UNIVERSIDAD SAN PEDRO

VICERRECTORADO ACADÉMICO

ESCUELA DE POSGRADO

PROPUESTA DE CLOUD COMPUTING, USANDO EL ENFOQUE DE LA NORMA ISO /IEC 27001.

Tesis Para Obtener El Grado De Maestro En Ingeniería Informática Y De Sistemas Con Mención En Gestión De Tecnologías De Información Y Comunicaciones

Autor:

Solano Ruiz, Isaías José

Asesor:

ORCID:

Chimbote – Perú

2023

ÍNDICE

PALABRAS CLAVE

Tema	Tecnologías de Información y Comunicación.
Especialidad	Seguridad de la información y Comunicación.

KEYWORDS

Theme	Information and Communication Technologies
Specialty	Information Security and Communication.

LINEA DE INVESTIGACIÓN

Línea de Investigación	Tecnologías de la información y comunicación
Área	Ingeniería y Tecnología
Subárea	Ingeniería eléctrica, electrónica e informática
Disciplina	Ingeniería de sistemas y comunicaciones

USP UNIVERSIDAD SAN PEDRO | VICERRECTORADO DE INVESTIGACIÓN

CONSTANCIA DE ORIGINALIDAD

El que suscribe, Vicerrector de Investigación de la Universidad San Pedro:

HACE CONSTAR

Que, de la revisión del trabajo titulado **"PROPUESTA DE CLOUD COMPUTING EN LA UNIVERSIDAD SAN PEDRO, USANDO EL ENFOQUE DE LA NORMA ISO /IEC 27001"** del (a) estudiante: **SOLANO RUIZ ISAIAS JOSE**, identificado(a) con Código N° **2005275056**, se ha verificado un porcentaje de similitud del **9%**, el cual se encuentra dentro del parámetro establecido por la Universidad San Pedro mediante resolución de Consejo Universitario N° 5037-2019-USP/CUpara la obtención de grados y títulos académicos de pre y posgrado, así como proyectos de investigación anual Docente.

Se expide la presente constancia para los fines pertinentes.

Chimbote, 19 de diciembre de 2024

UNIVERSIDAD SAN PEDRO
VICERRECTORADO DE INVESTIGACIÓN

Dr. JAVIER MARTÍNEZ CARRIÓN
VICERRECTOR

NOTA: Este documento carece de valor si no tiene adjunta el reporte del Software TURNITIN.

TÍTULO

PROPUESTA DE CLOUD COMPUTING EN LA USP, USANDO EL ENFOQUE DE LA NORMA ISO /IEC 27001.

TITLE

PROPOSAL OF CLOUD COMPUTING AT USP, USING THE APPROACH OF THE ISO/IEC 27001 STANDARD.

RESUMEN

El objetivo de este estudio fue proponer la propuesta del modelo Cloud Computing tomando como base el enfoque de la ISO/IEC 27001, para garantizar la conectividad de la información y un manejo eficiente de las TIC evitando los riesgos en la Universidad de San Pedro Chimbote.

El método utilizado en este estudio corresponde al descriptivo, no experimental, en la recolección de datos se usó un cuestionario a una población de 30 trabajadores de diferentes áreas administrativas de la Sede Central, para identificar su satisfacción con la infraestructura y la necesidad de crear una oferta de plataforma basada en Cloud Computing.

Como resultado, el 60 por ciento de los encuestados manifestó que los procesos de seguridad y las políticas de archivos debían mejorarse para administrar el acceso de los usuarios. Concluyendo que es necesario que la plataforma debe estar basada en computación en la nube, utilizando el enfoque ISO/IEC 27001, para la conectividad y la gestión de las TIC de forma segura, el cual permita identificar y evaluar los riesgos.

ABSTRACT

The objective of this study was to propose the implementation of the Cloud Computing model based on the ISO/IEC 27001 approach, to guarantee the connectivity of information and efficient management of ICT, avoiding risks at the University of San Pedro Chimbote.

The method used in this study corresponds to the descriptive, non-experimental, in the data collection a questionnaire was used to a population of 30 workers from different administrative areas of the Headquarters, to identify their satisfaction with the infrastructure and the need to create a platform offering based on Cloud Computing.

As a result, 60 percent of respondents said security processes and file policies needed to be improved to manage user access. Concluding that it is necessary that the platform must be based on cloud computing, using the ISO/IEC 27001 approach, for the connectivity and management of ICT in a secure way, which allows risks to be identified and evaluated.

INTRODUCCIÓN

La presente investigación está fundamentada en base los antecedentes que describen a continuación:

Goyes (2020) en su "Estudio sobre el Impacto del Modelo de Computación en la Nube en la Gestión de MIS en Banca Privada" en Quito, Ecuador, con el objetivo de explorar las ventajas de este modelo y del Banco Internacional del Ecuador en la gestión de sus servicios, de enfoque exploratorio y descriptivo. Cuyo resultado fue que el 64,45% de los encuestados aceptaron este modelo como una alternativa para la gestión de las TIC, y concluyó que la disponibilidad tanto de la nube como en los lugares de trabajo superó el 99,9%, lo que se considera apta para el control y seguridad del servicio de TI.

Romero (2020) analizó el potencial de las aplicaciones y servicios de computación en la nube para procesos de control de calidad y corte térmico a través de visión artificial. Se implementó un sistema de servicios en la nube a través de Cloud platform de google y Web Server de Amazon, se integraron en una red local híbrida tanto con protocolos de Ethernet. Esta red está formada por robots KUKA- KR3- R540 y sus correspondientes controladores KR C4, conectados vía Profinet a PLC s7-1200s, que a su vez están conectados a los cabezales láser que cortan las piezas de fomix. El ordenador local, una vez configurado con las credenciales, habilita la función de capturar imágenes troceadas y enviarlas mediante el protocolo de comunicación FTP, siendo por tanto cliente de un servidor virtual de Web Services de Amazon, en el cual se realiza su control de calidad. Para realizar el proceso, se dispone de aplicaciones en un servidor web del PLC.

Guerra (2019) publicó un artículo titulado "Prototipo de Registro de Asistencia Estudiantil Móvil en el Instituto Tecnológico Nacional Utilizando Código QR y Computación en la Nube" en Quito, Ecuador para desarrollar un prototipo de asistencia estudiantil móvil en la nube, utilizo el método Kamba para el desarrollo de software, el cual se logra diseñando e implementando la capa de presentación. Su diseño se basó en arquitectura con capas, el cual separa las operaciones lógicas de

datos, negocios y los módulos que integran el sistema, y asigna funciones a las capas. Los resultados muestran que el 75% de registros de asistencia son con lectura QR y sestan sincronizados. y almacenados en la nube y se refleja en los informes que reciben los profesores y los alumnos después del registro. Asimismo, el índice de satisfacción de la interacción con la aplicación fue del 82%. Por otro lado, el 87% de los usuarios consideró que la interfaz prototipada durante el trabajo en la aplicación fue amigable. Esto se puede verificar realizando una encuesta a los usuarios que desempeñan el rol de docente y rol respectivamente.

Acosta (2019) su objetivo fue implementar una arquitectura tecnológica Cloud en la empresa Aje para optimizar los tiempos de respuesta de los procesos críticos. Se logró obtener una infraestructura técnica en la nube centralizada con mejor poder de procesamiento, alta disponibilidad, procesos de copia de seguridad eficiente y de acceso; asimismo, redujo costos de instalaciones de TI en aproximadamente un 20% y un incremento anual del 18% respecto a la infraestructura anterior ya que ahora los servicio en la nube están bajo la responsable de supervisión y gestión como parte del servicio global a cargo del proveedor. Se elimina la tarifa de operación del antiguo servicio. Así como, también se logró reducir el uso de recursos de espacio en disco y memoria, el tiempo de generación de reportes y de ejecución de los procesos de cierre contable.

Lizarraga y Pachas (2018) implementaron la arquitectura técnica basada en la nube como soporte para el portafolio de EISC" en Lima, Perú. Para comenzar a diseñar la arquitectura de nube, se analizó 9 herramientas, divididas en tres categorías: Nube Privada, Nube Pública y Cloud Manager. Esto permite elegir la herramienta óptima basada en criterios técnicos y de costes. Se verificaron 14 casos de prueba durante el proyecto, asegurando que los componentes de la arquitectura están diseñados para respaldar el logro de los objetivos del proceso de prestación de servicios de la empresa especialista en TI.

Gil y Mahihuiri (2019) realizaron “Proceso de gestión en infraestructura TI para Venus Peruana SAC, donde se realizó un estudio exhaustivo con el objetivo principal de aplicar la metodología PPDIOO para la migración de servicios básicos a la computación en la nube. La aplicación del enfoque PPDIOO es recomendable y puede adaptarse a cualquier proceso de infraestructura tecnológica en el campo técnico, y financiera permitiendo renovar repentinamente los suministros técnicos en base al plan estratégico planteado. El objetivo es transportar sus servicios que actualmente se ubican en su centro de datos, reduciendo costes, mejorando la seguridad y facilitando el acceso y la gestión. Como investigadores hemos llegado a la conclusión de que es necesario requerir servicios de procesos y/o actividades a terceros para facilitar nuestro trabajo diario como parte del ámbito tecnológico. Resaltar una sugerencia de que computación en la nube es necesario, factible y útil en determinadas situaciones, por lo tanto, al poner en producción algunos procesos que pueden promover el desarrollo de la empresa y agregar valor, es necesario implementar pilotos primero.

Domínguez (2017) su estudio se basó sobre la continuidad del servicio TIC mediante computación en la nube de acuerdo con las normas de seguridad de TI. Fue de tipo descriptiva, no experimental y transversal, como herramienta encuesta con un cuestionario aplicado a 23 empleadores, y se obtuvo que el 86,96% piensa que se puede controlar bien la información, Américas Potash Perú SA, utilizando como propuesta la computación en la nube para los servicios continuos de TIC. En cuanto a la gestión y seguridad de TI, el 91,3% de los empresarios manifestaron que es necesario plantear sugerencias para mejorar la seguridad; y en cuanto a requerimientos externos, el 100% afirmaron que los requisitos externos para las TIC, como los proveedores de servicios, establecen que deben contratar proveedores con manejo de protocolos de seguridad.

Rojas y Romero (2018) en su tesis de “Aplicación de la norma ISO 27001 para la gestión de la seguridad de la información en la empresa Plataforma Buscador Académico BUSAC. S.A.” en Quito, Ecuador, se desarrolló un manual de políticas de seguridad para una empresa de telecomunicaciones, con el fin de establecer controles que mitiguen riesgos y vulnerabilidades en la protección de la información, se empleó encuestas y entrevistas para recopilar información sobre las prácticas actuales de seguridad de la información en la empresa, así como un análisis de los riesgos existente. Asimismo, con la implementación del manual de políticas de seguridad permitió identificar y mitigar un 75% de las vulnerabilidades previamente existentes. Además, se observó un aumento del 60% en la percepción de seguridad entre los empleados tras la implementación de los controles establecidos. La investigación concluyó que la falta de controles de seguridad en la empresa de telecomunicaciones representaba un riesgo significativo para la protección de la información.

Mejía, J. (2015) analizó las ventajas y desventajas del Sistema de Gestión de la Seguridad de la Información y su influencia en la competitividad de las empresas que utilizan Cloud Computing y Big Data, en Quito, Ecuador. Donde se estudiará la factibilidad para la implementación eficiente y segura de Cloud Computing en las empresas PYMES del Ecuador, utilizando encuestas y entrevistas estructuradas para recopilar datos sobre la percepción de las empresas respecto a la seguridad y eficiencia del Cloud Computing. Donde el estudio reveló que el 75% de las empresas encuestadas consideraron que la implementación de Cloud Computing podría aumentar su eficiencia operativa. Además, un 68% expresó preocupaciones sobre la seguridad de los datos, lo que indica la necesidad de un Sistema de Gestión de Seguridad de la Información. Se encontró que las empresas que ya utilizaban herramientas de Cloud Computing reportaron un incremento del 30% en su productividad. Concluyendo que, a pesar de las preocupaciones sobre la seguridad, la implementación de Cloud Computing es viable y puede ofrecer ventajas significativas en términos de eficiencia y productividad para las PYMES en Ecuador. Se recomienda la adopción de un

Sistema de Gestión de Seguridad de la Información para mitigar los riesgos asociados y maximizar los beneficios de esta tecnología.

Galindo, Gómez y Hernández (2019) su artículo se basó en la Seguridad en la nube, evolución indispensable en el siglo XXI, de la Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, donde se trató de evaluar la seguridad en la computación en la nube, enfocándose en los modelos de servicio IaaS, PaaS y SaaS, considerando sobre 30 documentos académicos sobre seguridad en la nube, publicados en los últimos cinco años. Y empleando una Matriz de recolección de información y análisis cualitativo de literatura. Donde se pudo identificar que el 75% de los documentos revisados destacaron la vulnerabilidad de los modelos SaaS a ataques cibernéticos, con un aumento del 30% en incidentes reportados en los últimos tres años. La investigación concluye que es urgente desarrollar y perfeccionar sistemas de seguridad en la nube, especialmente en SaaS, para mitigar riesgos y proteger datos, alineándose con el objetivo de fortalecer la seguridad en la infraestructura digital.

Pérez, J. (2021) Implemento el estudio de impacto del modelo cloud computing en la gestión de servicios de información gerencial en la banca privada del Banco Internación en Quito, Ecuador, donde se evaluar la eficiencia del modelo cloud computing en la gestión de servicios de información gerencial en el sector bancario, la una población de 74 empleados del Banco Internacional de Ecuador, con una muestra final de 59 encuestados estructuradas y entrevistas a funcionarios responsables de la gestión del cambio, donde se encontró que el modelo cloud computing reduce los costos operativos en un 30% en comparación con el modelo On Premise, con un nivel de aceptación del nuevo sistema del 85% entre los usuarios. Por tal razón la adopción del modelo cloud computing mejora significativamente la eficiencia en la gestión de servicios de información, lo que respalda su implementación en el Banco Internacional de Ecuador.

Pérez, J. y López, M. (2020) Se enfoco en el "Analisis Y Diseño De Un Modelo Para Establecer Un Sistema De Gestion De La Seguridad De La Informacion Dentro De Un Ambiente Cloud Computing, Aplicando La Norma Iso 27001", en la empresa DATA-FIBER, en lima,Peru. Donde trata de evaluar la efectividad de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001 en empresas de tecnología en la nube, realizando e realizó con una muestra de 50 empresas de tecnología en la nube que implementaron la norma ISO 27001 en los últimos 3 años. Y se utilizó encuestas estructuradas y entrevistas semiestructuradas para recopilar datos sobre la implementación de la norma y su impacto en la seguridad de la información. Además, se aplicaron pruebas de auditoría de seguridad. Obteniendo el 85% de las empresas que implementaron la norma reportaron una disminución del 40% en incidentes de seguridad ($p < 0.01$).Se observó una mejora del 30% en la satisfacción del cliente respecto a la seguridad de sus datos ($p < 0.05$).Las auditorías revelaron que el 70% de las empresas cumplían con al menos el 90% de los requisitos de la norma ISO 27001. En Conclusión, se ha demostrado ser efectiva en la reducción de incidentes de seguridad y en la mejora de la satisfacción del cliente en empresas de tecnología en la nube. Estos resultados sugieren que la adopción de estándares internacionales de seguridad puede ser un factor clave para mejorar la confianza de los clientes y la integridad de los datos en entornos de cloud computing.

La presente investigación, está fundamentada en relación con las variables de estudio.

Evaluación de plataforma Cloud Computing.

En esta década, casi todas las grandes empresas del ámbito de las TIC se han embarcado en una estrategia de cloud computing. Del mismo modo, los mayores operadores de telecomunicaciones e Internet son empresas de computación en la nube. 2008-2009 vio el surgimiento de un nuevo paradigma de tecnología en la nube, y todas las tecnologías asociadas se hicieron populares poco después de convertirse en la corriente principal. Ya en 2008, dos de los principales diarios financieros del mundo, Businessweek y The Economist, predijeron el surgimiento de esta arquitectura y estudiaron en detalle el cloud computing y su impacto en las empresas. Nos enfrentamos a cambios disruptivos que enfrentan las áreas de TI. Por tanto, se debe adaptar un plan para obtener y luego difundir cierta información protegiendo así a la empresa. Además, las empresas deben aprovechar los recursos innovadores adaptándolos al mercado. Finalmente, la computación en la nube nos permite salvaguardar los datos y poder acceder a ella sin restricciones de tiempo y lugar de ubicación (Aguilar, 2010).

Arquitectura de la nube

Su arquitectura se basa en los siguientes niveles: actividades, roles, componentes y subcomponentes, que se encuentran en el nivel más alto y brindan la aplicación en función de los servicios solicitados por los clientes.

Los proveedores de servicios TIC brindan SaaS a través de aplicaciones de operaciones y mantenimiento que se encargan de brindar servicios a todos los clientes de la red sin instalar software. La aplicación es utilizada por clientes del servicio en tiempo real y maneja la distribución de uno a muchos.

Los proveedores de servicios SaaS son responsables de probar la usabilidad y la funcionalidad de los servicios ofrecidos a los clientes. Estas operaciones se

gestionan desde una oficina central que proporciona a cada cliente acceso remoto a las aplicaciones requeridas a través de Internet. Las actualizaciones también están centralizadas porque los usuarios no necesitan descargar parches. Ejemplo: un programa que nos permite gestionar el correo electrónico a través de un navegador.

Plataforma como Servicio (PaaS)

Se basa en ofrecer prestaciones de servicios sobre una plataforma y de ejecución de los ciclos de planificación, desarrollo y servicios web para dar soporte a las aplicaciones que utilizan servidores web. El proveedor de servicios debe ser responsable de garantizar que la aplicación tenga los recursos que necesita para funcionar correctamente y que se proporcione acceso. Los software requieren administradores de BD, lenguajes de programación y servidores web. PaaS aumenta la productividad y mejora los procesos físicos, lo que permite a los clientes concentrarse en las operaciones, la depuración y las pruebas mientras entregan software o aplicaciones a través de Internet. PaaS se deriva del hardware y eventualmente reemplazará a las empresas de alojamiento tradicionales.

Infraestructura como Servicio (IaaS)

Pertenece al nivel más bajo. Permite el acceso remoto a los servidores, ahorra tiempo en discos, BD, enrutadores, conmutadores, hardware y, por lo tanto, reduce los costos de la empresa en términos de infraestructura, equipos, mantenimiento y conectividad a Internet. Con esta tecnología obtienes una solución óptima y menores costos de mantenimiento, porque solo pagas por los recursos que utilizas: capacidad de almacenamiento en disco, tiempo utilizado por dispositivos como CPU, capacidad de DB disponible, transmisión de datos, etc.

Entre las plataformas utilizadas para brindar servicios, IaaS puede adaptarse a los usuarios más rápidamente debido a su flexibilidad, pero tiene mayores requisitos de disponibilidad del usuario para la instalación, configuración y mantenimiento.

Algunos proyectos incompatibles no son adecuados para ninguna PaaS, o los proyectos desarrollados de forma independiente requieren infraestructura para brindar servicios. Nos permiten mover a los proveedores en función de los factores y cómo se relacionan con la gestión de las instalaciones, lo que reduce los costos de servicio y mantenimiento. IaaS también proporciona escalado automático o semiautomático para que podamos obtener más recursos según el servicio deseado.

Marco de trabajo

El marco elegido fue la ISO/IEC 27001, el cual abarca sus objetivos en el control de los sistemas de TI, el cual evaluará los procesos de computación en la nube de la universidad privada de San Pedro para luego describir los conceptos básicos del SGSI.

SGSI

Es un estándar para ejecutar sistemas de protección a la información y consta de tres pilares: Disponibilidad, confiabilidad e integridad. También brinda protección a la información.

ISO /IEC 27001

La serie ISO 27000, esta complementada con la ISO/IEC 27001-27002, tiene los siguientes objetivos principales: crear un plan para SGSI, aplicando medidas de control relacionadas con el riesgo percibido, protocolo y procedimientos, definir responsabilidades y dividirlas en niveles apropiados, se formalizan sistemáticamente y metódicamente, monitorizada y auditada, generación y conservación de pruebas, resolución de incidencias y mejora continua del SGSI.

El SGSI se basa en la ISO 27001 y brinda protección contra las amenazas de TIC que pueden amenazar a las empresas públicas y privadas. El estándar ISO 27001

permite mitigar las incertidumbres y amenazas de diversas fuentes, así como las herramientas TIC que utilizan los ejecutivos y los gerentes de TI de las organizaciones.

Tabla 1

Objetivos de control de la Norma ISO / IEC 27001

Objetivo de Control	Controles
Política de Seguridad	Documentar política de seguridad de información.
	Revisión de la política de seguridad de la información.
	Compromiso de la gerencia con la seguridad de la información.
	Coordinación de la seguridad de información.
	Asignación de responsabilidades de la seguridad de la información.
	Proceso de autorización para los medios de procesamiento de información.
	Acuerdos de confidencialidad.
	Contacto con autoridades.
	Contacto con grupos de interés especial.
	Revisión independiente de la seguridad de la información.
	Identificación de riesgos relacionados con entidades externas.
	Tratamiento de la seguridad en contratos cuando se trabaja con clientes.
	Tratamiento de la seguridad en contratos con terceras personas.
Gestión de Activos	Inventarios de activos.
	Propiedades de los activos.
	Uso aceptable de los activos.
	Lineamientos de clasificación
	Etiquetado y manejo de la información.
Seguridad de los Recursos Humanos	Roles y responsabilidad
	Selección
	Términos y condiciones de empleo.
	Gestión de Responsabilidades
	Capacitación y educación en seguridad de la información
	Proceso disciplinario
	Responsabilidades de terminación
	Devolución de activos
	Eliminación de derechos de acceso
Seguridad Física y Ambiental	Perímetro de la seguridad de la información.
	Controles de entrada físicos.

	Seguridad de oficinas, ambientaciones y medios.
	Protección contra amenazas externas y ambientales.
	Trabajos en áreas seguras.
	Áreas de acceso público, entrega y carga.
	Ubicación y protección de equipos.
	Servicios públicos.
	Seguridad en el cableado.
	Mantenimiento de equipo.
	Seguridad del equipo fuera del local.
	Eliminación segura o rehusó del equipo.
	Traslado de propiedades.
Gestión de la Comunicación y Operaciones	Procedimientos de operación documentadas.
	Gestión de cambio.
	Segregación de deberes.
	Separación de los medios de desarrollo y operacionales.
	Entrega de servicios.
	Monitoreo y revisión de los servicios de terceros.
	Manejar los cambios en los servicios de terceros.
	Gestión de la capacidad.
	Aceptación del sistema.
	Controles sobre Software maliciosos.
	Controles contra códigos móviles.
	Backup o controles de la información.
	Control de Red.
	Seguridad de los servicios de Red.
	Gestión de los medios removibles.
	Eliminación de medios.
	Procedimientos de los manejos de información.
	Seguridad de documentación del sistema.
	Procedimientos y políticas de información y Software.
	Acuerdos de intercambios.
	Medios físicos en tránsito.
	Mensajes electrónicos.
	Sistemas de información comercial
	Comercio electrónico.
	Transacciones en línea.
	Información disponible públicamente.
	Registro de auditoria
	Uso del sistema de monitoreo.
	Protección del sistema de monitoreo.
	Protección de la información del registro.
	Registro del administrador y operador.

	Registro de fallas.
	Sincronización de relojes.
Control de Acceso	Política del control de accesos.
	Inscripción del usuario.
	Gestión de privilegios.
	Gestión de clave de usuarios.
	Revisión de los accesos de los derechos del usuario.
	Uso de clave.
	Equipamiento de usuario desatendido.
	Política de pantalla y escritorio limpio.
	Políticas sobre el uso de servicios en Red.
	Autenticación del usuario para conexiones externas.
	Identificación del equipo en Red.
	Protección del puerto de diagnóstico remoto.
	Segregación en redes.
	Control de conexiones en redes.
	Control de routing en redes.
	Procedimientos de registro en el terminal.
	Identificación y autenticación del usuario.
	Sistema de gestión de claves.
	Uso de utilidades del sistema.
	Sesión inactiva.
	Limitación de tiempo de conexión.
	Restricción al acceso a la información.
	Aislamiento del sistema sensible.
	Computación móvil y comunicación.
	Tele-trabajo.

Nota: AENOR – ISO 27001

Gestión de Seguridad

Enfoque de Implementación GSI - Gestión de la Seguridad de la Información y Grupos Empresariales Jerárquicos. Este enfoque es un enfoque global y sistemático, teniendo en cuenta que la empresa pertenece a un determinado grupo empresarial, y al mismo tiempo es pragmático, por lo que no solo es posible, sino también práctico y efectivo para brindar una estructura u organización arreglo para lograr. A convenir individualmente. Determinar los procedimientos que deben completarse en fases no

solo promueve la reutilización segura y la consistencia general, sino que también promueve la sinergia entre las empresas y las unidades operativas. Este enfoque se caracteriza por estrategias para analizar y crear un plan de riesgos, así como por un enfoque mixto de planificación, implementación y seguimiento del SGSI con gestión centralizada, pero con la necesaria autonomía en cada área y en cada nivel de empresa, principalmente en la gestión del control. y conciencia de los impactos de los riesgos locales. Esto permitirá la consolidación de estándares y la optimización de recursos cuando los riesgos deban ser gestionados de forma conjunta. Entendemos que debe prevalecer un enfoque rentable para las necesidades de riesgo y evitar perdida de los datos comerciales, y adecuar un SGSI de manera completa y efectiva, la estrategia de varios pasos y los activos principales identificados en el proceso de la Fase 1 permiten que la energía y los recursos se concentren en activos reales y procesos. en una etapa posterior, lo que aumenta la eficacia y eficiencia del enfoque. Cabe señalar que el método se basa y cumple con la norma ISO/IEC 27.001 (Mega, 2009).

Gestión de Riesgos mediante ISO / IEC 27001.

ISO 27001 establece un sistema para gestionar medidas de seguridad que protejan la información en el que la gestión de riesgos es el elemento más importante. Según Rudas (2017) respecto a la identificación de riesgo manifiesta que:

Primero, identifique posibles riesgos en contra de la empresa y, luego, desarrolle un plan de seguridad que elimine los riesgos. Así pues, podemos dividir el plan de riesgo en dos fases principales: análisis y posteriormente un tratamiento. Por lo tanto, se analiza adecuadamente y ejecuta el plan de riesgos, debe crear la manera de definir sus procedimientos de gestión de riesgos. Hay muchos métodos en el mercado hoy en día, pero todos tienen mucho en común, como verás a continuación.

Identificación activa: Podemos considerar activos tales como: computadores, unidades de almacenamiento, servidores, programas. Dichos dispositivos poseen informacion: papel impreso, así también en formato digital, por tanto, se debe

organizar la informacion en base a su importancia. Además, puede detectar activos sin data, pero se complementan con otros activos que si presenta informacion.

Un caso evidente, sistemas de ventilación no usa información, aun así, evita el sobrecalentamiento del servidor y su mal funcionamiento. Además, es primordial enmarcar las dependencias que puedan contener los activos. El sistema se procesa en el servidor, así pues, si el servidor fallará, también el sistema fallaría.

Identificación de amenazas y vulnerabilidades.

Según Ambit (2017) manifiesta que todos los activos de una organización están en riesgo y explotados popensos a ser vulnerable. Están amenazados por cualquier cuestión que puedan afectar al negocio: ingeniería, desastres naturales, caballos de Troya, virus, etc. Por otro lado, la vulnerabilidad es una situación amenazante. Sin embargo, cada activo debe analizarse y probarse para determinar si existen suficientes amenazas/vulnerabilidades para coincidir con su categoría. Casi todos los métodos de prevención de riesgos, incluyen una lista de amenazas y nos sirve para identificarla en los activos afectados.

El cálculo del nivel de riesgo varía según el método en cuestión, es así, que los métodos calculan con distintas fórmulas (puede haber razones por las que algunos métodos sean diferentes de otros). Nos basaremos en una fórmula comprensible enfocada en 2 situaciones de la gestión de riesgos: Probabilidad de suceso de la amenaza, afectación en los activos. En algunos casos, también se considera una evaluación proactiva, útil para calcular los niveles de riesgo ya que tanto la efectividad como la probabilidad se pueden medir en porcentajes (ISOTools, 2014)

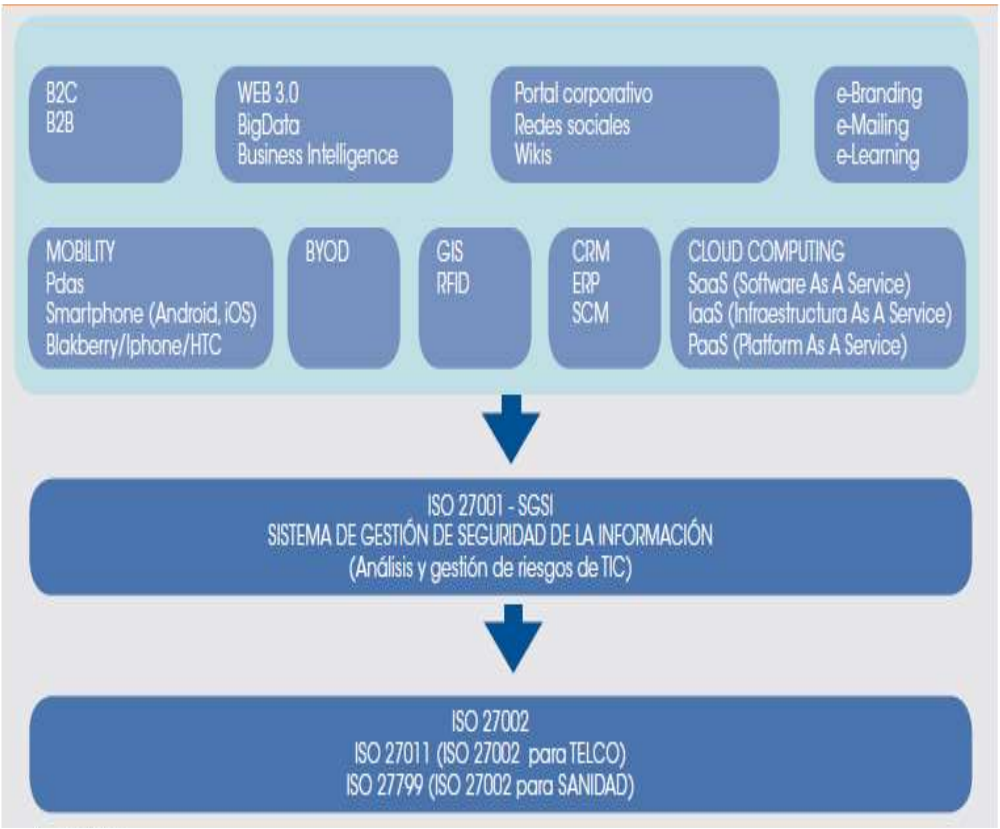
SGSI - ISO 27001

La información es esencial para la empresa y debe ser protegida de toda amenaza que afecte a las empresas. La realidad es que las organizaciones empresariales de hoy en día se exponen a múltiples riesgos de diversas fuentes (consulte la Figura 1), incluidos las herramientas TIC, CIO y CEO. Todas estas

herramientas deben funcionar juntas para garantizar los más altos niveles de seguridad, confidencialidad, disponibilidad e integridad. La información, como esencial activo de una organización, debe resguardarse, manteniendo y mejorando su seguridad para que pueda alcanzar sus metas comerciales, salvaguardar su reputación e imagen corporativa. La ISO/IEC 27001:2007 es una evaluación de riesgos lógicos y físicos. Por lo que, se desarrollan planes estratégicos y controles para evitar amenazas.

Figura 1

Herramientas TIC para CEO y CIO



Nota. Nuevos negocios y nuevas herramientas en las TIC para CEO y CIO

Garantizar que la información esté adecuadamente protegida y asegurada en todo momento, basado en el SGSI.

ISO/IEC 27001: 2007

La ISO/IEC 27001:2007 sigue una línea de procesos y mejora continua Deming consistente en Plan-Do-Check-Act, más conocido por la abreviatura en inglés PDCA (similar a la norma ISO 9001 más común y reconocida). Además, se respalda en la ISO/IEC 27002:2009, que incluye los objetivos de control y las listas de verificación necesarias para alcanzar los niveles de seguridad óptimos (ver Figura 2).

Figura 2

Sistemas de la gestión de la seguridad

Nota. SGSI ISO 270001 (Guerra, 2019)

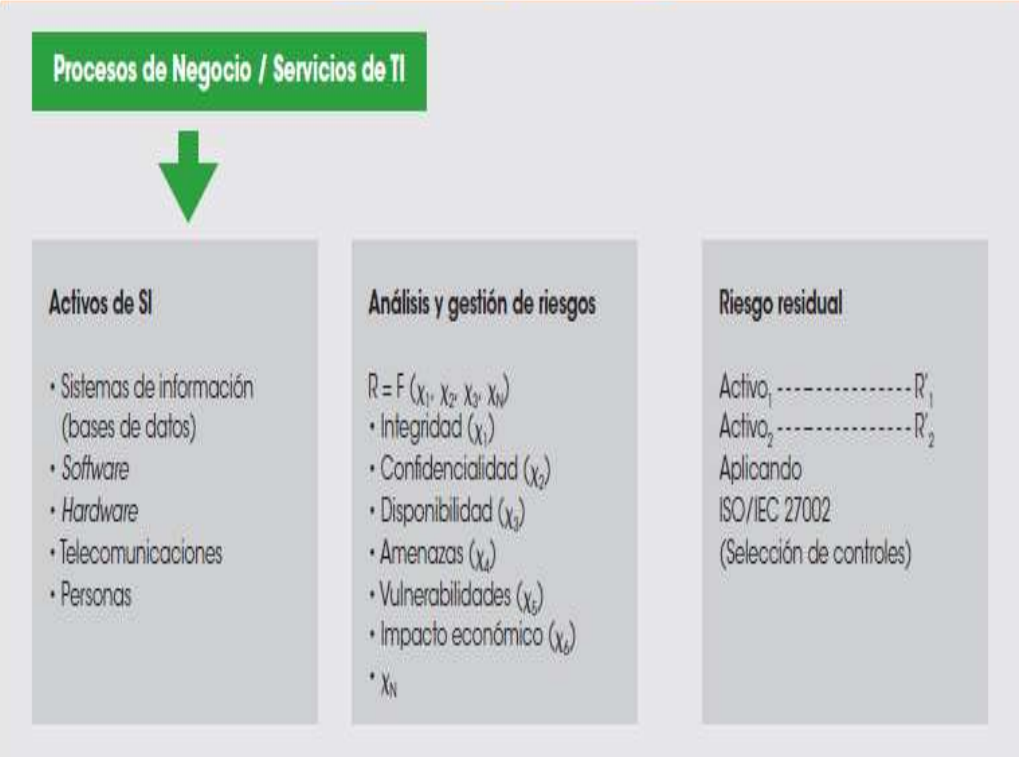
La piedra angular del sistema ISMS-ISO 27001 se basa en procesos comerciales y servicios (p. ej., ERP, CRM, inteligencia comercial, computación en la nube, redes sociales, subcontratación, traiga su propio dispositivo, etc.).

El análisis y gestión de riesgos basados en los negocio y servicios TIC, son primordiales para evaluar exhaustivamente y controlar los riesgos en activos TI de una organización. Es así que, el proceso de negocio y servicio se basa en activos de TI.

Esto requiere un análisis profundo para la gestión de los riesgos del sistema. Luego de ser evaluados los riesgos y aplicados adecuadamente los controles de acuerdo a la ISO/IEC 27002:2009 u otras normas, el resto de riesgos han sido aprobados por los directivos y estamos a una auditoría anualmente.

Figura 3

Análisis y gestión de riesgos



Nota. Modelo planteado (Guerra, 2019)

Cabe señalar que los sistemas de gestión, además de PDCA, SGSI, también cuenta con indicadores (indicador de medidas) y medidas de eficaces de control que aportan seguridad diariamente a los SI.

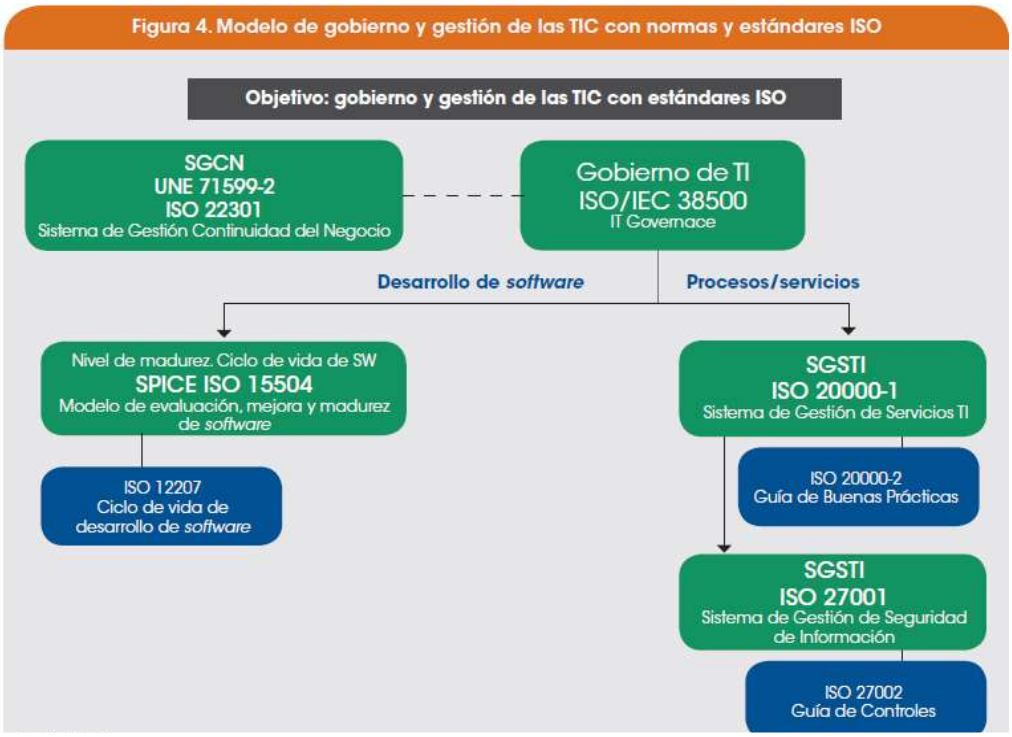
Modelo de gobierno y gestión para las TIC

La ISO 27001 está vinculada a modelos de gestión y control de las TIC planteadas por AENOR, manejando estándares reconocidos (ver Figura 4). Aplicando dicho modelo, a permitido que el centro de procesamiento de datos (CPD) y otras áreas de la institución pueden haber comenzado a comunicarse entre sí. El modelo ofrece dos niveles máximos de certificación: uno para la gestión empresarial TI (ISO 38500) y otro para los sistemas de continuidad del negocio (ISO 22301).

En primer lugar, la gestión se divide: sistemas de gestión de servicios TI y de seguridad. A través del sistema se puede procesar la calidad y seguridad, reduciendo así los riesgos.

Figura 4

Modelo de gobierno y gestión de las TICs



Nota. Modelo planteado (Guerra, 2019)

Este estudio es importante porque nos permitió evaluar la infraestructura de computación en la nube de la universidad privada de San Pedro con la ISO 27001.

Este estudio tiene una base técnica, ya que permitirá evaluar, aplicando la ISO/IEC 27001, la infraestructura técnica de computación en la nube en la universidad privada de San Pedro, que brinda comunicación y procesamiento de información en las diferentes unidades operativas. Esta investigación se justifica económicamente porque permitirá aumentar la seguridad, hacer confiables los procesos y ágiles, ahorrar tiempo y dinero en el manejo de información, que es el activo más valioso de la universidad privada de San Pedro.

La evaluación de la infraestructura técnica de computación en la nube permitirá mejorar los servicios recibidos y brindados a terceros aumentando el nivel de comunicación a través de mejores conexiones. Este trabajo de investigación puede ser aceptado por otros investigadores que estén interesados en el tema de investigación, las instituciones y nuestra institución como un documento de referencia para la comunidad universitaria, donde revelamos la relevancia de las evaluaciones de infraestructura técnica, sistemas de información de apoyo, debe evaluarse de acuerdo a la ISO/IEC 27001.

Esta investigación aportara al conocimiento, sobre el modelo Cloud Computing y evitar la vulnerabilidad a través del enfoque de ISO/IEC 27001, contribuyendo así a la mejora de conectividad y seguridad de información y gestión de las TIC en la Universidad de San Pedro Chimbote. También se justica de forma práctica debido a que se delimita su alcance y limitación del plan se seguridad de activos. Además, aporta socialmente dando a conocer un plan de seguridad activos y los riesgos o vulnerabilidades que presenta, de acuerdo a los resultados los directivos de la instrucción tomen medidas para mejorar su plan de seguridad y evitar los riesgos o vulnerabilidad que afecten drásticamente a la institución. Finalmente se justifica de forma metodológica, debido a los procedimientos y a los métodos que se aplique para implementar un plan de seguridad para Cloud Computing basándose en la norma ISO/IEC 27001.

Actualmente a nivel de todo el mundo, con el avance tecnológico las empresa e instituciones han optado por manejar sus procesos de forma digital y su información

son almacenadas en dispositivos electrónicos y en la nube. También los avances tecnológicos y las redes de comunicación también son aprovechados para realizar actos delictivos denominado como ciberdelincuencia (Tsakalidis y Vergidis, 2019). Según Kolesnikov (2024) indica que el informe del FBI en el año 2022 se registraron 800,944 ciberdelitos. En el 2024 el 90% de robo de información fueron por los ataques de phishing, quienes utilizan las identidades de empresas fiables para que los usuarios nos sospechen y brinden su información a través de las plataformas o comunicaciones digitales.

En América latina, según Riek et al. (2017) el fraude cibernético se manifiesta mediante las interrupciones del negocio, robos de datos de tipo confidencial y financiera. según Brodersen (2023) indica que el reporte de Global de Ransomware muestra que el 84% de las empresas e instituciones gubernamentales han sufrido delitos de cibernéticos durante el año 2023.

En el Perú, la ciberdelincuencia se ha incrementado, las micro empresas son las más atacadas. Según la empresa Kaspersky dedicada a la ciberseguridad, indica que el año 2023 se han registrado 9.6 millones de ataques a las empresas peruanas.

La Universidad san Pedro es una institución dedicada a la educación superior y maneja informacion clasificada, en el cual existe más alta criticidad en la data de sus estudiantes. La institución está obligada según la ley 29733. Así mismo, se requiere salvaguardar la informacion de sus estudiantes y la de sus activos porque es fundamental para realizar la matrícula de sus alumnos, asignarlos sus cursos, registrar notas, emitir constancias, grados de bachiller, título profesional, grados de maestría y doctorado. También debe velar por la informacion de sus docentes, personal, proveedores, colaboradores, recursos asignados, informacion administrativa y contable.

Actualmente, la universidad privada de San Pedro cuenta con una infraestructura tecnológica moderna que también soporta procesos de computación en la nube, pero creemos que estos procesos necesitan ser mejorados; política de

seguridad, recursos humanos, gestión de activos, física, comunicación, operativa y control de acceso. Los puntos anteriores le permitirán evaluar el proceso para mejorar la actualización y/o inversiones en tecnologías que soporten procesos de computación en la nube. Se ha observado que actualmente existen problemas con el procesamiento de la información y la conectividad, lo que genera malestar entre los usuarios de TI. El activo más valioso de la Universidad de San Pedro es su informacion, ya que de ella depende su reputación en la comunidad universitaria, y en este sentido fue evaluada utilizando la ISO/IEC 27001 permitiendo mayor confidencialidad, agilidad y flexibilidad. Muy importante. y precisión. Por otro lado, se considera necesario mejorar la comunicación en la red e Internet mediante la identificación de usuarios, permisos y roles con el fin de reducir la posibilidad de riesgos y vulnerabilidades en la red. Por lo cual se define como enunciado del problema general: ¿De qué manera la implementación del modelo Cloud Computing, bajo el enfoque de la ISO/EC 27001, mejorará el sistema de seguridad de información de la Universidad San Pedro?

Para la realización del estudio se tomaron bases teóricas para concepto y operación de las variables de estudio: Cloud Computing tomando como base la ISO/IEC 27001

Definición conceptual

> **Computación en la nube:** Este es el nombre de un tipo de distribución de servicios en Internet que proporciona estructuras y servicios a través de la nube bajo demanda de los usuarios en la web (Goyes, 2020).

Estándares ISO/IEC 27001: Son estándares estandarizados internacionalmente que fortalecen la seguridad y privacidad de la información procesada en las redes que utilizan los sistemas de la empresa. (Salir, 2020)

Definición Operacional

Cloud Computing: Denominadas nubes, funcionalmente permiten almacenar y ejecutar aplicaciones a través de una red y se componen de software y hardware que permiten el desarrollo y entrega de servicios TI a los usuarios que los solicitan (Acosta, 2019).

Estándares ISO/IEC 27001: implementados funcionalmente por todo tipo de empresas u organizaciones para proteger su información, son estándares y procedimientos utilizados como buenas prácticas que ayudan incrementar la seguridad de la información TI. (Acosta, 2019).

Tabla 2

Variable de operacionalización: Cloud Computing tomando como base el enfoque de la ISO/IEC 27001

Dimensiones	Indicadores	Ítems	Esc. de medición
Situación actual	Evaluar políticas	1	Ordinal
	Gestionar cambios	2	
	Recursos humanos	3	
	Verificar Seguridad	4	
	Evaluar gestión	5	
	Evaluar procesos	6	
Políticas de seguridad	Políticas de seguridad	1	Ordinal
	Revisión de políticas	2	
	Alta gerencia	3	
	Área de TI	4	
	Responsabilidad asignada	5	
	Confidencialidad	6	
	Módulos informáticos	7	
	Analizar data	8	
Gestión de activos	Inventarios de activos	1	Ordinal
	Responsables de TI	2	
	Activos de TI	3,4,5	
Seguridad de RR. HH.	Personal de TI	1,4,5	Ordinal
	Documentar procesos	2	
	Termino y condiciones	3	
	Procesos disciplinarios	6	
	Devolución de activos	7	
	Eliminación de acceso	8	
Seguridad física y ambiental	Equipos de procesamiento	1	Ordinal
	Control de ingreso	2	
	Ambientes seguros	3	
	Amenazas	4	

	Unidad operativa	5	
	Mantenimiento periódico	6	
	Procesos establecidos	7,8,9, 10	
Gestión de la comunicación y operaciones	Operaciones de TI	1	Ordinal
	Cambios de TI	2	
	Desarrollo y operatividad	3	
	Servicios de TI		
	Monitorear	4	
	Satisfacción de usuario	5	
	Software malicioso	6	
	Redes y conectividad	7	
	Backup	8	
	Acceso a la red	9, 10	
Control de acceso	Políticas de acceso	1	Ordinal
	Perfil de acceso	2	
	Privilegios	3	
	Clave de usuario	4	
	Mantenimiento correctivo	5	
	Acceso a la red	6	
	Autentificar usuarios	7	
	Teletrabajo	8	
		9	

Nota. Variable de operacionalización

Hipótesis general

La propuesta del modelo Cloud Computing tomando como base el enfoque de la ISO/IEC 27001, mejorará el sistema de seguridad de información de la Universidad San Pedro

Objetivo general:

Proponer la propuesta del modelo Cloud Computing tomando como base el enfoque de la ISO/IEC 27001, con el fin de mejorar el sistema de seguridad de informacion de la Universidad San Pedro

Y como objetivos específicos:

Analizar los modelos Cloud Computing tomando como base el enfoque de la ISO/IEC 27001.

Identificar los controles asociados a los riesgos identificados, empleando la ISO/IEC 27001.

Elaborar la documentación exigida por la ISO/IEC 27001.

METODOLOGÍA

Tipo de investigación

El tipo de la investigación fue descriptiva y enfoque cuantitativo, según Domínguez (2020) nos indican que es descriptiva debido a que la información o hechos son detallados de acuerdo a las circunstancias su citadas sin manipulaciones.

Diseño de investigación

De diseño no experimental y de corte transversal. Se describieron sistemáticamente las ocurrencias en una población, muestra o región de interés. No es experimental porque pretende desarrollar un plan que permita observar y evaluar los hechos. Estos estudios no deben muestrear (Domínguez, 2017).

La población muestra estuvo constituida por 30 Empleados de la Universidad San Pedro, seleccionada por conveniencia al área y relación con las TIC. La presente investigación se realizó mediante un muestreo de 30 empleados de la Universidad San Pedro, año 2017.

Tabla 2

Población de la investigación

Empleados			
Nivel	Varones	Mujeres	Total
Empleados	30	0	30
Total	30	0	30

Nota. Información recogida de la Universidad San Pedro.

Técnicas e instrumentos

Utilizamos la técnica de encuesta y un cuestionario como instrumento, el mismo que aplicamos a las unidades de análisis. La base de datos se elaboró usando el programa Excel y se construyeron las tablas distribuidas en cantidad y porcentaje respectivamente, luego se procedió a su interpretación precisando los aspectos más importantes sobre los hallazgos (Domínguez, 2017).

RESULTADOS

Se presenta los resultados en función del modelo Cloud Computing tomando como base el enfoque de la ISO/IEC 27001

Tabla 3

Evaluación de los objetivos de control.

Situación actual del Sistema de Gestión de la Seguridad de la información.	**SI**	**NO**
Evaluación de las políticas de seguridad de la información.		
Analizar la gestión de cambios.		
Revisar las funciones del recurso humano, relacionado a las TIC.		
Verificar la seguridad física y ambiental, donde se encuentran los equipos informáticos.		
Evaluar la gestión de las comunicaciones y operaciones.		
Evaluar los procesos de control de accesos.		

Nota. Objetivos de control de seguridad

Tabla 4

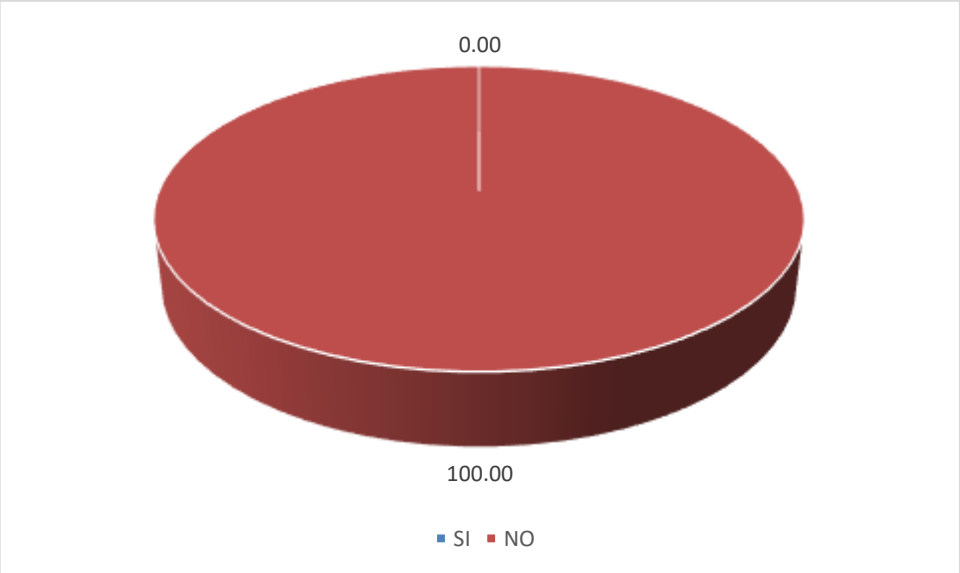
Políticas de Seguridad de Información - USP

Alternativas	n	%
SI	0	00,00
NO	30	100,00
Total	30	100,00

Nota. Datos de encuesta realizada a empleados - USP

Figura. 5

Políticas de Seguridad en la USP



El 100 % manifestaron que **N**o existen políticas de seguridad en la USP

Tabla 5

Análisis de la gestión de activos de TI.

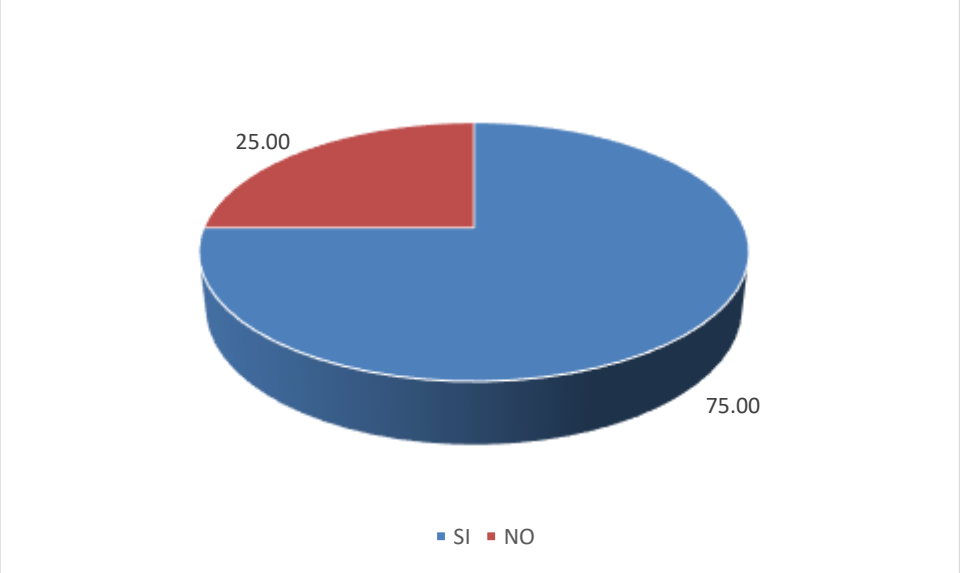
Alternativas	n	%
SI	24	75,00
NO	6	25,00
Total	30	100,00

Nota. Datos de encuesta realizada a los empleados de la UPSP

Figura 6

Análisis de la gestión de activos de TI.

.



Se observa que el 75 % indicaron que No existe una adecuada gestión de activos en la UPSP, mientras que 25% indican que Si existe.

Tabla 6

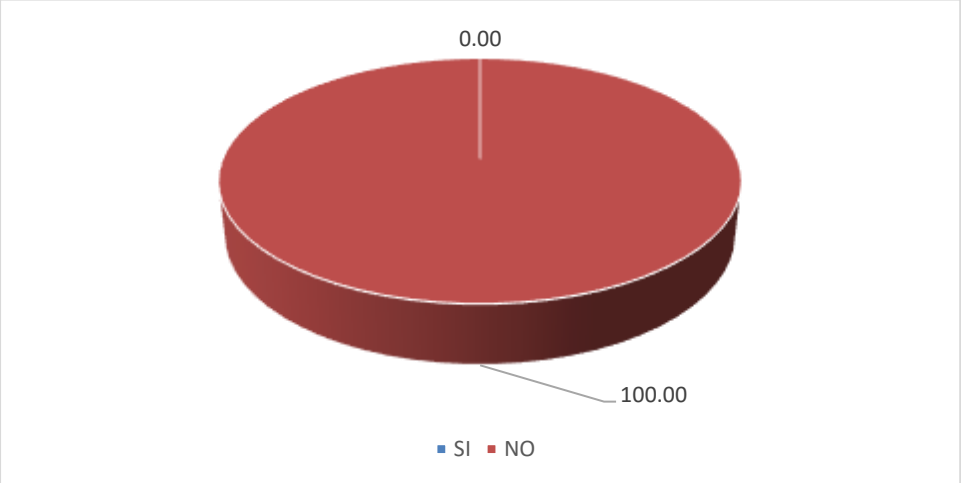
Procesos documentados de roles y responsabilidades.

Alternativas	n	%
SI	0	00,00
NO	30	100,00
Total	30	100,00

Nota. Datos de encuesta realizada a los empleados de la UPSP

Figura 7

Procesos documentados de roles y responsabilidades.



El 100% manifestaron que, No existen procesos documentados de roles y responsabilidades del personal.

Tabla. 7

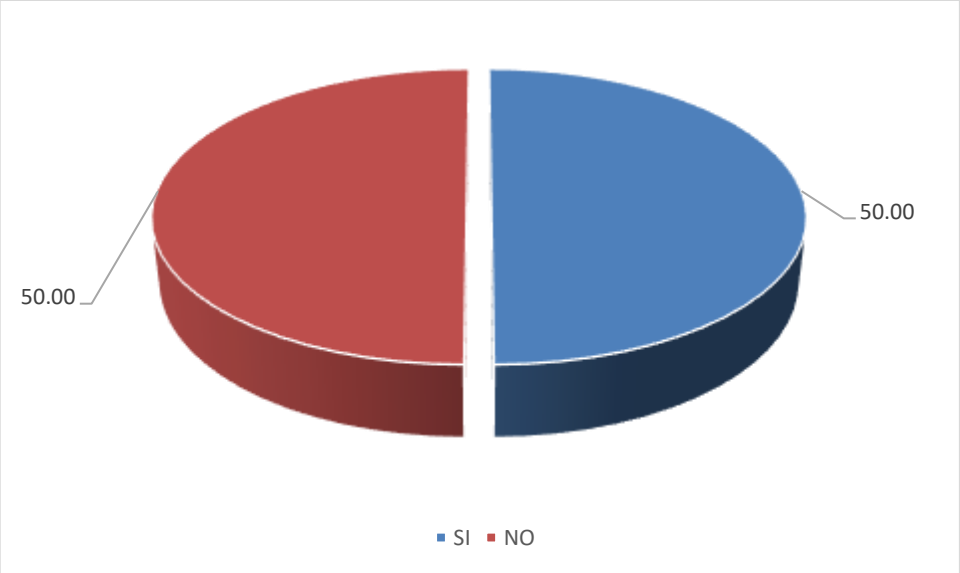
Verificación de seguridad física y ambiental

Alternativas	n	%
SI	15	50,00
NO	15	50,00
Total	30	100,00

Nota. Datos de encuesta realizada a los empleados de la UPSP

Figura 8

Análisis de la gestión de activos de TI.



El 50 % manifestaron que, No existen procesos para salvaguardar los equipos en función a los problemas medio ambientales u otro , mientras que el otro 50 % respondieron que Si.

Tabla *8*

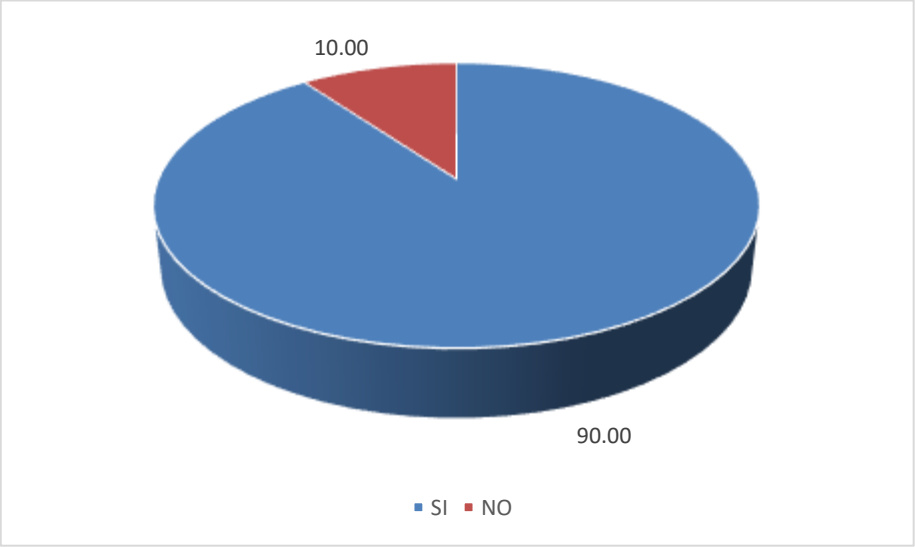
Evaluación de la Gestión y Operación.

Alternativas	n	%
SI	27	90,00
NO	3	10,00
Total	30	100,00

Nota. Datos de encuesta realizada a los empleados de la UPSP

Figura 9

Evaluación de la Gestión y Operación.



El 90% manifestaron que, no existe una adecuada evaluación de gestión y operación en la USP, mientras que, el 10 indica que Si.

Tabla 9

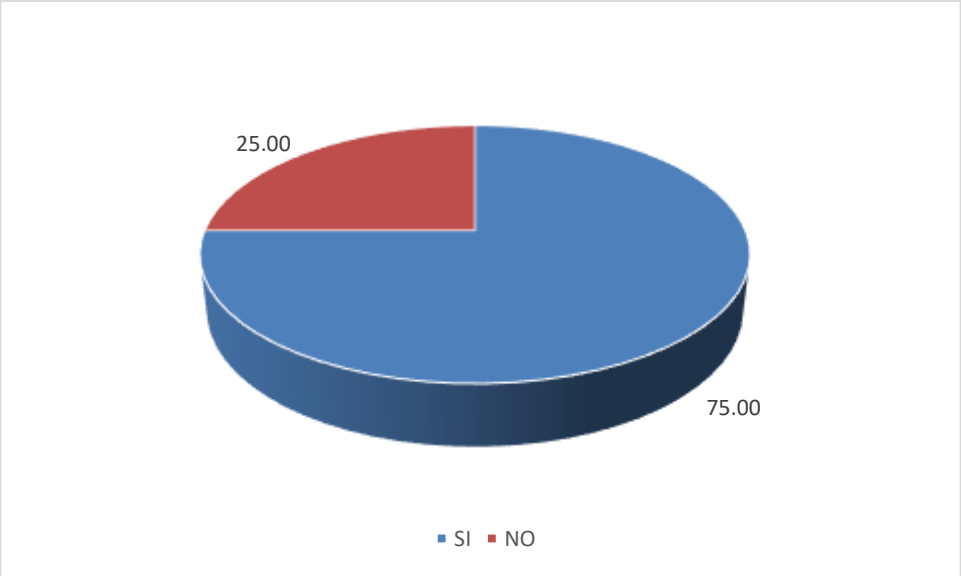
Evaluación de procesos de control de acceso.

Alternativas	n	%
SI	6	25,00
NO	24	75,00
Total	30	100,00

Nota. Datos de encuesta realizada a los empleados de la UPSP

Figura 10

Evaluación de procesos de control de acceso.



.

Se observa que el 50% indican que, Si existen en la USP un proceso de control y gestión de acceso de usuarios, y el 50% indican que No existe.

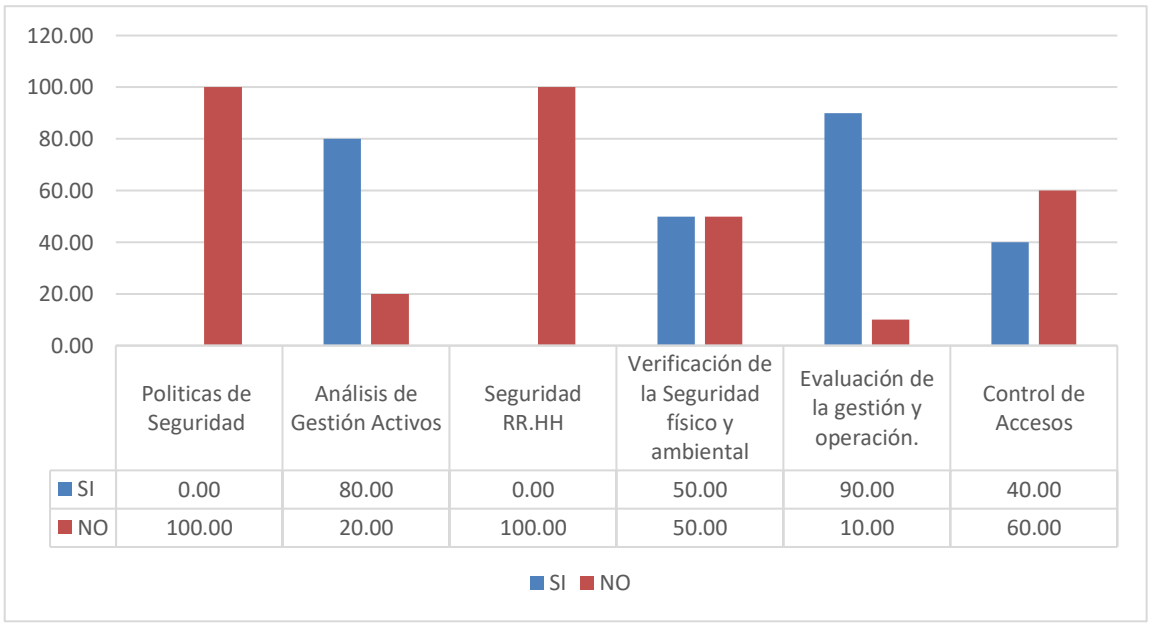
Tabla 10

Resumen de resultados de los objetivos de control

Procesos	SI	NO
Políticas de Seguridad	0 %	100%
Análisis de Gestión Activos	80 %	20 %
Seguridad RR. HH	0 %	100 %
Verificación de Seguridad físico y ambiental	50 %	50 %
Evaluar la gestión y operación.	90 %	10 %
Control de Accesos	20 %	60 %

Figura 11

Resumen de resultados de los objetivos de control



DESARROLLO DE IMPLEMENTACIÓN DEL PROYECTO UTILIZANDO LA ISO /IEC 27001.

Utilizaremos para su desarrollo el modelo: ciclo de Deming o PDCA(Planear-Hacer-Chequear-Actuar)

Etapa 1: Planear

Fase 1: Objetivos de la institución

En base a los requerimientos, misión, visión y normas de la USP, se establecieron sus objetivos para desarrollar su SGSI

Figura 12

Objetivos de la USP para desarrollar el SGSI

Nota. Objetivos establecidos para desarrollar el SGSI

Fase 2: Obtener el apoyo de las autoridades de la USP

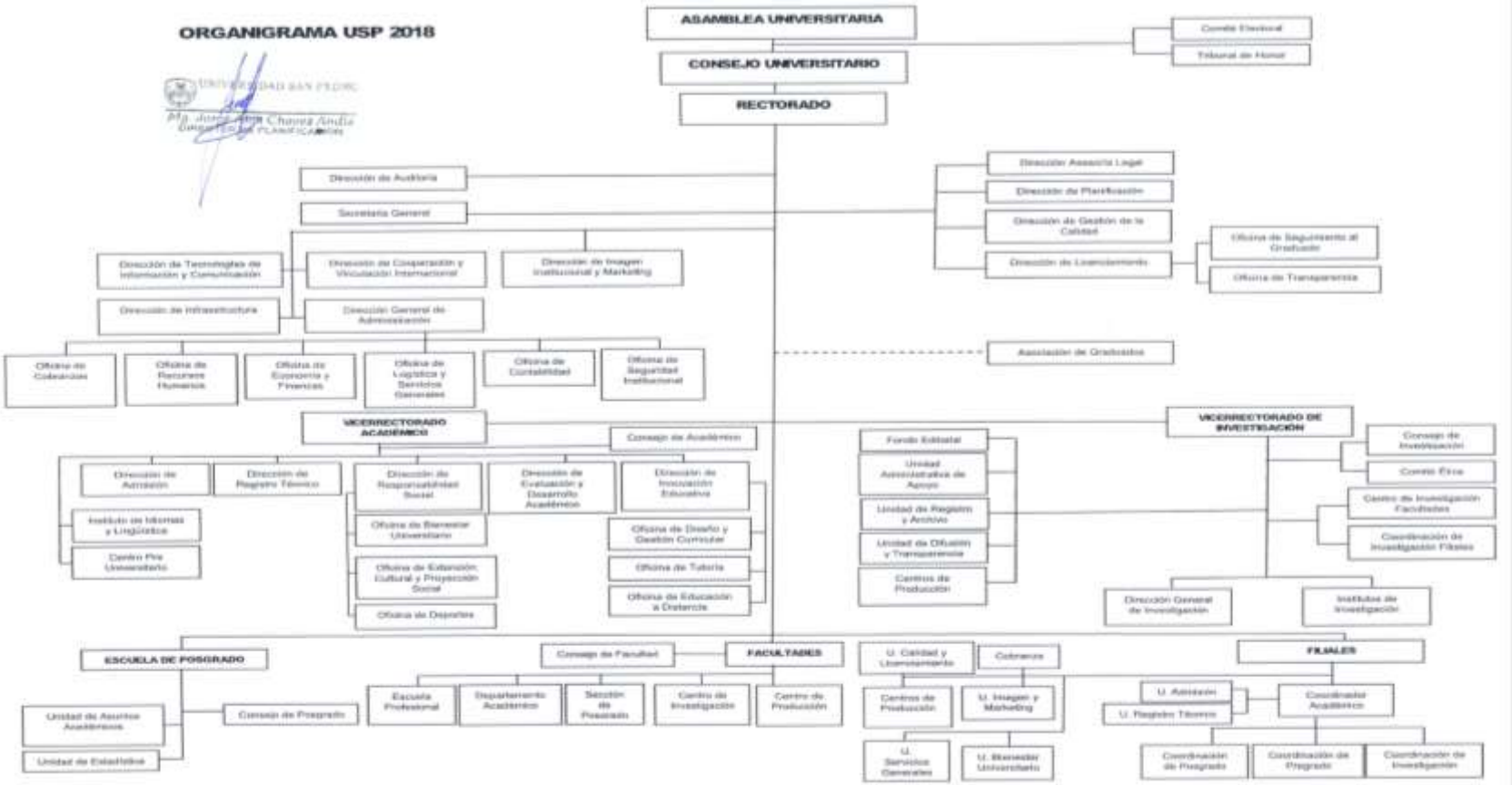
Las políticas para la seguridad y control del SGSI se establecieron conjuntamente con las autoridades de la USP, en el cual se establecieron reglas y la responsabilidad del personal encargado de cada área y sus colaboradores, que permita brindar una protección eficiente de cualquier amenaza que pueda sufrir la institución, también se establecieron sanciones a quienes incumplan las normativas de seguridad establecidas.

Fase 3: Alcance del *SGSI*

Abarcará a toda la USP, debido a que todas ellas cuentan con equipos tecnológicos, información y documentación clasificada. Se tomaron en cuenta a los procesos que presentan deficiencias en seguridad de TI. A continuación, se presenta el organigrama de la institución.

Figura 13

Organigrama de la USP.



Nota. Áreas para desarrollar el SGSI

Fase 4: Define el método de evaluación de riesgos

Se considero la ISO/IEC 27001, nos brinda la lista de riesgos de acuerdo al activo de información establecido en la institución. Se estableció una tabla para identificar las amenazas y vulnerabilidad en función al tipo de activo de información. Las amenazas son de forma: Deliberado(D), Accidental(A), Ambiental (E), se utiliza la letra A cuando es ocasionado por la persona de forma involuntaria y la letra E cuando son ocasionadas por la naturaleza.

Tabla 11

Amenazas – Norma ISO/IEC 27001-27005

Tipo	Amenaza	Origen
Daños Físicos	Incendio	A, D, E
	Chorreo de agua	A, D, E
	Accidentes	A, D, E
	Rupturas de equipos	A, D, E
	Sulfatación por polvo o humedad	A, D, E
Situaciones Naturales	Hechos climáticos	E
	Sismos	E
	Hechos volcánicos	E
	Hechos meteorológicos	E
	Huaycos	E
Falla en servicios principales	Agua, luz	A, D
	Aire acondicionado	A, D, E
	Internet	A, D
Radiación	Electromagnética	A, D, E
	Térmica	A, D, E
	Pulsaciones electromagnéticas	A, D, E
Riesgos de la información	Interceptar señales	D
	Espionaje	D
	Monitoreo no autorizado	D
	Sustraer documentos	D
	Sustraer equipos	D
	Recuperar equipos desechados	D
	Difundir información	A, D
	Datos obtenidos de fuentes no confiables	A, D
	Alteración de software	A, D
	Alteración de hardware	D
	Detectar ubicación	D
	Equipos fallados	A
	Fallas en funcionamiento de equipos	A

Fallas técnicas	Sistemas de información saturados	A, D
	Malfuncionamiento de Software	A
	Software sin mantenimientos	A, D
Acciones no autorizadas	Uso de equipos no asignados	D
	Copias de Softwares fraudulentos	D
	Softwares piratas	A, D
	Data corrupta	D
	Data procesada ilegal	D
Funcionalidad	Error de uso	A
	Uso inadecuado de accesos	A, D
	Falsificación de acceso	D
	Accesos no autorizados	D
	Personal no disponible	A, D, E

Nota. Amenazas establecidas según la ISO/IEC 27001:2705

Tabla 12

Vulnerabilidades – ISO/IEC 27001-27005

Tipo	Vulnerabilidad
Hardware	Mantenimientos esporádicos / instalaciones fallidas en medios de almacenamiento
	sustitución periódica – no asignadas
	Sensibles a la humedad, suciedad y polvo
	Sensibles a la radiación - electromagnética
	Control inadecuado de cambios
	Rupturas de equipos
	Sulfatación por polvo o humedad
	Sensible a las alteraciones de temperaturas o voltaje
	Almacenamientos vulnerables
	sin control de disposición de hardware
	sin control de copias
Software	Software sin pruebas de errores
	deficiencias de software
	Sesiones de usuario sin cerrar
	Dispositivos de almacenamiento utilizados sin borrado adecuadamente
	Prueba de auditoria inexistente
	Deficiencia en la designación de accesos
	Aplicaciones utilizadas con datos inciertos en función de tiempo
	Interfaces no amigables con el usuario
	No documentado
	Parámetros configurados de forma incorrecta

	Fechas desactualizadas
	Sin protocolos de autentificación
	Matriz - contraseñas vulnerables
	Inadecuado gestor de password
	Servicios no utilizados permitidos
	Softwares recién adquiridos
	Descripciones a medias o no precisas de los desarrolladores
	Control inadecuado de cambios
	Descargas y software utilizados sin control
	Respaldos inexistentes
	No cuenta con personal de seguridad el edificio
	Deficiencia en reportes de gestión
Red	Comunicación de mensajería sin pruebas
	Vías vulnerables de comunicación
	flujo frágil vulnerable
	Cableado inadecuado
	Punto único de error
	Emisor y receptor sin autentificación
	diseño vulnerable
	Entrega de password habilitadas
	Manejo ineficiente de red
	Conectividad publica sin autorización
Personal	Personal ausente
	Contrataciones deficientes
	No cuentan con capitaciones en seguridad
	Uso indebido de Software y Hardware
	Desconocimiento en seguridad
	Mecanismos inexistentes de monitoreo
	Personal externo no supervisado
	Sin protocolos para uso de líneas de comunicaciones.
Sitio	Acceso físico inadecuado a las instalaciones de la institución
	Ubicada en zona vulnerable a desastres
	Corriente eléctrica inestable
	Edificio, puertas y ventanas sin protección
Institución	Procesos informales en registro y eliminación de los usuarios.
	Procesos informales en control de acceso de usuarios.
	Monitoreo inexistente en medios para procesar datos
	No se ejecutan auditorias periódicas
	No hay un plan de identificación y evaluación de riesgos
	No existe reportes de errores y fallas de acceso de administradores y usuarios
	Respuestas tardías de mantenimiento de servicios

	Acuerdos informales de nivel de servicios
	Procesos informales de control de cambio
	Procesos informales de revisión de documentos del SGSI
	Planes inexistentes de continuidad de negocios
	Políticas inexistentes de uso de correos
	Procesos informales de uso de nuevos softwares
	Accesos no habilitados de administradores y usuarios
	Procedimientos informales en uso de datos reservados.
	No existe manual de funciones de seguridad de acuerdo a cada puesto de trabajo o uso de equipos tecnológicos.
	No existe un reglamento en caso de accidentes de seguridad.
	No existe reglas de uso de laptops
	No existe controles de activos fuera de la institución
	No existe políticas de mantenimientos preventivos de bienes y equipos
	No se cuenta con aprobación en manejo de información
	Mecanismos inexistentes de monitoreo
	No existe supervisión por parte del administrador de la institución
	No existe un plan de reportes de vulnerabilidades en la seguridad

Nota. Vulnerabilidades establecidas según ISO/IEC 27001:2705

Se estableció en función de amenazas y fragilidad la ISO/IEC 27001 en relación con los activos de información de la institución.

Tabla 13

Análisis de riesgos

Campo	Descripción
cod_activo	Código del activo
Amenaza	Amenaza contra el activo
Vulnerabilidad	Vulnerabilidad contra el activo

Nota. Análisis de riesgos de los activos

En la siguiente tabla se establece el riesgo y las consecuencias en base a las relaciones de amenazas y fragilidad en activos de datos, por lo cual se determinan como factores de la criticidad: la probabilidad y su impacto.

Tabla 14

Tasa de ocurrencias de riesgo

Criterios de riesgos	
Probabilidad	**Periodo de ocurrencia**
Raro	Excepciones, ocurren 1 vez cada 5 años
Improbable	3 veces cada 5 años
Posible	1 vez al año
Probable	2 o 3 veces al año
Casi probable	4 a mas veces durante un año

Nota. Criterios de ocurrencia de riesgos

También se determinaron los criterios que permitan medir el nivel de impacto si se presentaran amenazas y fragilidad en activos de datos (ver tabla), por lo cual, se debe identificar los controles previos que nos indica la norma ISO/IE 27001-27005 y se debe considerar el riesgo residual.

Tabla 15

Criterios de impacto de riesgo

Criterios de riesgos	
Probabilidad	**Periodo de ocurrencia**
Bajo	Imagen o reputación deteriorada de la institución; pérdidas económicas, sanciones aplicadas; pérdida de estudiantes; mal manejo en gerencia o autoridades.
Moderado	Agravio a gran escala a la institución, riesgo inusual; auditorias y sanciones por faltas graves; mal manejo en gerencia o autoridades, gastos elevados de operación; pérdidas económicas.
Relevante	afectación directa a la institución de nivel medio, gastos justificados de operación, sanciones por faltas leves, imagen expuesta de la institución con nivel de impacto medio.
Alto	Riesgos aceptables; reputación aceptable, observaciones por reguladores sin sanciones, gastos operacionales mínimos.
Crítico	No se afectación a directa a la institución, no afecta su imagen, no existen sanción legal ni afectación operacional o económica; no es notado por clientes y si por los aliados.

Nota. Criterios que permiten medir el nivel de impacto de riesgos

Se debe considerar la probabilidad, así como también el afecto de ocurrencias en riesgos, para obtener los niveles de criticidad que se muestran en la siguiente imagen.

Figura 14

Niveles de criticidad.

Impacto	Crítico	Medio	Alto	Alto	Crítico	Crítico
	Alto	Bajo	Medio	Alto	Alto	Crítico
	Relevante	Bajo	Medio	Medio	Alto	Alto
	Moderado	Bajo	Bajo	Medio	Medio	Medio
	Bajo	Bajo	Bajo	Bajo	Bajo	Medio
		Raro	Improbable	Posible	Probable	Casi probable
		Probabilidad				

Nota. Permiten medir el nivel de criticidad

Actualmente la USP no tiene un plan de apetito de riesgos, por lo cual solo debe exponerse a riesgos “bajos” y “medios”, porque los riesgos “altos” y “críticos” pueden generar perdidas económicos y fuga de estudiantes que afecten a gran escala la imagen institucional.

Se debe identificar los niveles de criticidad y analizar los riesgos para determinar un tratamiento adecuado y luego tomar la decisión de: aceptar el riesgo, reducirlo, evitarlo o transferirlo. En la tabla siguiente se detalla la metodología a seguir.

Tabla 16

Tratamientos de riesgo

Tratamiento de riesgos	
Tratamiento	**Descripción**
Reducción de riesgos	Se reduce el riesgo al seleccionar un adecuado control para reevaluar el riesgo residual y aceptarla.
Retención de riesgos	Se acepta el riesgo luego de evaluar su nivel de criticidad.
Evitar riesgos	No se acepta el riesgo por tener un nivel de criticidad alto.
Transferir riesgos	Se evalúa el riesgo y se transfiere a otra área donde se maneje con mayor eficacia dicho riesgo y su criticidad pueda ser controlada.

Nota. Tratamiento para reducir el nivel de riesgos

Luego de haber identificado las amenazas y vulnerabilidades, y haberse analizado los riesgos se debe generar la matriz de riesgos que se detalla a continuación.

Tabla 17

Matriz de riesgo

Matriz de riesgos	
Campo	**Descripción**
Cod_riesgo	Identifica el tipo de riesgo.
Riesgo	Describe el riesgo.
Consecuencias	Materialización luego de aceptar el riesgo
Probabilidad	Posibilidad que ocurra el riesgo
Impacto	Impacto de riesgo
Criticidad	Nivel de afectación del riesgo (probabilidad – consecuencia)
Tratamiento del riesgo	procesos para controlar el riesgo

Nota. Campos considerados en la matriz de riesgos

Fase 5: Inventariar los activos de información

Se fija los activos de información y se efectúa su valoración en los procesos y estados críticos del negocio con la ISO/IEC 27001-27005 para determinar la vía de identificación y su valoración.

Nos permite establecer los activos de datos en la operatividad de sus procesos y su nivel de criticidad, además para clasificarlos se debe considerar lo siguiente: Primario (Procesos de información o negocios) y soporte (Personal, sitio, software, hardware y redes).

Tabla 18

Identificación de activos

Identificación de activos	
Campo	**Descripción**
Cod_riesgo	Identifica el tipo de riesgo.
Proceso	Participación del activo de datos
Sub-proceso	Participación del activo de datos
Nombre	Nombre del activo
Describir	Detalles del activo
Clasificación	Primario / soporte
Sub clasificación	activo de datos
Propietario	Persona o área donde se ubica el activo de información
Ubicación	Área física o lógica donde está el activo de información

Nota. Campos de los activos.

En la tabla 19, se presentará los activos de información identificados en los procesos de operatividad de la USP.

Tabla 19

Activos de la USP (inventario)

Cod_activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación	Sub Clasificación	Propietario	Ubicación
R01	Autoridades	Responsables aprobar las normativas y establecer los planes estratégicos en la institución.	Todos	Administración y Supervisión	Primario	Recurso humano	No aplica	Laderas del Norte
R02	Docentes	Brindan los conocimientos a los estudiantes, evaluarlos y registrar sus asistencias y notas	Ingreso	Atención Ocupacional	Primario	RR.HH	No aplica	Laderas del Norte
R03	Administrativos y Tecnicos	Deben cumplir con sus funciones establecidas dentro de la Institución.	Gestión administrativa y otros	Gestión administrativa y otros	Primario y soporte	Recurso humano	No aplica	Laderas del Norte

S1	Página web/ sistemas web	Permite desarrollar los procesos educativos y administrativos de forma automatizada	Todos	Proceso de matrícula, enseñanza, administrativa y, logística	Primario	Software	Jefe de TI, docentes, alumnos y administrativos	Local principal Y sucursales
H1	Equipos de computo Y otros	Permite desarrollar las clases prácticas dictadas en la UPSP y desarrollar investigaciones.	Todos	Varios	Primario	Hardware	Jefe de TI, docentes, administrativos	Local principal Y sucursales
H2	Fotocopiadoras/ impresoras	Permite transformar documentos o información digital a físicos.	Todos	Varios	Primario	Hardware	Jefe de TI, docentes, administrativos	Local principal Y sucursales
H3	Office	Software de ofimática para producir documentos	otros	otros	Soporte	Software	Jefe de TI, docentes, alumnos y administrativos	Local principal Y sucursales
H4	Servidor de aplicaciones	Equipo para administrar TI de la institución.	Todos	Varios	Primario	Hardware	Jefe de TI	Principal Y sucursales

H5	Servidor de correos	Equipo para administrar las y gestionar los correos electrónicos	Todos	Varios	Primario	Hardware	Jefe de TI	Local principal Y sucursales
H6	Equipos de laboratorio	Permite desarrollar las clases prácticas dictadas en la UPSP y desarrollar investigaciones.	Todos	Varios	Primario	Hardware	Jefe de TI, docentes, administrativos	Local principal Y sucursales
S01	Sucursales	Local institucional en el cual se desarrollan actividades educativas, operativas y administrativas	otros	Soporte administrativa y educativa de los procesos	Soporte	Sitio	Autoridades, personal docente y administrativo	Zonas fuera de Chimbote
Se01	Internet	Permite mantenerse interconectados y compartir información entre todas las áreas de la UPSP y también con sus docentes, alumnos y proveedores	Todos	Envió y recepción de información de la UPSP	Primario	Servicio	Jefe de TI	Laderas del Norte
S04	Base de datos	Gestor de BD para su página web y demás sistemas automatizados de la UPSP	Todos	Participa en todos los procesos de gestión educativa y administrativa de la USP	Primario	Software	Jefe de TI	Servidor web

Nota. inventario de activos identificados.

Luego de la identificación de los activos de cada proceso, se tiene que valorizar de acuerdo a las dimensiones de la ISO/IEC 27001.

Tabla 20

Dimensiones del activo

Valor	Dimensiones		
	Confidencialidad	**Disponibilidad**	**Integridad**
1	Son libres, se difunde al público en general.	Tiene una tolerancia de no estar disponible es de 1 semana	Los errores o modificaciones sin autorización no afectan a la institución.
2	Activos restringidos, es solo de uso interno, no ocasiona riesgo en caso de ser filtrado.	Tiene una tolerancia de no estar disponible como máximo un día.	Los errores o modificaciones sin autorización, afectan a la institución de forma leve.
3	Activo protegido, debe controlarse su acceso. En caso de filtrarse existe un riesgo moderado para la institución	Tiene una tolerancia de no estar disponible como máximo una hora.	Los errores o modificaciones sin autorización, afectan moderadamente a la institución.
4	Activo confidencial, es información clasificada, está prohibida su difusión, en caso de filtrarse existiría un riesgo critico para la institución.	No existe tolerancia de este activo	Los errores o modificaciones sin autorización, ocasiona daños criticos a la institución.

Nota. Valores asignados a las dimensiones de los activos.

Luego de la identificar el nivel y la dimensión que le corresponde a cada activo, se calcula el promedio de valorización del activo. Para el análisis de riesgo, tratamiento y plan de controles, se consideró a los activos cuyos promedios sean 3 o mayor. Tal como se muestra en siguiente tabla

Tabla 21

Valorización de los activos

Cod_activo	Nombre	Crit. de valorización			Valor final
		Confidencialidad	Disponibilidad	Integridad	
R01	Autoridades	0	2	0	1
R02	Docentes	0	4	0	1
R03	Administrativos y Técnicos	0	3	0	1
S1	Página web/ sistemas web	4	4	4	4
H1	Equipos de computo Y otros	1	4	3	3
H2	Fotocopiadoras/ impresoras	1	2	2	2
H3	Office	1	1	2	1
H4	Servidor de aplicaciones	4	3	4	4
H5	Servidor de email	2	2	2	2
H6	Equipos de laboratorio	2	3	2	2
S01	Sucursales	0	4	0	1
Se01	Internet	4	4	4	4
S04	Base de datos	4	4	4	4

Nota. Valores asignados de acuerdo a su valoración.

Etapa 2: Hacer

Fase 6: Atender los riesgos y generar el plan de tratamiento

Para desarrollar esta fase se utilizará la metodología que se determinó en la fase 4.

Tabla 22

Valorización de los activos

Cod_activo	Nombre de activo	Vulnerabilidad	Amenaza
S1	Página web/ sistemas web	Falta de cerrar sesión de usuario	Abuso de derecho
		Deficiencias de software	Fallas al usarlo
		Deficiencias en asignar accesos	Abuso de derecho
		No documentada	Uso erróneo
		Configuración incorrecto	Uso erróneo
		Faltas de copias de seguridad	Saturación
		Falta de supervisión y monitoreo de medios de TI	Uso ilegal de datos
		No documentada ni reglamentada la gestión de usuarios	Error de uso
		No hay documentación y reglamentación para administrar información reservada.	Error de uso
H1	Equipos de computo Y otros	Mantenimientos esporádicos / instalaciones fallidas en medios de almacenamiento	Falla de equipos
		inexistente sustitución periódica	Error de uso
		Sensibles a la humedad, suciedad y polvo	Falla de equipos
		Sensibles a radiación - electromagnética	Falla de equipos
		Control inadecuado de cambios	Error de uso
		Rupturas de equipos	accidentes
		Sulfatación por polvo o humedad	Polvo o humedad
		Sensible a las alteraciones de temperaturas o voltaje	Falla eléctrica
		Almacenamientos vulnerables	Robo de informacion
		sin control de disposición de hardware	Error de uso
		sin control de copias	Error de uso

H4	Servidor de aplicaciones	Falta de mantenimiento preventivo	Falla de equipos
		Sulfatación por polvo o humedad	polvo o humedad
		Sensibilidad a la alteración del voltaje corriente	Falla eléctrica
		Deficiente control en canjeo de equipo	Error de uso
		Conexiones de cableado inadecuados	Error de uso
		Arquitectura deficiente de red	Error de uso
Se01	Internet	Falta de mantenimiento preventivo	Abuso de derecho
		Sulfatación por polvo o humedad	polvo o humedad
		Conexiones de cableado inadecuados	Error de uso
		Arquitectura deficiente de red	Error de uso
		Ancho de banda de transmisión de datos inadecuados	Error de uso
		Saturación de equipos conectados usando la red	Abuso de derecho
		Uso inadecuado del servicio de red.	Error de uso
		Abuso de privilegios	Abuso de derecho
S04	Base de datos	Falta de cerrar sesión de usuario	Abuso de derecho
		Deficiencias en asignación de accesos	Divulgación de información
		No documentada	Error de uso
		Configuración incorrecta	funcionamiento incorrecto de software
		Faltas de copias de seguridad	Data Corrupta
		No se autentifica a usuarios	Data Corrupta
		Panel de password vulnerables	Divulgación de información
		manejo inadecuado de password	Data Corrupta
		Falta de copias de respaldos	Error de uso
		Protección física inadecuada	Manipulación de software

Nota. Valores asignados de acuerdo a su valoración.

Una vez culminada el análisis, se debe desarrollar la matriz de riesgos indicando sus consecuencias, a continuación, se detalla.

Tabla 23

Matriz de riesgos

cod_riesgo	Cod_activo	Nombre de activo	Riesgo	Consecuencia	Prob.	Impacto	Criticidad	Tratamiento
R1	S1	Página web/ sistemas web	Ingreso de intrusos por sesión no cerrada.	Manipulación o robo de data.	Improbable	Critico	Alto	Reducir
R2			Acceso de usuarios sin permisos, por defectos de software.	Manipulación o robo de data.	Raro	Critico	Medio	Retener
R3			Error en manejo de data, por déficit de software.	Perdida de Data 0 alterada	Improbable	Relevante	Medio	Retener
R4			Accesos no autorizados, por error en la asignación de permisos.	Robo de información, manipulación, data corrupta.	Improbable	Critico	Alto	Reducir
R5			Manejo deficiente de los aplicativos, por no contar con manuales de usuario u otra documentación.	Data corrupta Demoras en los procesos	Probable	Relevante	Alto	Reducir

R6			Manejo inadecuado en transacciones y uso de los sistemas, por no configurar los parámetros correctos al inicio.	Data corrupta Demoras en los procesos	Raro	Relevante	Bajo	Retener
R7			Indisponibilidad permanente o parcial de los sistemas, por no contar con respaldos de seguridad.	Sistema en desuso y Perdida de información	posible	Alto	Alto	Reducir
R8			Modificaciones no autorizadas, no se puede identificar al usuario porque no existe un plan de supervisión de accesos al sistema.		posible	Relevante	Medio	Retener
R9			Acceso de extrabajadores o ex jefes de áreas – por falta de restricción de accesos.		posible	Critico	Alto	Reducir
R10			Manejo inapropiado de data confidencial en los sistemas, por falta de documentación y reglamentación del manejo de los datos.		Improbable	Alto	Medio	Retener
R11			Malfuncionamiento de equipos por no contar con mantenimientos	Indisponibilidad de equipo – fuga de data	Posible	Relevante	Medio	Retener

	H1	Equipos de computo Y otros	correctivos o preventivos.					
R12			Fallas por estar obsoletos, no existe un plan de reposición de equipos.	Indisponibilidad de equipo – fuga de data	posible	relevante	Medio	Retener
R13			Equipos dañados, por estar expuesto al polvo, sulfatación.	Indisponibilidad de equipo – fuga de data	posible	relevante	Medio	Retener
R14			Equipos dañados, por la inestabilidad de corriente.	Indisponibilidad de equipo – fuga de data	improbable	relevante	Medio	Retener
R15			Robo de información confidencial, por no contar con autentificación de contraseña.	Robo da data	probable	Alto	Alto	Reducir
R16			Robo de información confidencial, por no contar con contraseña el equipo.	Robo de data	Probable	Alto	Alto	Reducir
R17			Error en el equipo, por mala configuración.	Indisponibilidad de equipo	Improbable	relevante	Medio	Retener
R18			Robos de equipos, no se cuenta con seguridad física eficiente.	Robo de data	probable	Alto	Alto	Reducir

R19	H4	Servidor de aplicaciones	Malfuncionamiento de los servidores por no contar con mantenimientos periódicos.	Indisponibilidad del servidor	posible	relevante	Medio	retener
R20			Equipos dañados, por estar expuesto al polvo, sulfatación.	Indisponibilidad del servidor	posible	relevante	Medio	retener
R21			Equipos dañados por no contar con estabilizadores de corriente.	Servidor no disponible	raro	critico	Medio	retener
R22			Servidor con fallas, por error de configuración.	Servidor no disponible	probable	Alto	Alto	reducir
R23			Equipos dañados, por estar expuestos en zonas no seguras.	Indisponibilidad del servidor	improbable	Alto	Medio	retener
R24			Fallas en los sistemas y lentitud en la transmisión de la información, no se cuenta con sistemas de enrutamientos eficaces	Servidor no disponible	posible	relevante	Medio	retener
R25			fuga de información, por contar con una red vulnerable	Fuga de data	raro	critico	Medio	retener
R26			Indisponibilidad permanente o parcial de la BD por no	Indisponibilidad de equipo – fuga de data	posible	critico	Alto	reducir

			realizar respaldo de la data.					
R27			Sistemas lentos, conflictivos, por tener habilitados servicios innecesarios.	Data alterada – retraso en procesos	posible	relevante	Medio	retener
R28	Se01	Internet	Sistemas lentos por Falta de mantenimiento de la red	Indisponibilidad del equipo Demora en los procesos	posible	relevante	Medio	retener
R29			Fallas en la transmisión de datos por Sulfatación, polvo o humedad en el cableado o equipos de red	Indisponibilidad del equipo Demora en los procesos	improbable	moderado	Bajo	retener
R30			Fallas en la red por Conexiones de cableado inadecuados	Demora en los procesos	improbable	moderado	Bajo	retener
R31			Inseguridad por Arquitectura deficiente de red	Robo de información.	relevante	medio	Medio	relevante
R32			Sistemas lentos por contar con Ancho de banda de transmisión de datos inadecuados	Demora en los procesos	posible	relevante	Medio	retener
R33			Lentitud en los sistemas por Saturación, por contar con mus	Demora en los procesos	posible	relevante	Medio	retener

			dispositivos o equipos conectados en la red					
R34	S04	Base de datos	Denegación de acceso, por estar abierta la sesión.	fuga o Data corrupta Accesos no autorizados	improbable	alto	Medio	retener
R35			Accesos no autorizados, por error en la asignación de permisos.	robo de información. Inserción de Data corrupta Accesos no autorizados	improbable	relevante	Medio	retener
R36			Error en el manejo de la BD, por no contar con la documentación de funciones o manuales de usuario.	Data corrupta Demora en los procesos.	improbable	moderado	Bajo	retener
R37			Error en la transmisión de datos, por mala configuración en los parámetros de la BD.	fuga o Data corrupta Accesos no autorizados	improbable	moderado	Bajo	retener
R38			Accesos no autorizados de usuarios, por no contar con políticas autentificación de usuarios.	Robo de información. Inserción de Data corrupta Accesos no autorizados	improbable	critico	Alto	reducir

R39			Accesos no autorizados de usuarios, por los password ser vulnerables	fuga o Data corrupta Accesos no autorizados	improbable	alto	Medio	retener
R40			Accesos no autorizados de usuarios, por no contar con políticas de gestión de contraseñas.	fuga o Data corrupta Accesos no autorizados	improbable	alto	Medio	retener
R41			Indisponibilidad permanente o parcial de la BD por falta de backup.	Perdida de data. Indisponibilidad de la BD	improbable	critico	Alto	reducir
R42			Data corrupta por modificaciones no autorizadas.	Data manipulada	improbable	moderado	Medio	reducir

Nota. Matriz de Riesgos de los activos de información.

Luego de identificar los riesgos como altos y críticos, se debe desarrollar un plan para el tratamiento y control de los riesgos que está expuesta la institución y también establecer un plan con política de seguridad. A continuación, se detalla los controles identificados para evitar los riesgos.

Tabla 24

Controles identificados

Cod_riesgo	Riesgo	Criticidad	Cláusulas	Controles ISO/IEC 27001
R1	Acceso de usuarios no autorizados, debido que la sesión está abierta.	Alto	A.9. Control de acceso A.11.Seguridad física y ambiental	A.9.4.3. El sistema de gestión de contraseñas debe tener interfaces amigables y permitir combinaciones de números, letras y símbolos para tener contraseñas mas seguras. A.11.2.9. Aplicar políticas que limite el uso de papel y de medios removibles, también se deben adoptar políticas de pantalla limpias para optimizar las instalaciones y configuraciones de procesamiento de información.
R4	Accesos no autorizados, por error en la asignación de permisos.	Alto	A.9. Control de acceso	A.9.2.1. Se debe documentar, reglamentar e implementar el proceso de registro y baja de usuarios, para asignar privilegios de acceso. A.9.2.5. El jefe de cada área debe supervisar los derechos asignados de acceso a cada usuario.
R5	Manejo deficiente de los aplicativos, por no contar con manuales de usuario u otra documentación.	Alto	A.12.Seguridad de las operaciones	A.12.1.1. Debe documentarse los procedimientos operativos y distribuirlos a todos los usuarios de la institución.
R7	Indisponibilidad permanente o parcial de los sistemas, por no contar con respaldos de seguridad.	Alto	A.12.Seguridad de las operaciones	A.12.3.1. Debe realizarse copias de seguridad de los softwares y crear imágenes de los sistemas periódicamente y realizar pruebas siguiendo las políticas determinadas por la institución.

R9	Acceso de usuarios que ya no son parte de la institución, debido a que no se dio de baja o restricción de accesos.	Alto	A.9. Control de acceso	A.9.2.1. Se debe documentar, reglamentar e implementar el proceso de registro y baja de usuarios, para asignar privilegios de acceso. A.9.2.5. El jefe de cada área debe supervisar los derechos asignados de acceso a cada usuario.
R15	Robo de información confidencial, por no contar con autentificación de contraseña.	Alto	A.9. Control de acceso	A.9.4.3. El sistema de gestión de contraseñas debe tener interfaces amigables y permitir combinaciones de números, letras y símbolos para tener contraseñas mas seguras. A.11.2.9. Aplicar políticas que limite el uso de papel y de medios removibles, también se deben adoptar políticas de pantalla limpias para optimizar las instalaciones y configuraciones de procesamiento de información.
R16	Robo de información confidencial, por no contar con contraseña el equipo.	Alto	A.9. Control de acceso	A.9.4.3. El sistema de gestión de contraseñas debe tener interfaces amigables y permitir combinaciones de números, letras y símbolos para tener contraseñas mas seguras. A.11.2.9. Aplicar políticas que limite el uso de papel y de medios removibles, también se deben adoptar políticas de pantalla limpias para optimizar las instalaciones y configuraciones de procesamiento de información.
R18	Robos de equipos, no se cuenta con seguridad física eficiente.	Alto	A.11.Seguridad física y ambiental	A.11.2.9. Aplicar políticas que limite el uso de papel y de medios removibles, también se deben adoptar políticas de pantalla limpias para optimizar las instalaciones y configuraciones de procesamiento de información.
R22	Malfuncionamiento del servidor, debido a una mala configuración.	Alto	A.12.Seguridad de las operaciones	A.11.2.9. Aplicar políticas que limite el uso de papel y de medios removibles, también se deben adoptar políticas de pantalla limpias para optimizar las instalaciones y configuraciones de procesamiento de información.

R26	Indisponibilidad permanente o parcial de la BD por no realizar respaldo de la data.	Alto	A.12.Seguridad de las operaciones	A.12.3.1. Debe realizarse copias de seguridad de los softwares y crear imágenes de los sistemas periódicamente y realizar pruebas siguiendo las políticas determinadas por la institución.
R38	Accesos no autorizados de usuarios, por no contar con políticas autentificación de usuarios.	Alto	A.9. Control de acceso A.12.Seguridad de las operaciones	A.9.2.1. Se debe documentar, reglamentar e implementar el proceso de registro y baja de usuarios, para asignar privilegios de acceso. A.9.2.5. El jefe de cada área debe supervisar los derechos asignados de acceso a cada usuario.
R41	Indisponibilidad permanente o parcial de la BD por no contar con respaldo de seguridad.	Alto	A.12.Seguridad de las operaciones	A.12.3.1. Debe realizarse copias de seguridad de las BD y crear imágenes de los sistemas periódicamente y realizar pruebas siguiendo las políticas determinadas por la institución.

Nota. Muestra los Controles identificados para evitar los riesgos.

Fase 7: Elaborar un plan para controlar los riegos

Se identifica los riesgos y determinado los controles para evitar las amenazas, se diseña las políticas para la declaración de aplicabilidad en base a los controles de la ISO/IEC 27001.

Tabla 25

Declaración de aplicabilidad

Declaración de aplicabilidad	
Campo	**Descripción**
Sección	Cantidad de clausulas consideradas de la ISO/IEC 27001
Objetivo	Objetivos de la clausula
Control	Especificaciones del control
Aplicación	Si: Aplicable No: no aplicable
Justificación de exclusión	Se indica las razones de exclusión de control
Justificación de inclusión	Según Giraldo (2016) considera como criterios de controles a: LR (requerimientos legales), CO: obligaciones contractuales, BR/BP: Requerimientos del negocio / Mejores prácticas, RRA: Resultados de análisis de riesgo.
Adaptación a la Institución	Indicaciones para aplicar el control en la institución.

Nota. Campos establecidos de la declaración de aplicabilidad.

Luego se procede a elaborar el plan de aplicabilidad, observar tabla 26.

Tabla 26

Plan de declaración de aplicabilidad

Sec.	Objetivo	Control	Justificación de exclusión	Justificación de Inclusión				Aplicación	Adopción a la Institución
				LR	CO	BR/BP	RRA	Si/No	
5	**Políticas de seguridad de la información**								
5.1.									
5.1.1.	Políticas establecidas de seguridad de la información	Las políticas no están reglamentadas ni documentadas, se debe documentar y distribuir a todas las áreas e incluirlo en el SGSI.				X		Si	Se reglamento y documento las políticas de seguridad de la información. Control C-001
5.1.2.	Revisar las políticas de seguridad de la información.	Determinar el periodo y los procedimientos para revisar las políticas de seguridad.				X		Si	Se documento y reglamento el periodo de revisión de las políticas de seguridad. Control C-002
6	**Organizar la seguridad de la información**								
6.1.	**Organización interna**								
6.1.1.	Funciones y responsabilidades en la seguridad de la información	Establecer las Funciones y responsabilidades del personal involucrado en el SGSI.				X		Si	Se reglamento y documento las Funciones y responsabilidades del personal involucrado en el SGSI. Control C-003

6.1.2.	Separar funcionalidades	Cada área debe tener sus propias funciones y responsabilidades para evitar un manejo inadecuado de los activos de la institución.				X	X	Si	Los procesos de la institución están de acuerdo requerimientos funcionales de cada área C-004
6.1.3.	Contacto con entidades reguladoras	Las políticas de seguridad de la institución deben contener procedimientos para gestionar contacto con entidades reguladoras en seguridad informática.	La institución no tiene contacto con entidades reguladoras en seguridad informática.					No	
6.1.4.	Contacto con grupos de interés especial	La persona a cargo de la seguridad debe gestionar contactos constantes con grupos de interés, a través de foros, Chats, video conferencias con comunidades o grupos con intereses similares.	El personal operativo de la instrucción no dirige la seguridad de la información.					No	
6.1.5.	Seguridad de información en gestión de proyectos	Se debe considerar un plan de seguridad de información en todos los proyectos.	No existe riesgo crítico para la institución.					No	
6.2.	**Dispositivos móviles y trabajo remoto**								
6.2.1.	Políticas de uso de dispositivos móviles	Se debe reglamentar el uso de dispositivos móviles, el uso inadecuado puede vulnerar el acceso o riesgos de ataques a nuestra red informática.						Si	Se reglamento el uso de dispositivos móviles para evitar ataques al SGSI. Control C-005
6.2.2.	Trabajo remoto	Se debe manejar protocolos de seguridad para realizar trabajos remotos accediendo a la red informática de la institución.	La Institución no cuenta con esta modalidad de trabajo.					No	

7	**Seguridad de los recursos humanos**								
7.1.	**Antes contratar personal**								
7.1.1.	Selección	Se debe evaluar su experiencia y antecedentes para contratar al personal.	No existe riesgo crítico para la institución, mantiene su personal de años.					No	
7.1.2.	Términos y condiciones	Se debe considerar en los contratos al personal cláusulas de confidencialidad y uso responsable de los recursos tecnológicos.		X	X			Si	Se añadió cláusulas de confidencialidad a los nuevos contratos para evitar que el personal divulgue la información que maneja la institución. Control C-006
7.2.	**Personal contratado**								
7.2.1.	Responsabilidades de empleador	Debe supervisarse que el personal contratado o terceros cumplan las normativas de seguridad de información establecidas por la institución.	No existe riesgo crítico para la institución.					No	
7.2.2.	concientizar y educar en seguridad para proteger la información.	Capacitar al personal en seguridad de información.				X		Si	La institución brinda charlas para sensibilizar a su personal en seguridad de la información. Control C-007
7.2.3.	Disciplina	Debe documentarse el reglamento de sanciones para el							Se documento el reglamento de

		personal que incumpla las normas de seguridad.				X		Si	sanciones en el cual estipula las sanciones por incumplimiento o violación a las normas de seguridad. Control C-008
7.3.	**Terminación de contrato u otros**								
7.3.1.	Terminación de contrato u otros		No existe riesgo crítico para la institución, su personal tiene continuidad laboral y no hay rotación de personal.					No	
8.	**Gestión de activos**								
8.1.	**Responsabilidad de activos**								
8.1.1.	Inventario de activos	Debe existir un inventario de todos los activos que posee la institución.				X	X	Si	Se realizo el inventario de activos de información con los que cuenta la institución. Control C-009
8.1.2.	Propiedad de activos	Identificar a cargo de quien está actualmente el activo.				X	X	Si	Se actualizo el inventario para identificar la ubicación del activo de información y a cargo de quien está actualmente. Control C-010

8.1.3.	Uso adecuado	Debe documentarse el reglamento del uso adecuado de los activos de la institución.				X		Si	Se documento el reglamento del uso adecuado de los activos de información. Control C-011
8.1.4.	Devolución de activos	Se debe reglamentar la gestión de devolución de activos.				X		Si	Se documento y reglamento la gestión de devolución de activos. Control C-012
8.2.	**Clasificación de la información**								
8.2.1.	Clasificación de la información	Documentar la gestión de clasificación de la información en función a su valor.	No existe riesgo crítico para la institución.					No	
8.2.2.	Etiquetas de la información	Debe etiquetarse de acuerdo al valor del activo de información la institución.	No existe riesgo crítico para la institución.					No	
8.2.3.	Manejo de activos	Documentar un reglamento para un manejo adecuado de los activos de la institución.	Se aplicará el Control C-011					No	
8.3.	**Gestión de medios removibles**								
8.3.1.	Gestión de medios removibles.	Documentar la gestión para un uso adecuado de los medios removibles.				X	X	Si	Se Documento la gestión para un uso adecuado de los medios removibles. Control C-013
8.3.2.	Disposición de medios	Documentar la gestión para disponer de los medios removibles y realizar copias de seguridad para evitar perdida de información.	No aplica a la institución					No	

8.3.3.	Transferir medios físicos	Documentar la gestión para transferir medios físicos a otras áreas, en el cual el personal no divulgue, modifique o elimine la información contenida.		X		X	X	Si	Se Documento la gestión para transferir medios físicos en el cual el personal no está autorizado a divulgar, modificar o eliminar la información contenida en los medios físicos. Control C-014
9.	**Control de acceso**								
9.1.	**Requisitos para el control de acceso**								
9.1.1.	Políticas de control de acceso	Documentar protocolos de acceso a la información según el tipo de usuario y funciones del personal.				X		Si	Se documento los protocolos de acceso a la información. Control C-015
9.1.2.	Políticas de uso de servicio de red	Documentar protocolos de acceso a la red según sus funciones o tareas asignadas.	No existe riesgo crítico para la institución.					No	
9.2.	**Gestión de acceso de usuarios**								
9.2.1.	Registro y cancelación de acceso.	Los usuarios para tener acceso deben estar registrados y se debe dar baja a los usuarios que ya no laboraran o que han sido removido a otras áreas.		X	X	X	X	Si	Al personal cesado de la institución se le debe restringir el acceso a todos los sistemas de información. Control C-016
9.2.2.	Acceso de usuarios	Documentar la gestión de acceso o restricción de los usuarios a los sistemas de información.				X		Si	Las computadoras y los sistemas de información deben solicitar contraseñas

									para permitir sus accesos a ellos. Control C-017
9.2.3.	Acceso con privilegios	Establecer privilegios de accesos a la información.				X		Si	Se realiza supervisiones periódicas de control de acceso otorgados a los sistemas de la institución. Control C-018
9.2.4.	Gestión de información de Autentificación secreta de usuarios	Solo el personal con privilegios especiales podrá acceder a esta información.				X		Si	El personal autorizado tienes acceso a la gestión y administración de los sistemas de información. Control C-019
9.2.5.	Monitoreo de acceso de usuarios	Monitorear accesos asignados para verificar si los privilegios son los adecuados.				X	X	Si	Se aplicará el Control C-018
9.2.6.	Retiro de acceso con privilegios	Dar de baja o modificar los privilegios de accesos según las condiciones o funciones del personal.		X		X		Si	Se aplicará el Control C-016
9.3.	**Responsabilidad de usuarios**								
9.3.1.	Uso de información para la autentificación secreta.	Crear perfiles de usuario para acceder a la información clasificada de la institución.				X	X	Si	Se aplicará el Control C-018
9.4.	**Control de acceso a sistemas y aplicaciones**								
9.4.1.	Restricción de acceso a información	Restringir el acceso a las fuentes de información a los usuarios o personal no autorizado.		X	X	X	X	Si	Los activos de información clasificada en formato físico se

									deben ubicar en ambiente restringido al público y al personal no autorizado. Control C-020
9.4.2.	Acceso seguro	Se debe documentar los procedimientos que Restringir el acceso a la información a los usuarios o personal no autorizado.		X	X	X		Si	Se aplicará el Control C-017
9.4.3.	Gestión de contraseñas	Se debe documentar los procedimientos de gestión de contraseñas tales como: bloqueo luego de varios intentos fallidos, protocolos de creación o recuperación de contraseñas, validación y caducidad.				X	X	Si	Se han configurado los sistemas de información con las políticas de gestión de contraseñas determinadas por la institución. Control C-021
9.4.4.	Uso de programas utilitarios privilegiados	Restringir el uso de programas utilitarios privilegiados, para evitar la vulnerabilidad de las contraseñas.	No existe riesgo critico					No	
9.4.5.	Control de acceso a códigos fuentes de programas	Restringir el acceso a los códigos fuentes al personal no autorizado.	No aplica					No	
10	**Criptografía**								
10.1.	**Controles de criptografía**								
10.1.1.	Políticas sobre el uso de controles criptográficos	Establecer controles de criptografía para la confidencialidad, integridad y disponibilidad de la información.	Establecer controles de criptografía					No	

10.1.2.	Gestión de llaves	Establecer controles de criptografía para la confidencialidad, integridad y disponibilidad de la información.		X		X		Si	Las tablas de contraseñas o de información confidencial serán encriptadas desde la base de datos. Control C-022
11.	**Seguridad física y del entorno**								
11.1.	**Áreas seguras**								
11.1.1.	Perímetro de seguridad física	Establecer perímetros de seguridad en las zonas donde estén los activos para restringir el acceso.		X	X	X	X	Si	Se aplicará el Control C-020
11.1.2.	Controles físicos de acceso	Restringir el acceso a zonas y oficinas donde estén ubicados activos de información confidencial. Se debe mantener las puertas con llave.		X	X	X	X	Si	Las oficinas y salas de servidores están restringidas al personal no autorizado. Control C-023
11.1.3.	Seguridad de oficinas y otras zonas	Restringir el acceso del personal no autorizado, se debe señalizar y color avisos que son zonas restringidas.		X	X	X		Si	Se han señalizado las áreas restringidas. Control C-024
11.1.4.	Protección de amenazas externas y ambientales	Contar con extinguidores y alarmas contra incendios y póliza de seguros contra robos y desastres naturales.				X	X	Si	Se ha instalado alarmas contra incendios, robos y luces de emergencia. Control C-025
11.1.5.	Áreas seguras	Se deben mantener las zonas seguras donde estén ubicados los activos valiosos, para evitar que sufran vulnerabilidades o daños maliciosos.	Se aplicará el Control C-014					No	

11.1.6.	Áreas de despacho y carga	Designar zonas para despechar y cargar.	No aplica					No	
11.2.	**Equipos**								
11.2.1	Ubicación y protección de equipos	Deben ubicarse en zonas seguras y restringidas.		X	X	X		Si	Se aplicará el Control C-023
11.2.2.	suministros	Contar con suministros adecuados y respaldo de energía.	Existe procedimientos de continuidad institucional.					No	
11.2.3.	Seguridad de cableado	Mantener protegido el cableado de datos y eléctrico, para evitar daños y vulnerabilidad.	No existe riesgo critico					No	
11.2.4.	Mantenimiento de equipos	Realizar mantenimiento preventivos y correctivos periódicamente, para evitar daños de software y hardware.				X		Si	Se darán mantenimiento anualmente a los equipos y software. Control C-026
11.2.5.	Retiro de activos	Documentar procedimientos de retiro de activos de la institución.	No aplica					No	
11.2.6.	Seguridad de equipos y activos fuera de las instalaciones.	Brindar la misma seguridad que a los activos que se encuentran en la institución.	Se aplicará el Control C-023					No	
11.2.7.	Disponibilidad segura o reutilización de equipos.	Proteger la información clasificada que se encuentre en equipos en desuso o dados de baja.	No aplica					No	
11.2.8.	Equipos de usuarios desatendidos.	Documentar políticas de uso no autorizado de equipos cuando los responsables o usuarios del equipo no se encuentren.		X	X	X		Si	Se ha configurado los sistemas y equipos con bloqueo

									de sesión automática. Control C-027
11.2.9.	Políticas de escritorio limpios y pantallas limpias	Documentar políticas de uso de pantallas y escritorio sin papeles o medios de almacenamiento para evitar robos o filtración de información.		X	X	X	X	Si	No debe existir documentos de información clasificada en los escritorios Control C-028
12.	**Seguridad de las operaciones**								
12.1.	**Procedimientos operacionales y responsabilidades**								
12.1.1.	Procesos de operación documentados	Se debe documentar los procedimientos, crear manuales de operaciones y distribuirlos a todo el personal.				X	X	Si	Los procedimientos y políticas de la institución se encuentran disponibles para todos los que forman parte de ella. Control C-029
12.1.2.	Gestión de cambios	Documentar las políticas para la gestión de cambios por personal autorizado, se debe registrar para llevar un control adecuado.	No existe riesgo critico					No	
12.1.3.	Gestión de capacidad	Realizar monitoreos de los recursos y equipos para evitar demoras o fallas en los procesos.	No existe riesgo critico					No	

12.1.4.	Separación de los ambientes de desarrollo, pruebas y operación.	Los ambientes deben funcionar aislados y el acceso al personal no autorizado debe restringirse, para evitar manipulaciones sin autorizaciones.	No aplica					No	
12.2.	**Protección contra códigos maliciosos**								
12.2.1.	Controles contra códigos maliciosos.	Se debe instalar en los equipos antivirus o cortafuegos para evitar la vulnerabilidad y se mantener actualizados.				X		Si	Se realizar supervisiones para verificar que todos equipos y servidores tengan instalados antivirus actualizados. Control C-030
12.3.	**Copias de respaldo**								
12.3.1.	Respaldo de información	Realizar copias de la información y realizar las pruebas para verificar que se ha seguido con los procesos establecidos para el respaldo de la informacion.				X	X	Si	Realizar mensualmente copias de respaldo, revisarlas y luego guárdalas en sitios aislados del centro de TI y operaciones. Control C-031
12.4.	**Registro y seguimiento**								
12.4.1.	Registro de eventos	Controlar los eventos para determinar procedimientos para evitar o reparar daños.	No existe riesgo critico					No	
12.4.2.	Protección de la información de registro	Proteger la informacion de gestión de registros, restringiendo el acceso a personal no autorizado.	No existe riesgo critico					No	

12.4.3.	Registro del administrador y operador	Registrar todos los accesos y procesos del administrador y operador de TI.	No existe riesgo critico					No	
12.4.4.	Sincronización de relojes	Sincronizar los relojes de todos los dispositivos o equipos del procesamiento de la informacion.	No existe riesgo critico					No	
12.5.	**Control de software operacional**								
12.5.1.	Instalación de software en los sistemas operativos	Controlar y registrar las instalaciones y configuraciones de software. Solo debe realizarlo el personal autorizado.	No existe riesgo critico					No	
12.6.	**Gestión de vulnerabilidad técnica**								
12.6.1.	gestión de vulnerabilidad técnica	Determinar procedimientos para minimizar riesgos de vulnerabilidad de los activos de TI	El error en las aplicaciones de la institución son mínimas, se ha restringido el acceso al personal no autorizado.				X	No	
12.6.2.	Restricción de instalación de software	Controlar y registrar las instalaciones y configuraciones de software. Solo debe realizarlo el personal autorizado.	No existe riesgo critico					No	
12.7.	**Consideraciones sobre auditorias de sistemas de informacion**								
12.7.1.	Controles de auditorías de sistemas	Determinar perecimientos para el uso eficiente de herramientas de autoría de sistemas.	No existe riesgo critico					No	

13.	**Seguridad de las comunicaciones**								
13.1.	**Gestión de seguridad de redes**								
13.1.1.	Controles de redes	Instalar software para controlar el acceso a la red y solicitar autentificación de usuario.				X	X	Si	Solicitar autentificación de usuario para acceder a los activos de software. Control C-032
13.1.2.	Seguridad de los servicios de red	Determinar controles de acceso, monitorear para detectar intrusos.	No existe riesgo critico					No	
13.1.3.	Separación en las redes	Separara las redes de la intranet e implementar un DMZ.	No existe riesgo critico					No	
13.2.	**Transferencia de informacion**								
13.2.1.	Políticas y procedimientos de transferencia de informacion	Establecer políticas adecuadas para evitar robos en la transmisión de la informacion, manteniendo su confidencialidad e integridad	No aplica					No	
13.2.2.	Acuerdos sobre transferencias de informacion	Determinar controles para respetar acuerdos de intercambio o transferencia de la informacion	No aplica					No	
13.2.3.	Mensajería electrónica		No existe riesgo critico					No	
13.2.4.	Acuerdos de confidencialidad o de no divulgación	Cumplir las políticas según los acuerdos de confidencialidad o de no divulgación	Se aplicará el Control 7.1.2.					No	

14.	**Adquisición, desarrollo y mantenimiento de sistemas**								
14.1.									
14.1.1.	Análisis y especialización de requisitos de seguridad de la información	Tener en cuenta la especialización de requisitos al realizar un cambio o implementar un nuevo sistema de informacion	No aplica					No	
14.1.2.	Seguridad de servicios de las aplicaciones en redes publicas	Implementar procesos de seguridad en los servicios que se transfieren por la red pública, como cookies, autentificaciones	No aplica					No	
14.1.3.	Protección de transacciones de los servicios de las aplicaciones	Implementar procesos de seguridad en los servicios que se transfieren por la red pública, como cookies, autentificaciones	No aplica					No	
14.2.	**seguridad en procesos de desarrollo y soporte**								
14.2.1.	Políticas de desarrollo seguro	Determinar políticas de código seguro para en el desarrollo de software y evitar la vulneración de los sistemas	No aplica					No	
14.2.2.	Procedimientos de control de cambios de sistemas	Documentar los cambios de los programas y registrarlos utilizando procedimientos seguros.	No aplica					No	
14.2.3.	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Realizar pruebas a las aplicaciones, para evitar alteraciones o mal funcionamiento.	No aplica					No	

14.2.4.	Restricción en los cambios a los paquetes de software	Los cambios o modificaciones que se realizan a las aplicaciones deben estar restringidos para evitar fallas no deseadas.	No aplica					No	
14.2.5.	Principios de construcción de sistemas seguros	Determinar políticas seguras para las construcciones de las aplicaciones	No aplica					No	
14.2.6.	Ambiente de desarrollo seguro	Aislar los ambientes de desarrollo y aplicar las medidas de seguridad para el control de acceso e instalación	No aplica					No	
14.2.7.	Desarrollo contratado externamente	Realizar seguimiento a los sistemas y validarlos antes de ponerlo en marcha	No aplica					No	
14.2.8.	Pruebas de seguridad de sistemas	Probar los sistemas para identificar la vulnerabilidad	No aplica					No	
14.2.9.	Pruebas de aceptación de sistemas	Probar los sistemas para identificar la vulnerabilidad	No aplica					No	
14.3.	**Prueba de datos**								
14.3.1.	Protección de datos de pruebas	Ingresar datos validos para realizar pruebas de las aplicaciones	No aplica					No	
15.	**Relación con proveedores**								
15.1.	**Seguridad de la informacion en las relaciones con los proveedores**								
15.1.1.	Políticas de seguridad de la informacion para las relaciones con proveedores	Determinar acuerdos de confidencialidad, intercambio de información, control de acceso de informacion y seguridad física	No existe riesgo critico					No	
15.1.2.	Tratamiento de la seguridad dentro de los	Determinar acuerdos de confidencialidad	No existe riesgo critico					No	

	acuerdos con proveedores								
15.1.3.	Cadena de suministro de tecnología de informacion y comunicación	Determinar acuerdos para minimizar riesgos de seguridad de la cadena de suministros	No existe riesgo critico					No	
15.2.	**Gestión de la prestación de servicios con los proveedores**								
15.2.1.	Seguimiento y revisión de los servicios de los proveedores	Revisar, monitorear y auditar las entregas de proveedores	No existe riesgo critico					No	
15.2.2.	Gestión de cambio en los servicios de proveedores	Contar con alternativas de proveedores para la continuidad del servicio en caso de cambio de proveedor	No existe riesgo critico					No	
16.	**Gestión de incidentes de seguridad de la informacion**								
16.1.	**Gestión de incidentes y mejoras en la seguridad de la información**								
16.1.1.	Responsabilidad y procedimientos	Determinar procedimientos de emergencias para solucionar problemas a causa de la seguridad de la informacion				X		Si	Se documento las políticas de gestión de incidentes y su plan de respuesta. Control C-033
16.1.2.	Reportes de eventos de seguridad de la información	Informar los eventos ocasionados por seguridad de la informacion para documentar y registrar la solución				X		Si	Solicitar autentificación de usuario para acceder a los activos de software. Control C-034
16.1.3.	Reporte de debilidades de seguridad de la información	Informar de forma inmediata de eventos para identificar las ocurrencias y vulnerabilidades en la seguridad de la informacion				X		Si	Se aplicará el Control C-034

16.1.4.	Evaluación de eventos de seguridad de la información y decisiones sobre ello	Evaluar los eventos para identificar si es un incidente o no	Considerar a todos los eventos					No	
16.1.5.	Respuestas a incidentes de seguridad de la información	Determinar procesos a seguir ante un incidente				X		Si	Se documento las políticas de gestión de incidentes y su plan de respuesta Control C-035
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	La experiencia en resolver incidentes, es primordial para controlar y minimizar los impactos en la seguridad de la informacion	No existe riesgo critico					No	
16.1.7.	Recolección de evidencias	Determinar procedimientos para documentar incidentes para registrarlas como evidencias				X		Si	Se registrara en un Excel los incidentes que se presenten en la institucion. Control C-036
17.	**Aspectos de seguridad de la informacion de la gestión de continuidad de negocio**								
17.1.	**Continuidad de seguridad de la información**								
17.1.1.	Plan de la continuidad de la seguridad de la información	Determinar políticas para la gestión de continuidad así exista crisis en la institución				X		Si	Se aplicará el Control C-033
17.1.2.	Implementar la continuidad de la seguridad de la información	Implementar procedimientos para la continuidad ante situaciones que generen retrasos				X		Si	Se documento las políticas de gestión de incidentes y su plan para la continuidad de su operatividad del negocio Control C-037

17.1.3.	Verificación, revisión y evaluación de continuidad de la seguridad de la información	Revisar los procedimientos de gestión de continuidad para verificar si son eficientes o no	No existe riesgo critico					No	
17.2.	**Redundancia**								
17.2.1.	Disponibilidad de instalaciones de procesamiento de informacion	Determinar redundancias en las instalaciones de procesamiento d información para evitar la disponibilidad de la informaciónón				X		Si	Se implemento el documento de gestión de copias de respaldo y se cuenta con instalaciones alternas para continuar con las operaciones. Control C-038
18.	**Cumplimiento**								
18.1.	**Cumplimiento de requisitos legales y contractuales**								
18.1.1.	Identificar la legislación aplicable y de los requisitos contractuales	Determinar el marco legal para la seguridad de la informacion		X	X			Si	Se implementó el documento de Política de Seguridad de la Información, en esta política se especifica las leyes que son consideradas: - Ley 29733 - 2011 - Ley de Protección de Datos Personales, Artículo 16.- Seguridad del tratamiento de datos personales. Y Artículo 17.-

									Confidencialidad de Datos Personales. Control C039
18.1.2.	Derechos de propiedad intelectual	Cumplir con las políticas de derecho de propiedad intelectual	No existe riesgo critico					No	
18.1.3.	Protección de registros	Procedimiento de custodia de registros ante robo, modificación, divulgación.		X	X	X		Si	Se determino controles preventivos para la seguridad de los registros: Controles: C015, C016, C021, C022, C027 y C032.
18.1.4.	Privacidad y protección de datos personales	Respetar las políticas de protección de datos personales		X	X	X	X	Si	Se determino controles preventivos para la seguridad de los registros: Controles: C015, C016, C021, C022, C027 y C032.
18.1.5.	Reglamentación de controles criptográficos	Respetar las normas de controles criptográficos	No aplica					No	
18.2.	**Revisiones de seguridad de la información**								
18.2.1.	Revisión independiente de la seguridad de la informacion	Revisar periódicamente el SGSI, estas deben ser adicionales a las determinadas en las políticas de seguridad de la información.	No existe riesgo critico					No	
18.2.2.	Cumplimiento con las políticas y normas de seguridad	Revisar los cumplimientos de las políticas de seguridad de la información establecidas de acuerdo a su	No existe riesgo critico					No	

		área de responsabilidad.							
18.2.3.	Revisión del cumplimiento técnico	Revisar que todo el personal conozca y cumpla con las políticas de seguridad de la información						Si	Realizar revisiones anuales al sistema de gestión de seguridad de la información. Control C040

Nota. Campos del plan de la declaración de aplicabilidad.

Se identificaron las políticas que deberán ser implementadas, las cuales están basadas en función de la política general de seguridad de la informacion, están son:

- ✓ Polt. de gestión de contraseñas
- ✓ Polt. de gestión de accesos
- ✓ Polt. de escritorios limpios
- ✓ Polt. de gestión de copias de respaldo
- ✓ Polt. de gestión de activos
- ✓ Polt. de gestión de incidentes de seguridad

ANALISIS Y DISCUSION

El análisis de los resultados reveló que la USP no tenía políticas de seguridad de datos y que sus sistemas informáticos eran vulnerables. Este resultado es similar al obtenido por Cabrera (2013) En su documento "Estudios sobre la implementación del servicio del centro de datos basado en el modelo de computación en la nube" no hay herramientas ni estándares de seguridad obsoletos, eligieron el costo de implementación de seguridad deseado después de investigar y contratar a una empresa de tecnología profesional. Las empresas e infraestructuras prestan servicios de seguridad en sus sistemas de información. Según Padilla, J. & Pinzón, J. indicó que la norma sería administrada por un grupo de trabajo responsable de computación en la nube y un grupo de gestión de SI responsable de la seguridad en la nube de los SI de la agencia.

Los resultados también mostraron que no había un proceso documentado para las funciones y responsabilidades del personal de TI, resultados similares a los de Jasso. N insiste en su artículo "Computación en la nube: seguridad en la gestión de la información" en que no existe un proceso documentado y el rol del personal de TI, pero que la definición de los mecanismos de seguridad debe considerarse un esfuerzo conjunto, donde las responsabilidades y los roles deben dividirse entre los proveedores de servicios y los clientes. Esto es según los autores Narbona y Jiménez . Desde la creación de la institución se debe crear un conjunto de roles y responsabilidad que no deben cambiar drásticamente para no afectar a la unidad.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

De acuerdo a los resultados, ser observa la existencia de un nivel alto de insatisfacción en función al sistema actual de Gestión de Seguridad de información por lo cual se concluye Proponer la implementación del modelo Cloud Computing tomando como base el enfoque de la ISO/IEC 27001.

De los objetivos específicos se concluye:

- ✓ Se analizó los modelos Cloud Computing tomando como base el enfoque de la ISO/IEC 27001 y se precisó el modelo adecuado para su implementación

- ✓ Se identificó los controles asociados a los riesgos, mediante la ISO/IEC 27001. De acuerdo a las amenazas identificadas que afectan a la institución se debe reglamentar roles y responsabilidades para fortalecer las políticas de seguridad en el manejo de las TIC y se debe manejar y monitorear un gestor de riesgos.

- ✓ Se elaboró la documentación exigida por la ISO/IEC 27001, estableciendo políticas de seguridad para el manejo de las TIC siguiendo las directivas para una administración optima, con seguridad y minimizando la vulnerabilidad e incidentes de riesgo en el manejo información.

RECOMENDACIONES

- ✓ Rediseñar las políticas de seguridad en los documentos normativos.
- ✓ Establecer una mesa de trabajo para mejorar la gestión de activos de TI.
- ✓ Documentar las responsabilidades y roles del personal de TI y usuarios con acceso a las TIC.
- ✓ Mejorar la seguridad física y ambiental que albergan las TI.
- ✓ Implementar procesos para mejorar la gestión y operación de las TI.
- ✓ Documentar las políticas para gestionar los accesos de los usuarios.
- ✓ Se recomienda implementar el modelo Cloud Computing con la ISO/IEC 27001.

REFERENCIAS BIBLIOGRÁFICAS

Acosta, R. (2019). *Implementación de una arquitectura tecnológica para servicios de TI de la empresa grupo AJE.* Obtenido de https://repositorio.usil.edu.pe/handle/usil/8845

Aguilar, L. J. (2010). COMPUTACIÓN EN LA NUBE Notas para una estrategia española en cloud computing. *Escuela de Ingeniería y Arquitectura, I Edicción*(89), 24.

Ambit. (2017). *Tipos de Vulnerabilidades y Amenazas informáticas*. Obtenido de https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Baranovic, L. (2010). *Informática en la Nube: Confidencialidad y Disponibilidad de los Datos.* Santa Fe - Colombia: Universidad Católica de Santa Fe.

Bocchio, F. (2014). *Modelo Cloud Computing como Alternativa para Escalabilidad y Recuperación de Desastres.* Tesis, UTN.BA, Ingeniería de Sistemas de Información, Buenos Aires .

Cabrera, A. (2013). *Estudio para implementación de servicios data center basado en el modelo Cloud Computing.* Universidad de Cuenca, Quito. Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/4667

Cáceres, L. A. (2014). *Propuesta de computación en nube para mejorar los sistemas informáticos de la Universidad nacional Santiago Atunez de Mayolo, Huaraz 2014.* Tesis, Santiago Antunez de Mayolo, Facultad de Ciencias, Huaraz.

Domínguez, W. (2017). *Modelo de continuidad de servicios de las tecnologías de la información y comunicación utilizando cloud computing en la Empresa Américas Potash Perú S.A.* Obtenido de https://hdl.handle.net/20.500.13032/2377

Duffaut., A. E. (2013). *Estudio para implementación de servicios data center basado en el modelo cloud computing.* Tesis, Universidad de Cuenca, Facultad de Ingeniería, Quito.

Gil, J., & Maihuiri, L. (2018). *Implementación de un data center virtual en cloud computing para mejorar los servicios del departamento de ti en la empresa Venus Peruana S.A.C.* .

Goyes, J. (2020). *Estudio de impacto del modelo cloud computing en la gestión de servicios de información gerencial en la banca privada. tesis para optar el grado de maestro en administración de empresas.* Universidad Andina Simón Bolívar, Ecuador.

Guadiana, N. J. (2010). *Cómputo en la nube: Seguridad en el gestionamiento de la información.* Autonoma de Mexico: Facultad de Ingeniería.

Guerra, C. (2019). *Desarrollo de un prototipo móvil de registro de asistencia estudiantil mediante códigos QR y CLOUD COMPUTING.* Escuela Politecnica Nacional, Ecuador. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/20562

ISOTools. (2014). *Las claves del Éxito para la Gestión de Riesgos de Seguridad de la Información.* (ISOTools Excellence ed.). (I. Excellence, Ed.) Madrid: ISOTools Excellence.

L., J. (2011). *Procesos para la implementación de infraestructura Cloud Computing y sus ventajas sobre la infraestructura de servidores dedicados tradicioanles.* Tesis, Universidad de San Carlos de Guatemala, Facultad de Ingeniería, Guatemala.

Leyva, H. (2014). *Propuesta de computación en nube para mejorar los sistemas informáticos de la Universidad nacional Santiago Antúnez de Mayolo, Huaraz 2014.* Tesis pregrado, UNASAM, Huaraz. Obtenido de http://repositorio.unasam.edu.pe/handle/UNASAM/1150

Lizarraga, R., & Pachas, A. (2018). *Implementación de una Arquitectura Tecnológica basada en Cloud Computing como soporte al portafolio de proyectos profesionales de la EISC.* Obtenido de http://hdl.handle.net/10757/623029

Mega, G. P. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.* Tesis , Universidad de la República, Facultad de Ingeniería, Montevideo, Uruguay.

Romero, R. (2020). *Diseño e implementación de un sistema de control cloud computing para el robot kuka KR3 R540.* Universidad de las Fuerzas Armadas, Ecuador. Obtenido de http://repositorio.espe.edu.ec/handle/21000/21964

Rudas, L. (2017). *Modelo de gestión de riesgos para proyectos de desarro tecnológico.* Obtenido de https://ciateq.repositorioinstitucional.mx/jspui/bitstream/1020/86/1/RudasTayoLeidyP%20MDGPI%202017.pdf

ANEXOS

USP
UNIVERSIDAD SAN PEDRO

REPOSITORIO INSTITUCIONAL DIGITAL

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE DOCUMENTOS DE INVESTIGACIÓN

1. Información del Autor		
Solano Ruiz Jose Isaias	41929662	Josesolano22@gmail.com
Apellidos y Nombres	DNI	Correo Electrónico

2. Tipo de Documento de Investigación

X	Tesis		Trabajo de Suficiencia Profesional		Trabajo Académico		Trabajo de Investigación

3. Grado Académico o Título Profesional [1]

	Bachiller		Título Profesional		Título Segunda Especialidad	X	Maestría		Doctorado

4. Título del Documento de Investigación

PROPUESTA DE CLOUD COMPUTING EN LA UNIVERSIDAD SAN PEDRO, USANDO EL ENFOQUE DE LA NORMA ISO /IEC 27001.

5. Programa Académico

Maestría en Ingeniería Informática y de Sistemas con mención en Gestión de las Tecnologías de la Información

6. Tipo de Acceso al Documento

X	Abierto o Público [2] (info:eu-repo/semantics/openAccess)		Acceso restringido [3] (info:eu-repo/semantics/restrictedAccess) (*)

(*) En caso de restringido sustentar motivo

A. Originalidad del Archivo Digital

Por el presente dejo constancia que el archivo digital que entrego a la Universidad, es la versión final del trabajo de investigación sustentado y aprobado por el Jurado Evaluador y forma parte del proceso que conduce a obtener el grado académico o título profesional.

B. Otorgamiento de una licencia CREATIVE COMMONS [5]

I autor, por medio de este documento, autorizo a la Universidad, publicar su trabajo de investigación en formato digital en el Repositorio Institucional Digital, al cual se podrá acceder, preservar y difundir de forma libre y gratuita, de manera íntegra a todo el documento. [6]

Lugar	Día	Mes	Año
Chimbote	23	12	2024

Huella Digital

Firma

Importante

1. *Según Resolución de Consejo Directivo N° 033–2016–SUNEDU–CD Reglamento del Registro Nacional de Trabajos de Investigación para optar Grados Académicos y Títulos Profesionales, Art. 8, inciso 8.2.*
2. *Ley N° 30035, Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto y D.S. 006–2015–PCM.*
3. *Si el autor elegió el tipo de acceso abierto o público, otorga a la Universidad San Pedro una licencia no exclusiva, para que se pueda hacer arreglos de forma en la obra y difundir en el Repositorio Institucional Digital. Respetando siempre los Derechos de Autor y Propiedad Intelectual de acuerdo y en el Marco de la Ley 822.*
4. *En caso de que el autor elija la segunda opción, únicamente se publicará los datos del autor y resumen de la obra, de acuerdo a la directiva N°004–2016–CONCYTEC–DIGC (Numerales 5.2 y 6.1) que norma el funcionamiento del Repositorio Nacional Digital*
5. *Las licencias Creative Commons (CC) es una organización internacional sin fines de lucro que pone a disposición de los autores un conjunto de licencias flexibles y de herramientas tecnológicas que facilitan la difusión de información, recursos educativos, obras artísticas y científicas, entre otros. Estas licencias también garantizan que el autor obtenga el crédito por su obra.*
6. *Según el inciso 12.2, del artículo 12° del Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales –RENATI) "Las universidades, instituciones y escuelas de educación superior tienen como obligación registrar todos los trabajos de investigación y proyectos, incluyendo los metadatos en sus repositorios institucionales precisando si son de acceso abierto o restringido, los cuales serán posteriormente recolectados por el Repositorio Digital RENATI, a través del Repositorio ALICIA".*

Nota: – En caso de falsedad en los datos, se procederá de acuerdo a ley (Ley 27444, art. 32, núm. 32.3).

PROPUESTA DE CLOUD COMPUTING EN LA UNIVERSIDAD SAN PEDRO, USANDO EL ENFOQUE DE LA NORMA ISO /IEC 27001

INFORME DE ORIGINALIDAD

9%	6%	%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	1%
2	repositorio.ucv.edu.pe Fuente de Internet	1%
3	repository.unad.edu.co Fuente de Internet	1%
4	docplayer.es Fuente de Internet	1%
5	repositorio.uladech.edu.pe Fuente de Internet	<1%
6	repositoriobibliotecas.uv.cl Fuente de Internet	<1%
7	www.researchgate.net Fuente de Internet	<1%
8	repositorio.usanpedro.edu.pe Fuente de Internet	<1%
9	issuu.com Fuente de Internet	

		<1 %
10	revistas.uss.edu.pe Fuente de Internet	<1 %
11	Submitted to Universidad TecMilenio Trabajo del estudiante	<1 %
12	repositorio.unfv.edu.pe Fuente de Internet	<1 %
13	repositorio.upn.edu.pe Fuente de Internet	<1 %
14	1library.co Fuente de Internet	<1 %
15	archive.unu.edu Fuente de Internet	<1 %
16	repositorio.ug.edu.ec Fuente de Internet	<1 %
17	www.przetargi.info Fuente de Internet	<1 %
18	www.sothis.tech Fuente de Internet	<1 %
19	www.stromereien.ch Fuente de Internet	<1 %
20	ant.unicesar.edu.co Fuente de Internet	<1 %

21	docshare.tips Fuente de Internet	<1 %
22	renati.sunedu.gob.pe Fuente de Internet	<1 %
23	revistas.udistrital.edu.co Fuente de Internet	<1 %
24	risti.xyz Fuente de Internet	<1 %
25	riunet.upv.es Fuente de Internet	<1 %
26	www.escuelaeuropeaexcelencia.com Fuente de Internet	<1 %
27	www.fiepbulletin.net Fuente de Internet	<1 %
28	www.revfine.com Fuente de Internet	<1 %
29	documentos.uru.edu Fuente de Internet	<1 %
30	iso25000.com Fuente de Internet	<1 %
31	noticiassin.com Fuente de Internet	<1 %
32	repositorio.ucsm.edu.pe Fuente de Internet	<1 %

33	repositorio.ulasamericas.edu.pe Fuente de Internet	<1 %
34	repositorio.upla.edu.pe Fuente de Internet	<1 %
35	sedici.unlp.edu.ar Fuente de Internet	<1 %
36	www.conavi.com Fuente de Internet	<1 %
37	www.coursehero.com Fuente de Internet	<1 %
38	www.seguridadprofesionalhoy.com Fuente de Internet	<1 %
39	www.sintaxsistemas.com Fuente de Internet	<1 %
40	xmltvwiki.timefor.tv Fuente de Internet	<1 %

Excluir citas	Apagado	Excluir coincidencias	< 6 words
Excluir bibliografía	Activo		

ANEXO I: MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVOS DE LA INVESTIGACIÓN	VARIABLES	METODOLOGÍA
¿De qué manera la implementación del modelo Cloud Computing, bajo el enfoque de la norma ISO/EC 27001, contribuirá a mejorar la gestión de las TIC de la Universidad San Pedro?	Objetivo general: Proponer la implementación del modelo Cloud Computing tomando como base el enfoque de la norma ISO/IEC 27001. **Objetivos específicos** OE1: Analizar los modelos Cloud Computing tomando como base el enfoque de la norma ISO/IEC 27001. OE2: Identificar los controles asociados a los riesgos identificados, empleando la norma ISO/IEC 27001. OE3: Elaborar la documentación exigida por la norma ISO/IEC 27001.	Independiente: Cloud Computing. Dependiente: Norma ISO/IEC 27001	**Tipo de Investigación:** **Nivel:** Descriptiva **Diseño** No experimental **Muestra** 30 empleados **Técnicas e instrumentos** Encuesta Cuestionario

Fuente: Elaboración propia

ANEXO II: CUESTIONARIO

TITULO: Propuesta de implementación de Cloud Computing en la Universidad San Pedro, usando el enfoque de la ISO/ IEC 27001

TESISTA: José Solano.

Estimado colaborador (a):

Muchas gracias por su disposición a completar este cuestionario, tan solo necesitaremos unos minutos.

Este cuestionario forma parte de un estudio desarrollado por la Universidad San Pedro, sobre la propuesta de implementación de Cloud Computing en la Universidad San Pedro, usando el enfoque de la ISO/ IEC 27001. Le rogamos que trate de ser más objetivo posible en las respuestas que le pedimos, con el fin de garantizar a máxima confidencialidad, sus respuestas serán tratadas anónimamente y de manera segura.

INSTRUCCIONES:

A continuación, se le presenta una lista de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa ("X") en el recuadro correspondiente (SI o NO) según considere su alternativa, de acuerdo al siguiente ejemplo:

Situación actual del Sistema de Gestión de la Seguridad de la información.	**SI**	**NO**
Evaluación de las políticas de seguridad de la información.		
Analizar la gestión de cambios.		
Revisar las funciones del recurso humano, relacionado a las TIC.		
Verificar la seguridad física y ambiental, donde se encuentran los equipos informáticos.		
Evaluar la gestión de las comunicaciones y operaciones.		
Evaluar los procesos de control de accesos.		

Políticas de Seguridad.			
N°	**PREGUNTA**	**SI**	**NO**
01	¿Las políticas de seguridad se encuentran documentadas?		
02	¿Existe revisión de la política de seguridad?		
03	¿La alta gerencia se encuentra comprometido con las políticas de seguridad?		
04	¿El área de TI, vela por la seguridad de la información?		
05	¿Existen responsables asignados para la seguridad de la información?		
06	¿Existen procesos establecidos para velar por la confidencialidad de la información?		
07	¿Los funcionarios que hacen uso de los módulos informáticos, conocen acerca de las políticas de seguridad?		
08	¿Existe análisis de la información proporcionadas a terceros?		

Gestión de Activos.			
N°	**PREGUNTA**	**SI**	**NO**
01	¿Se realizan inventarios de los activos de TI?		
02	¿Se han asignado los responsables de TI?		
03	¿Los activos de TI, son usados de manera adecuada?		

04	¿Los activos de TI, se encuentran se encuentran clasificados?		
05	¿Los activos de TI, esta inventariados?		

Seguridad de los Recursos Humanos.			
N°	**PREGUNTA**	**SI**	**NO**
01	¿Los roles y responsabilidades del personal de TI se encuentran documentados?		
02	¿Existen un proceso documentado para la selección del personal de TI?		
03	¿Existen políticas sobre el término y condiciones de empleo del personal de TI?		
04	¿La gestión y responsabilidades del personal de TI, se encuentra documentado?		
05	¿El personal de TI, realiza capacitación y educación en seguridad de la información?		
06	¿Los procesos disciplinarios, se encuentran documentados?		
07	¿Existe un proceso documentado, respecto a la devolución de activos de TI?		
08	¿Existen procesos establecidos con respecto a la eliminación de accesos?		

Seguridad física y ambiental			
N°	**PREGUNTA**	**SI**	**NO**
01	¿El perímetro en donde se encuentras los equipos de procesamientos de información son los adecuados?		
02	¿Se realiza un control del ingreso de equipos informáticos?		
03	¿Los ambientes donde se encuentran los equipos informáticos son seguros?		

04	¿Los equipos se encuentran protegidos contra amenazas externas y ambientales?		
05	¿Los cables no representan peligros para los usuarios y visitantes a las diversas unidades operativas?		
06	¿La zona donde se encuentra el procesamiento de la información, está restringida al público no autorizado?		
07	¿Se establecen mantenimiento periódico de los equipos informáticos?		
08	¿Existe un proceso establecido para sacar los equipos a los ambientes externos?		
09	¿Existe un proceso establecido para dar de baja un equipo informático?		
10	¿Existe un proceso establecido para el traslado de propiedades?		

Gestión de la Comunicación y operaciones			
N°	**PREGUNTA**	**SI**	**NO**
01	¿Las operaciones de TI, se encuentran documentadas?		
02	¿Existen un proceso establecido para la gestión de cambios en TI?		
03	¿El área de TI, tiene definido las actividades de desarrollo y operatividad de los sistemas de información?		
04	¿Existe un proceso establecido para evaluar la entrega de servicios de TI?		
05	¿Existe un proceso establecido para monitorear y revisar los servicios de los terceros?		
06	¿Existe evaluación de la satisfacción de los usuarios, con respecto a la aceptación de los sistemas informáticos?		
07	¿Existe un proceso establecido para controlar los Software maliciosos?		

08	¿El acceso de redes y conectividad son seguros y se encuentran protegidos contra acceso de equipos móviles?		
09	¿Existe un proceso establecido para los Backup o controles de la información?		
10	¿Existe control sobre el acceso a la red de comunicación e información?		
Control de accesos			
N°	**PREGUNTA**	**SI**	**NO**
01	¿Las políticas de accesos se encuentran documentadas?		
02	¿Los usuarios que hacen uso de los sistemas informáticos se encuentran registrados, según perfil de accesos?		
03	¿Se encuentran identificados y listados los privilegios que tienen los administradores de los sistemas informáticos?		
04	¿Existe un proceso establecido para gestionar la clave de usuarios?		
05	¿Existe un proceso establecido para el equipamiento eventual del usuario que sus equipos, ingresan a mantenimiento correctivo?		
06	¿Existe un proceso establecido para evaluar de manera periódicamente que los usuarios no hagan usos de software no autorizados?		
07	¿Existe un proceso establecido para el acceso a la red?		
08	¿Existe un proceso establecido para autenticar a los usuarios externos?		
09	¿Existe un proceso establecido para realizar teletrabajo?		

Fuente: Elaboración propia