015.
9.2.2	**Suministro de acceso de usuarios**	Implementar un procedimiento que permita a los usuarios del sistema acceder al sistema o negar el acceso a este cuando se considere necesario.				x		si	Los ordenadores deben requerir usuarios y contraseña para el acceder a los mismos. Control C016.
9.2.3	**Gestión de derechos de acceso privilegiado**	Se deben establecer privilegios de acceso a la información de acuerdo al desempeño de sus funciones.				x		si	Existe una revisión periódica de accesos otorgados en el sistema Mediweb. Control C017.

9.2.4	**Gestión de información de autenticación secreta de usuarios**	Esta información sólo debe ser accesada por personal con privilegios especiales				x		si	Sólo personal autorizado tiene acceso a la Gestión de Accesos en los sistemas de información. Control C018.
9.2.5	**Revisión de los derechos de acceso de usuarios**	Monitoreo de privilegios asignados a usuarios con el fin de identificar si los privilegios asignados son adecuados para el desarrollo de sus funciones.				x	x	si	Se cubrirá con el control C017.
9.2.6	**Retiro o ajuste de los derechos de acceso**	Se debe dar de baja o modificar los privilegios de acceso a la información en caso de traslado del usuario o retiro de la organización.		x		x		si	Se cubrirá con el control C015.
9.3	**Responsabilidades de los usuarios**								
9.3.1	**Uso de la información de autenticación secreta**	Se deben crear perfiles para el acceso a información considerada de suma importancia para la empresa							
9.4	**Control de acceso a sistemas y aplicaciones**								
9.4.1	**Restricción de acceso Información**	Restringir el acceso a la información por parte de personal no autorizado.							

9.4.2	**Procedimiento de ingreso seguro**	Se deben establecer procedimientos que restrinjan el acceso a la información a personal no autorizado							
9.4.3	**Sistema de gestión de contraseñas**	Se deben establece políticas de gestión de contraseñas como caducidad, bloqueo después de determinado número de intentos, parámetros para creación de contraseñas seguras.							
9.4.4	**Uso de programas utilitarios privilegiados**	Restringir el uso de programas utilitarios ya que pueden violentar la seguridad de las contraseñas, pues algunos revelan las contraseñas, vulnerando la seguridad.							
9.4.5	**Control de acceso a códigos fuente de programas**	Políticas de acceso al código fuente, este sólo debe ser accesado por el personal autorizado.							

10	**Criptografía**								
10.1	**Controles criptográficos**								
10.1.1	**Política sobre el uso de controles criptográficos**	Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad y no repudio de la información							
10.1.2	**Gestión de llaves**	Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad y no repudio de la información							
11	**Seguridad física y del entorno**								
11.1	**Áreas seguras**								
11.1.1	**Perímetro de seguridad física**	Se debe establecer un perímetro de tal forma que los sitios donde se encuentren los activos tengan accesos restringidos							
11.1.2	**Controles físicos de entrada**	Se debe restringir el acceso a sitios seguros como centro de cableado, ubicación del servidor, espacios donde se encuentre información confidencial, estos sitios deben permanecer con llave.							

11.1.3	**Seguridad de oficinas, recintos e instalaciones**	Restringir el acceso a personal no autorizado, las áreas deben estar demarcadas dando aviso que son sitios restringidos							
11.1.4	**Protección contra amenazas externas y ambientales**	Se debe contar con detectores de humo y humedad, ubicación de extinguidores en sitios estratégicos, cuartos técnicos con aire acondicionado, adquisición de pólizas contra robo y desastres naturales							
11.1.5	**Trabajo en áreas seguras**	Se deben preservar los sitios donde se encuentren activos valiosos con el fin de protegerlos contra daños intencionados							
11.1.6	**Áreas de despacho y carga**	Se deben designar sitios especiales para carga y despacho, lo recomendable es que estén aislados de los denominados sitios seguros o restringidos							
11.2	**Equipos**								
11.2.1	**Ubicación y protección de los equipos**	Los equipos deben estar ubicados en sitios seguros, de esta forma se protege contra robo, accesos no autorizados.							

11.2.2	**Servicios de suministro**	Se debe contar con un adecuado suminist ro y respaldo de energía.							
11.2.3	**Seguridad del cableado**	Se debe proteger el cableado eléctrico y de datos de posibles daños como interceptaciones con el fin de causar daño.							
11.2.4	**Mantenimiento de equipos**	Se debe contar con mantenimiento preventivo y correctivo en períodos de tiempo establecidos, con el fin de evitar daños en hardware, actualización de software.							
11.2.5	**Retiro de activos**	Se debe definir un procedimiento que autorice el retiro de activos de la empresa tales como equipos de cómputo, software.							
11.2.6	**Seguridad de equipos y activos fuera de las instalaciones**	Aplicar la misma seguridad que se realiza a los equipos dentro de la empresa							
11.2.7	**Disposición segura o reutilización de equipos**	Se debe proteger la información confidencial de equipos en desuso o cuando son dados de baja.							
11.2.8	**Equipos de usuario desatendidos**	Establecer políticas para equipos cuando los usuarios no están presentes, evitando así el acceso no autorizado o robo de información.							

11.2.9	**Política de escritorio limpio y pantalla limpia**	Definir procedimientos para que los escritorios estén libres de papeles, medios de almacenamiento que puedan permitir filtración de información, además políticas de pantallas limpias.							
12	**Seguridad de las operaciones**								
12.1	**Procedimientos operacionales y responsabilidades**								
12.1.1	**Procedimientos de operación documentados**	Los procedimientos deben estar documentados y puestos al alcance de todos, también manuales de operaciones específicas							
12.1.2	**Gestión de cambios**	Establecer políticas donde los cambios sean realizados por personal autorizado, además deben quedar soportados para llevar un control para evitar contratiempos.							
12.1.3	**Gestión de capacidad**	Se debe realizar un monitoreo de los recursos de tal forma que no afecten la operación, algunos pueden ser capacidad de banda ancha, circuitos descalibrados que afecten el fluido eléctrico, equipos de cómputo lentos.							

12.1.4	**Separación de los ambientes de desarrollo, pruebas y operación**	Los ambientes de desarrollo prueba y operación deben estar aislados, con restricciones de acceso con el fin de evitar cambios o modificaciones no autorizadas.							
12.2	**Protección contra códigos maliciosos**								
12.2.1	**Controles contra códigos maliciosos**	Los equipos de cómputo deben contar con software contra código malicioso, el cual se debe actualizar constantemente con el fin actualizar parches que mitiguen las nuevas vulnerabilidades.							
12.3	**Copias de respaldo**								
12.3.1	**Respaldo de información**	Se debe realizar respaldo de la información, además se deben realizar pruebas para comprobar que estos cumplen con las políticas de respaldo-							
12.4	**Registro y seguimiento**								
12.4.1	**Registro de eventos**	Se debe llevar un control de los eventos con el fin de establecer procedimientos que ayuden a repararlos o eliminarlos definitivamente, con el fin de que no se vuelvan a presentar							

12.4.2	**Protección de la información de registro**	Se debe proteger la información de registro de personal no autorizado, sólo el administrador o encargado será quien pueda tener acceso a estos, se deben realizar copias de logs.							
12.4.3	**Registros del administrador y del operador**	Todas las tareas que desarrollen el administrador y el operador del sistema de información deben estar registradas, además se debe realizar un respaldo de estos registros.							
12.4.4	**sincronización de relojes**	Los relojes de los dispositivos que intervienen en el procesamiento de información deben estar sincronizados.							
12.5	**Control de software operacional**								
12.5.1	**Instalación de software en sistemas operativos**	La instalación de software debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas.							

12.6	**Gestión de la vulnerabilidad técnica**								
12.6.1	**Gestión de las vulnerabilidades técnicas**	Se deben establecer procedimientos que minimicen las vulnerabilidades a que están expuestos los activos tecnológicos.							
12.6.2	**Restricciones sobre la instalación de software**	La instalación de software debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas.							
12.7	**Consideraciones sobre auditorias de sistemas de información**								
12.7.1	**Información controles de auditoría de sistemas**	Se deben establecer procedimientos que permitan el buen uso de las herramientas de auditoría a los sistemas, pero siempre procurando minimizar la interrupción del servicio a causa de estas.							
13	**Seguridad de las comunicaciones**								
13.1	**Gestión de la seguridad de las redes**								
13.1.1	**Controles de redes**	Se deben instalar dispositivos o software que permita controlar el acceso a la red como Firewall, Ids, autenticación para su ingreso							

13.1.2	**Seguridad de los servicios de red**	Establecer controles de acceso, acuerdos de servicio en su utilización, monitoreo constante para detectar intrusos							
13.1.3	**Separación en las redes**	Es necesario loa separación de las redes como la intranet de la red con acceso a internet, para lo cual se debe implementar un DMZ							
13.2	**Transferencia de información**								
13.2.1	**Políticas y procedimientos de transferencia de información**	Se deben establecer todas las políticas que sean necesarias para proteger la información en el momento de ser transferida (intercambio de información), permitiendo integridad y confidencialidad.							
13.2.2	**Acuerdos sobre transferencia de información**	Se deben establecer controles que permitan respetar acuerdos de intercambio o transferencia de información							

13.2.3	**Mensajería electrónica**	Deben existir controles sobre el uso adecuado de la mensajería electrónica, para ello se deben instalar programas que detecten antivirus y spam, además se debe existir capacitación sobre situaciones donde existan correos sospechosos, también políticas del uso adecuado de los recursos, en este caso uso del correo electrónico sólo para el desarrollo de las funciones asignadas.							
13.2.4	**Acuerdos de confidencialidad o de no divulgación**	Se deben cumplir las políticas de confidencialidad de la información, las cuáles fueron aceptadas en el momento de la firma del contrato.							
14	**Adquisición, desarrollo y mantenimientos de sistemas**								
14.1	**Requisitos de seguridad de los sistemas de información**								
14.1.1	**Análisis y especificación de requisitos de seguridad de la información**	Las especificaciones de requisitos se deben tener en cuenta cuando se vaya a realizar un cambio o implementar un nuevo sistema de información							

14.1.2	**Seguridad de servicios de las aplicaciones en redes publicas**	Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información							
14.1.3	**Protección de transacciones de los servicios de las aplicaciones**	Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información							
14.2	**Seguridad en los procesos de desarrollo y soporte**								
14.2.1	**Política de desarrollo seguro**	Es importante establecer políticas de código seguro en el desarrollo de software, es aquí donde se deben implementar procedimientos de seguridad como paso de variables por cabecera, sesiones, entre otros, los cuáles deben blindar el sistema de información para evitar vulnerabilidades							

14.2.2	**Procedimientos de control de cambios en sistemas**	Todos los cambios que se realicen a los programas se deben documentar y quedar registrados, para lo cual se deben establecer procedimientos							
14.2.3	**Revisión técnica de las aplicaciones después de cambios en la plataforma de operación**	Se deben realizar pruebas a las aplicaciones que han sido modificadas, con el fin de evitar alteraciones en la prestación del servicio o mal funcionamiento a causa del desarrollo.							
14.2.4	**Restricciones en los cambios a los paquetes de software**	Los cambios o modificaciones que se le realizan a las aplicaciones deben estar restringidos con el fin de evitar fallas no deseadas.							
14.2.5	**Principios de construcción de sistemas seguros**	Establecer procedimientos y políticas que permitan la construcción de aplicaciones seguras							
14.2.6	**Ambiente de desarrollo seguro**	Los ambientes de desarrollo deben estar aislados y contar con todas las medidas de seguridad en cuanto a control de acceso a la información y a las instalaciones							

14.2.7	**Desarrollo contratado externamente**	Cuando se adquieran sistemas externos, realizar seguimiento, es necesario validarlos antes de ponerlos en funcionamiento							
14.2.8	**Pruebas de seguridad de sistemas**	Someter los sistemas a pruebas con el fin de identificar vulnerabilidades, se podría contemplar pruebas de hacking ético.							
14.2.9	**Prueba de aceptación de sistemas**	Someter los sistemas a pruebas con el fin de identificar vulnerabilidades, se podría contemplar pruebas de hacking ético.							
14.3	**Datos de prueba**								
14.3.1	**Protección de datos de prueba**	Hay que tener cuidado con los datos que se van a ingresar para realizarle pruebas a la aplicación, esto con el fin de evitar alguna fuga de información importante.							
15	**Relación con los proveedores**								
15.1	**Seguridad de la información en las relaciones con los proveedores**								

15.1.1	**Política de seguridad de la información para las relaciones con proveedores**	Igual que con los usuarios de la organización, con los proveedores se deben establecer acuerdos de confidencialidad, control de acceso a l información, seguridad física, intercambio de información entre otros para no ver afectada la seguridad de la información.							
15.1.2	**Tratamiento de la seguridad dentro de los acuerdos con proveedores**	Definir acuerdos de confidencialidad							
15.1.3	**Cadena de suministro de tecnología de información y comunicación**	Se deben establecer acuerdos que permitan mitigar los riesgos de la seguridad de la información derivados de la cadena de suministro.							
15.2	**Gestión de la prestación de servicios con los proveedores**								
15.2.1	**Seguimiento y revisión de los servicios de los proveedores**	Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.							
15.2.2	**Gestión de cambios en los servicios de proveedores**	Se debe contar con otras alternativas de proveedores que permitan la continuidad del servicio en caso de cambio de proveedor							

16	**Gestión de incidentes de seguridad de la información**								
16.1	**Gestión de incidentes y mejoras en la seguridad de la información**								
16.1.1	**Responsabilidad y procedimientos**	Definir procedimientos que permitan una reacción rápida ante problemas generados por causa de la seguridad de la información.							
16.1.2	**Reporte de eventos de seguridad de la información**	Se debe informar sobre eventos generados a causa de seguridad de la información con el fin de documentar la solución, es necesario llevar un registro de estos.							
16.1.3	**Reporte de debilidades de seguridad de la información**	Informar oportunamente sobre eventos generados, con el fin de identificar recurrencias y debilidades en seguridad de la información.							
16.1.4	**Evaluación de eventos de seguridad de la información y decisiones sobre ellos**	Cada vez que se presente un evento se seguridad de la información es importante evaluar si será considerado como un incidente o no.							
16.1.5	**Respuesta a incidentes de seguridad de la información**	Se debe establecer un proceso que permita establecer los pasos a seguir para atender el incidente.							

16.1.6	**Aprendizaje obtenido de los incidentes de seguridad de la información**	La experiencia que se ha adquirido en resolver los incidentes, es pieza fundamental para reducir el impacto que pueda causar este incidente a la seguridad de la información							
16.1.7	**Recolección de evidencia**	Definir un procedimiento para documentar los incidentes de tal forma que exista una evidencia.							
17	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**								
17.1	**Continuidad de seguridad de la información**								
17.1.1	**Planificación de la continuidad de la seguridad de la información**	Definir políticas que permita la gestión de la continuidad del negocio, aunque la organización presente una crisis							
17.1.2	**Implementación de la continuidad de la seguridad de la información**	Implementar procedimientos que permitan la continuidad del negocio ante situaciones imprevistas que podrían causar retrasos en la operación.							
17.1.3	**Verificación, revisión y evaluación de la continuidad de la seguridad de la información**	Realizar revisiones a los procedimientos implementados para la gestión de la continuidad del servicio para determinar si son efectivos o no.							
17.2	**Redundancias**								

17.2.1	**Disponibilidad de instalaciones de procesamiento de información.**	Es necesario establecer redundancias en las instalaciones donde se procesa la información con el fin de que no se vea afectada la disponibilidad de la información.							
18	**Cumplimiento**								
18.1	**Cumplimiento de requisitos legales y contractuales**								
18.1.1	**Identificación de la legislación aplicable y de los requisitos contractuales**	Definir el marco legal con el cual se debe regir la seguridad de la información.							
18.1.2	**Derechos de propiedad intelectual**	Cumplir a cabalidad las políticas de derechos de propiedad intelectual, software patentado.							
18.1.3	**Protección de registros**	Procedimiento que permita la custodia de los registros ante situaciones de robo, modificación, divulgación.							
18.1.4	**Privacidad y protección de datos personales**	Cumplir con las políticas de la protección de datos personales							
18.1.5	**Reglamentación de controles criptográficos**	Cumplir con las normas relacionadas con controles criptográficos							

18.2	**Revisiones de seguridad de la información**								
18.2.1	**Revisión independiente de la seguridad de la información**	Se debe revisar periódicamente el SGSI, estas revisiones deben ser adicionales a las establecidas en las políticas de seguridad de la información.							
18.2.2	**Cumplimiento con las políticas y normas de seguridad**	La dirección debe revisar los cumplimientos de las políticas de seguridad de la información establecidas de acuerdo a su área de responsabilidad.							
18.2.3	**Revisión del cumplimiento técnico**	Se deben revisar que todo el personal conoce y cumple con las políticas de seguridad de la información							

POLITICAS Y PROCEDIMIENTOS PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACIÓN DE LOS SERVICIOS EN LA NUBE EN EL MINSA

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
Política general de la seguridad de la información	

La Política de Seguridad de la Información de Servicios en la Nube es el compromiso de la alta dirección y de los colaboradores del MINSA con respecto a la protección de los activos informáticos que soportan los procesos de la compañía y declaran su apoyo a la implementación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27017.

El MINSA se compromete a proteger la información creada, procesada, transmitida o resguardada, orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad y a la continuidad de las operaciones de la compañía. Creando cultura y conciencia de seguridad de la información en los empleados, proveedores y personas que hagan uso de los activos informáticos de la compañía.

Toda información generada por los empleados, proveedores y practicantes universitarios o aprendices del MINSA será en beneficio y desarrollo de las actividades propias de la compañía, es decir, será de total propiedad del MINSA.

El MINSA se compromete a renovar las instalaciones físicas de la compañía a fin de proteger todos los activos informáticos que reposan dentro de ella, estableciendo controles de acceso y garantizando adecuadas condiciones ambientales.

El MINSA procura dar cumplimiento a normatividades y leyes creadas para proteger la información y los activos informáticos.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P01 - Política general de gestión de activos	

El área de TI debe disponer de un inventario de los activos informáticos del MINSA y mantenerlo actualizado.

Es responsabilidad del área de TI crear una codificación para identificar cada activo informático.

Es responsabilidad del área de TI crear una hoja de vida para cada activo informático donde se evidencie toda la información referente a este, factura de compra, datos de licenciamiento de SW e historial de mantenimientos preventivos y correctivos.

El área de TI debe participar en la definición de pólizas de seguros que cubran los activos informáticos en caso de siniestro.

El área de TI al asignar equipos a los empleados nuevos, deberá diligenciar de forma completa el formato de entrega de herramientas de trabajo, donde se evidencie descripción de la herramienta entregada, serial, cantidad, observaciones si son necesarias y hacer firmar el formato por el empleado.

El área de TI es responsable de asegurar con cables de seguridad los equipos portátiles entregados a los empleados y por parte del empleado es responsable revisar que su equipo de cómputo este siempre asegurado y si no debe informar inmediatamente.

Una vez finalizado el contrato de trabajo, el empleado deberá hacer entrega de los implementos informáticos al área de TI, para que este genere un formato donde quede constancia de la entrega de estos y se haga revisión de su estado, a su vez, el área de TI validando lo anterior, procederá a firmar el formato de devolución de activos.

Para los empleados del MINSA que, habitualmente salen con sus equipos portátiles, deben ser cautelosos con la manipulación de los activos y la seguridad de los mismos, en caso de pérdida o robo deberán informar al área de TI y poner una denuncia a la policía. Deberán presentar los equipos cada 30 días al área de TI y cada vez que esta área lo solicite para control de estado del activo.

Para otros empleados que requieran hacer uso de algún activo informático fuera de las instalaciones del MINSA, deberá enviar una solicitud de salida de activos informáticos al área de TI, diligenciar dicha solicitud y solicitar la firma de autorización de la Gerencia de TI.

Los equipos informáticos asignados son para el uso exclusivo de las labores y para almacenamiento de información dentro del MINSA.

Está prohibido el intercambio de partes como cargadores, mouse o teclados, en caso de requerir cambio por daños o mal funcionamiento debe reportase al área de TI para su diagnóstico, reparación o reposición.

Es responsabilidad del empleado del MINSA mantener su equipo en buenas condiciones, está prohibido colocarle pegatinas, marcarlos o rayarlos, evitando por todos los medios su deterioro, caso contrario, se procederán a realizar descuentos según sea dicho daño.

Es responsabilidad de la líder de selección y calidad, verificar la veracidad de la documentación de la hoja de vida del aspirante al cargo antes de la contratación.

El área de RRHH del MINSA debe exigir que todos los empleados conozcan y cumplan las políticas establecidas para la seguridad de los activos informáticos.

Al inicio de actividades laborales del empleado nuevo, la líder de selección y calidad debe entregar el manual de funciones y responsabilidades para el puesto de trabajo. De igual manera, hacer firmar el acuerdo de confidencialidad, y guardar copia en el archivo junto con la hoja de vida y contrato laboral.

Al término del contrato laboral, la líder de selección y calidad deberá informar al área de TI el cese del colaborador para inactivar cuentas de usuario y solicitar la entrega de activos informáticos entregados al inicio de contrato.

El área de RRHH del MINSA debe exigir que todos los empleados conozcan y cumplan las políticas establecidas para la seguridad de los activos informáticos.

Al inicio de actividades laborales del empleado nuevo, la líder de selección y calidad debe entregar el manual de funciones y responsabilidades para el puesto de trabajo. De igual

manera, hacer firmar el acuerdo de confidencialidad, y guardar copia en el archivo junto con la hoja de vida y contrato laboral.

Al término del contrato laboral, la líder de selección y calidad deberá informar al área de TI el cese del colaborador para inactivar cuentas de usuario y solicitar la entrega de activos informáticos entregados al inicio de contrato.

Con el propósito de cumplir con la ley de protección de datos, la información confidencial de cada empleado deberá archivarse de forma que solo tendrán acceso las personas autorizadas.

El área de capacitación del MINSA con apoyo del área de TI deberá promover capacitaciones a los empleados sobre temas de seguridad de la información con el fin de mantenerlos actualizados y de esta manera prevenir futuras amenazas informáticas por desconocimiento en el tema.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P03 - Política para el uso correcto de la Información	

Todo candidato que aspire a un determinado cargo dentro del MINSA, adicional a su contrato de trabajo deberá firmar un acuerdo de confidencialidad, en el cual acepta las cláusulas donde se comprometen a no divulgar, usar o robar información de la institución a la cual tenga acceso.

Todo desarrollo realizado por los colaboradores del MINSA será propiedad intelectual de la institución.

Es necesario no entregar ningún tipo de información confidencial por teléfono, por celular, por mensajería instantánea, por correo electrónico, hasta no ser verificada la identidad del solicitante.

El área de TI, como administrador de servidores y bases de datos debe garantizar la confidencialidad de la información y el uso de credenciales de acceso a las diferentes plataformas.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P04 - Política para el Acceso físico	

Todas las áreas donde se encuentren activos informáticos, así como el acceso a las diferentes oficinas, deben de ser protegidos contra accesos no autorizados, utilizando procedimientos, monitoreo y registro de entrada y salida.

El MINSA deberá disponer de cámaras de vigilancia para monitorear eventos de seguridad.

Todos los proveedores y contratistas deben portar en un lugar visible el carnet que los identifica para el acceso a la institución.

Debe contratarse un vigilante para mantener la seguridad dentro de las instalaciones de la institución.

La coordinadora de Sistema de Gestión de Calidad, debe mantener señalizada las áreas de accesos no autorizados y demarcación de zonas de trabajo.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P05 - Política de copias de respaldo	

El área de TI es el responsable de realizar los respaldos de la información almacenada en los servidores y por ende de las bases de datos, a través de una tarea programada desde el SQL Server para que se generen automáticamente, definir el contenido de los respaldos, tipo de respaldo, la frecuencia del respaldo, la codificación para identificarlos y la ubicación de estos.

El área de TI debe mantener un inventario de las copias de respaldo de la información del sistema de Información, Nómina, configuración del Fortigate, carpeta de archivos compartidos, repositorios de adjuntos del sistema de información, entre otros.

El área de TI debe verificar la correcta ejecución de los procesos de Backup, y el estado del inventario de los respaldos.

Las copias de seguridad se guardarán con el objetivo de utilizarse en caso de contingencia para la recuperación de la información luego de haberse presentado una amenaza ya sea por ataque de un virus informático, daños lógicos de los equipos, contaminación, catástrofes ambientales o industriales, donde se necesite restaurar el sistema.

El área de TI será el responsable de almacenar las copias de seguridad donde se tenga control de acceso y otra ubicación fuera de las instalaciones de la institución ya sea de forma física o almacenada en un espacio en la nube como Google Drive donde solo tendrán acceso las personas indicadas.

El área de TI deberá cifrar las copias de respaldo de la base de datos a través de herramientas como GPG para asegurar la confidencialidad en otro lugar fuera de las instalaciones del MINSA o en la nube.

El área de TI deberá mantener en su custodia las claves para desencriptar las copias de seguridad en caso sea necesario.

Es necesario tener un plan de contingencia en el cual se detalle el uso correcto de las copias de respaldo de la información para restaurar el sistema en caso de un siniestro.

Los usuarios no podrán guardar información en el servidor de archivos compartidos que no sea pertinente a la institución. Se prohíbe guardar información personal como fotos, documentos, música o videos.

El área de TI solo se responsabilizará por realizar copias de seguridad de información de los usuarios que estén contenidas en el servidor de archivos compartidos. Los usuarios son responsables de la información local de sus equipos.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P06 - Política para el uso correcto del internet	

El acceso a internet es un recurso para contribuir a actividades laborales como accesos a portales de proveedores, portales bancarios, portales gubernamentales entre otros según las necesidades del cargo y funciones desempeñadas.

El acceso a redes sociales no es permitido a excepción de la persona encargada del manejo comercial y promocional de la institución.

Los empleados autorizados para el uso de Internet, no podrán descargar, copiar, instalar software que necesiten de licenciamiento y que puedan generar sanciones a la institución por derechos de autor.

El área de TI, definirá niveles de acceso a internet aplicado a los usuarios, bloqueando accesos a sitios web que sean categorizados como inapropiados a través del Fortigate y en caso de que se requiera algún permiso especial debe ser autorizado por la Gerencia de su área en la que labora.

Los usuarios son responsables de las actividades que se realicen desde sus equipos hacia internet, por eso la importancia de cuidar sus sesiones.

Cada usuario es responsable de cualquier evento no deseado que se provoque al intentar acceder a algún sitio no autorizado.

Los empleados autorizados para el uso de Internet deben reportar al área de Sistemas, cualquier anomalía que pueda afectar la seguridad de los activos informáticos de la compañía.

El área de TI debe programar la descarga de las actualizaciones del sistema operativo en horas que no afecte las actividades del negocio.

Para ingreso a portales bancarios digitar la URL y verificar que sea establezca conexión segura a través de HTTPS y usando el token proporcionado por la entidad bancaria.

Los usuarios por seguridad no deben guardar credenciales cuando se los pregunte el navegador utilizado al ingresar a algún sitio.

Solicitar reporte mensual al proveedor de servicios móviles, el consumo de datos de los equipos de los colaboradores con el fin de monitorear el uso.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P07 - Política para el uso del correo institucional	

El correo institucional deberá ser creado por el área de TI para los empleados autorizados por la Gerencia del MINSA a las áreas en las que labora.

Todos los mensajes tanto enviados o recibidos por medio de correo electrónico institucional pertenecen al MINSA y está podrá acceder a ellos cuando lo requiera.

El correo institucional solo será utilizado con propósitos laborales.

Es responsabilidad del empleado evitar que su cuenta de correo electrónico sea utilizada por terceros.

El área de TI debe supervisar que todos los correos institucionales creados deben configurársele la firma digital del empleado que hará uso.

No se permite el envío de spam a clientes con fines comerciales

Será sancionado el uso del correo institucional para cometer acciones ilícitas.

El empleado es responsable de cualquier archivo adjunto que envíe a terceros a través del correo institucional.

El empleado debe ser precavido con la descarga de archivos adjuntos que reciba de terceros a través del correo institucional.

Es responsabilidad del empleado archivar los mensajes de correos electrónicos para efectos de soportar ante terceros en caso de requerirse.

El área de TI definirá el tamaño del buzón de acuerdo a las actividades que desempeñará el empleado y a la capacidad del Hosting contratado.

Ningún usuario tiene información de la cuenta de correo electrónico institucional, ya que esta se entrega configurada en el Outlook del equipo asignado.

El área de TI debe tener un inventario sobre las cuentas de correos creados y sus respectivas contraseñas.

El área de TI debe utilizar contraseñas seguras basadas en la política de gestión de contraseñas.

El área de TI será la encargada de crear y administrar las cuentas de correo de Gmail para la configuración de las cuentas de Google Play Store de los smartphones.

Los usuarios no podrán configurar cuentas de correos personales en los celulares asignados por la institución.

El área de TI podrá desactivar las cuentas de correo que no demuestren su uso durante más de dos (2) meses consecutivos.

El área de RRHH deberá informar al área de TI sobre los usuarios que saldrán a vacaciones o licencias de trabajo, para desactivar temporalmente las cuentas y configurar un mensaje de respuesta automática, con el fin de evitar que los buzones de mensajes se llenen y bloqueen las demás cuentas.

Las cuentas de correo serán desactivadas después de 7 días hábiles a partir de la fecha en la cual la persona termine su vinculación con la institución.

El área de TI deberá crear medidas de control en el Fortigate y en el servidor de correos para filtrar correos maliciosos con contenidos perjudiciales.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P08 - Política de seguridad en el Data center	

El MINSA debe disponer de un área restringida para la ubicación de los activos informáticos críticos que soportan la infraestructura tecnológica del sistema de información.

Este centro de datos debe tener un sistema de refrigeración por aire acondicionado que mantenga la temperatura adecuada, las tomas eléctricas deben estar debidamente organizadas e instaladas.

El área de TI debe garantizar que todos los activos informáticos ubicados dentro del centro de datos estén protegidos con UPS, el cual permita un tiempo considerable mientras se restablece la energía o se realice un apagado correcto.

Dentro del centro de datos se prohíbe comer o beber.

En el centro de datos no debe almacenarse papelería, materiales inflamables o combustibles que generen riesgo de propagación de fuego.

Las puertas del centro de datos deben permanecer cerradas. La Gerencia de TI será la responsable de las llaves del sitio.

Cuando se realicen mantenimientos dentro del centro de datos por parte de terceros, deberán ser supervisadas por el área de TI.

Debe controlarse y vigilarse el acceso al centro de datos, ya que contiene los activos informáticos críticos.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P09 - Política de uso de software	

No está permitido la descarga ni instalación de software sin autorización previa del área de TI, con el fin de evitar piratería y sanciones de tipo legal para el MINSA

El área de TI deberá mantener inventariada las licencias con sus respectivos soportes de compra y medios de instalación

El área de TI deberá velar por la vigencia de las licencias del software adquiridos.

Es responsabilidad del área de TI, instalar el software necesario para cada equipo de cómputo del empleado del MINSA.

En caso de fallas del software y se solicita mantenimiento correctivo en el cual se repare o se actualice deberá quedar registrado en la hoja de vida del equipo de cómputo donde se presentó.

El área de TI deberá supervisar los mantenimientos correctivos, en caso de formateo de un equipo, suministrar al técnico los medios de instalación, licencias y exigir no realizar ningún tipo de instalación de software pirata o instalaciones sin autorización previa.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P10 - Política de uso correcto de contraseñas	

Es responsabilidad de cada empleado hacer buen uso de las cuentas de usuario asignadas sea para acceso al equipo, acceso remoto o sistemas informáticos de la institución, evitando compartir el uso de las cuentas, ni dejando en evidencia los datos de acceso que puedan ser usados por otra persona.

El área de TI inicialmente asignará la contraseña al empleado, pero deberá configurarse de tal manera que solicite ser inmediatamente cambiada en el primer inicio de sesión, cumpliendo con algunos parámetros de seguridad:

- Tener mínimo ocho caracteres.
- La contraseña debe estar compuesta por caracteres: mayúsculas, minúsculas, alfanuméricos y algún carácter especial.
- La contraseña no debe ser igual o parecida a la anterior.

El área de TI debe definir una política para que le exija al empleado el cambio de contraseña cada 30 días, el sistema debe informarle al empleado al inicio de sesión cumplido los días pactados.

El área de TI no restablecerá la contraseña a un usuario, a menos que este mismo lo solicite y se identifique a sí mismo.

Se deberán cambiar las contraseñas en caso de que exista o haya algún indicio de una posible vulnerabilidad del sistema.

Si al superar cinco intentos consecutivos al acceder a una cuenta de usuario de equipo o al sistema sin éxito, la cuenta se bloqueará por motivos de seguridad en la cual tendrá que intervenir El área de TI.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P11 - Política de protección contra software malicioso	

Es responsabilidad del área de TI gestionar el licenciamiento del antivirus que brinde protección contra software malicioso.

El área de TI debe instalar en cada equipo de cómputo y servidores el software antivirus.

Es responsabilidad El área de TI monitorear desde la consola del antivirus las actividades anormales que se presentan para mitigar los riesgos.

Los empleados deben reportar fallas si el antivirus informa alguna falla o detección de virus.

Los empleados deberán analizar previamente con el antivirus el medio de almacenamiento como USB antes de abrir los archivos contenidos para evitar riesgos de seguridad al MINSA.

No está permitido el uso de medios de almacenamiento virtual que no estén previamente autorizados por el área de TI.

Cualquier sospecha de anomalías en el equipo asignado a causa de infección de virus, deberá ser informado inmediatamente al área de TI para la revisión y solución de la amenaza.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P12 - Política de equipo sin uso	

El área de TI debe garantizar que todos los equipos de cómputo estén configurados de tal forma que cuando detecte el sistema periodos de inactividad del empleado, después del tiempo establecido se bloquee la sesión del usuario y requiera de datos de accesos para iniciar sesión.

Es responsabilidad del empleado al realizar pausas activas o alejarse del puesto de trabajo, bloquear la sesión para evitar suplantación de identidad, sabotajes o robo de información.

Los usuarios no deben utilizar el sistema de una sesión que no sea la asignada.

El usuario deberá asumir parte de las responsabilidades en su sesión de usuario en caso de algún incidente ya sea por préstamo de credenciales o por no bloquear su sesión.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P13 - Política de Acceso remoto	

El servicio de acceso remoto solo será habilitado a usuarios con fines laborales.

El servicio de acceso remoto debe permitir solo acceso al sistema de información de la institución y a archivos compartidos en la intranet.

El área de TI debe definir un canal seguro para la conexión de usuarios externos a través de la configuración y asignación de datos de acceso a los empleados mediante la VPN de la institución.

El área de TI deberá configurar políticas en el servidor donde se conectan los usuarios remotos para que después de determinado tiempo de inactividad o detección de usuarios desconectados, las sesiones se cierren completamente evitando el consumo de recursos por procesos activos en el servidor sin utilizarse.

El área de TI deberá gestionar licencias de usuarios remotos necesarios para el acceso al servidor de Terminal.

Está prohibido utilizar herramientas de soporte remoto como Anydesk, Team viewer, Zoom, etc. Solo se podrán utilizar con autorización y supervisión del área de TI.

El área de TI debe garantizar la disponibilidad del servicio de internet a los usuarios remotos para que accedan al sistema.

PERÚ MINSA	Versión 1.0
	Autor: Dávila Chunga Dayán Ray
	Fecha: 07/11/2022
RPS-P14 - Política de gestión de incidentes	

El MINSA, debe establecer procedimientos para la gestión y tratamiento de incidentes de seguridad de los activos informáticos, con el fin de detección temprana y prevención de incidentes, crear una bitácora de incidentes con su respectiva solución para ir documentando los planes de acción ante determinada incidencia y auditar la respuesta de incidentes para una mejora continua.

Los empleados están obligados a reportar a el área de TI situaciones sospechosas o anómalas que puedan considerarse como incidencias de seguridad informática. A su vez el área de TI deberá analizar y valorar la incidencia reportada y comunicarla a la Gerencia de TI. En última instancia el Gerente evaluará la incidencia y tomará acciones sancionando al implicado o recurrir ante las autoridades competentes.

Toda la información referente a los incidentes reportados, debe ser manejada con discreción y confidencialidad.

PROCEDIMIENTOS

El MINSA describe los siguientes procedimientos con el fin de apoyar los procesos que ayudan a mejorar y proteger los activos informáticos.

P-RPS-01 - Gestión de usuarios.

La creación, modificación y eliminación de usuarios requiere atención óptima y oportuna para que todo colaborador inicie sus actividades sin ningún inconveniente hasta el cese de su vínculo laboral, es en esta fase en la que se debe de bloquear las cuentas asociadas al usuario, impidiendo de esta manera delitos informáticos como fuga o robo de información.

Objetivo. Establecer los lineamientos para gestionar usuarios.

Alcance. El procedimiento de gestión de usuario, indica los pasos a seguir

Para la óptima gestión de cuentas y accesos de los empleados de MINSA para el uso de sus sistemas de informáticos.

Responsabilidades:

a. Coordinador de TI.

- Vigilar el cumplimiento del procedimiento.
- Asignar cuentas de usuarios para los diferentes accesos según rol.
- Mantener registro de inventario de cuentas creadas e historial de cambios de usuarios.

b. Líder de calidad.

- Solicitar e informar al área de TI la vinculación y desvinculación de empleados que tengan designados equipos de cómputo y acceso al sistema.

c. Usuario.

- Cumplir con los acuerdos de confidencialidad.
- No compartir credenciales de cuentas de usuarios asignadas.

Descripción.

I. La líder de calidad informa al área de TI sobre dar de alta o baja al usuario a través de un correo electrónico. La solicitud debe indicar datos básicos del empleado como número de documento de identificación, nombre completo, cargo y el área en la que desempeña funciones.

II. Si corresponde a solicitud de creación de nuevo usuario, se debe contar adicionalmente con datos como teléfono, dirección, correo electrónico, así como rol que desempeñará para definir el perfil de la cuenta de usuario. Los datos deben enviarse completos para procesar la solicitud.

III. Seguidamente se dan permisos de acceso a la red, se asigna usuario y licencia para el uso de los sistemas, también se asigna un correo institucional y si es usuario remoto se crea una VPN con la que podrá conectarse.

IV. Se envía un correo electrónico de respuesta al líder de calidad informando de las cuentas y perfiles creados. Se envía a la cuenta de correo electrónico

proporcionada los datos de acceso a los sistemas. Adicional a ello, Se adjunta copia del manual de políticas de seguridad de la institución.

V. Si la solicitud corresponde a un usuario que será dado de baja, se debe de informar la fecha en la que la cuenta ya no tendrá más acceso a los sistemas de la institución.

VI. Se envía correo electrónico al líder de calidad indicando que se procedió a realizar la baja del usuario.

P-RPS-02 - Mantenimiento Preventivo.

Los activos informáticos correspondientes a hardware y software requirieren de un mantenimiento trimestral, con el fin de alargar la vida útil de los equipos y evitar fallos de los equipos, logrando prevenir las incidencias antes de que estas ocurran.

Objetivo. Crear un cronograma anual de mantenimiento preventivo de los activos informáticos de la institución que soportan los datos y aplicarlo, con el fin de protegerlos y mantenerlos en condiciones aptas para garantizar el buen funcionamiento y rendimiento del sistema de información.

Alcance. Este procedimiento es aplicable para cubrir el servicio de mantenimiento preventivo de los activos informáticos y de redes que sean de propiedad de la institución y correspondan a la sede Principal del MINSA.

Responsabilidades

a. Coordinador de TI.

- Verificar el cumplimiento del procedimiento.
- Supervisar la ejecución de los mantenimientos preventivos en las fechas estipuladas y bajo las condiciones en las que se contrató el servicio con el proveedor.
- Revisar y firmar los reportes de mantenimiento
- Verificar registros de las actividades y observaciones realizados en la hoja de vida de cada activo informático.

b. Soporte TI.

- Cumplir con el soporte programado.
- Utilizar los implementos de protección necesarios para realizar las actividades de mantenimiento.
- Informar de cualquier novedad que evidencie en los activos informáticos a el Coordinador TI
- Registrar y documentar las actividades realizadas en las hojas de vida de los activos e informes de soporte.

Descripción.

I. El área de TI deberá acordar junto con el proveedor contratado de los mantenimientos, la programación anual de los mantenimientos preventivos. El contrato deberá incluir, frecuencia de mantenimientos, sedes las cuales se le harán mantenimiento, cantidad de equipos por sedes, recomendaciones de utilización de implementos de protección necesarios para la realización de las actividades, entregar mensualmente copias del pago de seguridad social y demás parafiscales del técnico encargado y si la actividad a realizar lo requiere deberá certificar curso de altura.

II. Elaborar y publicar programa general de mantenimientos preventivos, para que los usuarios estén atentos a la fecha correspondiente a su equipo.

III. Informa a los usuarios y a los proveedores sobre la realización de actividades programadas de mantenimiento preventivo.

IV. En el momento de realización de los mantenimientos preventivos por parte del proveedor, darle las indicaciones y recomendaciones necesarias sobre las actividades a realizar como:

- Limpieza física de los equipos, si hay algún equipo en garantía no destapar.
- Limpieza de software: borrado de temporales, análisis del antivirus, revisión de instalación de software no autorizado.
- Revisión lógica: ejecución de Scandisk, desfragmentación del disco.
- Actualizaciones pendientes de software.
- Revisión de batería de UPS
- Registrar en cada orden de mantenimientos, la fecha, número de equipo, serial del equipo, actividades realizadas dentro en cada equipo, novedades, fallas encontradas.

V. El área de TI deberá supervisar la jornada de mantenimientos, para verificar el trabajo realizado en cada equipo, dando su aprobación en cada orden de mantenimiento.

VI. En caso de que el técnico encuentre una falla y sea necesario reemplazar algún componente, como por ejemplo la batería de la UPS, deberá registrarlo e informarle al área de TI.

VII. El área de TI hará las cotizaciones pertinentes referentes a la parte afectada y si es de cambio urgente, presentará las necesidades a la Gerencia de TI para que apruebe la asignación de presupuesto.

P-RPS-03 - Mantenimiento Correctivo.

El mantenimiento correctivo se origina inesperadamente a causa de una falla o avería en un activo informático por tal motivo no se puede considerar como una actividad panificable, en caso de falla en hardware puede representar costos por cambio o reparación del componente.

Objetivo. Realizar mantenimiento correctivo de los activos informáticos de la institución, que soportan los datos con el fin reparar daños y reestablecer el buen funcionamiento del mismo.

Alcance. Este procedimiento es aplicable para cubrir el servicio de mantenimiento correctivo de los activos informáticos y de redes que sean de propiedad de la institución y correspondan a la sede Principal del MINSA.

Responsabilidades

a. Coordinador TI.

- Vigilar el cumplimiento del procedimiento.
- Supervisar las actividades realizadas por el técnico que brinda el soporte, enviado por el proveedor contratado.
- Analizar la valoración del activo dada por el técnico para tomar decisiones.
- Gestionar la compra de la pieza o activo averiado con el Gerente.
- Verificar que el activo que presenta fallas quede funcional.
- Asegurarse de que el registro de las actividades realizadas haya quedado detallado en la hoja de vida del activo informático afectado.

b. Soporte TI

- Atender el soporte de acuerdo a los niveles de atención contratadas.
- Utilizar los implementos de protección necesarios para realizar las actividades de mantenimiento.
- Informar de cualquier novedad que evidencie en los activos informáticos a la Coordinador TI para cambio de partes.
- Registrar y documentar las actividades realizadas en la hoja de soporte.

c. Usuario.

- Informar el mal funcionamiento del activo informático.
- Describir las acciones que estaba realizando en el momento de presentar la falla.
- Realizar pruebas sobre el activo para confirmar solución de falla.

Descripción.

I. El área de TI deberá descartar fallas de primer nivel, con el fin de resolver. Si es algo crítico, solicitar el servicio de mantenimiento correctivo al proveedor. Llamando a la línea de soporte, para que se agende el servicio según la prioridad que se le asigne.

II. Registrar en la orden de mantenimientos, la fecha, número de equipo, serial del equipo, actividades realizadas dentro en cada equipo, novedades, fallas encontradas.

III. En caso de que el técnico encuentre una falla y sea necesario reemplazar algún componente, como por ejemplo la batería de la UPS, deberá registrarlo e informarle al área de TI.

IV. El área de TI hará las cotizaciones pertinentes referentes a la parte afectada y si es de cambio urgente, presentará las necesidades a la Gerencia de TI para que apruebe la asignación de presupuesto.

V. El área de TI deberá supervisar la jornada de mantenimientos, para verificar el trabajo realizado en cada equipo, dando su aprobación en la orden de mantenimiento.

VI. Evaluar el servicio prestado para garantizar la calidad de este.

P-RPS-04 – Procedimiento de Gestión de Incidentes.

La gestión de incidentes consiste en resolver de manera rápida y eficaz, cualquier evento causante de interrupción parcial o total de las actividades realizadas por un activo informático, comprometiendo la confidencialidad, integridad, disponibilidad, autenticidad o confiabilidad de la información.

Objetivo.

Definir responsables que atiendan los incidentes y garanticen la operatividad del negocio, la continuidad y la disponibilidad del servicio.

Establecer el seguimiento que se debe aplicar a los incidentes de seguridad de la información para ser analizados y clasificados.

Aplicar salvaguardas adecuadas a los incidentes en la institución y operaciones de negocio con el fin de mitigar el impacto causado.

Llevar bitácora de incidencias ocurridas, las cuales incrementa las oportunidades de prevenir las ocurrencias de futuros incidentes.

Alcance. Este procedimiento contempla desde la detección y reporte de Incidentes por parte del usuario, hasta el seguimiento que le dé el responsable de la gestión de incidentes: recepción, análisis de Incidentes, rastreo de ataque, custodia de evidencia, recuperación de datos o sistemas afectados, restauración de la información y registro en bitácora para manejo de incidentes futuros.

Responsabilidades

a. Coordinador TI.

- Vigilar el cumplimiento del procedimiento.
- Bloquear conexiones de red del equipo afectado para evitar replicas.
- Resolver la incidencia y solicitar apoyo al proveedor si es necesario.
- Documentar las incidencias para prevenir futuras amenazas.

b. Usuario.

- Informar incidente inmediatamente a El área de TI.
- Describir las acciones que estaba realizando en el momento de presentar la falla.
- Seguir indicaciones y recomendaciones dadas por la coordinara de sistemas.

Descripción.

I. En el momento en que se detecte comportamientos extraños en el funcionamiento de un equipo o servicio prestado en el MINSA, el usuario tiene la obligación de informar inmediatamente al coordinador de TI, el cual validará el incidente e informará al Gerente de TI si el impacto es alto.

II. A continuación, se detallarán indicaciones de cómo debe proceder el coordinador de TI ante un incidente:

- Desconectar el equipo afectado para aislarlo de la red.

- El usuario responsable del equipo afectado debe brindar información y el apoyo que requiera el área de TI para realizar el levantamiento de información.
- El área de TI determinará el origen y destino de la incidencia.
- Analizar el impacto causado en el equipo o sistemas involucrados.
- Etiquetar y poner en custodia la evidencia
- Identificar y aplicar el tratamiento o solución al incidente
- Documentar el Incidente en una bitácora, teniendo en cuenta aspectos como:
  - Fecha
  - Equipo afectado
  - Responsable del equipo
  - Resumen del incidente
  - Acciones realizadas.
  - Evidencias recopiladas
  - Observaciones.
  - Recomendaciones
  - Tratamiento de la incidencia.

III. Si el incidente tiene probabilidad de replicarse en otros equipos, el coordinador de TI implementará las mismas medidas preventivas en los demás equipos.

IV. El área de TI tiene el deber de reportarle al gerente los incidentes presentados si es de alto impacto en el mismo instante o si es de medio o bajo luego de solucionarlo.

V. El área de TI deberá dar recomendaciones a los usuarios si es necesario realizar capacitación sobre las medidas preventivas.

VI. Los usuarios responsables de los equipos involucrados deben acatar las medidas correctivas indicadas por la coordinadora.

VII. Una vez concluido el proceso de descartes de incidentes o restauración del equipo, El área de TI restablecerá las conexiones de red al equipo.

P-RPS-05 - Actualización de Sistemas Operativos y Software.

Los fabricantes de software constantemente están liberando nuevas versiones, parches de actualizaciones aplicadas a sistemas operativos, aplicaciones, controladores de hardware, antivirus para corregir fallas de seguridad, mejoras o corrección de errores para mitigar vulnerabilidades.

Objetivo.

Definir los lineamientos para llevar a cabo procesos de actualización y cambios en los sistemas operativos y software.

Alcance.

El procedimiento contempla indicaciones para efectuar actualizaciones y cambios en los sistemas operativos y software autorizados por la Gerencia de TI y el coordinador TI.

Responsabilidades

a. Coordinador TI.

- Controlar el cumplimiento del procedimiento.
- Mantenerse informada de actualizaciones y mejoras de sistemas operativos y software.
- Tener un ambiente de pruebas para las actualizaciones.
- Programar horarios de actualizaciones para no afectar la operatividad de actividades.

- Informar y solicitar autorización a Gerencia de TI para programación de actualizaciones críticas.
- Realizar pruebas de migraciones en ambiente de pruebas antes de pasar a producción.
- Documentar cambios de sistemas operativos y software para control y seguimiento.
- Solicitar generación de licencias en caso de necesitarse.

b. Proveedor de software.

- Proveer repositorios para descarga de instaladores de actualizaciones.
- Proveer información sobre mejoras y versiones.
- Proveer licencias.
- Ofrecer acompañamiento y canales de soporte

c. Gerente de TI.

- Dar apoyo y autorización a El área de TI para la realización de actualizaciones.
- Coordinar la seguridad de las instalaciones para trabajar en actualizaciones en días no laborables.

Descripción.

Sistemas Operativos de Servidores

I. Se deberá abrir una ventana de mantenimiento para programar la actualización del sistema operativo de los servidores. Debido a que para

este proceso se requiere el reinicio del servidor, debe programarse en horario que no afecte la actividad laboral.

II. Algunas actualizaciones pueden generar incompatibilidades con las aplicaciones, por lo tanto, es necesario revisar e investigar sobre los parches liberados por los fabricantes antes de cualquier cambio.

Sistemas Operativos de PC

I. Para no afectar el ancho de banda de internet, es necesario configurar en los equipos que el horario para realizar las actualizaciones del sistema operativo se haga en un horario determinado que no afecte las actividades laborales del empleado y evitar que estas no se descarguen en todos los equipos simultáneamente. Por tal motivo no se deben dejar automáticas sino programarse.

Software de los servidores.

I. Para actualizaciones de firmware o sistema de algún hardware como el Fortigate, es necesario tener respaldo de la configuración del equipo y programar una ventana de mantenimiento ya que este equipo soporta toda la administración de la red del MINSA, así que debe ejecutarse en horas fuera de la jornada normal.

II. En cuanto a actualizaciones de la consola del Antivirus, es necesario recurrir al uso de la consola para que primero se descargue en el servidor donde se administra la consola y luego se programe su distribución a los demás equipos de cómputo en un horario establecido que no afecte el rendimiento de la red, aunque esto no genera interrupción de las

actividades se evidencia lentitud en los equipos, por lo que se recomienda hacerlo en horarios laborales no muy concurridos por clientes.

P-RPS-06 - Operaciones del Centro de Datos.

Es necesario disponer de un sitio seguro y con condiciones adecuadas para establecer un Centro de Datos, en el cual se ubiquen y protejan los activos informáticos más críticos que soportan la infraestructura tecnológica para el funcionamiento del sistema de información y las comunicaciones del MINSA. Este centro de datos debe estar acondicionado para que la operatividad de la institución no se interrumpa.

Objetivo.

Establecer las normas para crear y mantener el centro de datos de la institución que contenga los activos informáticos críticos del MINSA

Alcance.

El procedimiento contempla las acciones a implementar para el buen funcionamiento del centro de datos de la institución en la Sede principal.

Responsabilidades

a. Coordinador TI.

- Verificar el cumplimiento del procedimiento.
- Controlar el Centro de Datos de la institución
- Supervisar el acceso al centro de datos.

- Asegurar que los activos ubicados en el centro de datos operen correctamente
- Hacer un chequeo semanalmente de las condiciones del centro de datos para corregir, mejorar y aplicar cambios necesarios.
- Programar y supervisar mantenimientos preventivos de los equipos.

b. Gerencia de TI.

- Brindar recursos financieros para mantener las condiciones óptimas del centro de datos del MINSA.

Descripción.

I. El procedimiento describe medidas que se deben aplicar para el centro de datos que debe crear el MINSA.

II. Suministro eléctrico y Sistema de alimentación ininterrumpida

III. Dentro del centro de datos se resguardan los activos informáticos más importantes que soportan la infraestructura tecnológica del sistema de información y comunicaciones del MINSA, en caso de fallo del suministro eléctrico, el sistema de alimentación ininterrumpida (UPS) entra a jugar un papel importante para mantener la disponibilidad de los activos como servidores, equipos de redes y comunicaciones.

IV. Las UPS deben cubrir todos los activos informáticos ubicados en el centro de datos previniendo el riesgo ante un corto o fluctuaciones de energía, no solo la caída de la conexión con los servidores generando pérdida de

información y de trabajo sino viéndose afectado los componentes lógicos y físicos de los activos.

V. Se debe realizar una estimación de la duración del tiempo de descarga de las baterías de la UPS para proveer el tiempo con el que se dispone para guardar documentos abiertos y realizar un apago correcto de los equipos para protegerlos de daños, en caso donde el corte de energía eléctrica sobrepasa el tiempo de disponibilidad de la UPS.

Sistema de Aire acondicionado

I. Mantener una temperatura adecuada es fundamental dentro del centro de datos, ya que las temperaturas generadas por los equipos y por las condiciones climáticas de la ciudad de Lima resultan bastantes altas y pueden ocasionar problemas a los activos informáticos que se encuentren resguardados en el centro de datos.

II. Si se presentan fallas en el sistema de aire acondicionado, la coordinadora de sistemas deberá aplicar medidas para mejorar las condiciones de temperatura y controlar el nivel de temperatura, solicitar soporte urgente con el proveedor de mantenimiento de aires acondicionados y si es necesario considerar apagar los equipos mientras se da una solución inmediata.

Canal de Internet, red MPLS y Central telefónica.

I. Al presentar caídas del servicio de internet, MPLS o telefonía, afecta las actividades del MINSA, denegando la conexión con las demás sedes en especial con las sedes donde las transacciones migran en tiempo real, esto

genera una desfase en la migración de la información creando duplicidad de documentos en algunos casos; el bloqueo de accesos a los portales de proveedores para realizar pedidos de mercancía; cese en el envío de cotizaciones y documentos a través de internet, las cuales están siendo solicitadas con urgencia por clientes, Por lo tanto, se deberán tomar medidas preventivas como otro canal de internet para contingencia y configuradas las IP públicas del servidor como plan opcional cuando la red MPLS no esté disponible; tener disponibles varias líneas celulares para solventar el problema de telefonía fija.

II. Los equipos propiedad de terceros correspondientes a los servicios subcontratados no deberán ser manipulados internamente, a menos que lo solicite el proveedor. En caso de fallos se deberá reporta a las líneas de atención para soporte, garantizando el cumplimiento de los niveles de atención contratados.

III. Se deberá supervisar y dar información necesaria a los proveedores de los servicios subcontratados con el fin de dar una rápida solución a alguna falla.

Equipos de redes y comunicaciones

I. Los equipos propiedad de terceros correspondientes a los servicios subcontratados no deberán ser manipulados internamente, a menos que el proveedor lo exija para apoyar en caso de soporte remoto o indique las instrucciones telefónicamente.

II. Se deberá realizar copias de respaldos del Fortigate, con el objeto de respaldar las políticas creadas y las demás configuraciones ante una falla

del dispositivo. En caso de avería de este activo debe disponerse de un plan de contingencia debido a que este equipo soporte toda la administración de la red LAN, WAN y WIFI.

P-RPS-07 - Seguridad de Redes.

Los usuarios del MINSA, para acceder al sistema de información o archivos compartidos, utiliza varios servicios ofrecidos por la administración de la red. Por tal motivo, es necesario establecer medidas que aseguren la integridad, confidencialidad y disponibilidad de la información.

Objetivo.

Definir lineamientos para controlar la seguridad de las redes y proteger la transmisión de la información al utilizar los servicios de red.

Alcance.

El procedimiento establece medidas para el MINSA.

Responsabilidades

a. Coordinador TI.

- Supervisar el cumplimiento del procedimiento.
- Administrar las redes del MINSA.
- Brindar soporte a usuarios con respecto al acceso a redes de la institución.
- Asegurar el cumplimiento de los servicios subcontratados de Internet, telefonía y Red MPLS.

- Monitorear las redes de comunicaciones.

b. Usuarios.

- Proteger las claves de acceso y sesiones a las redes que esté autorizado de MINSA.

Descripción

Administración de la red y de equipos de conectividad

I. El tipo de encriptación aplicada para la contraseña de red WIFI debe ser de WPA2-PSK (AES).

II. Los equipos de red y comunicaciones no deberán tener claves por defecto de fábrica, están deberán asignársele una clave segura.

III. Solo El área de TI podrá tener acceso y a la administración de los equipos de red que sean propiedad del MINSA.

IV. Deberán contemplarse en los mantenimientos preventivos.

Administración de la red privada virtual

I. El área de TI deberá crear un canal seguro, utilizando una red privada virtual (VPN) para accesos remotos al sistema de información del MINSA.

II. Se debe establecer horarios y duración de la conexión remota a los servidores para uso del sistema de información.

Administración de acceso inalámbrico (WIFI)

I. La administración del WIFI es responsabilidad del área de TI y solo el tendrá la clave de acceso para acceder a la red inalámbrica del MINSA.

II. Proveedores, clientes o visitantes a la institución, tendrán acceso a la red WIFI, solo en casos donde el coordinador de TI haya dado previa autorización y se conectarán a una red aislada para visitantes.

III. El área de TI deberá cambiar la contraseña y el nombre de la red WIFI con frecuencia para evitar accesos no autorizados, el nombre de la red no deberá ser algo que identifique la institución como tal, para pasar desapercibida, pero si se deberá usarse como tipo de seguridad WPA2-PSK (AES) para cifrar contraseñas.

IV. Dentro de la configuración del Fortigate, siendo este el dispositivo que libera las direcciones a las conexiones WIFI, deberá mantener reservadas las direcciones para los dispositivos inalámbricos autorizados identificados a través de sus direcciones MAC, nombre de usuario y dirección IP.

Seguridad del cableado de red de datos

I. Todo equipo de cómputo incluyendo equipos portátiles del MINSA, tendrá asignado una dirección IP estática por red cableada, configurada desde el Fortigate, con el fin de acceder más ágilmente y tener mayor estabilidad de conexión.

II. Solo se habilitará la red inalámbrica a equipos autorizados y que la requieran para movilidad del equipo.

P-RPS-07 - Monitoreo de Redes.

Los ataques a las redes son muy frecuentes y su transcendencia depende de los controles y mecanismos que se apliquen para monitorear y mantener la seguridad de ellas, pudiéndose detectar oportunamente la amenaza y tomar acciones para minimizar el impacto sobre los activos de información del MINSA.

Objetivo.

Implementar lineamientos para el monitoreo de redes y servicios

Alcance.

El procedimiento contempla el monitoreo de redes y servicios asociados a la Sede Principal del MINSA y a las sedes.

Responsabilidades

1.4.1. Coordinador TI.

- Asegurar el cumplimiento del procedimiento.
- Monitorear el tráfico de la red y servicios utilizando herramientas confiables que garanticen la optimización de la red.
- Configurar alertas sobre las aplicaciones de monitoreo para facilitar la administración de la red y los servicios.

Descripción

El MINSA cuenta con un dispositivo para proteger la red local y servicios como correo electrónico, control de navegación entre otros. Este dispositivo es un Fortigate, el cual

administra toda la red, asigna direccionamiento DHCP, monitorea y bloquea tráfico de red entrante y saliente según las políticas de configuración establecidas.

I. Para acceder y monitorear la red desde el Fortigate es necesario tener datos del usuario administrador, conocimientos de redes y otros conocimientos necesarios para el manejo de la interfaz.

II. Es indispensable realizar copias de respaldos del Fortigate, con el objeto de respaldar las políticas creadas y las demás configuraciones ante una falla del dispositivo.

III. En caso de avería de este activo se requiere de un plan de contingencia debido a que este equipo soporte toda la administración de las redes disponibles en el MINSA.

IV. Se deberá analizar con frecuencia los puertos, protocolos y servicios habilitados e identificar si están siendo usados, de lo contrario deshabilitarlos para evitar explotación de vulnerabilidades.

V. Se debe configurar desde el Fortigate el análisis de los protocolos IMAP y POP, aplicando filtros que ayuden a detectar y bloquear correos maliciosos.

VI. Para mayor control en la seguridad, se requiere analizar frecuentemente los logs de eventos proporcionados por Windows para el caso de los servidores o equipos y aplica también para los dispositivos como el Fortigate, con el fin de revisar la ocurrencia de eventos que puedan perjudicar los sistemas y activos de información.

Anexo 13. Formato T1

	AUTORIZACIÓN DEL AUTOR (ES) (LICENCIA DE USO)	Código:	F1.PP2-PR.02
		Versión:	02
		Fecha:	18/04/2024
		Hoja:	1 de 1

Pimentel, 02 de agosto del 2024

Señores

Vicerrectorado de investigación

Universidad Señor de Sipán S.A.C

Presente. -

El suscrito:

DAYAN RAY DAVILA CHUNGA con DNI 10467519

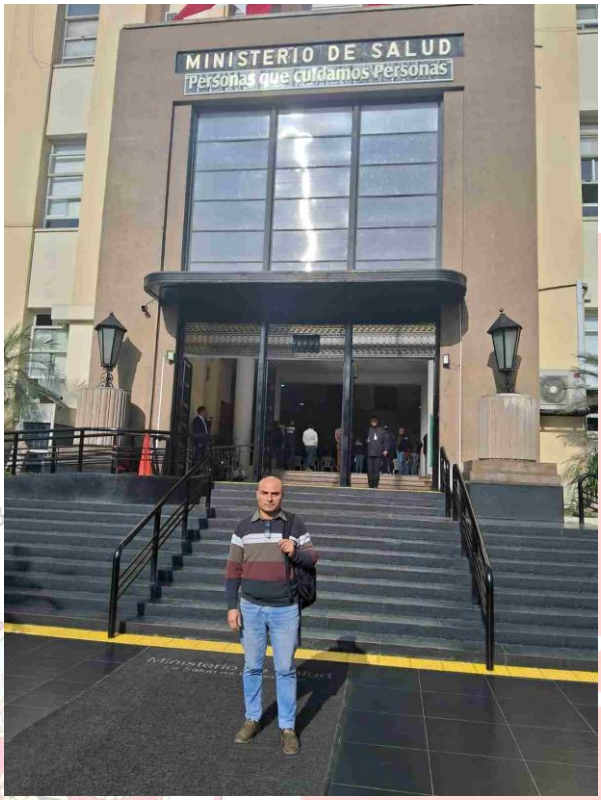
En mí (nuestra) calidad de autor (es) exclusivo (s) del trabajo de investigación/tesis titulada: **Sistema de Gestión de Seguridad de la Información de Servicios en la Nube basado en ISO/IEC-27017 para Instituciones Públicas**. presentado y aprobado en el año 2024 como requisito para optar el título de Ingeniero de Sistema de la facultad de ingeniería, arquitectura y urbanismo de la escuela profesional de ingeniería de sistemas de posgrado, programa , Programa de estudios de ingeniería de sistemas, por medio del presente escrito autorizo (autorizamos) al Vicerrectorado de investigación de la Universidad Señor de Sipán para que, en desarrollo de la presente licencia de uso total, pueda ejercer sobre mi (nuestro) trabajo y muestre al mundo la producción intelectual de la Universidad representado en este trabajo de investigación/tesis, a través de la visibilidad de su contenido de la siguiente manera:

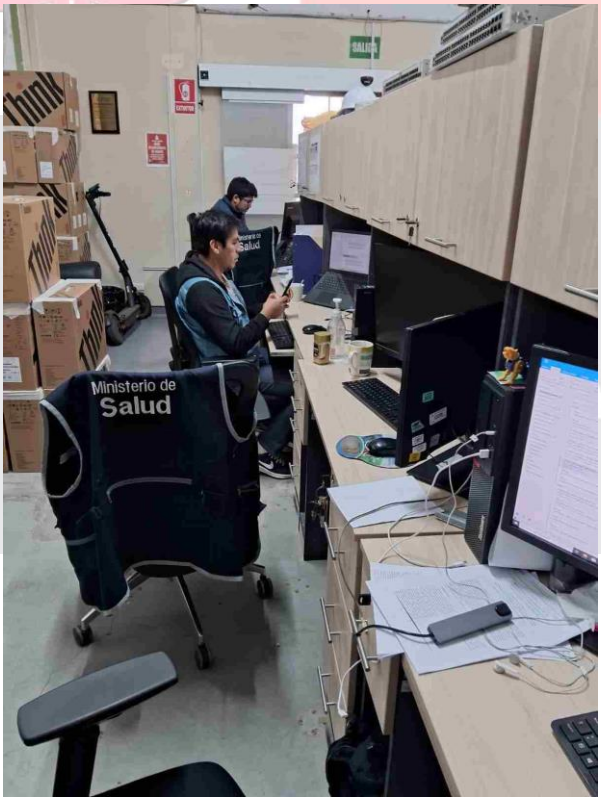
- Los usuarios pueden consultar el contenido de este trabajo de investigación a través del Repositorio Institucional en el portal web del Repositorio Institucional - https://repositorio.uss.edu.pe. así como de las redes de información del país y del exterior.
- Se permite la consulta, reproducción parcial, total o cambio de formato con fines de conservación, a losusuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, siempre y cuando mediante la correspondiente cita bibliográfica se le dé crédito al trabajo de investigación/informe o tesis y a su autor.

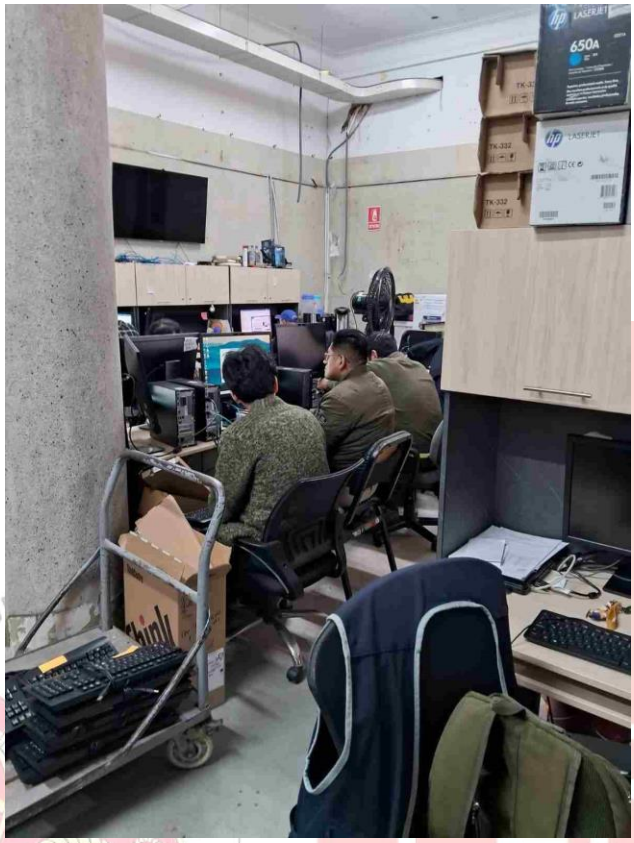
De conformidad con la ley sobre el derecho de autor decreto legislativo N° 822. En efecto, la Universidad Señor de Sipán está en la obligación de respetar los derechos de autor, para lo cual tomará las medidas correspondientes para garantizar su observancia.

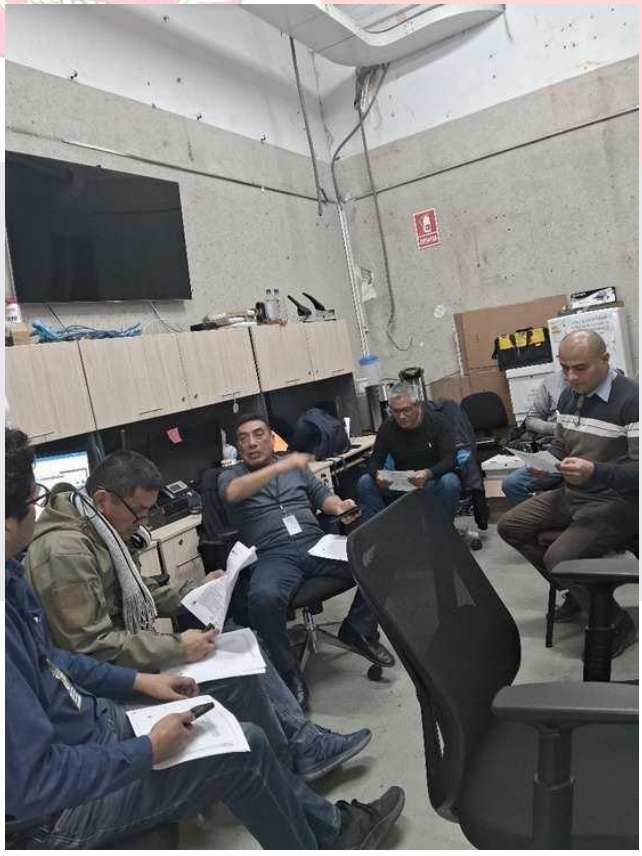
APELLIDOS Y NOMBRES	NÚMERO DE DOCUMENTO DE IDENTIDAD	FIRMA
Dayan Ray Davila Chunga	10467519	

Anexo 14. Evidencias fotográficas






650A



Anexo 15. Reporte Turnitin

Reporte de similitud

NOMBRE DEL TRABAJO

DAVILA_CHUNGA_DAYAN_RAY-TURNITIN.docx

RECUENTO DE PALABRAS	RECUENTO DE CARACTERES
42066 Words	**229394 Characters**
RECUENTO DE PÁGINAS	TAMAÑO DEL ARCHIVO
229 Pages	**10.6MB**
FECHA DE ENTREGA	FECHA DEL INFORME
Sep 10, 2024 10:30 AM GMT-5	**Sep 10, 2024 10:33 AM GMT-5**

14% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 12% Base de datos de Internet
- 4% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 7% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)

Anexo 16. Acta de originalidad

USS	ACTA DE CONTROL DE REVISIÓN DE SIMILITUD DE LA INVESTIGACIÓN	Código:	F3.PP2-PR.02
		Versión:	02
		Fecha:	18/04/2024
		Hoja:	1 de 8

Yo, **Enrique David Asenjo Carranza**, coordinador de investigación del Programa de Estudios de Ingeniería de Sistemas, he realizado el control de originalidad de la investigación, el mismo que está dentro de los porcentajes establecidos para el nivel de Pregrado, según la Directiva de similitud vigente en USS; además certifico que la versión que hace entrega es la versión final de la Tesis titulado: **Sistema de Gestión de Seguridad de la Información de Servicios en la nube basado en ISO/IEC-27017 para Instituciones Públicas**

elaborado por el (los) Bachiller(es):

Davila Chunga Dayan Ray

Se deja constancia que la investigación antes indicada tiene un índice de similitud del "14%" , verificable en el reporte final del análisis de originalidad mediante el software de similitud TURNITIN.

Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre índice de similitud de los productos académicos y de investigación vigente.

Pimentel, 23 de Setiembre del 2024

Mg. Enrique David Asenjo Carranza

Coordinador de Investigación

DNI N° 16753899