FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:

Bach. Moron Peredo Kristopher Renzo

ORCID: https://orcid.org/0000-0001-6276-0310

Asesor:

Mg. Atalaya Urrutia Carlos William

ORCID: https://orcid.org/0000-0002-2761-4868

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú 2023

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC

APROBACIÓN DEL JURADO

_____

Bach. Moron Peredo Kristopher Renzo

Autor

_____

Mg. Atalaya Urrutia Carlos William

Asesor

_____ _____

Mg. Bravo Ruiz Jaime Arturo

Presidente de Jurado

Mg. Mejia Cabrera Heber Ivan

Secretario de Jurado

_____

Mg. Diaz Vidarte Miguel Orlando

Vocal de Jurado

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien(es) suscribe(n) la **DECLARACIÓN JURADA**, soy(somos) **egresado (s)** del Programa de Estudios de la **ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS** de la Universidad Señor de Sipán S.A.C, declaro (amos) bajo juramento que soy (somos) autor(es) del trabajo titulado:

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ S.A.C

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

En virtud de lo antes mencionado, firman:

MORON PEREDO, KRISTOPHER RENZO	DNI: 46642368	

Pimentel, 31 de 01 de 2023.

Dedicatorias

A mis padres, por ser ellos los seres quienes me han dado la vida, por sus persistentes exhortaciones y consejos, tolerancia y paciencia, su soporte y apoyo desmesurado y leal durante la totalidad del tiempo que ha conllevado la realización de esta extraordinaria carrera profesional. Gracias, padres por motivarme siempre a alcanzar mis sueños. Todo lo que yo hoy en día soy, es gracias a ustedes. Los amo.

Agradecimientos

Agradezco al Dios Todopoderoso por bendecirme todos los días de mi existencia y por permitirme completar esta meta que me propuse hace ya muchos años.

A la empresa Rash Perú S.A.C., a sus gerentes, jefes de área y demás colaboradores que intervinieron en esta tesis con su conocimiento y experiencias, las cuales en conjunto me han servido de grandioso provecho en la carrera que he comenzado.

A la Dirección de Tecnologías de la Información por el gran apoyo otorgado a mi persona para la consecución de esta tesis.

Un agradecimiento muy especial al Mg. Ing. Mejia Cabrera Heber Ivan, asesor metodólogo que la Universidad Señor de Sipán se ha dignado en ofrecerme, por su predisposición, orientación, paciencia y guía para la elaboración de la presente tesis.

A mi familia, y en especial a mis padres, por la tolerancia, el impulso y la paciencia en la culminación de este sueño que he llevado muchos años, y en los que nunca los he visto debilitarse.

Resumen

La presente tesis tiene como objetivo principal diseñar un Sistema de Gestión de Seguridad de la Información para la empresa Rash Perú S.A.C, que incorpore estándares internacionales ajustados a las nuevas TI con el fin de asistir a la seguridad de la información, tomando como caso de estudio a la empresa mencionada. Se desarrolló bajo una investigación de campo, lo que permitió la elaboración y desarrollo de una propuesta de un modelo viable para resolver los problemas de seguridad de la información en la compañía. La metodología utilizada se sustentó en el ciclo de Deming, tomando como referencia la Norma ISO 27002 y usando una combinación de metodologías para la evaluación de los riesgos que ayude a la toma de decisión sobre las opciones de tratamiento de riesgo adecuado. Los resultados en Seguridad de información, el valor promedio del Re-test fue de 69.90% y el valor promedio Post-test fue de 14.00%. Además, el valor mínimo del re-test fue 50%, el valor máximo es 88%, y el valor mínimo del post-test es 0% y el máximo es 27%. Se concluye el nivel de significancia en el Re-test fue de 0,265 y para el Post-test, 0,108. Por lo cual se determina que el indicador se ajusta a una distribución normal o paramétrica ($P > 0.05$). Esta tesis consta de seis capítulos en los cuales se desarrolla cada tema que permite obtener, aplicar y conocer los resultados de la propuesta del diseño: el Capítulo I - Problema de Investigación, en el cual se desarrolló la situación problemática y la formulación del mismo, la delimitación, la justificación e importancia, las limitaciones y objetivos de la investigación. Capítulo II - Marco Teórico, que contiene los antecedentes de estudios, el estado del arte, las bases teóricas - científicas y la definición de la terminología. Capítulo III - Marco Metodológico, que contiene el tipo y diseño de investigación, la población y muestra, la hipótesis, la Operacionalización, los métodos, técnicas, instrumentos y el procedimiento para la recolección de datos, el análisis estadístico e interpretación de los datos, los criterios éticos y de rigor científico. Capítulo IV - Análisis e Interpretación de los resultados, que contiene los resultados en tablas y gráficos, y la discusión de los mismos. Capítulo V - Propuesta de Investigación, que contiene las características y componentes de la propuesta elaborada. Capítulo VI - Conclusiones y Recomendaciones, donde se exponen las

conclusiones y recomendaciones. Finalmente, se muestran la bibliografía y los anexos.

Palabras Clave: TI, Políticas de Seguridad, SGSI, Seguridad de Información, ISO 27002.

Abstract

The main objective of this thesis is to design an Information Security Management System for the Rash Peru SAC Company, which incorporates international standards adjusted to the new IT in order to assist in the security of information, taking as a case study to the company mentioned. It was developed under a field investigation, which allowed the elaboration and development of a proposal of a viable model to solve the information security problems in the company. The methodology used was based on the Deming cycle, taking as reference the ISO 27002 standard and using a combination of methodologies for the evaluation of the risks that help to make the decision about the appropriate risk treatment options. The results in Information Security, the average value of the Re-test was 69.90% and the average Post-test value was 14.00%. In addition, the minimum value of the re-test was 50%, the maximum value is 88%, and the minimum value of the post-test is 0% and the maximum is 27%. It is concluded that the level of significance in the Re-test was 0.265 and for the Post-test, 0.108. Therefore, it is determined that the indicator fits a normal or parametric distribution ($P > 0.05$). This thesis consists of six chapters in which each topic is developed to obtain, apply and know the results of the design proposal: Chapter I - Research Problem, in which the problematic situation was developed and its formulation, the delimitation, the justification and importance, the limitations and objectives of the investigation. Chapter II - Theoretical Framework, which contains the background of studies, the state of the art, the theoretical - scientific bases and the definition of terminology. Chapter III - Methodological Framework, which contains the type and design of research, population and sample, hypothesis, operationalization, methods, techniques, instruments and procedure for data collection, statistical analysis and interpretation of data, the ethical criteria and scientific rigor. Chapter IV - Analysis and Interpretation of the results, which contains the results in tables and graphs, and their discussion. Chapter V - Research Proposal, which contains the characteristics and components of the proposal prepared. Chapter VI - Conclusions and Recommendations, where conclusions and recommendations are presented. Finally, the bibliography and the annexes are shown.

Keywords: IT, Security Policies, ISMS, Information Security, ISO 27002.

Índice

Índice de figuras

Índice de tablas

Índice de anexos

I. INTRODUCCIÓN

1.1. Realidad Problemática.

En la actualidad, frecuentemente aparecen inmensurables cantidades de amenazas y riesgos, los mismos que logran la total o parcial afectación de la Seguridad de la Información (SI), logrando más específicamente, la afectación de la triada que componen la confidencialidad, la disponibilidad y la integridad de la totalidad de los activos con las que disponen las compañías, sin distinción, alterando y aturdiendo, sin distinción alguna, a compañías de gran envergadura, como a aquellas de menor cuantía, verbigracia, las pequeñas compañías (Tsakalidis & Vergidis, 2019). Los avances en los sistemas informáticos y las redes han creado un nuevo entorno para actos delictivos, ampliamente conocido como ciberdelincuencia. Los incidentes de delitos cibernéticos son ocurrencias de delitos penales particulares que simbolizan una grave amenaza en la seguridad, economía y tranquilidad de las sociedades a nivel mundial.

Según Riek et al. (2017) la actividad cibernética maliciosa se manifiesta principalmente como interrupción del negocio y robo de datos financieros o confidenciales, entre otros. Sin embargo, no existen suficientes buenas prácticas dentro de las organizaciones en materia de SI. Este hecho puede deberse a que no existen políticas de código seguro para el SOFTWARE. desarrollado internamente (Alshaikh, 2020), o muchas empresas ahora mantienen su infraestructura de TI en el entorno de la nube (Arafat, 2018), o simplemente porque el capital humano no está capacitado en SI (Rodríguez, Rojas, & Mejía, Methodological model based on Gophish to face phishing vulnerabilities in SME, 2018). Todo esto se traduce en impactos físicos, digitales, económicos, psicológicos, reputacionales y daños sociales para las víctimas diariamente, tal y como lo mencionan Agrafiotis et al. (2018).

Según Diamantopoulou et al. (2019) los cibercrímenes que atentan contra la SI implican una mezcla de diversos delitos típicos con nuevos ilícitos. Los incidentes individuales de delitos cibernéticos son ocurrencias de delitos penales particulares y, como lo demuestran múltiples estadísticas y encuestas nacionales sobre delitos, están aumentando constantemente. Asimismo, el FBI (2021) reveló que, el Centro contra Delitos Cibernéticos publicó su informe anual sobre

delitos en Internet del 2020, el cual incluye información de 791 790 acusaciones correlacionadas con presunciones de delitos cometidos en la Internet (un aumento de más de 300 000 denuncias desde 2019) y pérdidas reportadas que superan los $4200 millones. También se han publicado estadísticas específicas por estado y se pueden encontrar en el Informe sobre delitos en Internet de 2020 y en los Informes estatales de 2020 que lo acompañan.

Como bien se menciona, Las tres (03) amenazas con más denuncias en el año 2020 han sido las estafas por phishing, las estafas por falta de entrega y extorsiones. Los estafados devastaron sus patrimonios perdiendo enormes sumas monetarias enteramente en fraudes por medio de compromisos comerciales vía correos electrónicos, verbigracia, Gmail, etcétera; transacciones de citas y aventura; y timos referentes con inversiones. El 2020 notó la llegada de estafas que aprovechan la pandemia de COVID-19. El Informe de Delitos Cibernéticos recibió más de 28 000 denuncias que son relacionadas con el COVID-19, con embaucadores dirigidos, ya sean con organizaciones, o a individuales.

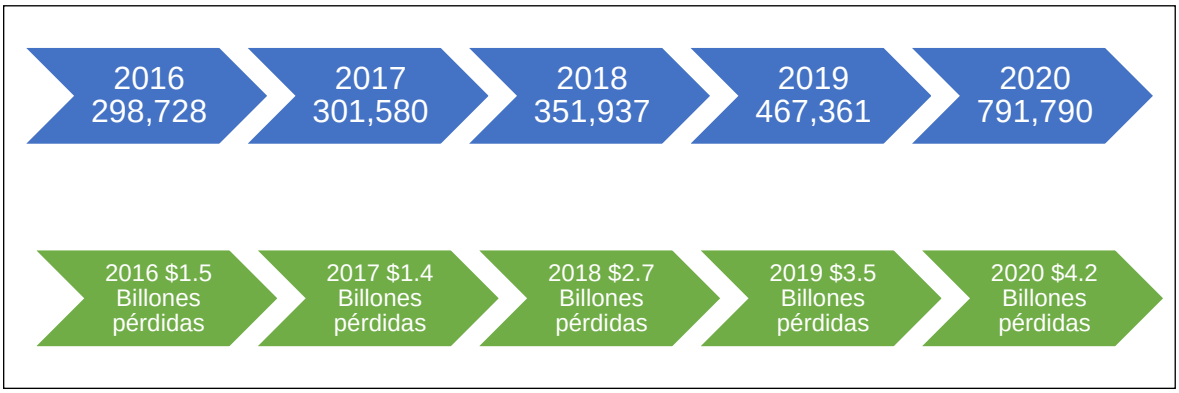


Figura 1 Estadísticas de quejas de los últimos 5 años

Fuente. FBI (2021).

Los distintos delitos de Ciber-delincuencia constituyen una amenaza grave para la economía global, el bienestar y la seguridad de la sociedad. En un estudio de la firma PriceWaterhouseCoopers (2021), se destaca que los casos de SI no solo aumentan en numerosidad, sino que se están tornando progresivamente más destructivos y abarcan una gama más amplia de información y segmentos

de ataque. Este avance simboliza una amenaza seria para las operaciones de empresas, organizaciones y economías nacionales, el daño económico mundial se estima en más de $ 225 mil millones. Además, tal y como lo revelaron Anderson et al. (2019) el impacto de los delitos de SI en las personas también es inmenso; desde el robo de identidad hasta la explotación sexual de niños y el acoso cibernético, los diversos delitos cibernéticos provocan desde una leve incomodidad hasta un daño mental severo, miedo público y pérdidas financieras.

La protección exitosa contra las amenazas cibernéticas es un gran desafío en todos los sectores, y el daño económico de la falta de SI se evidencia en el Noveno Estudio Anual del Costo del Delito Cibernético en el que se reportan aumentos del 67 % en las brechas de seguridad y del 72 % en el costo promedio que, para hacer frente a los ataques, en los últimos cinco años (Bisell, LaSalle, & Cin, 2019). Asimismo, estos autores revelaron que, los ataques basados en las personas son los que más han aumentado, lo cual mostraron en base a las siguientes estadísticas:

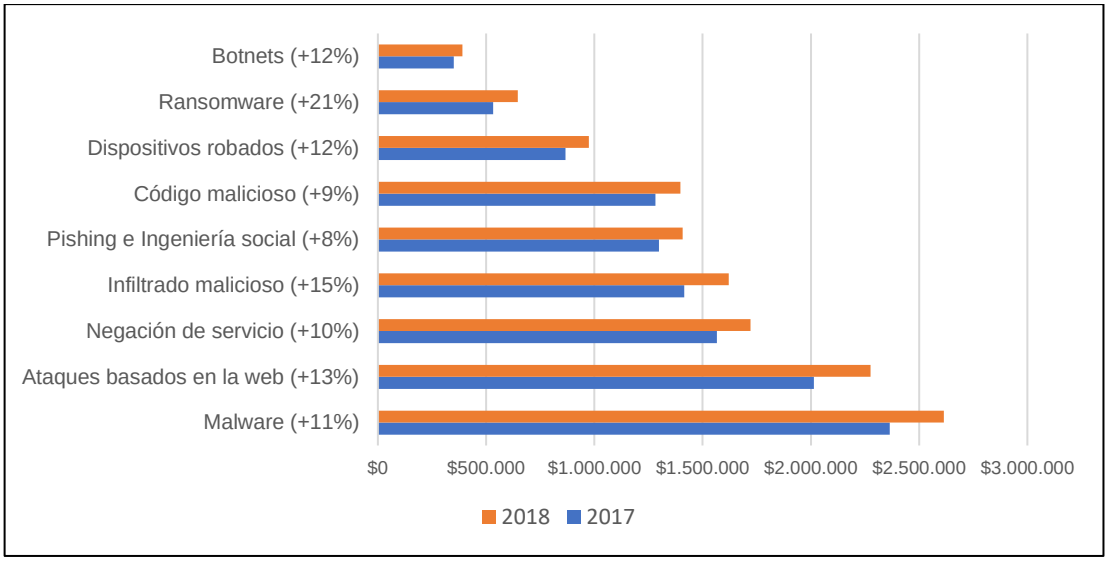


Figura 2 Ataques de SI basados en las personas durante los años 2017-2018

Fuente Bissell et al. (2019).

Dicho lo anterior, es necesario que las empresas posean un Sistema de Gestión de Seguridad de la Información (SGSI) alineadas a las correctas prácticas de SI que les permitan identificar vulnerabilidades y riesgos existentes y futuros en cuanto a ello. Por ejemplo, la ISO/IEC 27000, 27001 y 27002 son normas que permiten a las empresas conocer su estado actual en materia de SI e implementar de manera sistemática y efectiva los controles, procedimientos y

políticas necesarios con propósitos preservativos de la triada mencionadas previamente líneas arriba: confidencialidad, integridad y disponibilidad de activos informáticos (Disterer, 2017).

Un SGSI, es una herramienta para gestionar y controlar la información de seguridad. Se compone de un proceso bien documentado, ampliamente sistémico y, finalmente, totalmente reconocido la totalidad de la compañía. Sus estrategias y políticas se desarrollan para la preservación y aseguramiento de los tres (03) componentes de la triada de la SI, con propósitos de lograr la mantenibilidad de niveles menores referentes a exposiciones que tengan que ver con riesgos propios y asumidos por las organizaciones (Susanto & Almunawar, 2018). Con la implantación de un SGSI, las empresas pueden reconocer los riesgos de sus activos de información, y de esta manera abordarlos mitigándolos, transfiriéndolos o controlándolos. El SGSI debe ser parte de los procesos y estructura de total de la gestión de las informaciones de las que disponen las organizaciones, teniendo en cuenta que la SI es considerada en los diseños de procesos, sistemas informáticos y demás medidas o regulaciones (Qusef, Arafat, & Al-Taher, 2018).

Además, un SGSI permite que cualquier organización implemente un gobierno de SI fundamentado en un componente estructural de la compañía, en el cual se logran definir, verbigracia, recursos, procesos, procedimientos, políticas, roles, responsabilidades, etcétera, con propósitos de administrar los activos de información con precisión (Angraini, Alias, & Okfalisa, 2019). Entonces, un SGSI suministra herramientas útiles que permite a las diversas compañías establecer tales políticas mencionadas anteriormente, y que tienen concordancia con la SI, en alineamiento con las metas estratégicas de la empresa. Además, la implantación de un SGSI logra suministrar un modelo de mejoramiento continuo, logrando así poder renovarse, repeliendo los diversos tipos de amenazas, con la usanza de acciones preventivas y correctivas, las mismas que admitan control sobre cualesquiera que sean los incidentes que hacen la afectación de la SI.

Un modelo de SGSI, tal y como se revelaba previamente, localiza riegos y vulnerabilidades existentes en el momento en el que se logra dicha evaluación y también aquellos que pudiesen darse a posteriori. Además, determinan procedimientos, políticas y praxis de SI para tener un posible impacto menor de darse eventualidades que, a posteriori puedan materializarse en amenazas. Además, según revelaron Ozdemir et al. (2017) un modelo de SGSI se puede alinear con las mejores prácticas de una o más especificaciones como ISO 27001, ISO 27002, COBIT, ITIL, etcétera.

En Perú, las diversas compañías son conocedoras plenas de las amenazas que los ciberataques logran representar para sus operaciones, productividades y prestigios, en el giro de los negocios en los que se desenvuelven. Por tal motivo, actualmente la ciberseguridad ha dejado de ser considerada como cualidad simple de sistemas, logrando constituirse a manera de valor agregado a, verbigracia, cualquier prestación esencial (Atencio, 2019). Un servicio que, se muestra como un eslabón estratégico para sus respectivos negocios y que, se ha distado muchísimo de pensamientos y praxis contrarias que anteriormente replicaban los tan conocidos eslogan, verbigracia, “aquí no aplica”, “aquí no se pueden implementar dichas prácticas”, etcétera, y el rechazo a renovar los sistemas y las praxis que han manipulado durante tanto tiempo y hasta el día de hoy.

Dichas visiones arbitrarias en cuanto a la gestión de la SI hacen que, tal importante activo de la Ingeniería de Sistemas sea totalmente y plenamente desatendidos. Por ello es que, en nuestro país, la carencia de ello, ha venido reflejándose en niveles bajos de SI, en contraposición de algunos otros países caribeños y latinoamericanos, quienes muestran mejores índices en cuanto al anteriormente mencionado, posicionándonos en lugares incómodos dentro de diversos ránquines relacionados con la SI. Verbigracia, según The Business SOFTWARE. Alliance, en nuestro país el SOFTWARE. utilizado es en gran parte ilegal (65%), lo que equivale a decir que, de cada cuatro (04) SOFTWARE.s, uno (01) es, o bien infestado por algún tipo de virus o es pirateado, lo que conlleva a arriesgar las informaciones, llegando a ser pérdidas o hurtadas. Significancia clara de que, a pesar de los denodados esfuerzos y praxis de implementar

políticas de SI por parte de las compañías, aún se lidia con desbalances tal y como se indicaba líneas arriba, logrando ser una brecha muy alta y que conlleva a que las compañías trabajen con mayor ahínco en la optimización de estándares relacionados con la SI.

La carencia de estándares relacionados con la SI impide la mejora de nuestro país y amplía la brecha con los países desarrollados. Verbigracia de ello, claramente es que nuestro país no es considerado como una nación en la que se cuenten con adecuados niveles relacionados con la preservación de las informaciones personales, logrando el desaprovechamiento de ventajas económicas internacionales dado que, los flujos internacionales de informaciones son factores cardinales para el desenvolvimiento de diversas actividades comerciales y de negocios. En nuestro país hermano, Colombia, el Departamento Nacional de Planeación (DNP) logró considerar en su hoja de ruta relacionada con la conectividad, que "las naciones en vías de desarrollo deberían de soportarse en TI, de modo que puedan aprovecharlas para el logro de mejoramientos en diversos sectores, verbigracia, cultural, social, política y económica, que a posteriori permitan ese aminoramiento de brechas con otras naciones con mayores niveles de desarrollo en dicho sector" (Carrillo, Sánchez, & Villalobos, 2017).

Por otro lado, en el año 2005, más específicamente en la Cumbre Mundial sobre la Sociedad de la Información, llevada a cabo en Cartago, Túnez se logró destacar que la SI se ha convertido en un factor trascendental para fortalecer la convicción en la usanza de las TIC, las cuales admiten la presencia de sociedades digitales incluyentes y vinculantes (Latorre, Castro, & Potes, 2018). Asimismo, es importante recalcar que además de que la SI en las naciones es relevante, lo es también en sectores más específicos como el comercial, el cual es un ámbito que es fundamental en los desarrollos económicos. De darse una gestión inadecuada relacionadas con este tema de la SI, podrían darse escenarios de pérdidas, adulteraciones, divulgaciones y usanzas no autorizadas de informes, pudiendo ser estos de las empresas o cualquier cliente, etcétera. Ello conlleva a pérdidas de cualquier beneficio internacional pues se carecen de

garantías, logrando desconfianzas en los usuarios y las clientelas de, verbigracia, la prestación de servicios de ventas.

Dicho lo anterior, a la interna de este tipo de ámbitos es que se localiza Rash Perú S.A.C.; empresa que ha logrado concientizarse en que, descuidos en cuanto a la gestión de la SI y en cuanto a la manipulación de informaciones podría conllevar a secuelas negativas, reflejándose en diversos padecimientos, tales como, verbigracia, sobrecostes en tratamientos de riesgos asociados a la SI, pérdidas de información, demoras en dichas recuperaciones de tales informaciones, lo que conllevaría además a malas praxis en cuanto a la toma de decisiones, y posteriormente, desarticulación por parte de las diversas áreas que logran intervenir en las manipulaciones de dichas informaciones y en sus posteriores tomas de decisiones, tal y como se viene sucediendo.

Por esta razón, se propone diseñar e implementar un SGSI fundamentado en la norma ISO/IEC 27002, que no solo involucra al Área de TI, sino que además contemple la participación de la totalidad de áreas funcionales de la misma, en procesos horizontales dirigidos por políticas formuladas desde las gerencias y donde se tenga bien en claro que la correcta gestión de la SI, depende fundamentalmente del capital humano que componen Rash Perú S.A.C.

1.2. Trabajos previos

Jassim et al. (2022), realizaron la investigación, *Diagnosing the current Information Systems Security Department in the Information Technology Department according to the international standard (IS0/IEC 27001:2013)*, en la Al-Mustansiriya University, en Bagdad, Irak. Los sistemas informáticos y las redes informáticas son vulnerables a amenazas derivadas de la violación o intento de obtención de datos o informes, registros y archivos que contengan la información, por tanto, es importante la aplicación de la norma en mención para la protección de dicha información, por ello se requiere gestionarlo con los mejores métodos de protección adoptados globalmente. Por esta razón, asumieron como objetivo, desarrollar un SGISI basado en la ISO mencionada con propósito de salvaguardar dichas informaciones en esta institución estatal del gobierno iraquí. Para ello, primeramente, se caracterizó dicha norma ISO,

después se realizó un análisis de la gestión de la SI en dicho Departamento de TI, posteriormente se diseñó el SGSI fundamentado en la norma ISO/IEC 27001, para llevarlo a la praxis implementándolo y finalmente evaluar los resultados obtenidos. La metodología que se utilizó en esta investigación fue de tipo aplicada, de enfoque mixto y nivel exploratorio de instrumento se empleó la ficha de registro y la técnica de observación. Los resultados evidencian, que existía una brecha del 49% y 51% coincidente debido a la falta de instauración de una política de SI en la sección. Se concluyó que, con la implementación del SGSI se pudieron aminorar estas brechas iniciales pues se poseía una guía especial para la gestión de la SI que tenga como objetivo aclarar y crear un entorno de seguridad de alta confidencialidad para mantener la confidencialidad del trabajo en dicha institución y prevenir cualquier incumplimiento.

Risco (2021) en su investigación tiene por propósito analizar la influencia del SGSI en la empresa. La metodología que se aplicó en esta investigación fue de tipo aplicada, de enfoque mixto y nivel exploratorio de instrumento se empleó la ficha de registro y observación como tecnica. Los resultados mostraron que, de la implementación de las políticas de SI, el 78 % personas encuestadas se reducirá los problemas y además 80 % acepta el SGSI en la entidad. Se concluyó que, el SGSI impacta positivamente, la misma que está con base en la norma ISO 27001

Alvarado y Sánchez (2021), realizaron la investigación, *Information security in the process of system and product development through the implementation of security controls based on ISO 27002:2015 in the company BITNESS CORP S.A.C., 2020*, en la Universidad Peruana Unión, en Lima, Perú. *La* empresa caso de estudio es una compañía dedicada a la construcción de SOFTWARE.s a medida en la ciudad limeña, por ello, casi la totalidad de sus procesos en las TI, sin embargo, ante el actual panorama de crecimiento de los riesgos asociados a ataques cibernéticos, es que se hace necesario contar con políticas o lineamientos para salvaguardar la SI. Por esta razón, asumieron como objetivo, desarrollar un SGSI fundamentado en la ISO/IEC 27002:2015 con propósitos de resguardar las informaciones vertidas en cuanto a la construcción de sus

productos y servicios. Para ello, primeramente, analizaron la problemática acaecida en dicho caso de estudio en cuanto al cumplimiento de controles de SI, luego diseñaron el SGSI basado en la ISO en mención, posteriormente implementaron dicho SGSI en la empresa limeña constructora de SOFTWARE. y, finalmente, calcularon los resultados producidos posterior a la ejecución del SGSI. Los resultados conseguidos revelaron que, la empresa poseía el nivel Parcialmente Logrado en cuanto a controles de SI (48.95%), evidenciándose carencias en cuanto al proceso de construcción de SOFTWARE.. Se concluyó que con la implementación del SGSI en dicha compañía limeña constructora de SOFTWARE. se mejoró el nivel de la SI posicionándola en 81.8% con controles de seguridad, políticas de desarrollo seguro, protección de datos de pruebas, etcétera.

Fonseca et al. (2021), realizaron la investigación, *A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard*, en la Universidad EAN, en Bogotá, Colombia. En la actualidad, las TI han permitido el desarrollo de las compañías convirtiendo a sus informaciones en activos esenciales para las mismas, quienes deben evitar que se encuentren expuestas a los piratas informáticos, virus informáticos, ciber espionaje y falencias en las infraestructuras son algunos de las problemáticas existentes de las compañías cara a diario. Por esta razón, asumieron como objetivo, desarrollarlo un modelo de SGSI fundamentado en la NTC-ISO/IEC 27001:2013, el mismo que pudiese ser aplicado a cualquier compañía y coadyuve a conocer su actual situación en materia de SI. Para ello, primeramente, realizaron una revisión sistemática acerca de prácticas que pudieran ser alineadas con el modelo de SGSI, tales como ISO 27001, ITIL, COBIT, etcétera, posteriormente se diseñó el SGSI fundamentado en la NTC-ISO/IEC 27001 y que constó de tres (03) fases (a. diagnóstico del estado actual del manejo de la SI, b. Preparación para el SGSI y c. implementación del SGSI), luego se implementó dicho modelo del SGSI en una compañía colocha vinculada al sector de hidrocarburos y, finalmente evaluaron los resultados obtenidos posteriores a dicha implementación. Los resultados expusieron que, existían activos informáticos, riesgos técnicos y amenazas aplicadas a la totalidad de procedimientos en dicho caso de estudio,

también se evidenció falta de un plan formativo y educación en SI para las personas inmersas en los procesos. Se concluyó que, el modelo de SGSI se sirve de nacimiento para su implantación a posteriori legitimización en concordancia con el estándar NTC-ISO-IEC 27001:2013.

Solano (2020) en su estudio, su propósito fue plantear un prototipo para la gestión de la seguridad de la información sustentado en la norma ISO 27001 para minimizar los posibles riesgos en la empresa. Para el estudio de caso, se utilizó una metodología tipo aplicada, un enfoque cualitativo y un nivel explorativo. Los resultados que se consiguieron en el estudio, fueron que en la implementación de normas ISO, el 52,60 % de los encuestados dice que es factible en la pre-implementación, acrecentando un 11,40 % en la post-implementación, causando una reducción del 41,20 %. Se concluyó que se debe realizar capacitaciones constantes al personal y estar deben de ir de la mano que la alta gerencia apoye las nuevas políticas de cambio.

Seeba et al. (2021), realizaron la investigación, *Development of the Information Security Management System Standard for Public Sector Organisations in Estonia*, en la University of Tartu, en Tartu, Estonia. El objetivo de cada gobierno debe ser proporcionar servicios digitales a sus ciudadanos con un nivel aceptable de confidencialidad, integridad y disponibilidad, sin excepción, para lo cual deben de alcanzar el nivel de SI adecuado en el contexto de los riesgos conocidos y desconocidos en materia de ello, buscando contar con un SGSI acorde a sus necesidades. Por esta razón, asumieron como objetivo desarrollar un SGSI fundamentado en las mejores prácticas de SI y estandarizado para las organizaciones del sector público en dicho país báltico. Para ello, primeramente, evaluaron la situación actual de la SI en dichas instituciones públicas estonias, posteriormente realizaron una revisión de la literatura allegada con estándares para SGSI y, finalmente, desarrollaron el SGSI basado en los estándares seleccionados. La metodología que se utilizó en esta investigación fue de tipo aplicada, de enfoque mixto y nivel exploratorio de instrumento se empleó la ficha de registro y técnica la observación. Los resultados obtenidos revelaron un modelo fundamentado en la ISO/IEC 27001,

CIS20 y BSI ITG dado que dichos estándares eran los adecuados para trabajar con los requerimientos de dichas instituciones estonias. Se concluyó que, con este modelo se han obtenido los requisitos del SGSI para las organizaciones del sector público de una forma que permite la reutilización de los requisitos estructurados, así como también, se utilizó la estructura de los requisitos obtenidos para comparar tres normas de SGSI.

Aquino et al. (2020), realizaron la investigación, *Implementation of an Information Security Management System Based on the ISO/IEC 27001: 2013 Standard for the Information Technology Division*, en la Universidad Nacional Micaela Bastidas de Apurímac, en Apurímac, Perú. En las casas de estudios superiores se necesitan planes directrices o normas que permitan salvaguardar los activos informáticos, no siendo ajena la UNAMBA la misma que, a la fecha carecía de dicho sistema que le permita gestionar adecuadamente las TI. Por esta razón, asumieron como objetivo, coadyuvar al mejoramiento del grado de SI en dicha casa de estudios, implementando un SGSI ensimismado en el estándar ISO/IEC 27001:2013. Para ello, primeramente, recolectaron informaciones previas a la implementación del SGSI acerca de los activos informáticos, posteriormente implementaron dicho SGSI haciendo usanza de la metodología PDCA y la metodología MAGERIT III, luego recolectaron nuevamente informaciones posteriores a la implementación de dicho SGSI y finalmente evaluaron los resultados en cuanto a los riesgos según activos. La metodología que se utilizó en esta investigación fue de tipo aplicada, de enfoque mixto y nivel exploratorio de instrumento se empleó la ficha de registro y técnica la observación. Los resultados expusieron que, el nivel de riesgos de SI antecesores a la puesta en praxis del SGSI fue 86.15%, para conseguir 11.15% posteriormente; por tanto, se obtuvo una disminución del 75%. Además, hubo mejoramientos en las regulaciones de SI, ya que estos se aumentaron hasta 65 controles, representando un incremento del 41,23%. Asimismo, hubo también acrecentamientos de niveles varios, verbigracia, el de capacitaciones en programas de SI en usuarios de DTI debido a que esta cifra aumentó al 95% evidenciando que los encuestados tenían conocimientos en este tema

posteriores a la implementación. Se concluyó que el SGSI permitió la mejora en cuanto a la conducción de la SI en dicha casa de estudios superiores.

Fathurohman y Witjaksono (2020), realizaron la investigación, *Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City)*, en la Telkom University, en Bandung, Indonesia. En la que el Departamento de Comunicación e Información (DISKOMINFO) del Municipio de Bandung tiene la responsabilidad de llevar a cabo varias partes del Gobierno Regional en campo de la comunicación y la informática teniendo, como base trascendental para implantación de adiestramientos, el apoyo de TI, sin embargo, éstas no se vienen gestionando adecuadamente, encontrándose varias cláusulas que aún no se cumplen en materia de la SI afectando el desempeño de dicho gobierno indonesio. Por esta razón, asumieron como objetivo, diseñar un SGSI fundamentado en la ISO/IEC 27001:2013 con propósitos de salvaguardar la información o los activos que se consideran sensibles para dicha organización estatal. Para ello, primeramente, desplegaron una revisión de la literatura de SI, luego realizaron una identificación de dicha ISO, después caracterizaron el caso de estudio en materia de SI para, posteriormente diseñar el SGSI y, finalmente, validarlo. La metodología que se utilizó en esta investigación fue de tipo aplicada, de enfoque mixto y nivel exploratorio de instrumento se empleó la ficha de registro y técnica la observación. Los resultados obtenidos mostraron doce (12) riesgos asociados a la gestión de la SI, doce (12) vulnerabilidades y amenazas y, deficiencias del 71% y 78% en cuanto a seguridad operacional y el control de accesos respectivamente. Se concluyó que, el SGSI puede utilizarse como referencia en la creación de estrategias para aumentar la SI en la comunicación e informaciones del gobierno de la localidad.

Ferreira (2020), realizó la investigación, *Implementação de um Sistema de Gestão de Segurança da Informação em Conformidade com a ISO/IEC 27001*, en la Universidade de Coimbra, en Coímbra, Portugal. En las entidades públicas son conscientes de que sus activos de TI son relevantes para el desarrollo de sus objetivos organizacionales y que cumpliendo con los requerimientos de la

ISO/IEC 27001 podrían no solamente garantizar la confidencialidad, integridad y disponibilidad de sus informaciones, sino también mejorar su desempeño operativo y de mercado, reduciendo significativamente sus costos al prevenir y tratar de manera efectiva los incidentes de SI. Por esta razón, asumió como objetivo, implementar un SGSI para una entidad estatal perteneciente a dicho país europeo el cual debería estar ensimismado en la ISO/IEC 27001. Para ello, primeramente, analizaron la ISO en mención, luego caracterizaron el caso de estudio, después diseñaron el SGSI considerando el estándar en mención y haciendo usanza de la metodología PDCA, posteriormente implementaron dicho SGSI en el caso de estudio para, finalmente, evaluar los resultados obtenidos posterior a dicha implementación. Los resultados expusieron que, en dicho caso de estudio no se venían desplegando actividades para el aseguramiento de la SI, desembocando en que a veces se pedía que se realizaran tareas y no se daba un marco sobre el propósito de esa tarea o se tomaban decisiones y no se explicaban las razones, además de la carencia de controles de SI. Se concluyó que, con la ayuda de las normas ISO/IEC 27002 e ISO/IEC 27005, es posible establecer, efectuar y monitorear un sistema de gestión de riesgos y los controles de SI planteados por la norma ISO/IEC 27001 para cumplir con sus requisitos.

Fuentes (2020) realizó la investigación, *Information Security Management System based on the ISO/IEC 27003 Standard for the National University of Cajamarca*, en la Universidad Nacional Pedro Ruiz Gallo, en Lambayeque, Perú. Las instituciones de educación superior cuentan con áreas encargadas de gestionar adecuadamente las TI con las que disponen para sus procesos internos, sin embargo, algunas de ellas carecen de políticas que permitan el aseguramiento de la disponibilidad, integridad y confidencialidad de las informaciones, considerando que son procesos críticos, siendo este el caso de la Universidad Nacional de Cajamarca (UNC). Por esta razón, asumió como objetivo, desarrollar un SGSI fundamentado en la ISO/IEC 27003 con propósitos de lograr el mejoramiento de la SI en dicha casa de estudios superiores en la localidad cajamarquina. Para ello, primeramente, realizaron un análisis previo acerca del nivel de cumplimiento de políticas de SI, luego realizaron una revisión de la literatura referente de marcos y prácticas para la gestión de la SI,

posteriormente, diseñaron el SGSI fundamentado en la ISO/IEC 27003, el cual, a posteriori fue validado mediante juicio de expertos para, finalmente, llevarlo a la praxis en dicho caso de estudio seleccionado. Los resultados expusieron que, existían deficiencias en dicha casa de estudios evidenciándose en incumplimientos de gran significancia, sobre todo en consideración a la ISO/IEC 27003, asimismo, en cuanto al SGSI contó con tres dimensiones, mejorándose cada una de ellas, Contextualización en la UNC (35.7%), Liderazgo (4%) y Planificación (13%). Se concluyó que, con el SGSI se pudieron mejorar los niveles en cuanto a seguridad ambiental y física, gestión de incidencias, gestión de las comunicaciones, gestión de activos, etcétera.

Monev (2020), realizó la investigación, *Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002*, en la New Bulgarian University, en Sofía, Bulgaria. Las organizaciones que han adoptado la mayoría o todos los requisitos de ISO 27001 a menudo buscan un enfoque para medir la idoneidad de su SGSI para identificar deficiencias y oportunidades de mejora. Además, dado que los componentes integrales del estándar son el mejoramiento perenne, la medición de las eficacias del control de SI y las evaluaciones de cumplimiento, los expertos en SI, pueden beneficiarse del análisis de los resultados obtenidos de evaluar la madurez del SGSI. Por tal motivo, asumió de objetivo, plantear una metodología práctica para la evaluación de la madurez de los requisitos individuales de la norma ISO 27001 y la evaluación general del SGSI. Para ello, primeramente, caracterizaron el contenido de las ISO 27001 e ISO 27002, así como con las pautas de auditoría de la organización ISACA; conocimiento de otras pautas y estándares de SI, para posteriormente diseñar e implementar métricas de SI; implementación y operación del SGSI y, finalmente, evaluar los resultados posteriores a la implementación de dicho SGSI en una compañía constructora de SOFTWARE. cuyo nombre no fue revelado. Los resultados expusieron que, dicha compañía poseía un nivel de madurez promedio de 2.8, lo cual era traducido en un 56.6% en cuanto a cumplimiento de las políticas asociadas a la ISO/ 27001 e ISO/IEC 27002. Se concluyó que, con la implementación de dicha metodología y el SGSI se obtuvieron mejores

puntajes en cuanto a métricas estratégicas y tácticas sobre el desempeño de las estrategias y operaciones de seguridad.

Rodríguez et al. (2020) realizaron la investigación, *Application of ISO 27001 and its influence on the information security of a Peruvian private company*, en la Universidad César Vallejo, en Lima, Perú. En la actualidad, las TI han permitido el desarrollo de las compañías privadas peruanas convirtiendo a sus informaciones en activos esenciales para las mismas, quienes deben evitar que se encuentren expuestas a los piratas informáticos, virus informacionales, ciber espionaje y falencias en infraestructuras son algunos de las problemáticas existentes de las compañías cara a diario por lo que hacen usanza de la ISO/IEC 27001. Por esta razón, asumieron como objetivo, analizar la influencia de la implantación de un SGSI ensimismado en la IS0/IEC 27001 en una empresa privada peruana de un sector no especificado en cuanto a su SI. Para ello, primeramente, analizaron la ISO en mención, luego caracterizaron el caso de estudio en materia de SI haciendo usanza de una lista de cotejo considerando las tres dimensiones de la SI, posteriormente hicieron un comparativo de resultados pre y post test, para finalmente, mediante Prueba de Wilcoxon comparar los rangos de ambas muestras recolectadas. Los resultados expusieron que, en cuanto a los 14 dominios, éstos mostraron mejoramientos porcentuales posteriores a la implementación de dicho SGSI con un coeficiente Z=-3.828, reflejándose en algunos casos como el crecimiento del 100% en algunos dominios. Se concluyó que, que sí existía influencia del SGSI ensimismado en la ISO/IEC 27001 por sobre la SI que existía en dicho caso de estudio peruano.

Bravo y Yoo (2019), realizaron la investigación, *Developing an Information Security Management System for Libraries Based on an Improved Risk Analysis Methodology Compatible with ISO/IEC 27001*, en la Escuela Politécnica Nacional, en Quito, Ecuador. Debido a la incesante evolución de las TI, la SI convirtiese en requerimiento para la totalidad de organizaciones, pues la información es el más relevante de los recursos para la toma decisional acertadas y la aplicación de nuevas estrategias empresariales, no siendo ajenas

las bibliotecas que, actualmente, carecen de protocolos de gestión de la SI porque los administradores no comprenden su importancia, a pesar de que las bibliotecas manejan información sensible que constituyen la materia prima para sus funciones empresariales. Por esta razón, asumieron como objetivo, desarrollar un SGSI para bibliotecas ensimismado en una mejorada metodología de análisis de riesgos compatibilizada con la IS0/IEC 27001. Para ello, primeramente, desplegaron una revisión de la literatura concerniente de las metodologías para la gestión de la SI, posteriormente caracterizaron cada una de ellas, luego diseñaron cada una de las etapas del SGSI fundamentado en la IS0/IEC 27001 y, finalmente implementaron dicho SGSI en la biblioteca de una casa de estudios superiores perteneciente a dicho país ecuatoriano. Los resultados expusieron que, si bien las bibliotecas de este caso de estudio reflejan un nivel de madurez bajo, se puede notar que hay avances en varios dominios como la implementación de políticas de SI, ya que antes de implementar el SGSI, la mayoría de los controles de SI nunca habían sido desplegados, asimismo, el 51% de los controles especificados en la ISO/IEC 27002:2013 se encuentran en la fase “Inicial”, el 10% se encuentra en la fase “Repetible”, el 5% está en la fase “Definida” y el 3% de los controles están en fase “Gestionada”. Se concluyó que, con la implementación del SGSI se ha reforzado la SI de dicho caso de estudio a través de la documentación formal y los procedimientos estandarizados.

Carvajal et al. (2019) realizaron la investigación, *A proposal for the management of the information security applied to a Colombian public entity*, en la Universidad Autónoma de Manizales, en Manizales, Colombia. En la actualidad, la información ha logrado convertirse en un activo de gran relevancia para las diversas unidades organizacionales, llegando al punto de ser catalogada como recurso fundamental para el proceso del giro de los negocios, el cual debe de ser gestionado adecuadamente, buscando la confiabilidad, integridad y disponibilidad de la misma, lo cual no ha sido ajena a las instituciones del ámbito estatal colombiano. Por esta razón, desarrollaron un SGSI para las instituciones públicas colombianas, considerando las directrices preestablecidas por el Ministerio de TI de dicho país y fundamentado en una asociación de la IS0/IEC 27001 e IS0/IEC 27002. Para ello, primeramente, caracterizaron la SI en las

instituciones público-colombianas, luego analizaron las normas mencionadas previamente, después realizaron una identificación de los activos de una entidad estatal colombiana en materia de confidencialidad, integridad y disponibilidad, posteriormente diseñaron el SGSI basado en dichas normas y, finalmente, implementaron dicho SGSI para evaluar los resultados obtenidos a posteriori. Los resultados expusieron que, si bien es cierto existía algún tipo de avance en cuanto a la adopción de los lineamientos asociados a dichas normas, aún eran insuficientes pues existía, verbigracia, 53% de vulnerabilidad en cuanto a la disponibilidad de la información, siendo esta característica la más alta. Se concluyó que, con la implementación de dicho SGSI se disminuyeron los valores en cuanto a las vulnerabilidades existentes en sus niveles extremo, bajo, medio y alto.

Huayamave (2018) realizó la investigación, *Implementation of an information security management system (ISMS) applied to the assets of the construction company Coetecorpza SA, based on the ISO 27002 standard*, en la Escuela Superior Politécnica del Litoral, en Guayaquil, Ecuador. En la empresa caso de estudio perteneciente al sector constructor guayaquileño se carecen de políticas o lineamientos que permitan salvaguardar los accesos y usanzas de sus activos informáticos, y a pesar de que sigue creciendo en cuanto a personal y a estos activos, no se ha logrado implementar un SGSI para dicho fin. Por esta razón, asumió como objetivo, desarrollar un SGSI fundamentado en la ISO/IEC 27002 que permita evitar la materialización de dichos riesgos asociados a sus operaciones en sus activos informáticos. Para ello, primeramente, se hizo una identificación de la infraestructura tecnológica del caso de estudio, luego se tipificaron y valoraron los mismos señalando las vulnerabilidades y amenazas, después se diseñó el SGSI considerando la ISO en mención, considerando plan de tratamientos de riesgos, controles de SI, posteriormente se implementó el SGSI en la compañía guayaquileña y, finalmente, se analizaron los resultados posteriores a dicha implantación. Los resultados expusieron que, con al análisis y evaluaciones de riesgos amenorados, éstos disminuyeron en un 50% y, con el plan de tratamiento de los riesgos, éstos disminuyeron en 47.70%. Se concluyó que, con la usanza correcta del SGSI propuesto inicialmente, se garantizó la SI

de los activos informáticos de la compañía caso de estudio, así como también la continuidad de dicho negocio.

Yoseviano & Retnowardhani (2018), realizaron la investigación, *The use of ISO/IEC 27001:2009 to analyze the Risk and Security of Information System Assets: case study in XYZ, Ltd*, en la Bina Nusantara University, en Yakarta, Indonesia. Las informaciones convirtiesen en los activos más valiosos para la supervivencia de una compañía, institución gubernamental y universidad. La SI adquiere como meta mantener la necesidad, la confidencialidad, y la disponibilidad de la SI, sin embargo, esto no se viene llevando a cabo en XYZ, Ltd que aún no cuenta con pautas relacionadas con el proceso de SI. Por esta razón, desarrollaron un SGSI basándose en la IS0/IEC 27001 con propósito de planificar la gestión de los riesgos asociados a la SI de los activos de dicha compañía naviera taiwanesa caso de estudio. Para ello, primeramente, caracterizaron dicha compañía en materia de activos informáticos, luego analizaron la norma ISO mencionada previamente, después diseñaron el SGSI considerando la ISO/IEC 27001, posteriormente la implementaron en el caso de estudio para, finalmente, evaluar los resultados emanados de dicha implementación. Los resultados expusieron que, en dicha compañía naviera taiwanesa caso de estudio la madurez de la gestión de riesgos de la SI era igual al 71,48%, asimismo, en cuanto al dominio de gestión de activos era débil, con un valor de nivel de madurez del 50,00%. Se concluyó que, las políticas de la empresa relacionada con la gestión de los activos del sistema de SI están disponibles, pero la implementación aún es deficiente o inconsistente, por lo que el SGSI ensimismado en la ISO/IEC 27001 era apropiado para los aspectos de seguridad de los activos, con XYZ Ltd como caso de estudio.

1.3. Teorías relacionadas al tema

1.3.1. Información

Antes de aprender sobre la SI y ver lo importante que es, primero se deben de entender términos como información y seguridad. Cuando se vean estas dos palabras (información y seguridad) se preguntará de qué tipo de tipo de información y por qué hay que protegerla. La verdad es que la gente, sin

saberlo, hace muchas cosas que ponen en riesgo su información personal y, a menudo, no lo saben, ni conocen el impacto de este error (Susanto & Almunawar, 2018).

Según Chopra y Chaudhary (2020) asegurar la información es un gran reto. Esto incluye no sólo la salvaguarda de su información personal, sino también de las organizaciones que almacenan su información personal en sus sistemas. Damos a las organizaciones nuestro consentimiento para que guarden nuestra información y ellas tienen la responsabilidad de protegerla para que no caiga en manos equivocadas. Además, la información de una organización puede ser robada por sus competidores. Los sectores especialmente vulnerables son el bancario, el automovilístico, el de la aviación y de las ventas de telecomunicaciones en ventas de SOFTWARE. y HARDWARE.. El tipo de información que hay que proteger incluye datos personales y datos de la organización.

La información personal incluye los datos bancarios, como los detalles de las tarjetas de cajero automático, los detalles de las transacciones, la información relativa a las contraseñas bancarias y otros detalles personales. Los informes médicos también corren el riesgo de ser robados, ya sea en forma de informes electrónicos o de copias impresas. Los datos de la organización, como los secretos comerciales, los diseños de productos y la información de los clientes, también corren peligro y deben protegerse (Disterer, 2017). Por tanto, tenemos las siguientes definiciones:

Dato

Según Chopra & Chaudhary (2020) los datos pueden ser cualquier hecho en bruto utilizado para tomar decisiones. Los datos se definen como un grupo de números, letras, caracteres especiales en forma de texto, imágenes, grabaciones de voz, etc. Por ejemplo, el número 101034778 puede ser un número de cuenta bancaria, un número de matrícula en una universidad, un número de vehículo, etc. En este ejemplo, el número es un hecho en bruto y por eso se le llama dato.

Información

Según Chopra y Chaudhary (2020) la información son datos que pueden ser procesados para darles un significado. La información puede ser datos relacionados que permiten tomar decisiones. En otras palabras, la información aporta claridad a los datos para poder actuar sobre ellos. La información es conceptualizada como un dato que ya ha seguido un procedimiento previo, habiéndolo procesado en un modo que es significativo para cualquier tipo de receptor y que posee valor percibido o real en las acciones o disposiciones actuales o futuras. La siguiente figura muestra que la información son datos procesados que ofrecen a los usuarios conclusiones significativas.

Figura 3. Procesamiento de datos para obtener información

Fuente. Chopra y Chaudhary (2020).

1.3.2. Características de la Información

Según Chopra y Chaudhary (2020) estas son algunas particularidades de las que dispone la información:

Figura 4, Características de la información

Fuente, Chopra & Chaudhary (2020).

a. Disponibilidad: La información está disponible cuando se requiere (Chopra & Chaudhary, 2020, pág. 3). Verbigracia, si se necesitan unos datos antiguos que se guardaron en la nube hace unos años, debería estar disponible cuando se requiera.
b. Exactitud: La información es correcta. Las decisiones desplegadas se fundamentan en la exactitud de la información (Chopra & Chaudhary, 2020, pág. 3). Verbigracia, un miembro del equipo con experiencia estima el plazo del proyecto y su presupuesto se asigna en función de esa información. Si la información no es correcta, eso puede provocar retrasos en el proyecto o incluso su finalización.
c. Autenticidad: Este término se refiere a la originalidad de la información. No debe haber sido alterada por nadie más (Chopra & Chaudhary, 2020, pág. 3). Verbigracia, si presenta un informe de situación a su cliente, debe ser auténtico u original.
d. Confidencialidad: Sólo las personas que tienen derechos de acceso o están autorizadas pueden ver la información (Chopra & Chaudhary, 2020, pág. 4). Verbigracia, los datos salariales son confidenciales, por lo que solamente aquellos individuos autorizados deben poder acceder a esas informaciones.
e. Integridad: hace relación a la integridad de las informaciones. La información que se guarda debe estar completa y no corrompida (Chopra & Chaudhary, 2020, pág. 4). Verbigracia, usted guarda información importante en la base de datos. Cuando se accede a ella, debe recuperarse de la misma manera que se guardó.

1.3.3. Seguridad de la Información

Según Chopra & Chaudhary (2020) la SI es la práctica de resguardarla del uso no autorizado. La SI es fundamentalmente aquella praxis enfocada en prevenir accesos no debidamente autorizados, las usanzas, las divulgaciones, las interrupciones, las modificaciones, las inspecciones, las destrucciones, los registros u otro debidamente relacionado con la SI, siendo estas informaciones de naturaleza electrónica o física. Las informaciones podrían cristalizarse como cualquier cosa, verbigracia, atacando sus

particularidades previamente mencionadas en el punto anterior, en diversos contextos, tales como, verbigracia, los perfiles empleados en redes sociales tales como Twitter, Facebook, Twitch, Instagram,; informaciones residentes en teléfonos móviles, datos biométricos, etcétera. Por ello es que se considera que, la SI logra concentrar una diversidad de áreas investigativas tales como, verbigracia, criptográficas, informáticas móviles, análisis forenses cibernético, estructuras sociales online como las mencionadas anteriormente, etcétera.

Según Whitman & Mattord (2021) la SI se ocupa de protección de informaciones de accesos desautorizado, formando parte de la gestión informática relacionada con el despliegue de acciones para aminorar amenazas informáticas, implicando con ello también, la prevención y/o aminoramiento de probabilidades relacionadas con accesos desautorizados, usanzas, divulgaciones, interrupciones, eliminaciones, corrupciones, inspecciones, modificaciones, alteraciones y/o grabación que carezcan de autorizaciones respectivas. De darse algún tipo de incidentes de SI, los expertos en temas de SI se involucran en el aminoramiento de los impactos negativos por parte de dichas incidencias, siendo dichas informaciones intangibles o tangibles. Si bien el enfoque principal de cualquier programa de SI es proteger la confidencialidad, la disponibilidad y la integridad de dichas informaciones, mantener la productividad de la organización suele ser una consideración altamente relevante.

Según Peltier (2016) el término SI a menudo se usa como sinónimo de seguridad de TI, pero en sentido estricto va más allá. La SI abarca todo lo que protege los activos de información de una empresa contra amenazas (p. ej., ataques cibernéticos, sabotaje, espionaje y desastres naturales) y el daño resultante a su negocio o reputación. Las regulaciones legales como la Ley de seguridad informática alemana (IT-SiG) o el Reglamento General de Protección de Datos (GDPR por su acrónimo de General Data Protection Regulation) exigen medidas protectoras adecuadas para la información confidencial, que puede estar en formato electrónico, escrito o impreso.

Según Disterer (2017) la SI se refiere a la protección de las informaciones digitales contra los accesos no autorizados, la alteración, el robo y el uso. La SI a menudo se combina con la ciberseguridad. En realidad, sin embargo, la SI difiere ligeramente de la ciberseguridad. Mientras que la ciberseguridad se esfuerza por impedir los accesos no autorizado a los sistemas y redes informáticas, la SI tiene como objetivo proteger la información confidencial que contienen esos sistemas.

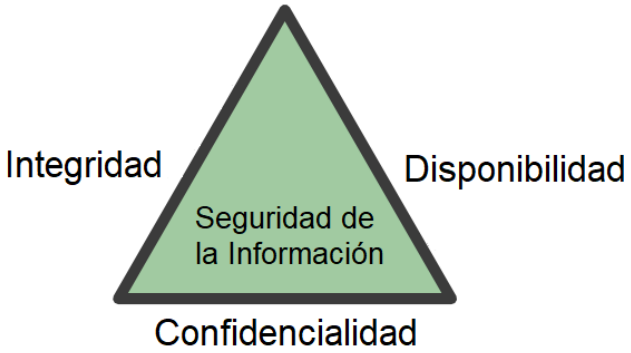


Figura 5 Triada de la Seguridad de la Información

Fuente. Disterer (2017).

Vivimos en una época en la que los dispositivos de usanza electrónica, verbigracia, los computadores portátiles tales como las Chromebook y los equipos celulares, ahora son elementos que forman parte de nuestras necesidades básicas. Guardamos mucha información en nuestros teléfonos inteligentes, ordenadores, tabletas, dispositivos de almacenamiento y en papel y luego solemos tratarlos como registros ordinarios de poca importancia. Pero si esta información llega a manos equivocadas, puede provocar inconvenientes, pérdidas monetarias y problemas de reputación para la organización. Por lo tanto, hay que asegurarse de que todos los documentos importantes están protegidos por contraseña, y hay que evitar el hábito de utilizar las mismas contraseñas para todo.

Según Tunggal (2021) la SI se logra por intermedio de un procedimiento estructurado de administración de amenazas y/o gestión de riesgos, el cual:

a. Identifica las informaciones, los activos concernientes y las amenazas, la vulnerabilidad y el impacto del acceso no autorizado.
b. Evalúa riesgos.
c. Toma decisiones sobre el modo en que debería abordarse y/o atender las amenazas, o sea, evitar, mitigar, compartir o aceptar.
d. Cuando está mitigado, selecciona, diseña e implementa directrices de SI.
e. Supervisa la labor operacional y realiza configuraciones con propósitos de abordarse con cualquier tipo de cambios, eventualidades, problemáticas o mejoramientos nuevos

1.3.4. Tipos de Seguridad de la Información

Al considerar la SI, hay muchos subtipos que deberían conocer. Estos subtipos cubren tipos específicos de información, herramientas utilizadas para salvaguardar informaciones y dominios donde la información necesita protección. Según Cassetto (2019) existen siete (07) tipos de SI los cuales se conceptualizaron del modo siguiente:

a. Seguridad de aplicaciones

   Este tipo de SI logra está enfocada en la salvaguarda y protección de la SI de las API, es decir, de las interfaces y de las aplicaciones. Aquí es que emplea maniobras de modo que se logre la prevención, detección y corrección de fallas u otro tipo de amenazas a la interna de dichos tipos de SOFTWARE.. Verbigracia, la SI de este tipo de SOFTWARE.s está fundamentada en un conjunto especializado de herramientas que protegen, escanean y hacen pruebas de monitoreo a dichos SOFTWARE.s, dejando en evidencia vulnerabilidades existentes en las mismas y en aquellos componentes que lo circundan. La SI de dichos SOFTWARE.s es aplicado a aquellas ya listo y que están en usanza, como de aquellas que se encuentran en fase de construcción, resaltando la importancia de la protección de las mismas (Cassetto, 2019).

b. Seguridad de infraestructuras

Este tipo de SI está enfocada en la salvaguarda y protección de los elementos constituyentes de las infraestructuras, verbigracia, redes informáticas, lo conjuntos de laptops en los que destacan servidores, dispositivos empleados por los clientes como las Chromebook, dispositivos celulares y Data Centers, ya que, entre dichos elementos constituyentes, como bien se mencionaba, existen conectividades entre ellos, los mismos que pudieran ser puestos bajo amenazas de no tomarse en consideración la precaución apropiada para este tipo de situaciones. Ante ello es que, es menester la minimización de riesgos asociados, aislando a dichos elementos constituyentes de dichas amenazas y riesgos, sin evitar la comunicación que sucedan en este tipo de redes e infraestructuras sistémicas (Cassetto, 2019).

c. Seguridad en la nube

Este tipo de SI está enfocada en la salvaguarda y protección de la SI pero de aquellas infraestructuras y aplicaciones que se encuentran alojadas de manera física pero que, de cualquier modo se encuentran almacenados de manera virtual en algún servidor especializado localizado en cualquier parte de nuestro planeta, agregando herramientas y protecciones suplementarias que permitan poseer un enfoque de cuidado en cuanto a la SI. Este tipo de SI toman en consideración los controles restringidos y establecen todo tipo de políticas limitantes en cuanto a vulnerabilidades y accesibilidades propias de este tipo de contextos de informáticas en las nubes (Cassetto, 2019).

d. Criptográfica

Este tipo de SI está enfocada en la salvaguarda y protección de la SI mediante la usanza de encriptaciones que oscurecen los contenidos de los que se disponen, logrando así que las informaciones estén disponibles tan solamente para aquellos usuarios que dispongan de claves criptográficas correctas para la desencriptación de las

informaciones, logrando que se totalmente ininteligible para aquellas que carezcan de las claves correctas. Lo que se busca es no ser vulnerables en cuanto a alteraciones, modificaciones, eliminación de informaciones y esto se puede lograr mediante, como bien indicábamos, herramientas criptográficas, verbigracia, cadenas de Blockchain, algoritmos criptográficos tales como AES (por su acrónimo en inglés de “Advanced Encryption Standard”), etcétera (Cassetto, 2019).

e. Respuesta al incidente

Este tipo de SI está enfocada en la salvaguarda y protección de la SI mediante la usanza de herramientas y procedimientos que identifican, investigan y dan respuesta a diversas eventualidades dañinas, reduciendo/eliminando significativamente los daños originados a causa de ataques hacia la SI, verbigracia, robos de informaciones, etcétera, en las cuales sobresale distinguidamente, los planes de respuestas a incidentes denominados IRP (por su acrónimo en inglés de Incident Response Plan), los mismos que caracterizan responsabilidades y funciones en cuanto a la gestión de estos incidentes de SI, brindando directrices que salvaguarden la SI haciendo usanza de medidas protectoras antes dichas eventualidades y amenazas (Cassetto, 2019).

f. Gestión de vulnerabilidades

Este tipo de SI está enfocada en la salvaguarda y protección oportuna y completa de la SI mediante la usanza de directrices que reduzcan las amenazas de dicha SI y que son propias de los SOFTWARE.s. Este tipo de praxis se encuentran fundamentadas en escáneres de seguridad, auditorías en SI, pruebas criptográficas, etcétera; los cuales pudiesen ser sistémicos, siguiendo directrices específicas, garantizando los descubrimientos oportunos de riegos asociados a la SI. Asimismo, existen varios métodos de este tipo, no siendo ajena la caza de riesgos, en los que, se investigan los SOFTWARE.s en tiempos

reales con propósitos de lograr la identificación de oportunísima de vulnerabilidades potenciales (Cassetto, 2019).

g. Recuperación de desastres

Este tipo de SI está enfocada en la salvaguarda y protección oportuna y completa de la SI mediante la usanza de estrategias recuperativas de informaciones, que han sido dañadas por diversos contratiempos, verbigracia, de los secuestros de informaciones, más comúnmente llamados “Ransomware”, de cualquier desastre natural o cualesquiera de las fallas en los SOFTWARE.s, etcétera. Aquí, en este tipo de estrategias se logra dar explicación acerca de la recuperabilidad de las informaciones, archivos, datos empresariales de las organizaciones, restauraciones de SOFTWARE.s y, también, de reanudaciones de las praxis organizacionales de acuerdo con el giro del negocio. Con estas estrategias de minimización de riesgos asociados a la SI, se mantienen las operaciones organizacionales contemplando tiempos de inactividad mínimos (Cassetto, 2019).

1.3.5. Sistema de Gestión de Seguridad de la Información

Según Chopra & Chaudhary (2020) un SGSI es un sistema de gestión documentado que está constituido por un listado de controles de SI que protegen la disponibilidad, integridad y confidencialidad de bienes intangibles y tangibles frente a amenazas y vulnerabilidades. Al crear, implementar, gestionar y mantener un SGSI, las organizaciones logran salvaguardar sus datos confidenciales, personales y confidenciales para que no se vean comprometidos.

Por otro lado, Szczepaniuk et al. (2020) conceptualizaron al SGSI como es una conjunción de procedimientos, praxis, directrices y políticas que permiten la gestión sistémica de informaciones con alto valor confidencial y de las cuales poseen y disponen las organizaciones o entidades. El propósito de dichos sistemas SGSI son los de lograr la minimización de amenazas/riesgos logrando, para beneplácito de las organizaciones,

garantía en cuanto a las continuidades de los giros de los negocios limitando proactivamente los impactos de alguna brecha en cuanto a SI. Un SGSI comúnmente logra el abordaje del proceder y procedimientos prácticos y empíricos desplegados por los colaboradores de una específica compañía, así como las informaciones, datas y las tecnologías. Podría estar dirigido a un target específico de informaciones, verbigracia, informaciones relevantes por parte de las clientelas, o puede implantarse de modo holístico convirtiéndose en elemento constituyente de la compañía, más específicamente de sus culturas organizacionales propias con las que deberían de contar.

Asimismo, Peltier (2016) reveló que, un SGSI define políticas, métodos, procesos y herramientas para certificar una SI sostenible en empresas y agencias gubernamentales. Esto incluye la introducción de procedimientos específicos y la implementación de medidas organizativas y técnicas que deben ser controladas, monitoreadas y mejoradas continuamente. El objetivo es garantizar, más allá del departamento de TI, márgenes adecuados de protección de la confidencialidad, disponibilidad e integridad de las informaciones dentro de toda la compañía o el alcance definido. Por lo tanto, el SGSI proporciona la base para implantar sistemática la SI dentro a la interna de las compañías y para certificar la ejecución de estándares de SI. Las amenazas potenciales afines con la SI se identifican, analizan y mitigan, haciéndolas controlables.

Desde la perspectiva de Raza (2019) un SGSI es una hoja de ruta que involucra controles, directrices, pautas y políticas que gestionen la SI y aquellas amenazas y riesgos en un modo sistémico y en la totalidad de su empresa: SI. Dichas directrices de SI podrían alinearse con estándares de SI que gozan de mayor frecuencia o aquellos que se encuentran con mayor enfoque en sus industrias en las que despliegan sus actividades. Verbigracia, ISO 27001, la cual es una agrupación sistémica de pautas, directrices y especificaciones que logran, a detalle, especificar los modos en que deberían de crearse, administrarse e implementarse controles y políticas de SGSI. Dicho estándar no pone sobre la mesa, ni mucho menos puntualiza de manera específica praxis determinadas a seguir; en cambio, lo que sí hace es suministrar una guía completamente concisa sobre la puesta en praxis de adecuadas e idóneas estrategias en cuanto al SGSI que se pretende implantar.

Figura 6. Proceso de formación de un riesgo de SI

Fuente. Raza (2019).

1.3.6. Beneficios de SGSI

Un SGSI es básicamente una lista de procedimientos y sistemas para evitar que la información se filtre a través de ciberataques, hackeos o robos. Garantiza la completitud y puesta en marcha de un conjunto de directrices/leyes y se centra en tres factores clave de información: confidencialidad, integridad y disponibilidad (Chopra & Chaudhary, 2020).

Según Proença & Borbinha (2018) las implementaciones de SGSI traen muchos beneficios a aquellas organizaciones que logran implantarlas. A continuación, se destacan los beneficios que estos autores revelan acerca de implementar eficientemente un SGSI:

a. Da seguridad a toda tu información

   Un SGSI proporciona seguridad a toda su información, ya sea propiedad intelectual, secretos empresariales, información y datos personales. No importa en qué formato se encuentre, ya sea en formato digital o impreso. El lugar de almacenamiento tampoco juega ningún papel (Proença & Borbinha, 2018).

b. Mejora la defensa contra ciberataques

   Con la implementación del SGSI, aumenta la resiliencia de su organización frente a los ciberataques (Proença & Borbinha, 2018).

c. Reduce los costos relacionados con la seguridad

   SGSI adopta un enfoque de evaluación y análisis de riesgos. Esto permite a las organizaciones reducir los costos que invierten en agregar capas y capas de tecnología defensiva que podrían no funcionar en absoluto (Proença & Borbinha, 2018).

d. Mejora la cultura laboral de la empresa

   El enfoque holístico estándar de SGSI no solo cubre el departamento de TI sino toda la organización, incluidas las personas, los procesos y las TI. Esto permite a los empleados comprender los riesgos de seguridad e incluir controles de SI como parte de su actividad rutinaria (Proença & Borbinha, 2018).

e. Salvaguardar confidencialidad, integridad y disponibilidad de las informaciones. Un SGSI eficiente ofrece un conjunto de políticas, control técnico y físico para ayudar a proteger la confidencialidad,

integridad y disponibilidad de los datos de la organización (Proença & Borbinha, 2018).

f. Brindar protección a toda la organización

   Un SGSI no solo protege a su organización de los riesgos de SI basados en la tecnología, sino que también protege a la organización de empleados poco informados o ineficientes (Proença & Borbinha, 2018).

g. Marco administrado centralmente

   Un SGSI proporciona un marco sistemático para proteger a su organización de los riesgos basados en la seguridad. Todo esto se puede administrar en un solo lugar (Proença & Borbinha, 2018).

h. Proteger contra los riesgos de seguridad en evolución

   Un SGSI se adapta continuamente a los riesgos de seguridad en evolución. Esto, por tanto, reduce los riesgos evolutivos tanto en el entorno como en la organización (Proença & Borbinha, 2018).

1.3.7. Estándares Internacionales

Las informaciones y los sistemas que a dichas informaciones manejan son el motor y motivo, dicho sea de paso, el más trascendental en la actualidad para las compañías de cualquier índole. Particularmente, las transferencias de informaciones que, a diario se van dando con mayor asiduidad, con informaciones internos e interempresariales y el empleo masivo de redes abiertas aumentan aquellos riesgos a los que están expuestos dichas informaciones, las TICS y los SI. Para lograr el aminoramiento de amenazas y riesgos y, adicionalmente a ello, impedir deterioros y perjuicios a las diversas compañías es que, deberían procurarse los cuidados necesarios con propósitos de certificar una adecuada SI (Kilian, 2007). Cuando de proteger y salvaguardar los SI y las informaciones, es ahí que estos estándares ISO, verbigracia, ISO/IEC 27000, ISO/IEC 27001 e ISO/IEC 27002 son aquellos estándares de dicha familia de ISO que brindan metas

relacionadas con la supervisión, monitoreo, controles, requisitos, directrices y lineamientos, con los cuales las compañías pueden alcanzar adecuados niveles de SI. Al llevarlo a la praxis, la ISO/IEC 27001 admite que las compañías obtengan la certificación en concordancia el estándar, por lo que la SI podría documentarse como aplicada y administrada severamente de acuerdo con un estándar organizacional reconocido de manera amplia mundialmente.

De disponer de la certificación ISO/IEC 27001, las compañías verifican el acatamiento real de estándares de SI conocidos y aceptados y, por lo tanto, incita a la confianza por parte de las diversas clientelas. Asimismo, una verificación del acatamiento de un estándar mundialmente reconocido logra el aminoramiento del riesgo de tener que acatar sanciones u otro tipo de pago, a modo de compensación, de modo que sea producto de enfrentamientos judiciales, ya que se pueden contrarrestar requisitos legales como el abastecimiento de acuerdo con “estado de corazón” y con “debido cuidado y diligencia”, con el cumplimiento de las normas (Calder, 2011).

Según Disterer (2017) los estándares se originan mediante la construcción de especificaciones totalmente detallados, considerando sus características genuinas de las que dispone un servicio o producto, cuyas especificaciones han sido desplegadas por un grupo de jueces expertos de diversas compañías y entidades de naturaleza científica. Estos estándares son representación de aquellos consensos existentes acerca de las particularidades que deben de poseer los antes mencionados, verbigracia, características de fiabilidad, seguridad y calidad, las cuales deberían de ser seguidas y aplicadas durante períodos de tiempos prolongados y, los cuales deberán de ser, primeramente, documentados y, posteriormente, publicados. Esta construcción de normas internacionales ISO tiene como meta la de ser soporte para las organizaciones o personas en cuanto a los procesos adquisitivos de servicios o productos, dependiendo de sus necesidades. Los agentes provisores, cuya función es proveer de dichas prestaciones de servicios o entregas de productos, podrían alcanzar

mayores niveles en cuanto a sus reputaciones de contar con certificaciones ISO, ya que demuestran el acatamiento de dichos estándares.

ISO, tal y como se mencionaba previamente en párrafos anteriores, es un organismo instituido en 1946 y respaldada por más de +150 naciones a nivel mundial; convirtiéndose así en el principal ente regulador y certificador de normas internacionales. Los estándares ISO/IEC 27000 e ISO/IEC 27002 han sido desarrollados en colaboración con la IEC (por su acrónimo en inglés de “Comisión Electrotécnica Internacional”), el cual también es un ente de categoría internacional en cuanto a estándares globales en el sector de las TIC y las mismas que deberán de encontrarse correlacionadas con la electrónica.

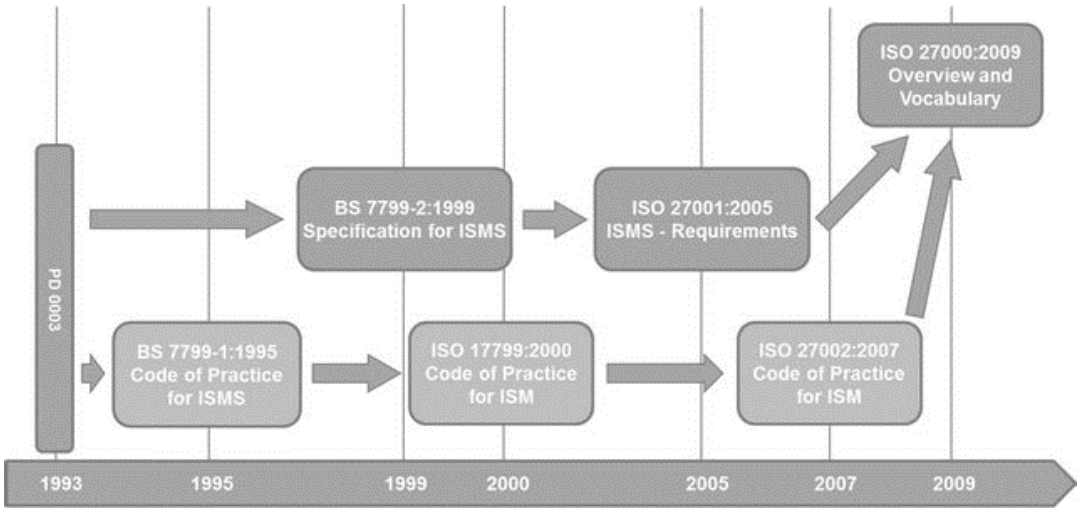


Figura 7. Desarrollo de las normas IS0/IEC 27000, IS0/IEC 27001 e IS0/IEC 27002

Fuente. Disterer (2017).

1.3.7.1. ISO 27000

La norma ISO/IEC 27000 se publicó a finales del 2009 con propósitos de suministrar visión holística del grupo familiar de normas ISO27K y un pilar conceptual común (ISO, 2013). En el apartado “Términos y condiciones” se definen y diferencian 46 términos básicos de SI. El significado de la SI y el compromiso sistemático con los aspectos de SI se derivan del riesgo que corren las compañías de las cuales, sus giros y operaciones del negocio penden, en demasía, del procesamiento de las informaciones y

las cuales complejas e interconectadas infraestructuras de TICS son ampliamente endebles a cualquier tipo de interrupciones, falencias y fallas.

Del mismo modo como suceden en otras normas de TIC, el grupo familiar de normas ISO 27K se refiere llanamente al ciclo “Planificar-Hacer-Verificar-Actuar” (Ciclo denominado PDCA por su acrónimo en inglés), muy bien distinguido por la clásica gestión de la calidad o catalogado como el Ciclo de Deming (conceptualizado en la Figura 8), el cual hace ampliamente reiteración en el requerimiento de la disposición a los procesos, asimismo como en la unificación de la prospección de las labores operacionales y la constante comprobación de la ejecución conforme a la planificación (Disterer, 2017).

Figura 8. Ciclo PDCA en la ISO/IEC 27000

Fuente. ISO (2013).

En la fase de planificación de un SGSI se definirán aquellos requerimientos con propósitos de salvaguardar las informaciones y los SI, además, se identificarán y evaluarán riesgos, con lo que, a posteriori, se podrán construir directrices y políticas adecuadas con propósitos de aminorar drásticamente, y para bien de las compañías, las amenazas/riesgos. Estas directrices se implementarán, a priori, mientras se desplieguen y lleven a cabo las labores operacionales. Las documentaciones generadas a través de los monitoreos continuos de las

labores operacionales serán empleadas con propósitos de alcanzar mejoramientos y para un mayor desarrollo del SGSI.

1.3.7.2. ISO 27001

La norma ISO/IEC 27001 se publicó a principios del 2005 con la etiqueta "Tecnologías de la Información - Técnicas de seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos". Esta norma, la cual se encuentra demarcada en cuarenta y dos (42) hojas logra describir aquellos requerimientos que debería de acatar y tomar en consideración un SGSI para lograr el pronto certificado que atestigüe su conformidad con dicho estándar. Vale mencionar que, dicho estándar está ensimismado y enfocado en compañías, las cuales no se ven separadas por el ámbito en el que se desempeñan, sino que, por el contrario, podrían ser de cualquier sector empresarial, sin ser limitante el tamaño de las mismas. Empero, existen ciertas incertidumbres acerca de la competencia para, verbigracia, las MYPES (Barlette & Fomin, 2008). La norma no estipula decretos concretos para el acatamiento oportuno de requerimientos, sino que, por el contrario, deberían ser desarrolladas e implementadas de forma determinada para las diversas compañías. Los requerimientos en cuanto a certificaciones relacionados con la ISO/IEC 27001 se aclaran por intermedio de la construcción de conceptualizaciones y términos y, las cuales se complementan con documentación acerca de la labor implantadora a la interna de dicha ISO.

El corazón de la ISO/IEC 27001 es requerimiento indiscutible para la labor prospectiva, implantadora, operacional, monitoreo continuo y mejoramiento del SGSI orientado a procesos. Dicha orientación debería estar alineada, tal y como se mencionaba previamente, con el Ciclo de Deming (conceptualizado anteriormente en la Figura 8). Las coberturas y alcances del SGSI deberían estar conceptualizados para su prospección e implantación. Se deberían identificar y evaluar los riesgos (ISO, 2013) y se deben definir metas controladoras para las informaciones y los SI. De ellos deben derivarse las medidas idóneas con propósitos de

salvaguardar y/o proteger las labores operacionales. Dicho estándar, más específicamente en su anexo A, enumera y así se estipulan expresamente una totalidad de treinta y nueve (39) objetivos de control y ciento treinta y cuatro (134) directrices para el control y administración de la SI. Los objetivos de control se encuentran sub divididos jerárquicamente en dominios. Estos se encuentran especificados más detalladamente en el estándar ISO/IEC 27002 (ISO, 2013).

Según Disterer (2017) se debe desarrollar una capacitación adecuada para la implementación con propósitos de impulsar las directrices estipuladas y establecerlos, y coadyuvar a la generación de conciencia de dicho requerimiento. La completitud y puesta en marcha de los procedimientos deben ser monitoreados inagotablemente en todas sus dimensiones. Dichas directrices deberían verificarse y mejorarse en el trámite mismo del mejoramiento continua y las amenazas de seguridad deberían identificarse y evaluarse para acrecentar perenemente las eficacias y las eficiencias de cualquier SGSI (ISO, 2013).

Los requerimientos que deben ser aplicados a los informes del SGSI son descritos, ampliamente, en dicho estándar mediante la disposición de contenidos esenciales, documentaciones necesarias, no dejando de lado también, los detalles y los aspectos relacionados con el seguimiento de gestionar los informes, verbigracia, los mencionados por Disterer (2017):

a. Procedimientos de aprobaciones y cambios
b. Monitoreo de las versiones
c. Pautas para derechos en cuanto a la protección de los accesos y de los accesos mismos
d. Especificaciones para sistemas de archivo

Son enumeradas los deberes de los altos directivos en la totalidad de los estados pertenecientes al Ciclo de Deming (ISO, 2013). Logran comprender la designación e implementación de políticas de seguridad,

establecimiento de responsabilidades y roles, la contratación y preparamiento de los recursos humanos y materiales necesarios, asimismo de las decisiones acerca de la administración de amenazas/riesgos.

El mejoramiento y el perfeccionamiento adicionales por parte del SGSI deben implementarse continuamente, en función de las políticas de SI, el en función de los registros y, finalmente, en función de la valuación de las labores operacionales, las pruebas y sus resultados obtenidos y, aquellos resultados producidos por las directrices para el mejoramiento propuestos inicialmente. Asimismo, las mejoras y los desarrollos adicionales deberían ser impulsados por intermedio de auditorías periódicas internas. La implementación correcta de las políticas de SI, así como de las idoneidades y exhaustividades deberían ser garantizadas por intermedio de exámenes con periodicidad anual por parte de la dirección (ISO, 2013).

1.3.7.3. ISO 27002

Los requisitos que se codifican dentro de la ISO/IEC 27001 son sumamente ampliados y explicados en la ISO/IEC 27002 en modo informe. Fue publicado inicialmente a principios del 2000, bajo la conceptualización de “ISO 17799”, bajo el título “Tecnología de la información - Técnicas de seguridad - Código de prácticas para la Gestión de la Seguridad de la Información”. Posteriormente, durante el segundo semestre del 2007, esto fue revisado y alineado con el grupo familiar 27K y la designación terminó modificándolo hasta dejarlo como ISO/IEC 27002. Con la inventiva de ISO/IEC 27002, las comunes praxis, menudamente llamadas como ideales praxis operacionales, fueron ofrecidas a manera de métodos y procedimientos comprobados en las praxis operacionales, que podría ser adaptables a requerimientos y especificaciones previamente determinadas de las unidades organizacionales. Para explicar la importancia de la SI para las unidades organizacionales, se exponen. Se describen los pasos necesarios para la identificación y valuación de los riesgos de SI con propósitos de establecer

el requisito de proteger la información y los sistemas de información (ISO, 2013). La construcción continua de ISO/IEC 27002 se fundamenta en la puesta en sociedad de ISO 27001, en la que se explican con más detalle los treinta y nueve (39) objetivos de control debidamente enunciados numéricamente en el anexo de ISO/IEC 27001. A estos objetivos se asignan un total de ciento treinta y cuatro (134) medidas.

Las pautas fundamentales para garantizar la SI deberían ser predefinidas y ampliamente detalladas en modo de directrices de SI por la dirección de la unidad organizacional. La propagación y posterior implantación de estas políticas a la interna de la compañía serviría, asimismo, también para la enfatización de la relevancia de la SI y las atenciones de la gestión para estos temas. La SI debe estar anclada organizacionalmente en la compañía para que las medidas de SI puedan ser promovidas y establecidas de modos eficientes. Por lo expuesto, deberían definirse roles y obligaciones y, particularmente, deben especificarse los deberes para la mantenibilidad de las reglas y la confidencialidad en torno a las comunicaciones con partes externas (proveedores, clientelas, directivos, etcétera).

Las amenazas concernientes a la SI también, en muchísimas ocasiones, originadas por vulnerabilidades que muestran los SOFTWARE.s TICS. Aquí se debe suponer que, alrededor de +50% de la totalidad de ataques cibernéticos son principiados por individuos pertenecientes a la interna de las compañías; empero, algún otro gran porcentaje también será principiada por operaciones en conjunto por el mismo personal de la interna y personal extrínseco, tercero u otro no perteneciente a las compañías (Richardson, 2008). Debido a que el personal a la interna de las compañías pudría emplear conocimientos internos (acerca de procedimientos intrínsecos, interrelaciones sociales, carencia, debilidades, hábitos, puntos débiles, oportunidades, etcétera) con propósitos de suministrar informaciones para los ataques que atenten contra la SI, deberían considerarse que poseen mayores potenciales de

daños y éxitos (D'Arcy & Hovav, 2007). Las amenazas apropiadas deberían tenerse en consideración con directrices personales tales como reclutamientos, selecciones y asignaciones. Así, verbigracia, las autorizaciones de accesos de algún/os usuarios deberían encontrarse restringidas en cuanto a medidas necesarias con propósitos de desplegar las labores que se le asigna. Con variabilidades en cuanto a sus obligaciones, compromisos, deberes o puestos de trabajo, las facultades en cuanto a los accesos deberían ser adaptadas en derivación y si se despide al capital humano de las compañías, dichas facultades deberían ser revocadas, preferentemente, de inmediato.

Deben proporcionarse directrices de seguridad física para salvaguardar las infraestructuras de entradas, accesos, robos, daños y destrucción no autorizados. Para certificar el despliegue adecuado y correcto de los SOFTWARE.s de TI, las operaciones de rutina ideales deben documentarse en un manual (procedimientos operativos estándar). Asimismo, se deben especificar y documentar los procesos y procedimientos ante circunstancias excepcionales, retrasos, cortes, fallas o eventos catastróficos. Los cambios técnicos u organizativos deben comprobarse en busca de posibles efectos en las operaciones de los sistemas de TI antes de implementarlos. Asimismo, los incidentes de SI deben ser documentados, analizados y evaluados para posibles o esenciales mejoras al sistema de SI. Por último, se deben implementar las medidas adecuadas para cumplir con los requisitos de cumplimiento. En particular, los derechos, ya sean éstos, de autores y los de explotación.

1.3.8. ISO 27001 vs. ISO 27002: ¿Cuál es la diferencia?

Cualquier persona interesada en la SI habrá encontrado la norma ISO 27001, el estándar universal que conceptualiza las mejores prácticas para un SGSI. Empero, es posible que no esté tan familiarizado con ISO 27002, la cual es una norma complementaria que brinda asesoramiento sobre cómo implementar los controles de SI enumerados en el Anexo A del estándar IS0/IEC 27001 (Disterer, 2017). Aunque la IS0/IEC 27001 es el estándar de

mayor conocimiento, y el que las organizaciones certifican, ninguno puede considerarse de forma aislada.

En primer lugar, la ISO 27001 es el marco central de la serie ISO 27000, que es una serie de documentos relacionados con varias partes de la gestión de la SI. El estándar contiene los requisitos de implementación para un SGSI. Estos son esencialmente una descripción general de todo lo que debe hacer para lograr el cumplimiento. Esto es particularmente útil al comienzo de un proyecto, o si está buscando consejos generales, pero no puede comprometerse con un proyecto de implementación a gran escala (Irwin, 2021).

Por otro lado, la ISO 27002 es una norma complementaria que se centra en los controles de SI que las organizaciones pueden optar por implementar. Estos controles se enumeran en el Anexo A del estándar IS0/IEC 27001, que es a lo que a menudo verá que se refieren los expertos en SI cuando analizan los controles de SI. Sin embargo, mientras que el Anexo A simplemente describe cada control en una o dos oraciones, ISO 27002 dedica un promedio de una página por control. Esto se debe a que el estándar explica cómo funciona cada control, cuál es su objetivo y cómo puede implementarlo (Irwin, 2021).

Según Irwin (2021) existen tres (03) diferencias principales entre la ISO 27001 y la ISO 27002:

Detalle	Si la ISO 27001 fuera tan detallada como la ISO 27002, sería innecesariamente larga y complicada. En cambio, proporciona un resumen de cada aspecto de un SGSI, con consejos específicos que se encuentran en estándares adicionales. ISO 27002 es sólo uno de ellos. Por ejemplo, ISO 27003 cubre la guía de implementación del SGSI e ISO 27004 cubre el seguimiento, las mediciones, los análisis y las evaluaciones del SGSI.
Certificación	Puede certificarse según ISO 27001 pero no según ISO 27002. Esto se debe a que ISO 27001 es un estándar de gestión que proporciona una lista completa de requisitos de cumplimiento, mientras que los estándares complementarios como ISO 27002 abordan un aspecto específico de un SGSI.
Aplicabilidad	Una cosa clave a tener en cuenta al implementar un SGSI es que, no todos los controles de SI se aplicarán a su organización. ISO 27001 lo deja claro, especificando que las organizaciones realizan una valuación de riesgos para identificar y priorizar las amenazas a la SI. La norma ISO 27002 no menciona esto, por lo que si tuviera que tomar la norma por sí sola, sería prácticamente imposible averiguar qué controles debería adoptar.

Figura 9. Diferencias entre ISO 27001 vs. ISO 27002

Fuente. Irwin (2021).

La ISO 27001 y la ISO 27002 tienen diferentes objetivos y serán útiles en diferentes circunstancias. Si se está comenzando con el estándar o se está planeando como marco de implementación de SGSI, entonces la ISO 27001 es ideal. Posteriormente, se debe consultar la norma ISO 27002 una vez que se haya identificado los controles que se implementará para obtener más información sobre cómo funciona cada uno (Irwin, 2021).

1.3.9. ISO 27002: Sistema de Gestión de Seguridad de la Información

Según Chopra & Chaudhary (2020) el grupo BSI (por su acrónimo de British Standards Institution) publicó originalmente la norma denominada BS 7799.

Fue redactada por el DTI (por su acrónimo de Departamento de TI) del gobierno británico y, el cual se componía de diversas partes.

La primera parte, la cual es contenedora de las mejores praxis para gestionar la SI, fue inspeccionada a finales de la década de los 90. Fue adoptada en 2000 por la ISO como ISO/IEC 17799, titulada “Tecnologías de la Información: Código de prácticas para la gestión de la seguridad de la información”. La norma IS0/IEC 17799 fue ampliamente revisada a mediados del 2005 e incorporada al grupo familiar ISO 27K conceptualizándola como IS0/IEC 27002 a mediados del 2007.

La segunda parte de la norma BS.7799 se publicó en 1999 con el título “Sistema de Gestión de la Seguridad de la Información”. Dicha BS 7799-2 se centraba en cómo implantar un SGSI. Posteriormente, se actualizó para abarcar el estudio y la gestión de riesgos y se denominó ISO/IEC 27001:2005.

La última versión publicada de la norma del SGSI es la BS ENG ISO/IEC 27001:2017. La versión ISO del estándar (2013) no se ha visto afectada por la publicación de 2017 y los cambios no introducen ningún requisito nuevo.

Según Chopra y Chaudhary (2020) un SGSI es una conjunción de procedimientos y políticas para mejorar el riesgo debiéndose seguir los siguientes pasos:

a. Definir una política de SI: El objeto principal de una política de SI es definir lo que la alta directiva pretende conseguir con sus medidas de SI. Esto indica a la dirección quién es responsable de qué elementos, con expectativas, funciones y responsabilidades claras (Chopra & Chaudhary, 2020).
b. Definir el alcance del SGSI: El alcance es un factor importante de acuerdo con la declaración de aplicabilidad. El alcance debe abarcar la ubicación de la auditoría de SI, las funciones implicadas en la auditoría,

así como el personal y los activos implicados (físicos, de SOFTWARE. y de información). Debe definir claramente cualquier exclusión. Verbigracia, digamos que está realizando una auditoría para una división de SOFTWARE. que incluye los departamentos de RR.HH., TI y administración (sin incluir ventas y marketing). En este caso, su documento de alcance debe definir claramente las ventas y el marketing como exclusiones (Chopra & Chaudhary, 2020).

c. Realice una valuación de riesgos: La valoración de dichas amenazas es apartado esencial de cualquier compañía y la norma ISO 27001 se centra en la planificación basada en el riesgo. La evaluación o análisis se basa en el registro de activos. En palabras sencillas, hay que identificar qué incidentes pueden ocurrir y determinar la mejor manera de hacer evaluaciones de riesgo basadas en los activos. Esto puede hacerse creando un grupo de discusión, celebrando una sesión de lluvia de ideas o entrevistando a los propietarios de los activos (Chopra & Chaudhary, 2020).
d. Gestionar los riesgos identificados: Al gestionar los riesgos identificados, es importante utilizar el documento del plan. Cuando se identifica un riesgo, debe registrarse en el registro de riesgos y clasificarse en función del método de gestión de amenazas/riesgos de la compañía. Los propietarios de los activos deben ser responsables del riesgo de sus activos; sin embargo, la norma no dice cómo tratar el riesgo (Chopra & Chaudhary, 2020).
e. Seleccione las metas de control y aquellos controles que deben aplicarse: Puesto que, hay una larga lista de controles en la norma ISO 27001 (Chopra & Chaudhary, 2020).
f. Prepare una declaración de aplicabilidad: Una declaratoria específica de aplicabilidad en la norma ISO 27001 también se denomina documento SOA. Es uno de los documentos más importantes del sistema y las organizaciones suelen dedicar más tiempo a su preparación. Este documento le dirá cómo implementan los controles. También identifica las inclusiones y exclusiones (Chopra & Chaudhary, 2020).

Este estándar mundial suministra aquellos requerimientos con propósitos de lograr el establecimiento, implantación, mantención y mejoramiento perenne de un SGSI. Un SGSI es un enfoque sistémico para la gestión de las informaciones sensibles de las compañías de manera que permanezcan seguras. Adoptar un SGSI es una decisión estratégica, ya que incluye a los colaboradores internos, las labores procedimentales y los SOFTWARE.s/SI. Podría coadyuvar cualquier tipo de compañía, gran, media y pequeña, sin distinción del número de sus colaboradores, sin siquiera distinguir una separación por sector comercial dado que no distingue la separación en mención, de modo que coadyuva a la mantenibilidad segura de sus activos relacionados con la SI.

La ISO 27001 no es prescriptiva. No le dice qué tipo de tecnología debe utilizar para proteger su red o con qué frecuencia debe realizar copias de seguridad, verbigracia. Esas decisiones deben ser tomadas por su organización. Imagínese que la norma prescribe que hay que hacer una copia de seguridad del sistema cada 24 horas. ¿Cómo sabe que ese es el intervalo adecuado para su organización? Las organizaciones tienen diferentes necesidades y diferentes tipos y cantidades de datos. Verbigracia, empresas como Facebook, Google, LinkedIn, etc. generan *petabits* de datos cada día. El ritmo de cambio de sus datos es muy rápido y necesitan una copia de seguridad en tiempo real (o si no en tiempo real, al menos cada hora). Por el contrario, hay organizaciones pequeñas para las que el ritmo de cambio de los datos es muy lento. Su intervalo de copia de seguridad podría ser fácilmente una vez a la semana (Chopra & Chaudhary, 2020).

Según Chopra & Chaudhary (2020) los SGSI se apoyan en tres pilares principales, denominados la tríada CID:

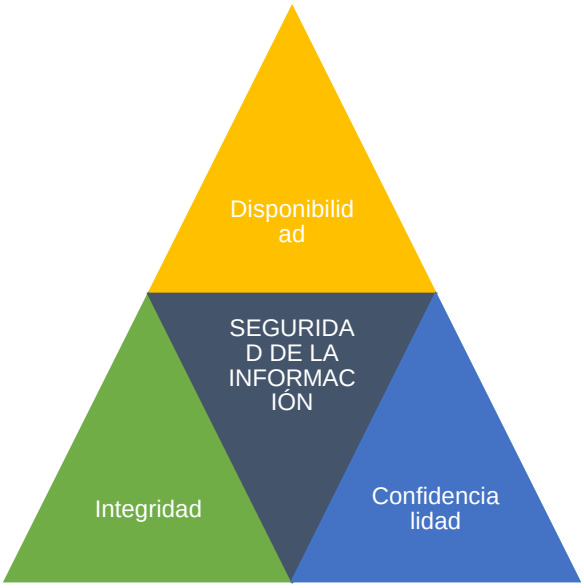


Figura 10, Triada de la Seguridad de la Información

Fuente. Chopra y Chaudhary (2020).

a. Confidencialidad

Según Chopra & Chaudhary (2020) la confidencialidad conceptualiza la protección de las informaciones para que no puedan acceder a ella personas no autorizadas. Imagine que ha creado una nueva empresa. Tiene activos físicos como un edificio, equipos y ordenadores. Tiene empleados y datos importantes, que también son activos. Quiere que sólo las personas autorizadas vean los datos, por lo que quiere aplicar la confidencialidad. De este modo, sólo las personas autorizadas pueden acceder a los datos y trabajar con ellos. Puedes implementar la confidencialidad encriptando los archivos de datos y almacenándolos en un disco. De este modo, sólo las personas que tienen acceso al disco pueden ver los datos y trabajar con ellos. En cuanto a la información personal, digamos que un usuario común desea abrir una nueva cuenta de ahorros en, verbigracia, el Banco BBVA y necesita invertir $10.000 dólares. Esta información es confidencial, ya que sólo el banco y el usuario podrán acceder a ella.

b. Integridad

La integridad conceptualiza a la consistencia, exactitud y fiabilidad de las informaciones a lo largo de la totalidad de su ciclo de vida. Si transfieres $1001 dólares a tu amigo, quieres estar seguro de que recibe $1001 dólares. Quieres estar seguro de que un atacante no autorizado no puede alterar o manipular para que sean 100 dólares, o que el banco no cometa un error.

c. Disponibilidad

La disponibilidad de los datos también es muy importante. Si las informaciones se conservan en una data base, es trascendental que la compañía o el usuario autorizado puedan acceder a ellos cuando los requieran. Los datos deben estar fácilmente disponibles para los usuarios autorizados. Si los datos están protegidos, pero no están disponibles cuando se solicitan, esto puede suponer un gran riesgo para la empresa. Digamos que usted va al banco a retirar dinero de su cuenta, pero el funcionario del banco le dice que el servicio no está disponible en ese momento. Es probable que pierda la confianza en ese banco. La disponibilidad se garantiza mediante el mantenimiento continuo del HARDWARE. y el SOFTWARE.. Es importante garantizar un entorno óptimo que esté libre de conflictos de SOFTWARE.. Los equipos de SI, como servidores proxys y los cortafuegos, pueden evitar el tiempo de inactividad y garantizar la protección contra los Ataques de Denegación de Servicio conceptualizados como DoS (por su acrónimo en inglés de “Denial of Service“).

Vulneraciones o riesgos: Según Salah, este marco del proceso de análisis peligros se publicó en 2009 a través de ISACA, diseñado y creado como una ayuda educativa para funcionarios de estadísticas, control superior y gestión de TI. (Salah, 2017)

Según Brito, es el riesgo empresarial relacionado con la utilización, posesión, operación, participación, efecto y adopción de TI en la

empresa. Aquel peligro incluye actividades asociadas con TI que pueden afectar a la empresa comercial. (Brito, 2017)

Acorde Risco (2021) RISK IT es un riesgo empresarial de tipo comercial, en otras palabras, el riesgo comercial relacionado con la utilización, posesión, operación, participación, impacto y adopción de TI en una agencia.

De acuerdo con Conexión ESAN, un peligro de TI es también una amenaza empresarial comercial, riesgos comerciales relacionados con la utilización, la participación, la operación, el efecto y la adopción de TI en una empresa.

Según Martins, estos están hechos de eventos que están relacionado con TI que probablemente pueden perjudicar a la empresa y esto puede surgir con una frecuencia e importancia inciertas, y plantea dificultades para lograr los objetivos estratégicos. (Martins, 2022)

1.4. Formulación del Problema.

¿Cómo mejorar el nivel de seguridad informática mediante la norma ISO/IEC 27002 en la empresa Rash Perú S.A.C?

1.5. Justificación e importancia del estudio.

Según Namakforoosh (2000), la justificación e importancia es dejar en evidencia el por qué se realiza la investigación o que soluciones genera a un problema o al menos, que estrategias desarrolla para coadyuvar en darle solución.

Para el sector tecnológico y comercial de nuestra nación se logran aproximar tiempos provechosos, ello a raíz del encadenamiento seguido de proyectos de inversión, los que aseguran el crecimiento del sector en mención. Durante estos años se inauguraron diversos centros comerciales con una inversión de casi US$200 millones en diversas localidades peruanas, tales como Mall Aventura Chiclayo, mientras que algunos otros se encuentran próximos a ser inaugurados, tales como Real Plaza en el distrito de Surco, entre otros (Ochoa, 2020). Lo anterior expuesto involucra que, lograrán aperturarse nuevos caminos a las

competencias que puedan aparecer para Rash Perú SAC y por tanto, dicha compañía debería estar ampliamente preparada para lograr desafiar de manera eficaz dichas variabilidades comerciales.

Asimismo; y, por otro lado, alineado a las directrices enfocadas en las reformas financieras es que se localiza la “Ley de Habeas Data”, la misma que se encuentra enfocada en regular la manipulación de las informaciones contenidas en bases de datos personales; especialmente las informaciones de tipo comercial, personales, de la prestación de servicios y las financieras. Para ello es que esta ley vio la luz, para regular constitucionalmente un derecho existente en tal constitución, “el derecho a la intimidad, al buen nombre, a salvaguardar las informaciones personales y a percibir informaciones veraces” pretendiendo ser y establecer un pilar fundamental para la SI de dicho ámbito comercial y tecnológico peruano (Tribunal Constitucional del Perú, 2020).

La conjugación de ambos elementos anteriormente mencionados revela la competitividad presente en dicho entorno actual, por ende, las diversas compañías que operan en este ámbito comercial requieren de la adecuación de sus estrategias con propósitos de ofrecer servicios mejores para sus clientelas. Aquí radica la importancia que tiene Rash Perú S.A.C por disponer de informaciones fiables, homogéneas, detalladas y rastreables a partir de las cuales se puedan avizorar y cuantificar los avances de su negocio, tomándose adecuadas decisiones, las mismas que deben de ser afines con sus estrategias organizacionales para evaluar así sus resultados obtenidos empresarialmente hablando. Por tanto, se necesita gestionar segura y eficientemente las informaciones puesto que dan soporte a su negocio.

1.6. Hipótesis.

Con la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 se podrá mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C.

1.7. Objetivos.

1.7.1. Objetivo general.

Implementar un SGSI(Sistema de Gestión de Seguridad de la Información) basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C.

1.7.2. Objetivos específicos.

a. Diagnosticar el estado actual de la seguridad informática en la empresa Rash Perú S.A.C.
b. Desarrollar un SGSI fundamentado en la Norma ISO/IEC 27002 para la empresa caso de estudio.
c. Validar mediante juicio de expertos el SGSI elaborado previamente.
d. Ejecutar una prueba piloto del SGSI en la empresa caso de estudio seleccionada.
e. Evaluar los resultados obtenidos posteriores a la implementación del SGSI.

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

2.1.1. Tipo de Investigación

Según Espinoza (2014), la investigación tecnológica aplicada "busca la resolución de alguna problemática específica, planteando y brindando respuestas solucionadoras e innovadoras a problemáticas que afecten a la sociedad, un grupo de individuos o a uno individualmente, haciendo usanza de la aplicación de conocimiento científico apoyado por las TI" (pág. 90).

De acuerdo con su naturaleza, la investigación de tipo aplicada, con la cual se estimó, dar solución, a través de la usanza de conocimiento científicos acerca de la ISO/IEC 27001 para la implantación de un SGSI fundamentado en dicha directriz el cual, a posteriori, permite dictaminar resultados, los cuales serán documentados en el caso de estudio.

2.1.2. Diseño de Investigación

Según Espinoza (2014), la investigación cuasi experimental es similar a los estudios experimentales en que hay usanza de la variable independiente, empero, se diferencia de la anteriormente mencionada dado que hay selección y asignación aleatoria, grupo de control y/o utilizaciones activas.

Por su naturaleza, el estudio corresponde al diseño cuasi experimental; pues la variable independiente "SGSI" se visualizó, debido al efecto que esta tiene por sobre la variable dependiente "gestión de la SI" pero de una manera previa o parcial a una implementación total y vigente. Por tanto, el diseño quedó estructurado del modo siguiente:

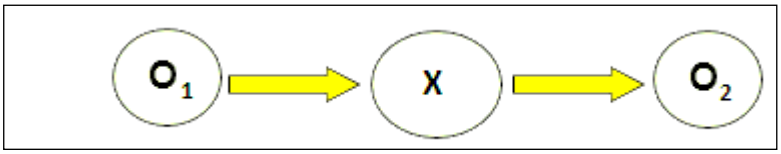


Figura 11. Diseño de la investigación

Fuente. Elaboración propia.

Donde:

O_1 = Nivel de SI en la empresa Rash Perú S.A.C, previo a implantar el SGSI fundamentado en la ISO/IEC 27002.

X = Implementación del SGSI fundamentado en la ISO/IEC 27002.

O_2 = Nivel de SI en la empresa Rash Perú S.A.C, post a implantar el SGSI fundamentado en la ISO/IEC 27002.

2.2. Población y muestra.

2.2.1. Población

Según Espinoza (2014), es el conjunto de personas vinculadas por su similitud en un determinado contexto (pág. 29).

Asimismo, la población con respecto a la aplicación de la norma 27002, mejoro la seguridad informática en la empresa Rash Perú S.A.C, la misma, se compone de un total de 100 colaboradores, sin embargo, se tomó el departamento de sistemas para la evaluación.

2.2.2. Muestra

Según Espinoza (2014) el muestreo por conveniencia se hace considerando ciertas particularidades, seleccionando alguna característica específica por la que seleccionar en este caso, verbigracia, una determinada familia.

Después de haber definido el área de estudio, para este caso el departamento de sistemas, se tomó una muestra de 20 trabajadores a los que se le realizó la encuesta en el área de TI, jefaturas de áreas, y oficinas administrativas, teniendo en cuenta que en esta área se desarrollan los procesos que se encuentran sujeto la investigación.

Por ello se tomó una muestra de 20 trabajadores, que conforman el área de sistemas de la empresa.

2.3. Variables, Operacionalización.

2.3.1. Variables

Variable Independiente: Sistema de Gestión de Seguridad de la Información fundamentado en la norma ISO/IEC 27002.

Según Chopra & Chaudhary (2020) un SGSI, es un sistema de gestión que se encarga de proteger ante cualquier amenaza ya sea interna o externa a una organización sobre sus activos informáticos. Al crear, implementar, gestionar y mantener un SGSI, las entidades protegen sus datos confidenciales, personales y confidenciales para que no se vean comprometidos.

Variable Dependiente: Seguridad informática en la empresa Rash Perú S.A.C.

Según Chopra & Chaudhary (2020) la SI, es la práctica de resguardarla del uso no autorizado. La SI es fundamentalmente aquella praxis enfocada en prevenir accesos no debidamente autorizados, las usanzas, las divulgaciones, las interrupciones, las modificaciones, las inspecciones, las destrucciones, los registros u otro debidamente relacionado con la SI, siendo estas informaciones de naturaleza electrónica o física. Las informaciones podrían cristalizarse como cualquier cosa, verbigracia, atacando sus particularidades previamente mencionadas en el punto anterior, en diversos contextos, tales como, verbigracia, los perfiles empleados en redes sociales tales como Twitter, Instagram, Facebook, Twitch; informaciones residentes en teléfonos móviles, datos biométricos, etcétera.

2.3.2. Operacionalización

Tabla 1

Operacionalización de la variable independiente

Variables	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos
VARIABLE INDEPENDIENTE: Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27002.	Aceptación del SGSI	Nivel de Claridad	$N_{Claridad} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	T: Juicio de Expertos I: Ficha de Juicio de Expertos
		Nivel de Objetividad	$N_{Objetividad} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	
		Nivel de Actualidad	$N_{Actualidad} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	
		Nivel de Organización	$N_{Organización} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	
		Nivel de Suficiencia	$N_{Suficiencia} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	
		Nivel de Intencionalidad	$N_{Intencionalidad} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	
		Nivel de Consistencia	$N_{Consistencia} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	
		Nivel de Coherencia	$N_{Coherencia} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	
		Nivel de Metodología	$N_{Metodología} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	
		Nivel de Pertinencia	$N_{Pertinencia} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$	

Fuente: elaboración propia.

Tabla 2

Operacionalización de la variable dependiente

Variables	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos
VARIABLE DEPENDIENTE: Seguridad informática en la empresa Rash Perú S.A.C.	Seguridad de la Información	Nivel de seguridad de equipos	1. ¿El nivel de seguridad de los equipos es óptimo para operar con el OFISMART?	T: Encuesta T: Observación I: Cuestionario I: Ficha técnica
		Nivel de políticas de gestión de claves de cifrado	2. ¿Existe una política o procedimiento para la gestión de claves de cifrado?	
		Nivel de procedimiento para la gestión de cambio	3. ¿Se dispone de un procedimiento para la gestión de cambio?	
		Nivel de políticas de control de accesos	4. ¿Existe una política de control de accesos debidamente documentada y se revisa constantemente?	
		Nivel de segregación de funciones y responsabilidades	5. ¿Con la finalidad de reducir alteraciones y/o modificaciones sin autorización o hacer mal uso de la información o servicios, las funciones y las responsabilidades son separados o segregados?	
		Nivel de aseguramiento de controles de seguridad	6. ¿Los controles aseguran que los usuarios sólo tienen acceso a los recursos de la red a los cuales han sido autorizados a utilizar según sus funciones?	
		Nivel de procedimientos para eliminación de accesos	7. ¿Existe un procedimiento para garantizar que los accesos de los usuarios sean eliminados al finalizar el vínculo laboral, contractual o cambio de puesto de trabajo?	
		Nivel de aceptación de acuerdos	8. ¿Todos los empleados y proveedores firman acuerdos de confidencialidad y no divulgación?	
		Nivel de existencia de procedimientos de destrucción	9. ¿Existe procedimientos para la destrucción de la data contenida en equipos sensibles cuando estos sean dados de baja?	
	Riesgo de la Información	Nivel de existencia de políticas criptográficas	10. ¿Existe una política sobre el uso de técnicas criptográficas para el tratamiento de la información transmitida en el OFISMART?	
		Nivel de protección de datos	11. ¿Los datos y/o documentos se encuentran protegidos contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales del negocio?	
		Nivel de planes para la continuidad operativa	12. ¿Se dispone de planes y equipamiento para la continuidad operativa del servicio del OFISMART?	
	Control informático	Nivel de capacitaciones de seguridad de la información	13. ¿Se realiza capacitación integral en temas de seguridad de la información a los empleados y usuarios del OFISMART?	
		Nivel de concientización de seguridad de la información	14. ¿Se elabora publicidad de concientización respecto a temas de seguridad de la información?	

Fuente: elaboración propia.

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

Para esta investigación se utilizó las técnicas e instrumentos:

Técnicas

En este estudio, se empleó como técnica la observación directa, ya que es el proceso por el cual se observa el fenómeno, y todo lo observado será anotado en la ficha técnica.

Además, para complementar este estudio se utilizó como técnica la entrevista para ello se dará al personal del área de sistemas un cuestionario que tendrán que responder. (Sandelowski, 2000).

Instrumentos

La ficha técnica, será el instrumento que se usó, donde se llevaron todos los sucesos, quedando constancia escrita en el historial, que se encuentra en los anexos nombrados a continuación:

Tabla 3

Descripción de las fichas técnicas de la variable dependiente.

Variable dependiente: **Seguridad informática en la empresa Rash Perú S.A.C.**		
Anexo	**Ficha**	**Dimensión**
14	Fichas Registro Test	Seguridad de la información
15	Fichas Registro Post Test	Seguridad de la información
	Fichas de Registro Test	Riesgo Informático
16	Fichas de Registro Re Test	Riesgo Informático
17	Fichas Registro Post Test	Riesgo Informático
18	Fichas de Registro Test	Control Informático
19	Fichas de Registro Re Test	Control Informático
20	Fichas de Registro Post Test	Control Informático

Fuente: elaboración propia.

Como muestra la tabla anterior, estos registros, se tomaron de un antes, durante y después de realizar la investigación, asimismo, se comparó los

tres estados del SGSI, según sus dimensiones, seguridad de la información, riesgo de información y control informático para la variable dependiente.
Con respecto a las dimensiones:

- Seguridad de la información, se utilizó la fórmula:

$$\text{ANA} = \frac{\text{RANA}}{\text{TAD}} \text{ x } 100$$

Donde:
ANA: Seguridad de la información
TAD: Total de Accesos seguridad de la información
RANA: Reporte de Accesos seguridad de la información

- Riesgo de información, se utilizó la fórmula:

$$\text{EBMD} = \frac{\text{EMBDNR}}{\text{TMDD}} \text{ x } 100$$

Donde:
EBMD: Riesgo de la información
TMDD: Total de Riesgo de la información: Eliminar, Manipular, Borrar

- Control informático, se utilizó la fórmula:

$$\text{VI} = \frac{\text{VINE}}{\text{VID}} \text{ x } 100$$

Donde:
VI: control informático
VINE: total controles informáticos
VID: total controles aplicados en el día

A continuación, se muestran las fichas de registro de los tres estados de implementación, registro, pre, re y pos-test, que se verán reflejadas en los anexos del 14 al 20, dando respuesta a los resultados:

Tabla 4

Fichas de registro Pre Test para seguridad de la información.

<table>
<tr><td>Investigador</td><td colspan="4"></td></tr>
<tr><td>Empresa</td><td colspan="4"></td></tr>
<tr><td>Dirección</td><td colspan="4"></td></tr>
<tr><td>Fecha de inicio</td><td colspan="4"></td></tr>
<tr><td>Fecha de terminación</td><td colspan="4"></td></tr>
<tr><td>Variable</td><td colspan="4">Formula</td></tr>
<tr><td colspan="2">Reportes</td><td colspan="3" rowspan="4">Donde:
ANA: seguridad de la información
TAD: Total de Accesos seguridad de la información
RANA: Reporte de Accesos
$ANA = \frac{RANA}{TAD} \times 100$
seguridad de la información</td></tr>
<tr><td>Indicador</td><td>Medida</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Seguridad de la información (pre Test)</td><td>Porcentaje</td></tr>
<tr><td>ÍTEM</td><td>FECHA</td><td>RANA</td><td>TAD</td><td>ANA %</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>TOTAL</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">PROMEDIO</td><td></td></tr>
</table>

Fuente: elaboración propia.

Tabla 5

Ficha de registro Re Test para seguridad de la información

Investigador				
Empresa				
Dirección				
Fecha de inicio				
Fecha de terminación				
Variable	Formula			
Reportes		Donde: ANA: seguridad de la información TAD: Total de Accesos seguridad de la información RANA: Reporte de Accesos seguridad de la información $ANA = \frac{RANA}{TAD} \times 100$		
Indicador	Medida			
Seguridad de la información (Re-Test)	Porcentaje			
ÍTEM	**FECHA**	**RANA**	**TAD**	**ANA %**
	TOTAL			
	PROMEDIO			

Fuente: elaboración propia.

Tabla 6

Ficha de registro Post Test para seguridad de la información

Investigador	
Empresa	
Dirección	
Fecha de inicio	
Fecha de terminación	

Variable	Formula			
Reportes		Donde: ANA: seguridad de la información TAD: Total de Accesos seguridad de la información RANA: Reporte de Accesos seguridad de la información $\mathbf{ANA} = \frac{\boldsymbol{RANA}}{\boldsymbol{TAD}} \times \mathbf{100}$		
Indicador	Medida			
Seguridad de la información (Post-Test)	Porcentaje			
ÍTEM	**FECHA**	**RANA**	**TAD**	**ANA %**
	TOTAL			
	PROMEDIO			

Fuente: elaboración propia.

Tabla 7

Fichas de registro Test para el riesgo de la información

Investigador				
Empresa				
Dirección				
Fecha de inicio				
Fecha de terminación				
Variable	Formula			
Reportes		Donde: EBMD: Riesgo de la información TMDD: Total de Riesgo de la información: Eliminar, Manipular, Borrar Datos No reconocidos $\mathbf{EBMD} = \frac{\mathrm{EMBDNR}}{\mathrm{TMDD}} \times \mathbf{100}$		
Indicador	Medida			
Eliminar, manipular, borrar, datos (TEST)	Porcentaje			
ÍTEM	**FECHA**	**EMBDNR**	**TMDO**	**EBMD%**

	TOTAL			
	PROMEDIO			

Fuente: elaboración propia.

Tabla 8

Fichas de registro Re Test para el riesgo de la información

Investigador					
Empresa					
Dirección					
Fecha de inicio					
Fecha de terminación					
Variable		Formula			
	Reportes		Donde: EBMD: Riesgo de la información TMDD: Total de Riesgo de la información: Eliminar, Manipular, Borrar Datos No reconocidos $\mathbf{EBMD} = \frac{\mathbf{EMBDNR}}{\mathbf{TMDD}} \times \mathbf{100}$		
Indicador		Medida			
Eliminar, manipular, borrar, datos (RE-TEST)		Porcentaje			
ÍTEM		**FECHA**	EMBDNR	TMDO	EBMD%
		TOTAL			
		PROMEDIO			

Fuente: elaboración propia.

Tabla 9

Fichas de registro Post Test para el riesgo de la información

Investigador	
Empresa	

Dirección				
Fecha de inicio				
Fecha de terminación				
Variable	Formula			
Reportes		Donde: EBMD: Riesgo de la información TMDD: Total de Riesgo de la información: Eliminar, Manipular, Borrar Datos No reconocidos $\mathbf{EBMD} = \frac{\mathbf{EMBDNR}}{\mathbf{TMDD}} \times \mathbf{100}$		
Indicador	Medida			
Eliminar, manipular, borrar, datos (Post-Test)	Porcentaje			
ÍTEM	**FECHA**	**EMBDNR**	**TMDO**	**EBMD%**
	TOTAL			
	PROMEDIO			

Fuente: elaboración propia.

Tabla 10

Fichas de registro Pre Test para el control informático

Investigador		
Empresa		
Dirección		
Fecha de inicio		
Fecha de terminación		
Variable	Formula	
Reportes		Donde: VI: control informático VINE: total controles informáticos VID: total controles aplicados en el día $\mathbf{VI} = \frac{\boldsymbol{VINE}}{\mathbf{VID}} \times \mathbf{100}$
Indicador	Medida	

Control informático (Pre Test)	Porcentaje			
ÍTEM	**FECHA**	**TEBMDS**	**EBMDR**	**EBMD %**
	TOTAL			
	PROMEDIO			

Fuente: elaboración propia.

Tabla 11

Ficha de registro Re Test para el control informático

Investigador				
Empresa				
Dirección				
Fecha de inicio				
Fecha de terminación				
Variable	Formula			
Reportes		Donde: VI: control informático VINE: total controles informáticos VID: total controles aplicados en el día $VI = \frac{VINE}{VID} \times 100$		
Indicador	Medida			
Control informático (Re-Test)	Porcentaje			
ÍTEM	**FECHA**	**TEBMDS**	**EBMDR**	**EBMD %**
	TOTAL			
	PROMEDIO			

Fuente: elaboración propia.

Tabla 12

Fichas de registro Post Test para el control informático

Investigador				
Empresa				
Dirección				
Fecha de inicio				
Fecha de terminación				
Variable	Formula			
Reportes		Donde: VI: control informático VINE: total controles informáticos VID: total controles aplicados en el día $VI = \frac{VINE}{VID} \times 100$		
Indicador	Medida			
Control informático (Pos-Test)	Porcentaje			
ÍTEM	**FECHA**	**TEBMDS**	**EBMDR**	**EBMD %**
	TOTAL			
	PROMEDIO			

Fuente: elaboración propia.

Asimismo, se utilizó como instrumento el cuestionario, ya que es un listado de pesquisas debidamente organizadas, las cuales se implantaron de manera presencial y/o virtual (Sandelowski, 2000).

2.5. Procedimiento de análisis de datos.

Para esta recopilación de datos, se revisó distintos tipos de documentación, manuales, informes y planes de seguridad, y se obtuvo información sobre las políticas de seguridad de la información de la empresa. (Hernández Sampieri, 2014)

Fuentes de información

La información que se tomó para el levantamiento de los resultados fue a través de:

- Informes del área sistemas de la empresa.
- Entrevistas al personal del área de sistema de la Empresa.
- Información de los problemas de seguridad informática del área de sistema del área de la empresa.

Instrumentos para recolectar datos

Con el fin de recolectar los datos para la investigación, se toman en consideración lo siguiente:

- Fichas de registros.
- Registro de incidentes del área de sistemas de la empresa.
- Entrevista con el gerente de la empresa.
- Entrevista a los colaboradores de la empresa.
- Informes de la gestión de riesgos.

Confiabilidad: Según Carrasco (2016) es una herramienta que nos hace medir los resultados para que sean sus datos seguros y confiables.

Una de estas herramientas es el coeficiente de correlación de Pearson que mide el nivel de confiabilidad, por ende, se muestra en la tabla siguiente:

Tabla 13

Niveles de confiabilidad

Valores	Nivel
De -1 a 0	No es confiable
De 0,01 a 0,49	Baja confiabilidad
De 0,5 a 0,75	Moderada confiabilidad
De 0,76 a 0,89	Fuerte confiabilidad
De 0,9 a 1	Alta confiabilidad

Datos obtenidos del estudio realizado por Carrasco (2016).

Se realizó una comparación del antes y después de los resultados que se obtuvieron luego de implementar el “Modelo seguridad informática”. Para la constatación de la hipótesis, se aplica la prueba t de “Student”, sirve para "aceptar" o "rechazar" al momento de tomar una decisión sobre la hipótesis. Para esto, se utilizó el SOFTWARE. SPSS V. 26.

Se realizó la evaluación del SGSI, para mejoramiento del nivel de SI en la compañía Rash Perú S.A.C, usando los siguientes indicadores:

$\boldsymbol{Nivel\ de\ Claridad}$: realizó el cálculo del valor del SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C está formulado

$$N_{Claridad} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Claridad}: Nivel\ de\ Claridad$
$CE: Calificación\ del\ Experto$
$n = Número\ Total\ de\ Expertos$

$\boldsymbol{Nivel\ de\ Objetividad}$: realizó el cálculo del valor del SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C está expresado

$$N_{Objetividad} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Objetividad}: Nivel\ de\ Objetividad$
$CE: Calificación\ del\ Experto$
$n = Número\ Total\ de\ Expertos$

$\boldsymbol{Nivel\ de\ Actualidad}$: realizó el cálculo del valor del SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C su fórmula es:

$$N_{Actualidad} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Actualidad}$: $Nivel\ de\ Actualidad$

CE: $Calificación\ del\ Experto$

$n = Número\ Total\ de\ Expertos$

Nivel de Organización: realizó el cálculo del valor del SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C su fórmula es

$$N_{Organización} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Organización}$: $Nivel\ de\ Organización$

CE: $Calificación\ del\ Experto$

$n = Número\ Total\ de\ Expertos$

Nivel de Suficiencia: realizó el cálculo del valor del SGSI si el SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C su fórmula es:

$$N_{Suficiencia} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Suficiencia}$: $Nivel\ de\ Suficiencia$

CE: $Calificación\ del\ Experto$

$n = Número\ Total\ de\ Expertos$

Nivel de Intencionalidad: realizó el cálculo del valor del SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C su fórmula es:

$$N_{Intencionalidad} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Intencionalidad}$: $Nivel\ de\ Intencionalidad$
CE: $Calificación\ del\ Experto$
$n = Número\ Total\ de\ Expertos$

Nivel de Consistencia: realizó el cálculo del valor del SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C su fórmula es:

$$N_{Consistencia} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Consistencia}$: $Nivel\ de\ Consistencia$
CE: $Calificación\ del\ Experto$
$n = Número\ Total\ de\ Expertos$

Nivel de Coherencia: realizó el cálculo del valor del SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C su fórmula es:

$$N_{Coherencia} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Coherencia}$: $Nivel\ de\ Coherencia$
CE: $Calificación\ del\ Experto$
$n = Número\ Total\ de\ Expertos$

Nivel de Metodología: realizó el cálculo del valor del SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C su fórmula es

$$N_{Metodología} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Metodología}: Nivel\ de\ Metodología$

$CE: Calificación\ del\ Experto$

$n = Número\ Total\ de\ Expertos$

Nivel de Pertinencia: realizó cálculo del valor del SGSI para mejorar el nivel de SI en la empresa Rash Perú S.A.C su fórmula es

$$N_{Pertinencia} = \frac{(CE_1 + CE_2 + \cdots + CE_n)}{n}$$

Leyenda:

$N_{Pertinencia}: Nivel\ de\ Pertinencia$

$CE: Calificación\ del\ Experto$

$n = Número\ Total\ de\ Expertos$

2.6. Criterios éticos

Según Gomm (2008), se tomó en consideración los siguientes criterios éticos en toda la investigación:

Honestidad

Se informó a la empresa y al departamento a evaluar, las experticias que sé consigan en el transcurso de la investigación. (Gomm, 2008, pág. 37).

Objetividad

Se mostró la información, sin sesgos en cuanto a los resultados (Gomm, 2008, pág. 37).

Respeto a la propiedad intelectual

Las citas y referencias, así como las informaciones pertenecientes a diversos autores, son respetadas, y se evitó la similitud pasando por el SOFTWARE. anti-plagio (Gomm, 2008, pág. 38).

Confidencialidad

Se respetó la confidencialidad de las informaciones de la compañía Rash Perú S.A.C en cuanto a informaciones sensibles (Gomm, 2008, pág. 38).

No discriminación

Se evitó discriminar a los colaboradores de la compañía Rash Perú S.A.C cuando se desplegaron las encuestas in situ (Gomm, 2008, pág. 39).

2.7. Criterios de Rigor Científico.

Los criterios esbozados por Erazo (2011) y que han sido empleados en esta investigación son los siguientes:

Credibilidad

Se estableció que la credibilidad de las informaciones solicitando el permiso respectivo a la compañía Rash Perú S.A.C (Erazo, 2011, pág. 116).

Aplicabilidad

Se realizó el SGSI enfocado primeramente en el caso de estudio y el cual puede ser replicado a otras compañías del sector (Erazo, 2011, pág. 117).

Coherencia

La investigación se realizó considerando a los colaboradores de Rash Perú S.A.C. en su totalidad logrando la coherencia de los resultados obtenidos (Erazo, 2011, pág. 117).

Neutralidad

Se buscó la neutralidad del investigador y de los colaboradores de Rash Perú S.A.C, para lograr resultados verdaderos en la investigación (Erazo, 2011, pág. 118).

Relevancia

Se justificó la investigación, haciendo que sea relevante para su sector de estudio y para la ingeniería de sistemas, sobre todo en la línea de investigación de la escuela profesional (Erazo, 2011, pág. 118).

III. RESULTADOS.

Rash Perú S.A.C ha logrado invertir en TIC, las mismas que ayudan y apoyan la gestión de sus SI, pero aún faltan políticas y procedimientos establecidos que apoyen el buen uso de dichas TIC y que permitan controlar la información que estas recién mencionadas manejan, por lo que el departamento de sistemas ha sido utilizado como modelo en la implementación de la Seguridad de la Información y el propósito de un buen Sistema de Gestión de Seguridad de la Información (SGSI).

A continuación, se muestran los resultados de los análisis descriptivos e inferenciales de los indicadores mencionados, cabe destacar, que los parámetros a usar para el levantamiento de los resultados, se tomó de las fichas de registros ubicados en los anexos del 14 al 20, respectivamente.

3.1. Resultados descriptivos e inferenciales de las fichas de registro

3.1.1. Análisis Descriptivos

3.1.1.1. Indicador Seguridad de la información.

Como se muestra en la tabla 14, para el indicador Seguridad de información, el valor promedio del Re-test fue de 69.90% y el valor promedio Post-test fue de 14.00%. Además, el valor mínimo del re-test fue 50%, el valor máximo es 88%, y el valor mínimo del post-test es 0% y el máximo es 27%, que fueron obtenidos luego de realizar la comparación mediante la ficha de registro. Esto quiere decir, que el personal encuestado, toma en consideración la falta de un SGSI que permita el control de los datos.

Tabla 14

Análisis descriptivo Re-test y Post-test de Seguridad de información.

	N	Mínimo (%)	Máximo (%)	Media (%)	Desv. típ. (%)
Seguridad_Información_Re	20	50	88	69,90	11,011
Seguridad_información_Post	20	0	27	14,00	8,259
N válido (según lista)	20				

Fuente: elaboración propia.

A continuación, se muestra en la figura 12 la comparación de un post SGI con el manejo actual de la información:

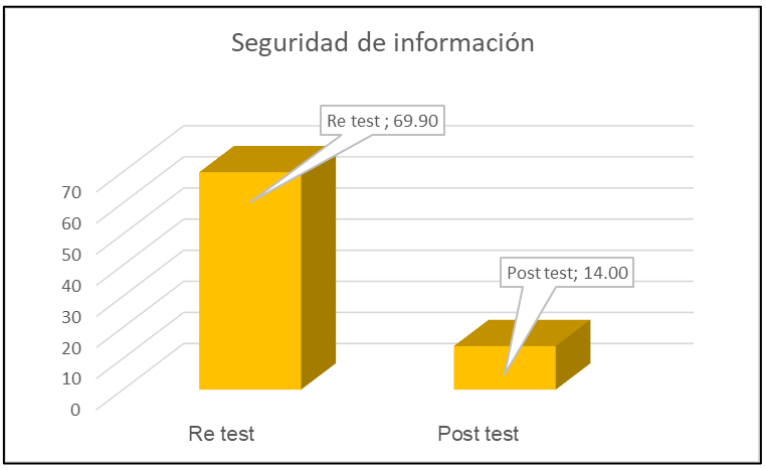


Figura 12, Comparación entre Re-test y Post-test de Seguridad de información.

Fuente, Elaboración propia.

3.1.1.2. Indicador Riesgo de la información.

A continuación, se muestra en la tabla 15, la descripción del indicador riesgo de la información, donde se encuentra que el valor promedio del Re-test fue de 52.60% y el valor promedio Post-test fue de 11.40%. Además, el valor mínimo del re-test fue 40%, el valor máximo es 70%, y el valor mínimo del post-test es 0% y el máximo es 22%, que fueron obtenidos luego de realizar la comparación mediante las fichas de registro.

Tabla 15

Análisis descriptivo Re-test y Post-test de riesgo de la información.

	N	Mínimo (%)	Máximo (%)	Media (%)	Desv. típ. (%)
Pre riesgo de la información	20	40	70	52,60	8,708
Post_ riesgo de la información	20	0	22	11,40	7,287
N válido (según lista)	20				

Fuente, Elaboración propia.

Asimismo, se muestra en la figura 13, para el indicador de riesgo de la información, se puede visualizar que la mitad aproximadamente de los encuestados tienen inquietud con respecto al riesgo de la información, ya que en el presente existen perdidas, duplicidad, etc.

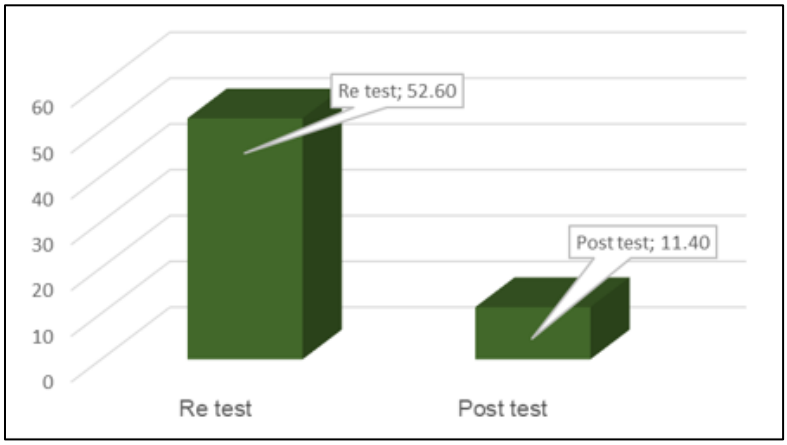


Figura 13, Gráfica de comparación entre Pre-test y Post-test de riesgo de la información.

Fuente, Elaboración propia.

3.1.1.3. Control informático.

Es importante destacar, que, para el indicador del Control informático, se muestra en la figura 14, el valor promedio del Pre-test fue de 47.15% y el valor promedio Post-test fue de 11.95%. Además, el valor mínimo del Pre-test fue 30%, el valor máximo es 75%, y el valor mínimo del post-test es 0% y el máximo es 29%, que fueron obtenidos luego de realizar

la comparación mediante las fichas de registro del antes durante y después, esto corresponde, que para los encuestados es importante mantener el control de los datos de información, en cada uno de los procesos, ya que permite generar una toma de decisiones y mantener la buena práctica.

Tabla 16

Análisis descriptivo Re-test y Post-test de Control informático

	N	Mínimo (%)	Máximo (%)	Media (%)	Desv. típ. (%)
Re_Control_informático	20	30	75	47,15	12,419
Post_Control_informático	20	0	29	11,95	9,795
N válido (según lista)	20				

Fuente, Elaboración propia.

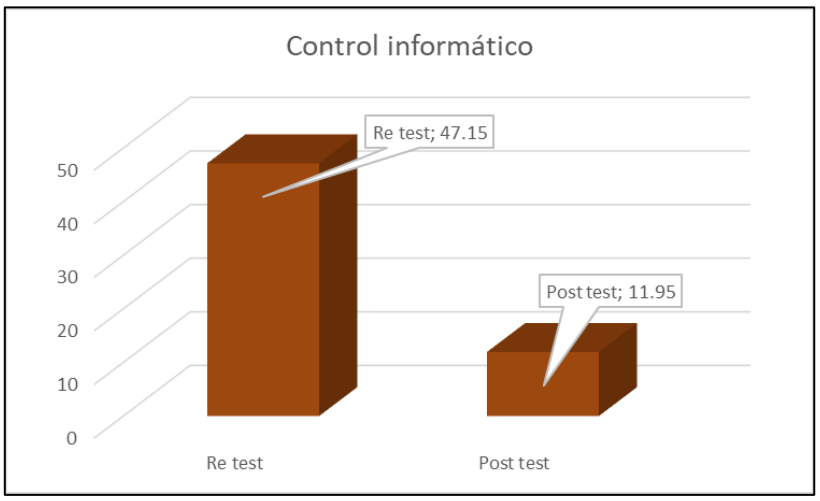


Figura 14, *Gráfica de comparación entre Re-test y Post-test de Control informático*

Fuente, Elaboración propia.

3.1.2. Análisis Inferencial

3.1.2.1. Indicador Seguridad de información

Para el análisis inferencial del indicador de seguridad de información, los resultados mostraron que el nivel de significancia en el Re-test fue de 0,265 y para el Post-test, 0,108. Por lo cual se determina que el indicador se ajusta a una distribución normal o paramétrica (P > 0.05), que fueron

obtenidos luego de realizar la comparación mediante las fichas de registro del antes durante y después. En el mismo orden de ideas, se puede apreciar, que en las figuras 15 y la figura 16, se muestra que cerca del 95% de los encuestados están de acuerdo con el manejo del SGSI a través de la seguridad de los datos bajo la norma ISO.

Tabla 17

Prueba de normalidad – Seguridad de información

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Seguridad_Información_Re	,942	20	,265
Seguridad_información_Post	,922	20	,108

Fuente, Elaboración propia.

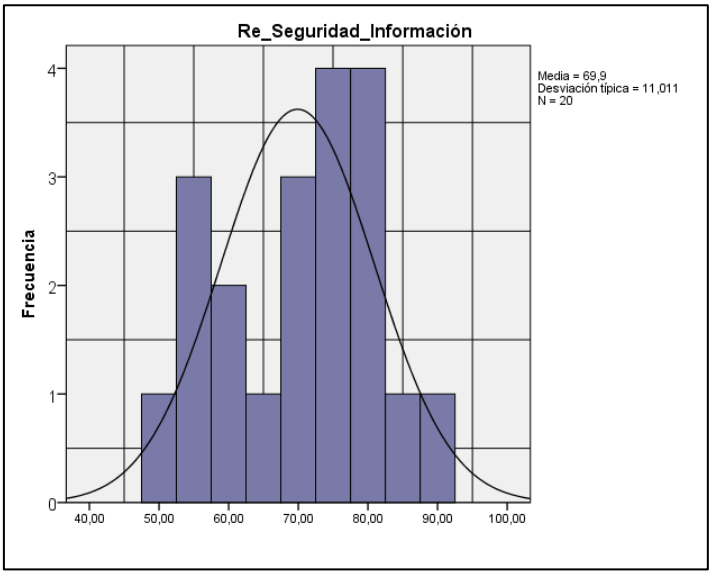


Figura 15, *Seguridad informática Re-test.*

Fuente, Elaboración propia.

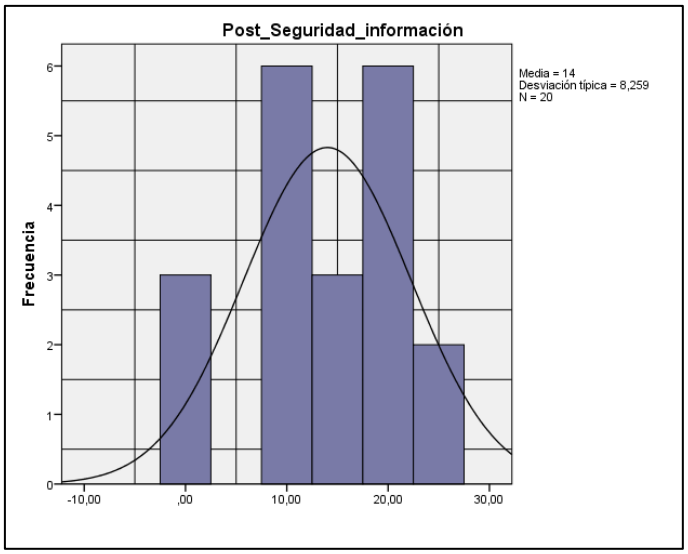


Figura 16, Seguridad informática Post-test.

Fuente, Elaboración propia.

3.1.2.2. Indicador riesgo de la información.

Para este indicador, los resultados mostraron que el nivel de significancia en el Pre-test fue de 0,213 y para el Post-test, 0,201. Por lo cual se determina que el indicador se ajusta a una distribución normal o paramétrica (P > 0.05). que fueron obtenidos luego de realizar la comparación mediante las fichas de registro del antes durante y después. A continuación, se muestra en la tabla 18 los resultados:

Tabla 18

Prueba de normalidad – riesgo de la información.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
riesgo de la información.	,937	20	,213
riesgo de la información.	,936	20	,201

Fuente, Elaboración propia.

Con el fin de tener una mejor visualización, los resultados que muestran las figuras 17 y la figura 18 nos indica que el nivel de significancia en el Pre-test fue de 0,213 y para el Post-test, 0,201. Por lo cual se determina que el indicador

se ajusta a una distribución normal o paramétrica (P > 0.05), que fueron obtenidos luego de realizar la comparación mediante las fichas de registro del antes durante y después, determinando el temor a la pérdida o malas prácticas de la información de la empresa.

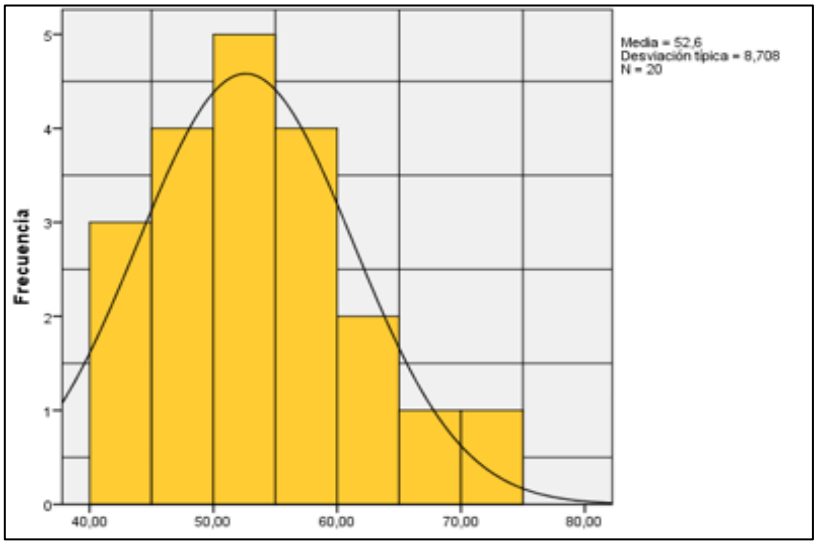


Figura 17, Riesgo de la información Re-test.

Fuente, Elaboración propia.

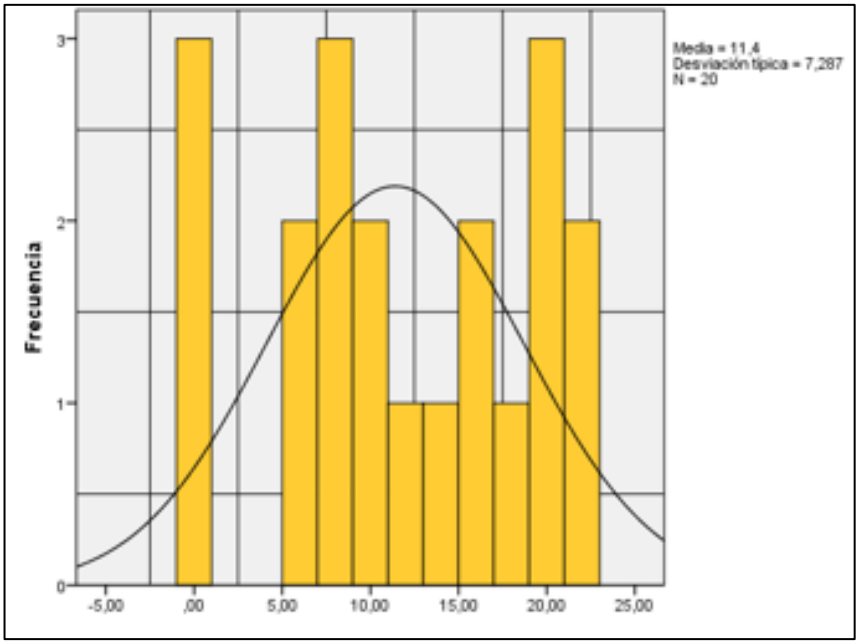


*Figura 18***,** Riesgo de la información Post-test.

Fuente, Elaboración propia.

3.1.2.3. Indicador Control informático

En la tabla 19, se visualiza que, para el indicador del control informático en su prueba inferencial, los resultados para el nivel de significancia en el Re-test fue de 0,070 y para el Post-test, 0,067. Por lo cual se determina que el indicador se ajusta a una distribución normal o paramétrica (P > 0.05). que fueron obtenidos luego de realizar la comparación mediante las fichas de registro del antes durante y después.

Tabla 19

Prueba de normalidad – Control informático.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Re_Control_informático	,867	20	,070
Post_Control_informático	,880	20	,067

Fuente, Elaboración propia.

Los resultados de la inferencia para el control informático se muestran en las figuras 19 y la figura 20, las mismas indican que el nivel de significancia en el Pre-test fue de 0,070 y para el Post-test, 0,067. Por lo cual se determina que el indicador se ajusta a una distribución normal o paramétrica (P > 0.05). que fueron obtenidos luego de realizar la comparación mediante las fichas de registro, dando como resultado que la mayoría de los encuestados aceptan y mantienen desde la gerencia, realizar un plan de mejora donde se mantenga el control informático.

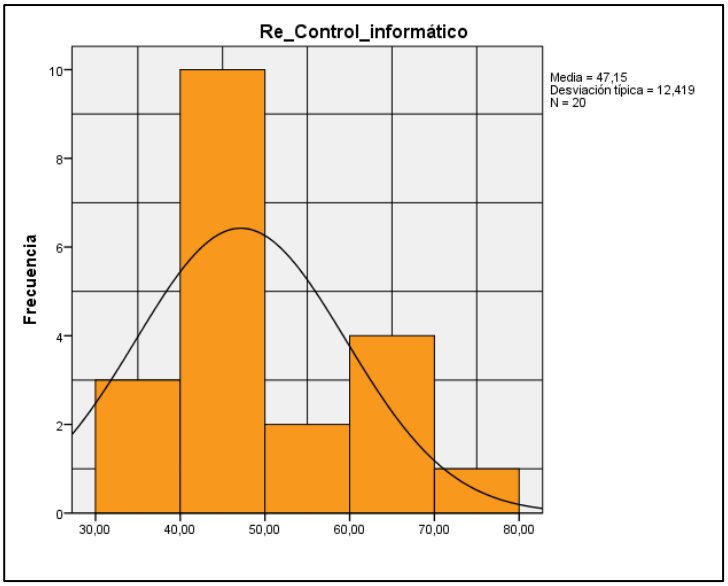


Figura 19, Control informático Re-test.

Fuente, Elaboración propia.

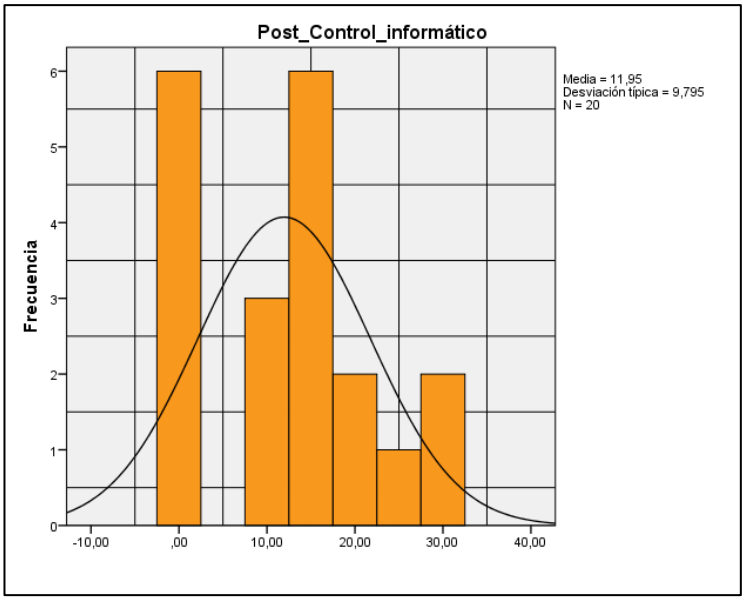


Figura 20, Control informático Post-test

Fuente, Elaboración propia.

3.2. Resultados de la Variable Independiente

Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27002.

Para darle respuesta, al sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27002, se sometió a evaluación mediante Juicio de Expertos el SGSI diseñado con propósitos de validar dicho diseño en base a los criterios de claridad, objetividad, actualidad, organización, suficiencia, intencionalidad, consistencia, coherencia, metodología, pertinencia. Los aspectos de validación y los puntajes obtenidos de dicho instrumento son mostrados a continuación:

Tabla 20

Resultados de la Variable Independiente

Experto	CLARIDAD	OBJETIVIDAD	ACTUALIDAD	ORGANIZACIÓN	SUFICIENCIA	INTENCIONALIDAD	CONSISTENCIA	COHERENCIA	METODOLOGÍA	PERTINENCIA
Experto 1	95	95	95	95	95	95	95	95	95	95
Experto 2	95	90	95	90	95	90	95	95	95	95
Experto 3	95	95	95	95	95	95	95	95	95	95
PROMEDIO	95.00	93.33	95.00	93.33	93.33	91.67	93.33	95.00	95.00	95.00

Fuente, Elaboración propia.

En relación con la tabla 20, se muestran los resultados acerca de los puntajes obtenidos por cada experto, a continuación, tabla 21, donde se concibe un 94,5% de fidelidad en el instrumento practicado:

Tabla 21

Promedio de validación del SGSI

Experto	Promedio	Promedio Final
Experto 1	95,00	
Experto 2	93,50	94,50
Experto 3	95,00	

Fuente, Elaboración propia.

A continuación, los resultados de la variable independiente basado en el juicio de expertos:

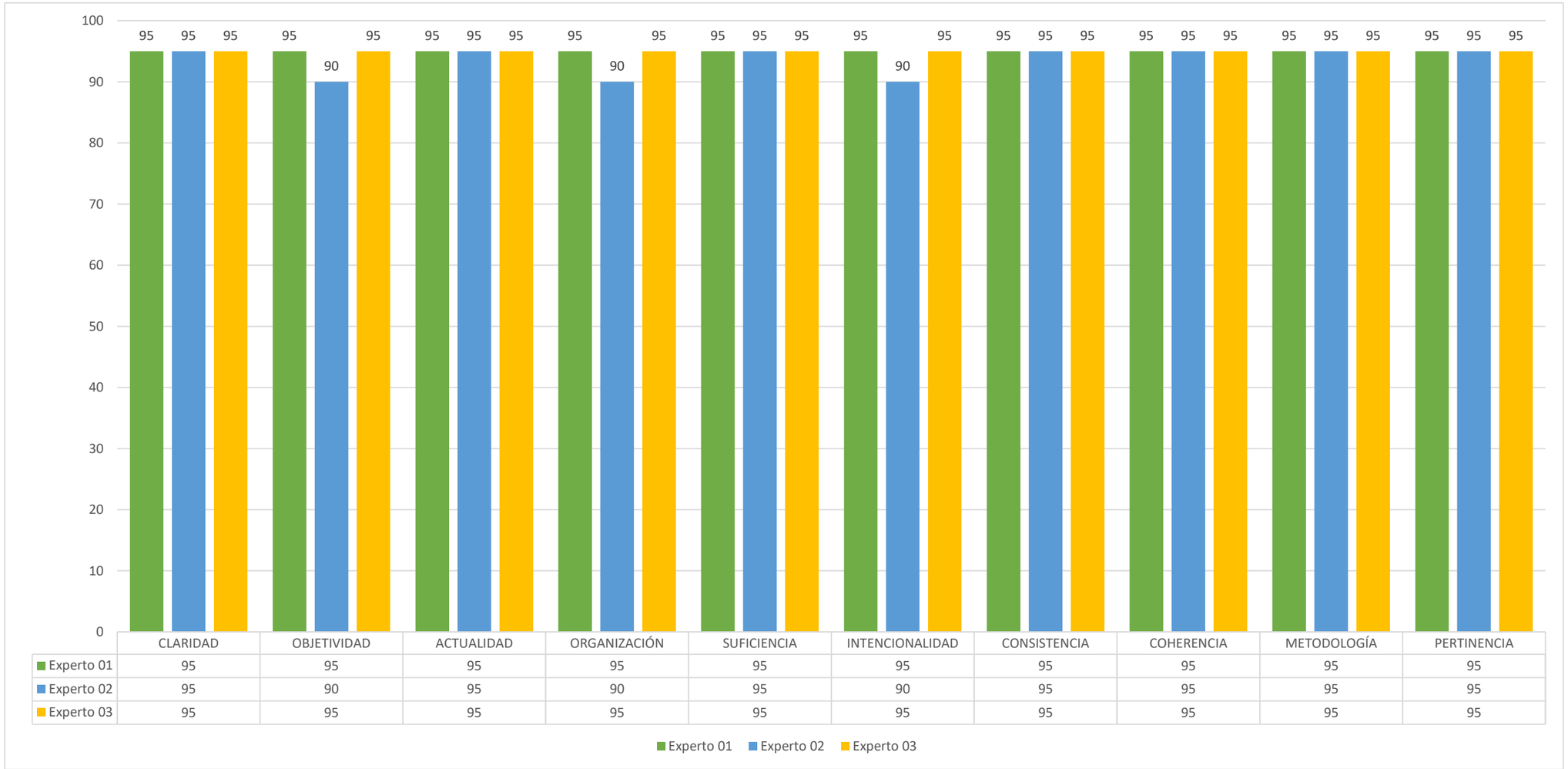


Figura 21, Resultados de la Variable Independiente.

Fuente, Elaboración propia.

3.3. Resultados de la Variable Dependiente

Seguridad informática en la empresa Rash Perú S.A.C.

Con respecto a la Seguridad informática en la empresa Rash Perú S.A.C. se presentan los indicadores respectivos:

3.3.1. Dimensión “Seguridad de la Información”

Pregunta 01: ¿El nivel de seguridad de los equipos es óptimo para operar con el OFISMART?

Objetivo: Establecer los procedimientos, herramientas y mecanismos implementados en los equipos de cómputo utilizados durante el proceso del OFISMART.

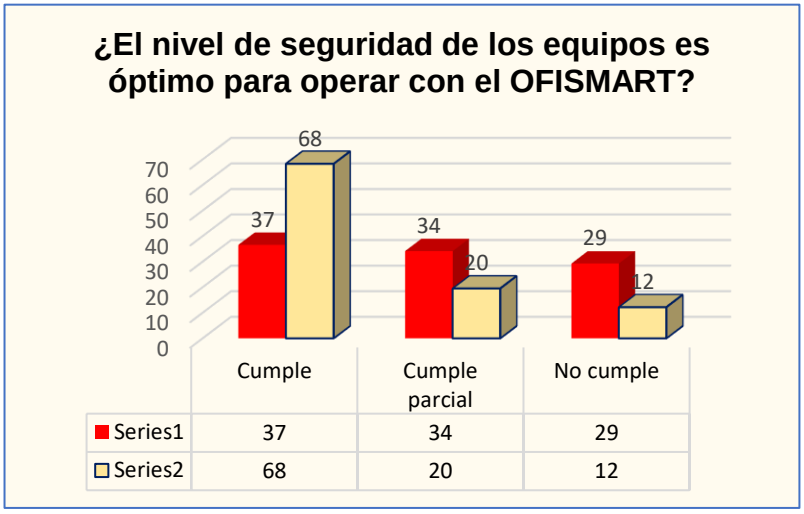


Figura 22, Indicador Nivel de seguridad de equipos.

Fuente, Elaboración propia.

Tabla 22

Indicador Nivel de seguridad de equipos

Criterio	% Pre test	% Post test
Cumple	37	68
Cumple parcial	34	20
No cumple	29	12

Fuente, Elaboración propia.

Se puede distinguir que solo el 37% de los usuarios que hacen uso del OFISMART tuvieron implementado procedimientos para asegurar el tratamiento de la data contenida en sus equipos de cómputo, por ejemplo, antivirus actualizado, SOFTWARE. original, acceso a los sistemas con claves, política de escritorio limpio, etc. Luego de aplicado las recomendaciones del SGSI fundamentado en la IS0/IEC 27002 se evidencia un mejoramiento en el nivel de SI y mayor confianza en los sistemas en línea al que pertenece el OFISMART. Cabe resaltar que es importante concientizar a los usuarios respecto a disminuir los niveles de riesgos tradicionales y nuevos a los que estamos expuestos, por lo tanto, cualquier política, procedimiento o técnica para asegurar la data no debe verse como un gasto, pero si como una inversión.

Pregunta 02: ¿Existe una política o procedimiento para la gestión de claves de cifrado?

Objetivo: Conocer la existencia y aplicación de gestores de claves criptográficas para proporcional altos niveles de seguridad, garantizar las políticas de SI y reducir los riesgos de violación a la integridad de los datos.

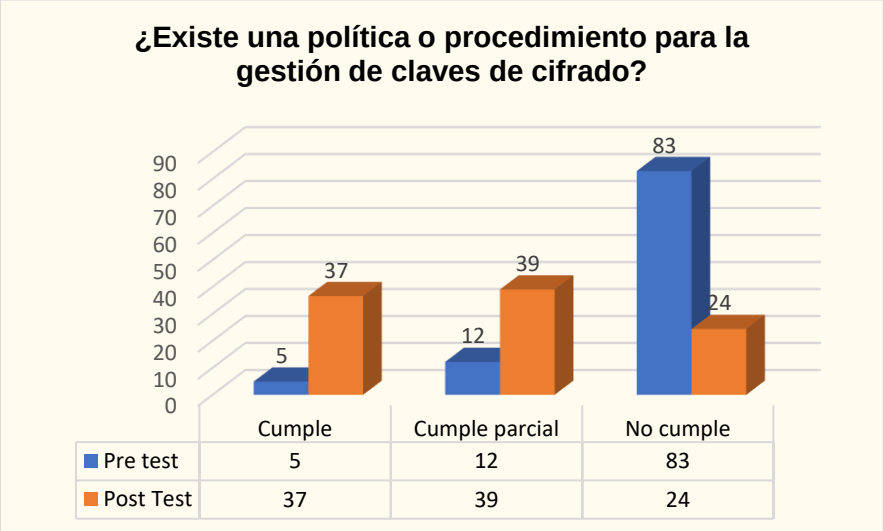


Figura 23, Indicador Nivel de políticas de gestión de claves de cifrado

Fuente, elaboración propia.

Tabla 23

Indicador Nivel de políticas de gestión de claves de cifrado

Criterio	% Pre test	% Post test
Cumple	5	37
Cumple parcial	12	39
No cumple	83	24

Fuente, elaboración propia.

Se puede distinguir que solo el 5% de los colaboradores tenían conocimiento de la existencia y por el ende la aplicación de políticas oficiales o procedimientos documentados para realizar el cambio de claves, aseguramiento de confidencialidad de claves y niveles de complejidad durante el acceso al sistema operativo, aplicaciones, dispositivos de seguridad tales como los lectores biométricos, utilizados para verificar la identidad de los participantes en la constitución de una empresa. Luego de la aplicación de las recomendaciones del SGSI se evidenció mejoramiento significativo en la seguridad otorgada a través de las herramientas utilizadas en el OFISMART.

Pregunta 03: ¿Se dispone de un procedimiento para la gestión de cambio?
Objetivo: Mejorar los procedimientos frente a una nueva actividad dentro de los procesos, creación de un nuevo cargo en la empresa, cambio de equipamiento, modificación del ambiente de trabajo, cuando exista un accidente y/o incidente de trabajo y/o cuando se implementen propuestas de acciones de mejoramiento.

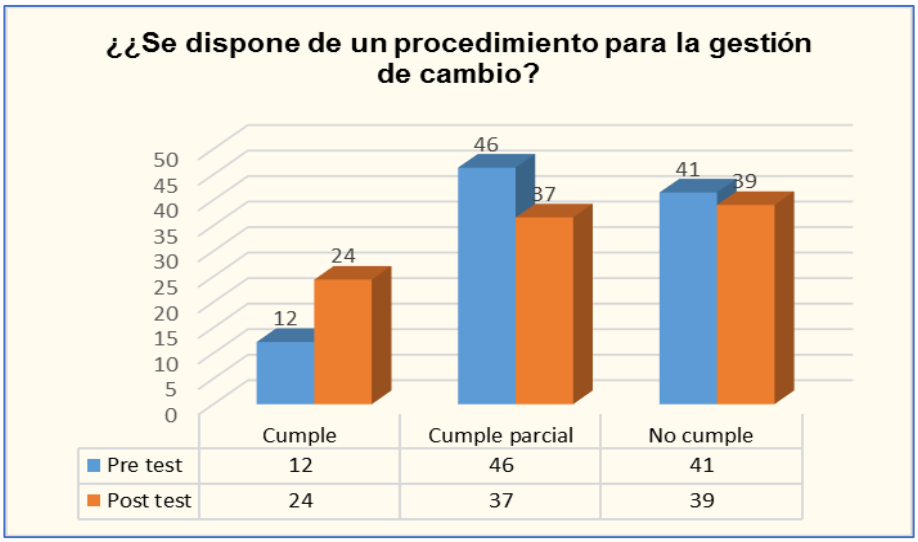


Figura 24, Indicador Nivel de procedimiento para la gestión de cambio.

Fuente, Elaboración propia.

Tabla 24

Indicador Nivel de procedimiento para la gestión de cambio

Criterio	% Pre test	% Post test
Cumple	12	24
Cumple parcial	46	37
No cumple	41	39

Fuente, Elaboración propia.

Se logró evidenciar que solamente el 12% de los colaboradores tenían conocimiento de políticas respecto un cambio de estado u operatividad de los sistemas o equipamiento, las actualizaciones, cambios de SOFTWARE., asignación de equipos a nuevo personal se realizaban de forma tradicional y monótona, el control de incidencias era artesanal y manual.

Pregunta 04: ¿Existe una política de control de accesos debidamente documentada y se revisa constantemente?

Objetivo: Establecer los mecanismos, procesos y procedimientos para llevar un mejor control de los niveles de acceso del personal y usuario externo que tenga acceso a la información.

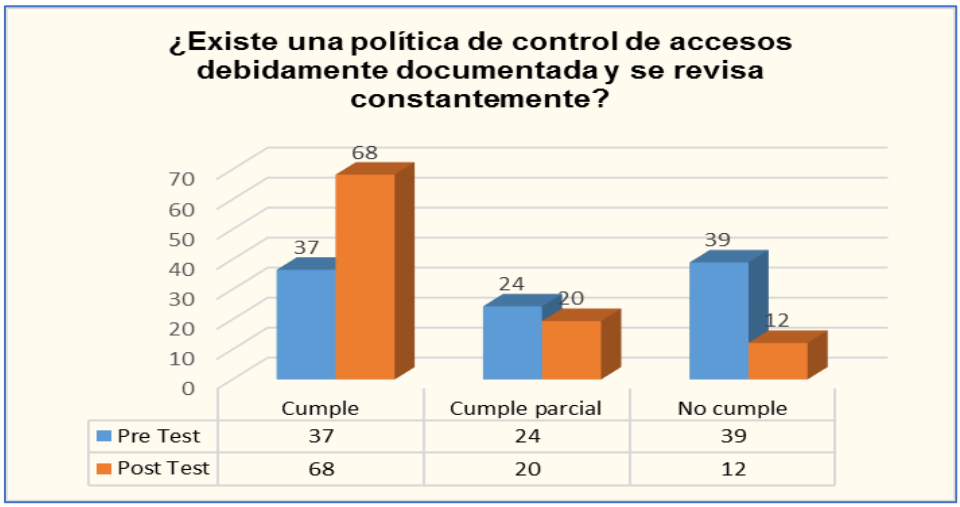


Figura 25, Indicador Nivel de políticas de control de accesos

Fuente, Elaboración propia.

Tabla 25

Indicador Nivel de políticas de control de accesos

Criterio	% Pre test	% Post test
Cumple	37	68
Cumple parcial	24	20
No cumple	39	12

Fuente, Elaboración propia.

Se puede distinguir que solo el 37% de los encuestados recibió información acerca del nivel de acceso a los sistemas al inicio de su relación laboral, no existía documentación al respecto durante el cambio de estado, descanso, permiso, vacaciones, cambio de puesto de trabajo. Luego de aplicado las recomendaciones del SGSI se revisaron los procedimientos y se elaboró políticas y documentos para el monitoreo de políticas de accesos a los sistemas.

Pregunta 05: ¿Con la finalidad de reducir alteraciones y/o modificaciones sin autorización o hacer mal uso de la información o servicios, las funciones y las responsabilidades son separados o segregados?

Objetivo: Establecer según la función a cumplir, las responsabilidades sobre la manipulación de la información y cuidado de los activos.

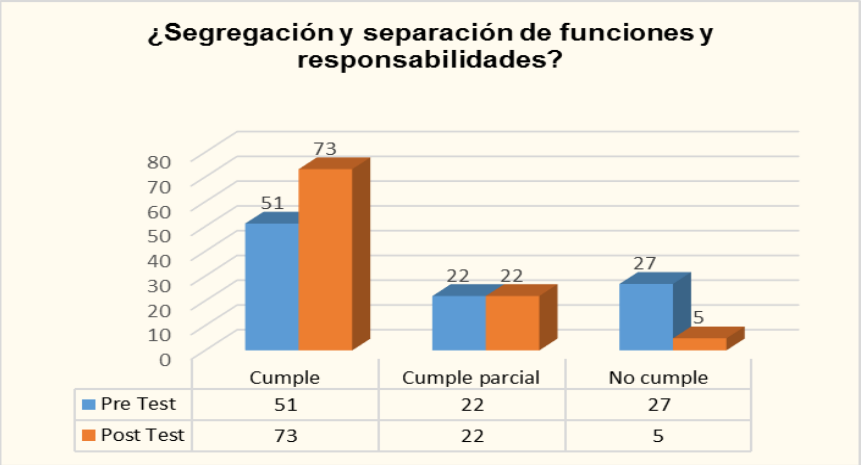


Figura 26, Indicador Nivel de segregación de funciones y responsabilidades.

Fuente, Elaboración propia.

Tabla 26

Indicador Nivel de segregación de funciones y responsabilidades

Criterio	% Pre test	% Post test
Cumple	51	73
Cumple parcial	22	22
No cumple	27	5

Fuente, Elaboración propia.

Se logró distinguir que 51% de los colaboradores tenían conocimiento que los encargados de las unidades de TI eran los responsables del tratamiento de la información y del mantenimiento del parque informático, en algunos casos por la escasez de personal de TI. Luego de aplicado las recomendaciones del SGSI se procedieron a seleccionar responsables para tareas importantes como la aplicación de las políticas del *backup*,

elaboración de planes de contingencia, implementación de controles para el aseguramiento de las informaciones.

Pregunta 06: ¿Los controles aseguran que los usuarios sólo tienen acceso a los recursos de la red a los cuales han sido autorizados a utilizar según sus funciones?

Objetivo: Validar el cumplimiento de los controles según el nivel de acceso establecido a cada empleado o proveedor en la función y cargo que desempeña en la institución.

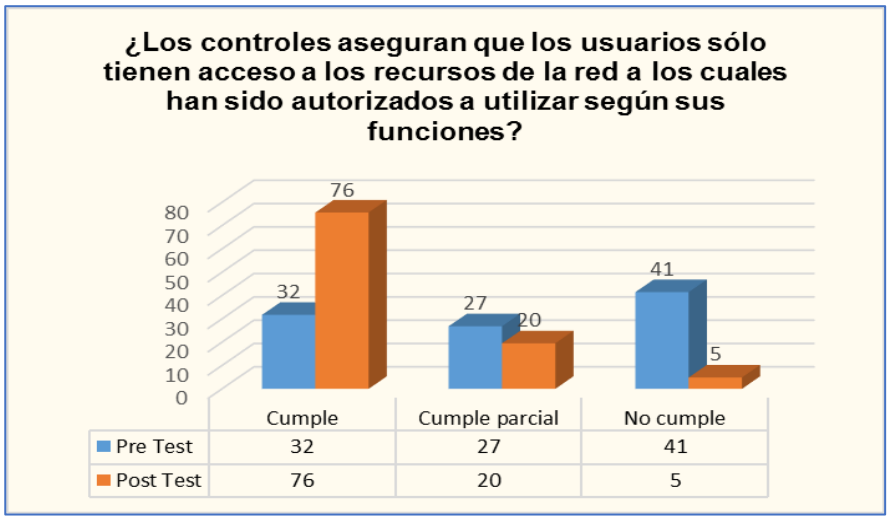


Figura 27, Indicador Nivel de aseguramiento de controles de seguridad.

Fuente, Elaboración propia.

Tabla 27

Indicador Nivel de aseguramiento de controles de seguridad

Criterio	% Pre test	% Post test
Cumple	32	76
Cumple parcial	27	20
No cumple	41	5

Fuente, Elaboración propia.

Se logró distinguir que el 32% de los colaboradores tenía acceso a los recursos autorizados y mencionados por el jefe de la unidad de TI, los demás tenían acceso a ciertos aplicativos de escritorio y Web en ciertas PC donde se encontraba guardado el usuario y contraseña, acceso a carpetas compartidas con información sensible, acceso a servidores a través de usuarios y claves por Default. Luego de aplicado las recomendaciones del SGSI se revisaron los accesos y se elaboraron políticas y documentación para proteger la información de Rash Perú S.A.C.

Pregunta 07: ¿Existe un procedimiento para garantizar que los accesos de los usuarios sean eliminados al finalizar el vínculo laboral, contractual o cambio de puesto de trabajo?

Objetivo: Establecer los mecanismos de control al finiquitar la relación laboral de los empleados y finalización contractual de los proveedores que tuvieron acceso a la información de Rash Perú S.A.C.

Tabla 28

Indicador Nivel de procedimientos para eliminación de accesos

Criterio	% Pre test	% Post test
Cumple	7	63
Cumple parcial	24	22
No cumple	68	15

Fuente, Elaboración propia.

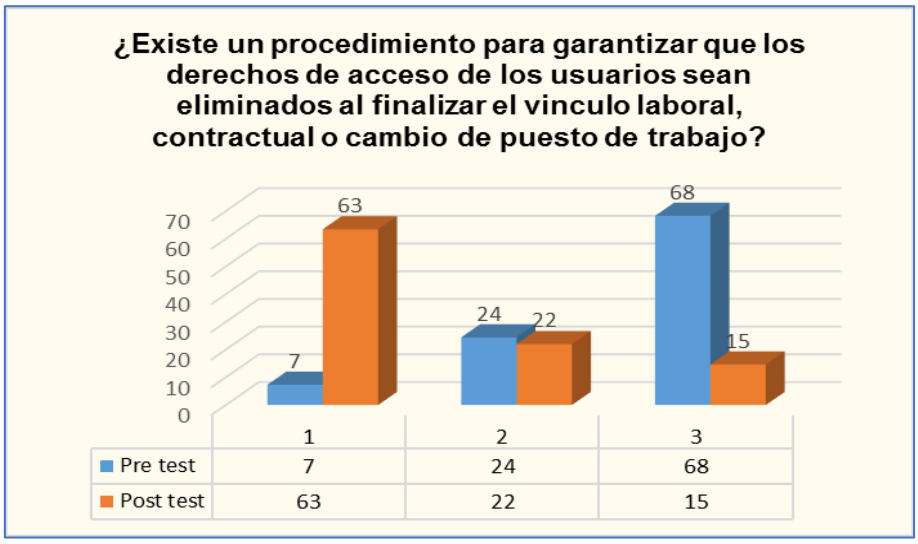


Figura 28, Indicador Nivel de procedimientos para eliminación de accesos.

Fuente, Elaboración propia.

Se puede distinguir que solo el 7% de los colaboradores realizaba labores de verificación de acceso a los sistemas del personal al momento que dejaba de laborar y en el caso de los proveedores, cuando estos terminaban su relación contractual. Luego de aplicado la recomendación del SGSI se implementó políticas para el control inmediato de cada personal de Rash Perú S.A.C.

Tabla 29

Resumen de contrastación indicadores de la Dimensión "Seguridad de la Información"

Ítem	Check list de preguntas realizadas a muestra de la población	Pre Test	Post Test	Observaciones
1	¿El nivel de seguridad de los equipos es óptimo para operar con el SID?	Medio	Alto	Valor aceptable
2	¿Existe una política o procedimiento para la gestión de claves de cifrado?	Bajo	Medio	En proceso

3	¿Se dispone de un procedimiento para la gestión de cambio?	Bajo	Medio	En proceso
4	¿Existe una política de control de accesos debidamente documentada y se revisa constantemente?	Medio	Alto	Valor aceptable
5	¿Con la finalidad de reducir alteraciones y/o modificaciones sin autorización o hacer mal uso de la información o servicios, las funciones y las responsabilidades son separados o segregados?	Medio	Alto	Valor aceptable
6	¿Los controles aseguran que los usuarios sólo tienen acceso a los recursos de la red a los cuales han sido autorizados a utilizar según sus funciones?	Medio	Alto	Valor aceptable
7	¿Existe un procedimiento para que los derechos de acceso de los usuarios sean eliminados al finalizar el vínculo laboral, contractual o cambio de puesto de trabajo?	Bajo	Alto	Valor aceptable

Fuente, Elaboración propia.

3.3.2. Dimensión "Riesgo de la Información".

Pregunta 08: ¿Todos los empleados y proveedores firman acuerdos de confidencialidad y no divulgación?

Objetivo: Establecer que los empleados de Rash Perú S.A.C cuenten en su contrato de relación laboral con la compañía, acuerdos de confidencialidad de las informaciones a la que puede a tener accesos. Del mismo modo con los proveedores y personal externo con acceso a los componentes críticos (Token criptográficos, lector biométrico, discos duros, *storage* y otros).

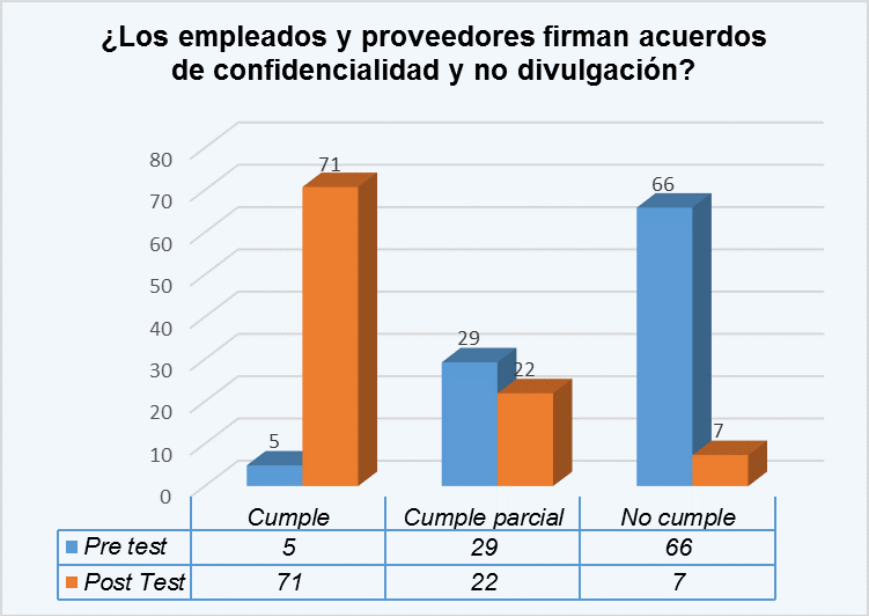


Figura 29, Indicador Nivel de aceptación de acuerdos.

Fuente, Elaboración propia.

Tabla 30

Indicador Nivel de aceptación de acuerdos

Criterio	% Pre test	% Post test
Cumple	5	71
Cumple parcial	29	22
No cumple	66	7

Fuente, Elaboración propia.

Se puede distinguir que solo el 5% de los colaboradores incluían en su relación contractual, ciertos acuerdos para preservar la confidencialidad de las informaciones a la cual se tiene acceso. La fuga de información se constituye en una pérdida para Rash Perú S.A.C, puesto que este se constituye en ingresos vía publicidad manual o en línea. Luego de aplicado la recomendación del SGSI se implementó políticas para el control de la información, desde medidas disciplinarias hasta bloqueo de acceso a internet, bloqueo de puertos, implementación de tablas de auditoria en los sistemas de publicidad.

Pregunta 09: ¿Existe procedimientos para la destrucción de la data contenida en equipos sensibles cuando estos sean dados de baja?

Objetivo: Establecer la existencia y aplicación de procedimientos para la eliminación y destrucción efectiva de dispositivos donde se almacena información sensible, claves, códigos de acceso utilizados en la institución, tales como discos duros, storage, memorias, insumos agotados de impresoras, cámaras digitales, y otros.

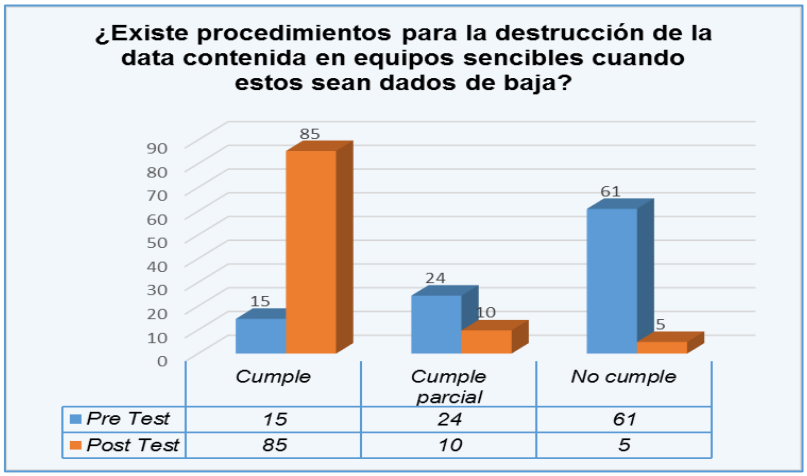


Figura 30, Indicador Nivel de existencia de procedimientos de destrucción.

Fuente, Elaboración propia.

Tabla 31

Indicador Nivel de existencia de procedimientos de destrucción

Criterio	% Pre test	% Post test
Cumple	15	85
Cumple parcial	24	10
No cumple	61	5

Fuente, Elaboración propia.

Se puede distinguir que solo el 15% de los colaboradores tenían procedimientos apropiados para la eliminación y destrucción de la data contenida en los equipos de cómputo, las PC eran dados de baja con la sin

la formatear los discos duros, los insumos de las impresoras térmicas contenían información sensible, memorias y disco externos con alguna avería solo eran desechados. Luego de aplicado la recomendación del SGSI se implementó políticas y procedimientos para dar de baja a los equipos de cómputo obsoletos o con alguna avería.

Pregunta 10: ¿Existe una política sobre el uso de técnicas criptográficas para el tratamiento de la información transmitida en el OFISMART?
Objetivo: Conocer las técnicas y herramientas utilizadas para proteger la información tratada a través de Token criptográficos y lectores biométricos, herramientas actualmente primordiales para verificar la identidad y autenticidad del usuario y colaborador que realiza movimientos en el sistema OFISMART.

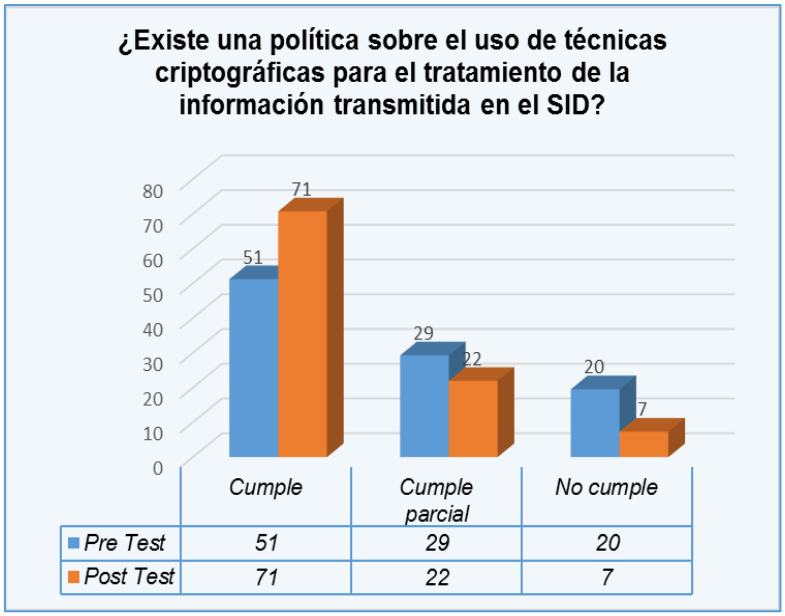


Figura 31, Indicador Nivel de existencia de políticas criptográficas.
Fuente, Elaboración propia.

Tabla 32

Indicador Nivel de existencia de políticas criptográficas

Criterio	% Pre test	% Post test
Cumple	51	71
Cumple parcial	29	22
No cumple	20	7

Fuente, Elaboración propia.

Se logró distinguir que el 51% de los colaboradores tenían conocimiento de la funcionalidad y la existencia incipiente de políticas de protección a las herramientas utilizadas en la actualidad en el tratamiento de información a través del OFISMART. Por ser una tecnología recién utilizada en este tipo de compañías, no se han presentado incidencias de pérdida, robo o secuestro, por lo que, en esta investigación se recomienda la implementación de políticas para proteger la confidencialidad de las claves de acceso a través de los lectores biométricos y que las firmas contenidas en los Token criptográficos no puedan ser utilizado por otra persona que tenga acceso a la clave o PIN personal.

Pregunta 11: ¿Los datos y/o documentos se encuentran protegidos contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales del negocio?

Objetivo: Verificar si se cuenta con políticas, procedimientos y documentación según las normas vigentes para proteger la información ante pérdida, siniestro, secuestro u otro que eleve el nivel de riesgos.

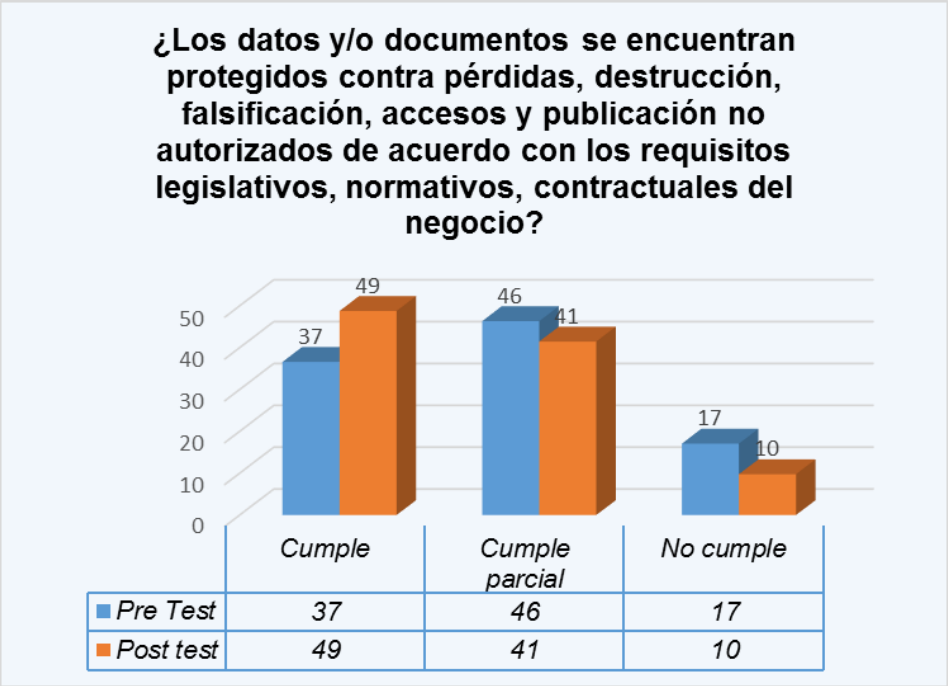


Figura 32, Indicador Nivel de protección de datos.

Fuente, Elaboración propia.

Tabla 33

Indicador Nivel de protección de datos

Criterio	% Pre test	% Post test
Cumple	37	49
Cumple parcial	46	41
No cumple	17	10

Fuente, Elaboración propia.

Se puede distinguir que el 37% de los encuestados tenían documentación de acuerdo a ley para frente a una incidencia o siniestro, los documentos de garantía de equipos de cómputo y SOFTWARE. establecían las condiciones de compra. Después de la implementación del SGSI se mejoró los procedimientos incrementando o actualizando los manuales de contingencia en Rash Perú S.A.C.

Pregunta 12: ¿Se dispone de planes y equipamiento para la continuidad operativa del servicio del OFISMART?

Objetivo: Mejorar la continuidad del OFISMART implementando políticas que permitan la alta disponibilidad del servicio.

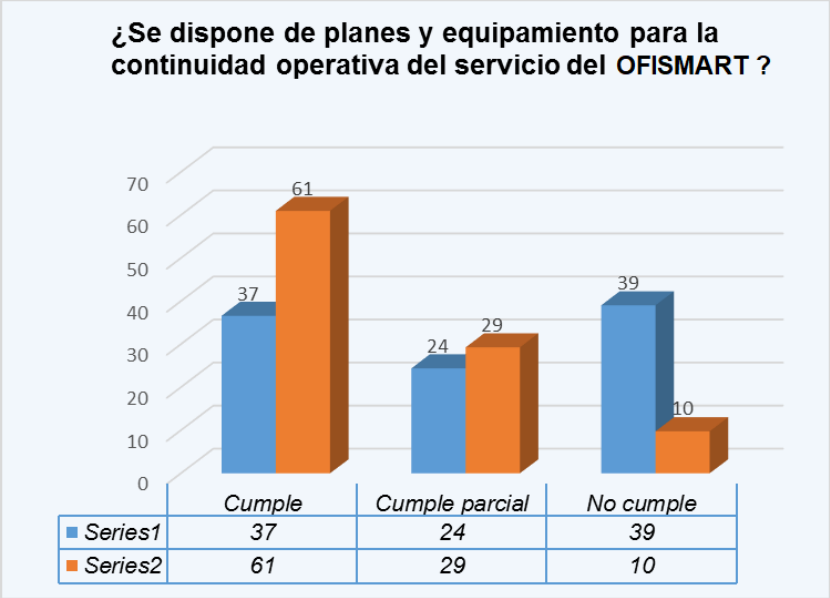


Figura 33, Indicador Nivel de planes para la continuidad operativa.

Fuente, Elaboración propia.

Tabla 34

Indicador Nivel de planes para la continuidad operativa

Criterio	% Pre test	% Post test
Cumple	37	61
Cumple parcial	24	29
No cumple	39	10

Fuente, Elaboración propia.

Se logró distinguir que el 37% de los colaboradores tenían planes y procedimientos para asegurar la continuidad del negocio, contando entre ellos, UPS y generadores eléctricos, PC de respaldo y *backup* de la data.

El punto crítico se presenta en la disponibilidad de los lectores biométricos y Token criptográficos, los cuales, ante una avería, o pérdida, son repuestos en un aproximado de un (01) mes posterior de haber realizado el trámite ante la oficina de TI, lo que conlleva a la inscripción tradicional de forma manual. Luego de aplicado las recomendaciones del SGSI se evidenciaron mejoras en la implementación de políticas para la reposición inmediata de las herramientas utilizadas por Rash Perú S.A.C.

Tabla 35

Resumen de contrastación indicadores de la Dimensión "Riesgo de la Información"

Ítem	Check list de preguntas realizadas a muestra de la población	Pre Test	Post Test	Observaciones
1	¿Todos los empleados y proveedores firman acuerdos de confidencialidad y no divulgación?	Bajo	Alto	Valor aceptable
2	¿Existe procedimientos para la destrucción de la data contenida en equipos sensibles cuando estos sean dados de baja?	Bajo	Alto	Valor aceptable
3	¿Existe una política sobre el uso de técnicas criptográficas para el tratamiento de la información transmitida en el OFISMART?	Alto	Alto	Valor aceptable
4	¿Los datos y/o documentos se encuentran protegidos contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales del negocio?	Medio	Medio	En proceso

5	¿Se dispone de planes y equipamiento para la continuidad operativa del servicio del OFISMART?	Medio	Medio	En proceso

Fuente, Elaboración propia.

3.3.3. Dimensión "Programas de Capacitación y Concientización"

Pregunta 13: ¿Se realiza capacitación integral en temas de seguridad de la información a los empleados y usuarios del OFISMART?

Objetivo: Sugerir al Área de TI de Rash Perú S.A.C, la implementación de cursos para los empleados y usuarios del OFISMART referente a temas de SI.

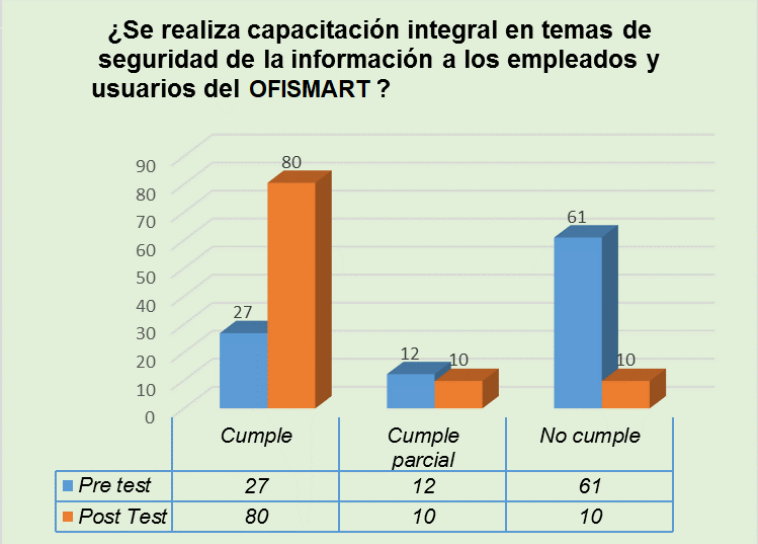


Figura 34, Indicador Nivel de capacitaciones de seguridad de la información.

Fuente, Elaboración propia.

Tabla 36

Indicador Nivel de capacitaciones de seguridad de la información

Criterio	% Pre test	% Post test
Cumple	27	80
Cumple parcial	12	10
No cumple	61	10

Fuente, Elaboración propia.

Se logró distinguir que el 27% de los colaboradores fue capacitado en la operatividad del OFISMART, en la configuración del terminal de red cumpliendo con los requerimientos del sistema. Luego de las recomendaciones del SGSI se elaboró manuales de configuración y de uso más detallados y se realizaron pruebas de ensayo en línea con la finalidad adiestrar al personal de TI para que sirva de apoyo a los demás usuarios del sistema.

Pregunta 14: ¿Se elabora publicidad de concientización respecto a temas de seguridad de la información?

Objetivo: Recomendar la elaboración de guías ilustrativas, manuales del OFISMART, panfletos y afiches de concientización respecto a temas de seguridad informática y de la información y que estos sean vistos de forma integral a todo el personal perteneciente a Rash Perú S.A.C.

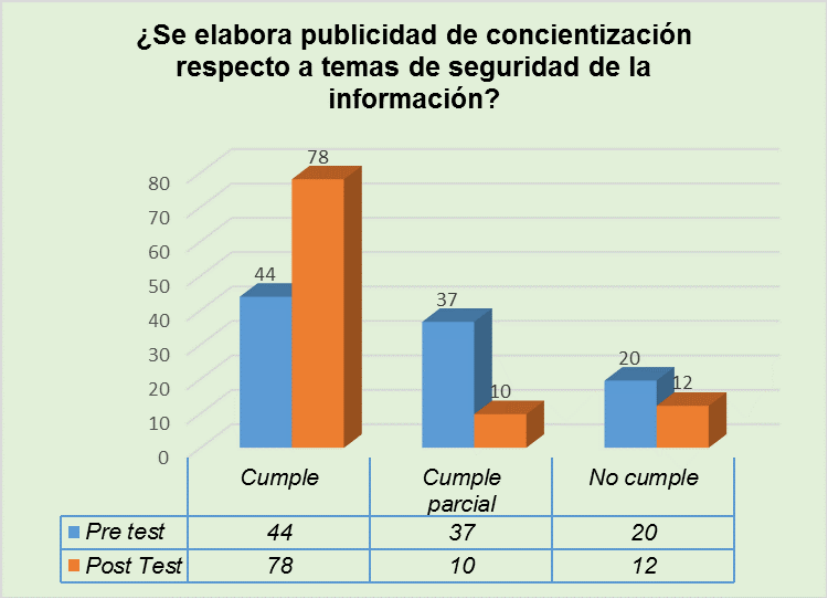


Figura 35, Indicador Nivel de concientización de seguridad de la información.

Fuente, Elaboración propia.

Tabla 37

Indicador Nivel de concientización de seguridad de la información

Criterio	% Pre test	% Post test
Cumple	44	78
Cumple parcial	37	10
No cumple	20	12

Fuente, Elaboración propia.

Se logró distinguir que el 44% de los colaboradores elabora afiches y coordina con personal del área de imagen con el fin de señalizar ambientes sensibles, verbigracia, alertas eléctricas, zonas de wifi, complejidad de claves de acceso, precaución en el uso de cuentas de usuario en los SOFTWARE.s de escritorio y con mayor énfasis en sistemas Web. Luego de aplicado el SGSI se mejoró la calidad de la información impresa en afiches y enviada digitalmente a los correos electrónicos de los colaboradores de Rash Perú S.A.C.

Tabla 38

Resumen de contrastación indicadores de la Dimensión "Programas de Capacitación y Concientización"

Ítem	Check list de preguntas realizadas a muestra de la población	Pre Test	Post Test	Observaciones
1	¿Se realiza capacitación integral en temas de seguridad de la información a los empleados y usuarios del OFISMART?	Medio	Medio	En Proceso
2	¿Se elabora publicidad de concientización respecto a temas de seguridad de la información?	Medio	Alto	Valor aceptable

Fuente, Elaboración propia.

3.4. Discusión de resultados

Respecto al objetivo específico 1 Diagnosticar el estado actual del Nivel de Seguridad Informática en la compañía Rash Perú S.A.C, se pudo evidenciar que Rash Perú presentaba deficiencia en cuanto a la gestión de la SI reflejándose en la tabla 6 Análisis descriptivo Re-test y Post-test de Seguridad de la información, el valor promedio del Re-test fue de 69.90% y el valor promedio Post-test fue de 14.00%. Además, el valor mínimo del re-test fue 50%, el valor máximo es 88%, y el valor mínimo del post-test es 0% y el máximo es 27%. Estos resultados se contrastan con los aludidos por Jassim et al. (2022) quienes mostraron que, existía una brecha del 49% y 51% coincidente debido a la falta de establecimiento de una política de SI en la sección. Asimismo, también se contrastan con los revelados por Fonseca et al. (2021) quienes mostraron que, existían activos informáticos, vulnerabilidades técnicas y riesgos aplicados la totalidad de procesos en dicho caso de estudio, también se evidenció falta de un plan de formación y educación en SI para las personas inmersas en los procesos mejorando el proceso en un 70% a comparación antes de haberse implementado la seguridad de la información. Finalmente, también concuerdan con los mencionados por Ferreira (2020) quien implementar un SGSI para una entidad estatal perteneciente a dicho país europeo el cual debería estar ensimismado en la norma IS0/IEC 27001 para entidades públicas portuguesas. Su estudio reveló que, en dicho caso de estudio no se venían desplegando actividades para el aseguramiento de la SI ya que antes de su implementación nos arrojaba un 35% mostrando una deficiencia en sus niveles de seguridad de la información lo que mejoró notablemente hasta alcanzar el 80% en sus niveles de seguridad de la información, desembocando en que a veces se pedía que se realizaran tareas y no se daba un marco sobre el propósito de esa tarea o se tomaban decisiones y no se explicaban las razones, además de la carencia de controles de SI.

Respecto al objetivo específico 2, Desarrollar un SGSI fundamentado en la Norma ISO/IEC 27002 para la empresa caso de estudio, se desarrolló dicho SGSI basada en dicha norma pues la ISO 27002 es una norma complementaria que se centra en los controles de SI que las organizaciones pueden optar por implementar. Asimismo, con el desarrollo de ISO 27002, las operaciones

comúnmente llevadas a cabo, conceptualizadas como mejores praxis, se ofrecieron como procedimientos y métodos probados en la práctica, que podría ser adaptados a los requisitos determinados de las unidades organizacionales, tal y como fue el caso de Rash Perú S.A.C en nuestros resultados de la tabla 9 mostraron que el nivel de significancia en el Re-test fue de 0,265 y para el Post-test, 0,108. Por lo cual se determina que la seguridad de la información se ajusta a una distribución normal o paramétrica (P > 0.05).

Estos resultados concuerdan con los revelados por Alvarado & Sánchez (2021) quienes desarrollar un SGSI fundamentado en la IS0/IEC 27002:2015 con propósitos de resguardar las informaciones vertidas en cuanto a la construcción de sus productos y servicios en una compañía dedicada a la construcción de SOFTWARE.s a medida en la ciudad limeña. Estos autores con la implementación del SGSI en dicha compañía mejoraron el nivel de la SI posicionándola en 81.8% con controles de seguridad, políticas de desarrollo seguro, protección de datos de pruebas, etcétera. Asimismo, contrastan también con los mencionados por Huayamave (2018) quien desarrolló un SGSI fundamentado en la ISO/IEC 27002 que permita evitar la materialización de dichos riesgos asociados a sus operaciones en los activos informáticos en una empresa caso de estudio perteneciente al sector constructor guayaquileño. Los resultados expusieron que, con al análisis y evaluación de los riesgos mitigados, éstos disminuyeron en un 50% y, con el plan de tratamiento de riesgos, de tratamiento de los riesgos, éstos disminuyeron en 47.70%.

Respecto al objetivo específico 3, Validar mediante juicio de expertos el SGSI diseñado previamente para la empresa Rash Perú S.A.C. Se validó dicho diseño mediante la técnica juicio de expertos con su instrumento ficha de juicio de expertos el cual se encuentra detallado en los anexos y que permitió darle el visto bueno a la que, en primera instancia fue la propuesta desarrollada por este investigador. Posterior e ello, se pudo implementar dicha propuesta en la empresa caso de estudio con lo que se pudieron documentar los resultados obtenidos según las dimensiones previamente detalladas. Esto concuerda con los resultados revelados por Aquino et al. (2020) quien contribuyó al mejoramiento del nivel de SI en una casa de estudios de la localidad de

Apurímac, lográndolo mediante implantación de un SGSI fundamentado en el estándar IS0/IEC 27001:2013. Para ello, primeramente, recolectaron informaciones previas a la implementación del SGSI acerca de los activos informáticos, posteriormente implementaron dicho SGSI haciendo usanza de la metodología PDCA y la metodología MAGERIT III, luego recolectaron nuevamente informaciones posteriores a la implementación de dicho SGSI y finalmente evaluaron los resultados en cuanto a los riesgos según activos. Asimismo, también concuerdan con los mencionados por Fuentes (2020) quien desarrolló un SGSI fundamentado en la ISO/IEC 27003 con propósitos de lograr el mejoramiento de la SI en una casa de estudios superiores en la localidad cajamarquina. Para ello, primeramente, realizaron un análisis previo acerca del nivel de cumplimiento de políticas de SI, luego realizaron una revisión de la literatura acerca de marcos y prácticas para la gestión de la SI, posteriormente, diseñaron el SGSI fundamentado en la ISO/IEC 27003, el cual, a posteriori fue validado mediante juicio de expertos para, finalmente, llevarlo a la praxis en dicho caso de estudio seleccionado.

Respecto al objetivo específico 4, Ejecutar una prueba piloto del SGSI en la empresa caso de estudio seleccionada, se ejecutó dicha prueba en la empresa RASH PERÚ S.A.C, para lo cual se requirió el permiso respectivo, con lo que posteriormente se procedió a realizar la aplicabilidad SOA, el diseño de los procedimientos y políticas internas en cuanto a seguridad informática y, el plan de capacitación y concientización, conllevando a obtener la mejora en resultados de mejoramiento significativo en el 100% de los indicadores para cada una de las tres (03) dimensiones, tanto “seguridad de la información” con un cumplimiento del 58.42%, “riesgo de la información” con un cumplimiento del 67.40% y, “Programas de Capacitación y Concientización” con un cumplimiento del 79.00% además en la tabla 10 los resultados mostraron que el nivel de significancia en el Re-test fue de 0,213 y para el Post-test, 0,201. Por lo cual se determina que el indicador se ajusta a una distribución normal o paramétrica (P > 0.05).

Estos resultados concuerdan con los obtenidos por, Alvarado & Sánchez (2021), quienes realizaron la investigación, *Information security in the process of system*

and product development through the implementation of security controls based on ISO 27002:2015 in the company BITNESS CORP S.A.C., 2020, en la Universidad Peruana Unión, en Lima, Perú, en la que también utilizaron un caso de estudio, una compañía dedicada a la construcción de SOFTWARE.s a medida en la ciudad limeña, en la que obtuvieron como resultados que, la empresa poseía el nivel Parcialmente Logrado en cuanto a controles de SI (48.95%), evidenciándose carencias en cuanto al proceso de construcción de SOFTWARE.. Se concluyó que con la implementación del SGSI en dicha compañía limeña constructora de SOFTWARE. se mejoró el nivel de la SI posicionándola en 81.8% con controles de seguridad, políticas de desarrollo seguro, protección de datos de pruebas, etcétera.

Respecto al objetivo específico 5, Evaluar los resultados obtenidos posteriores a la implementación del SGSI, para lograr dicho cometido, se llevó a cabo una encuesta considerando a la totalidad de colaboradores de RASH PERÚ S.A.C que ejecutaban operaciones asociadas con el manejo de los sistemas de dicha compañía, cuya población ascendió a 100 colaboradores a quienes se les remitió un cuestionario constituido por catorce (14) reactivos considerando las tres dimensiones de la seguridad informática, con lo que se pudo evaluar el mejoramiento de los indicadores asociados a cada una de dichas dimensiones, logrando que el 64.29% de los indicadores tuvieron un rango de valoración de “Valor Aceptable”, mientras que el 35.71% de los indicadores restantes tuvieron un rango de valoración “En Proceso”, pasando también a su vez, de carecer de controles de seguridad informática, a un total de 66 controles divididos en 14 dominios de la ISO/IEC 27002:2013, evidenciándose mejoramiento en cuanto al uso de los activos informáticos de los cuales dispone RASH PERÚ S.A.C además en la tabla 7 el valor promedio del Re-test fue de 52.60% y el valor promedio Post-test fue de 11.40%. Además, el valor mínimo del re-test fue 40%, el valor máximo es 70%, y el valor mínimo del post-test es 0% y el máximo es 22%.

Estos resultados concuerdan con los obtenidos por Bravo & Yoo (2019), quienes realizaron la investigación, *Developing an Information Security Management System for Libraries Based on an Improved Risk Analysis Methodology*

Compatible with ISO/IEC 27001, en la Escuela Politécnica Nacional, en Quito, Ecuador, quienes desarrollaron un SGSI para bibliotecas ensimismado en una mejorada metodología de análisis de riesgos compatibilizada con la IS0/IEC 27001, en la se pudieron notar avances en varios dominios como la implementación de políticas de SI, ya que antes de implementar el SGSI, la mayoría de los controles de SI nunca habían sido desplegados, asimismo, el 51% de los controles especificados en la IS0/IEC 27002:2013 se encontraban en la fase “Inicial”, el 10% se encontraban en la fase “Repetible”, el 5% se encontraba en la fase “Definida” y el 3% de los controles se encontraban en fase “Gestionada”.

3.5. Aporte práctico

Para la presente investigación, se tomó como caso de estudio a una compañía limeña dedicada a comercializar productos tecnológicos. A continuación, se muestran las características principales de dicha compañía:

Nombre: RASH PERÚ S.A.C.
Nombre Comercial: COOLBOX - RADIOSHACK - URBAN RIDER
RUC: 20378890161
Dirección: Av. Salaverry Nro. 3310, Magdalena del Mar, Lima, Lima.
Fecha de inicio de actividades: 01/11/1997
Actividades Económicas: La actividad económica principal de la empresa se centra en la venta al por menor de equipos de sonido y video en comercios especializados, mientras que su actividad económica secundaria incluye la venta al por menor de ordenadores, periféricos, programas de informática y equipos de telecomunicaciones en comercios especializados.

Figura 36, Logo RASH PERÚ S.A.C.

Fuente, Elaboración propia.

Acerca del negocio: Rash Perú S.A.C., compañía peruana que comercializa e importa productos de diversas variedades en materia de seguridad, productos y mercaderías de video, telefonía fija y móvil, audio, comunicación, y entretenimiento en general. Dispone de mercaderías de su propia marca individual y de marcas terceras de trayectoria muy reconocidas a nivel internacional (tales como Apple, Samsung, HP, Huawei, entre otras más), así como con un progresivo aumento de establecimientos anexos para el desarrollo de sus ventas, conservando actualmente un posicionamiento notable en el mercado nacional. Rash Perú S.A.C es una compañía subsidiaria de RS Investment Corporation S.A.C., empresa con domicilio fiscal en el Perú, la cual ostenta su capital social en un 90%. El otro 10%, corresponde a Hozkel Vurnbrand, empresario peruano de gran reputación y reconocido en el ámbito comercial peruano.

Misión: "RASH PERÚ S.A.C pretende ofrecer a sus clientelas productos que cuenten con alto grado de innovación en el ámbito electrónico, de tecnologías de la información, logrando a través de ello, satisfacer y sobrepasar las expectativas previas de sus clientes, asegurando también con ello, la garantía de las marcas que provee".

Visión: "RASH PERÚ S.A.C pretende ser la opción número uno en electrónica y tecnologías de la información mediante canales de atención diversos en puntos estratégicos de América Latina".

Valores:

- Responsabilidad.
- Trabajo en equipo.
- Calidad.
- Seguridad.
- Dinamismo.
- Integridad.

Alineamiento:

RASH PERÚ S.A.C por intermedio de sus valores, visión y misión busca incrementar como empresa considerando, como sus estrategias más trascendentales, la búsqueda de acercar a sus consumidores hacia la compañía mediante la usanza de los canales de atención. Además, busca que la clientela, cuando se encuentre al interior de sus establecimientos logre experiencias de compra valiosas, las mismas que logren superar las expectativas con las que cuentan, mediante productos de gran innovación, agradable atención y una calidad de servicio óptima.

Figura 37, Alineamiento de la Misión, Visión y Valores de RASH PERÚ S.A.C.

Fuente, Elaboración propia.

En cuanto a la organización jerárquica de Rash Perú S.A.C, la compañía cuenta con la siguiente estructura que se muestra en la siguiente figura:

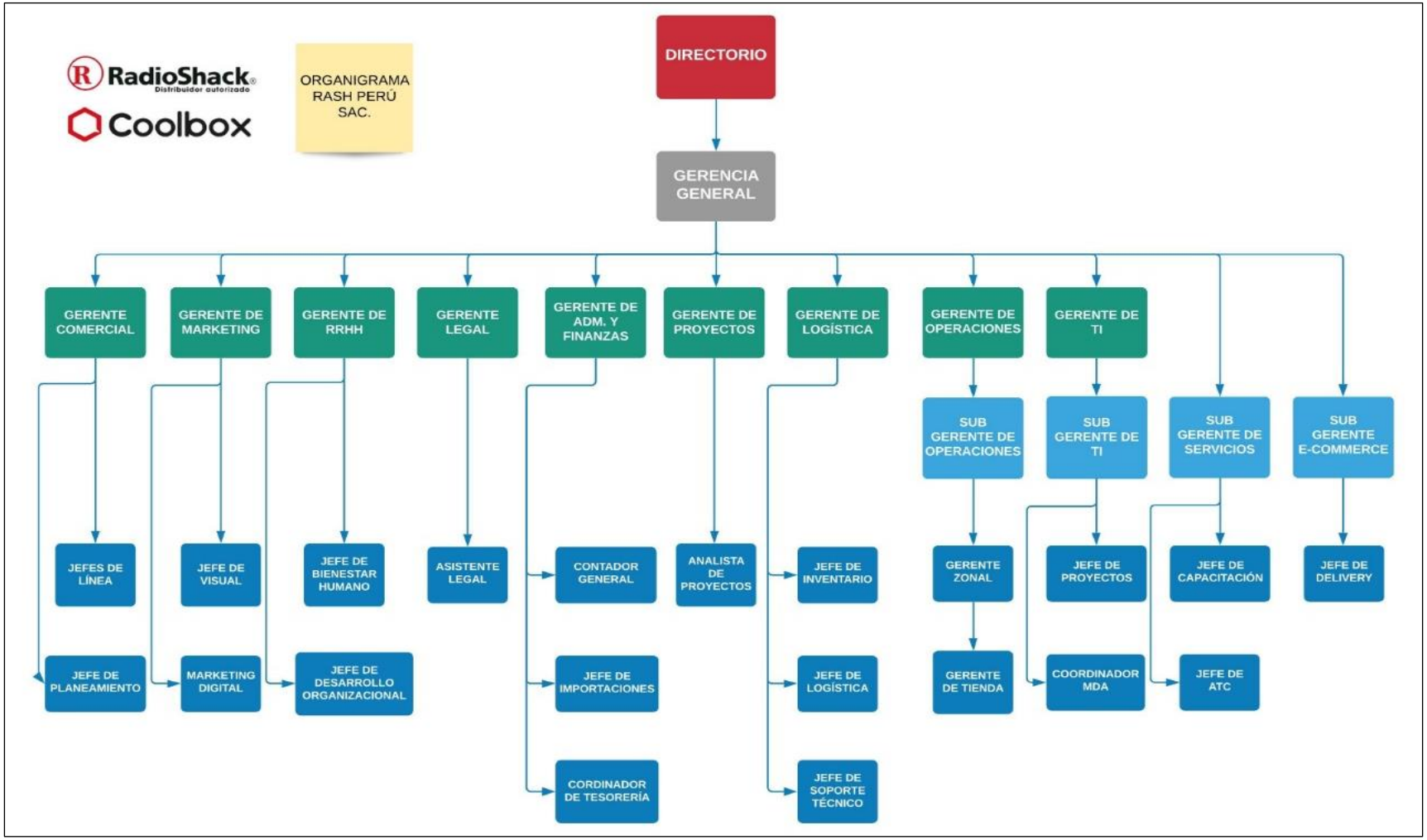


Figura 38, Organigrama Rash Perú S.A.C.

Fuente, Elaboración propia.

Tal y como puede visualizarse en la figura anterior, Rash Perú S.A.C cuenta con áreas bien definidas, las cuales son denominadas Gerencias. Se tienen entonces:

- Gerencia General:

  Es la gerencia máxima de la compañía, cuyo rol principal es netamente estratégico ya que dentro de sus obligaciones posee la labor de dar aprobación acerca de decisiones estratégicas que beneficien a dicha empresa, realizar el monitoreo, supervisión y control de todo Rash Perú S.A.C por intermedio de indicadores de gestión, asimismo, teniendo una responsabilidad civil y legal sobre la compañía, finalmente, es la encargada de la generación de valor ante la directiva. Vale mencionar que dicha gerencia tiene como cabeza jerárquica al Gerente General.

- Gerencia Comercial:

  Es la gerencia cuyo rol más importante es la de adquirir productos internacionales y nacionales, los mismos que son segmentados por intermedio de jefaturas de línea, además posee la responsabilidad de mantener los niveles de márgenes brutos que posee Rash Perú S.A.C, además su labor también implica la planeación del suministro de inventarios en la totalidad de establecimientos a nivel nacional. Vale mencionar que dicha gerencia tiene como cabeza jerárquica al Gerente Comercial.

- Gerencia de Marketing:

  Es la gerencia cuyo rol más relevante es el de determinar y llevar a la praxis los planes publicitarios de la totalidad del catálogo de productos por intermedio de canales diversos publicitarios, verbigracia, web sites, redes sociales, anuncios POP, medios escritos y otros canales comunicativos. Vale mencionar que dicha gerencia tiene como cabeza jerárquica al Gerente de Marketing.

- Gerencia de RR.HH.:

  Es la gerencia cuyo rol es el de administrar el capital humano de Rash Perú S.A.C, incluyendo la organización de procedimientos de reclutamiento, de gestión de planillas, de gestión de beneficios laborales para los colaboradores, de estrategias para el mejoramiento del clima organizacional, etcétera. Vale mencionar que dicha gerencia tiene como cabeza jerárquica al Gerente de Recursos Humanos.

- Gerencia Legal:

  Es la gerencia cuyo rol es la de supervisar, coordinar y gestionar la totalidad de aspectos legales de Rash Perú S.A.C, teniendo como responsabilidad el diseño de procedimientos que permitan a la compañía el cumplimiento de la normatividad jurídica peruana, incluyendo aquellas normativas que involucran los derechos y deberes laborales, como también las de carácter de legalidad empresarial. Vale mencionar que dicha gerencia tiene como cabeza jerárquica al Gerente Legal.

- Gerencia de Administración y Finanzas:

  Es la gerencia cuyo rol es la optimizar los flujos de efectivo de Rash Perú S.A.C, llevando una supervisión continua de las operaciones administrativas, financieras y contable de la compañía considerando la normatividad peruana vigente según los entes reguladores tales como SUNAT, ADUANAS, etcétera. Vale mencionar que dicha gerencia tiene como cabeza jerárquica al Gerente de Administración.

- Gerencia de Proyectos:

  Es la gerencia cuyo rol es el de aperturas y mantención de nuevos establecimientos para el expendio de sus productos, así como de oficinas administrativas, además realiza una búsqueda activa de localizaciones donde se puedan establecer nuevos locales, los cuales proponen a la gerencia general y que posteriormente pueden ser

aprobados. Vale mencionar que dicha gerencia tiene como cabeza jerárquica al Gerente de Proyectos.

- Gerencia de Logística:

  Es la gerencia cuyo rol es de controlar las operaciones logísticas, operaciones de logística inversa, así como también del servicio técnico y del abastecimiento diario a los diversos establecimientos a nivel nacional de los que dispone Rash Perú S.A.C. Vale mencionar que dicha gerencia tiene como cabeza jerárquica al Gerente de Logística.

- Gerencia de Operaciones:

  Encabezada por el Gerente de Operaciones, tiene como objetivo principal la comercialización de productos en los puntos de venta. Esta área está integrada por supervisores, encargados de ventas, vendedores y personal administrativo de apoyo. Es importante destacar que el Gerente de Operaciones ocupa el puesto de mayor jerarquía en esta gerencia.

- Gerencia de TI:

  Se encarga de asegurar el correcto desempeño de los sistemas de información, la supervisión de los activos informáticos y la exitosa ejecución de los proyectos tecnológicos. Es liderada por el subgerente de Tecnologías de la Información y se reporta al Gerente de TI.

Asimismo, en cuanto a personal, Rash Perú S.A.C. cuenta con más de 600 colaboradores distribuidos en las diversas áreas, tal y como puede visualizarse en la tabla siguiente:

Tabla 39

Total de colaboradores de Rash Perú S.A.C por áreas

Nº	Área	Total
1	Gerencia General	1
2	Gerencia Comercial	12

3	Gerencia de Marketing	7
4	Gerencia de RR.HH.	11
5	Gerencia Legal	3
6	Gerencia de Administración y Finanzas	12
7	Gerencia de Proyectos	3
8	Gerencia de Logística	15
9	Gerencia de Operaciones	600
10	Gerencia de TI	11
11	Sub Gerencia de Servicios	7
12	Sub Gerencia de E-Commerce	4
TOTAL GENERAL		**686**

Fuente, Elaboración propia.

Por otra parte, se identificaron los procesos de RASH PERÚ S.A.C en un mapa de procesos, en donde se identificaron 3 procesos operativos, 3 procesos estratégicos y 3 procesos de apoyo, los cuales se visualizan a continuación:

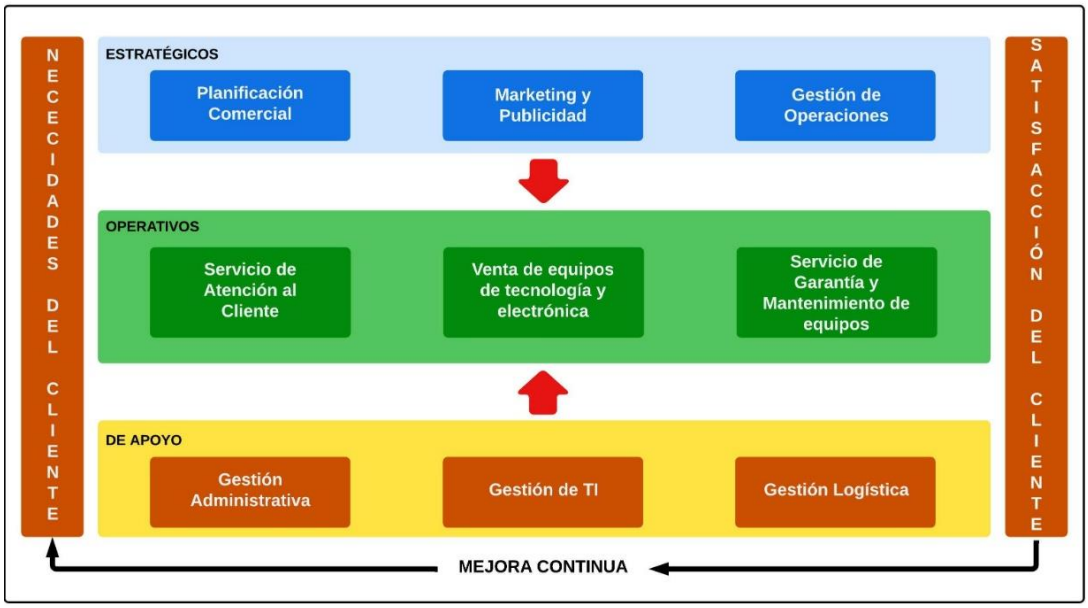


Figura 39, Mapa de procesos de RASH PERÚ S.A.C.

Fuente, Elaboración propia.

En cuanto a los procesos estratégicos, se identificaron los siguientes tres (03) procesos:

a. Planificación comercial (PE-01)

Este proceso se encarga de asegurarse que se cumplan los tratados comerciales internacionales y nacionales de modo que se logre la adquisición de los productos mediante alianzas con socios estratégicos de Rash Perú S.A.C.

b. Marketing y publicidad (PE-02)

Este proceso se encarga de gestionar y controlar el uso de medios publicitarios y el mejoramiento de valor agregado para Rash Perú S.A.C.

c. Gestión de operaciones (PE-03)

Este proceso se encarga de que se dé el cumplimiento de los objetivos de Rash Perú S.A.C., comunicándolos a la fuerza de ventas quienes son los encargados de gestionar los establecimientos.

En cuanto a los procesos operativos se identificaron los siguientes tres (03) procesos:

a. Servicio de atención al cliente (PO-01)

Este proceso se encarga de generar un vínculo entre Rash Perú S.A.C y sus clientes, de modo que se logre el propósito de satisfacción y obtención de beneficios hacia sus clientelas.

b. Venta de equipos de tecnología y electrónica (PO-02)

Este proceso se encarga de la venta de equipos de electrónica y tecnologías que son ofrecidos a las clientelas de Rash Perú S.A.C.

c. Servicio de garantía y mantenimiento de equipos (PO-03)

Este proceso se encarga de cubrir las reparaciones de los productos adquiridos por la clientela de Rash Perú, con el fin de cumplir con los estándares que esta empresa posee.

En cuanto a los procesos de apoyo se identificaron los siguientes tres (03) procesos:

a. Gestión administrativa (PA-01)

Este proceso se encarga de la coordinación administrativa de la totalidad de tareas, coadyuvando al empleo óptimo de los recursos que Rash Perú S.A.C posee.

b. Gestión de TI (PA-02)

Este proceso se encarga de dar soporte y mantenimiento tecnológico a la totalidad de equipos y servicios informáticos que son empleados en las labores operativas de las diversas áreas que componen Rash Perú S.A.C.

c. Gestión logística (PA-03)

Este proceso se encarga de brindar el soporte logístico para la distribución de los productos tecnológicos y electrónicos a los diversos puntos de ventas pertenecientes a Rash Perú S.A.C.

Posteriormente, se determinaron criterios de evaluación identificados en la norma, con el propósito de seleccionar los procesos más relevantes que Rash Perú S.A.C posee. A continuación, se muestran los criterios de evaluación en mención:

Tabla 40

Criterios de evaluación de los procesos

Código	Criterio	Descripción
C1	Valor estratégico del proceso	Es una valoración acerca del proceso que genere un impacto importante en la empresa.
C2	Criticidad de los activos	Es una valoración acerca de los activos de información involucrados.
C3	Importancia operativa y comercial	Es una valoración de la confidencialidad, integridad y disponibilidad operativa y comercial de los procesos
C4	Expectativas y percepciones	Se trata de una evaluación de las expectativas y opiniones de los stakeholders, así como de las posibles consecuencias negativas para la reputación y la imagen de la empresa.

Fuente, Elaboración propia.

Después de haber establecido los criterios de evaluación de criticidad se prosiguió con evaluar los nueve (09) procesos que posee Rash Perú S.A.C y los cuales se encuentran identificados. Para ello, estableció una escala de valoración con el que se pudieran seleccionar los procesos más relevantes de Rash Perú S.A.C, tal y como se muestra a continuación:

- Débil (1)
- Leve (2)
- Normal (3)
- Moderado (4)
- Fuerte (5)

A continuación, se muestran las valoraciones hechas a dada uno de los nueve (09) procesos de Rash Perú S.A.C:

Tabla 41

Resultados de la evaluación de los procesos de Rash Perú S.A.C.

Código	Proceso	C01	C02	C03	C04	Total
(PE-01)	Planificación comercial	3	3	3	3	12
(PE-02)	Marketing y publicidad	3	2	4	2	11
(PE-03)	Gestión de operaciones	3	4	4	3	14
(PO-01)	Servicio de atención al cliente	5	5	5	5	20
(PO-02)	Venta de equipos de tecnología y electrónica	5	5	5	5	20
(PO-03)	Servicio de garantía y mantenimiento de equipos	5	5	5	4	19
(PA-01)	Gestión administrativa	3	2	4	2	11
(PA-02)	Gestión de TI	3	4	4	3	14
(PA-01)	Gestión logística	3	4	4	3	14

Fuente, Elaboración propia.

Posteriormente, a la evaluación de criticidad de los procesos con los que cuenta Rash Perú S.A.C, se optó por seleccionar los tres (03) procesos más relevantes teniendo en cuenta la sumatoria de los criterios previamente seleccionados, tal y como se muestra en la siguiente tabla:

Tabla 42

Resultados generales de criticidad de los procesos de Rash Perú S.A.C.

Código	Proceso	Total
(PE-01)	Planificación comercial	12
(PE-02)	Marketing y publicidad	11
(PE-03)	Gestión de operaciones	14
(PO-01)	Servicio de atención al cliente	20
(PO-02)	Venta de equipos de tecnología y electrónica	20
(PO-03)	Servicio de garantía y mantenimiento de equipos	19

(PA-01)	Gestión administrativa	11
(PA-02)	Gestión de TI	14
(PA-01)	Gestión logística	14

Fuente, Elaboración propia.

Luego de haber seleccionado los procesos con mayor criticidad, se procedió al diseño de cada uno de estos tres procesos, obteniendo los siguientes resultados:

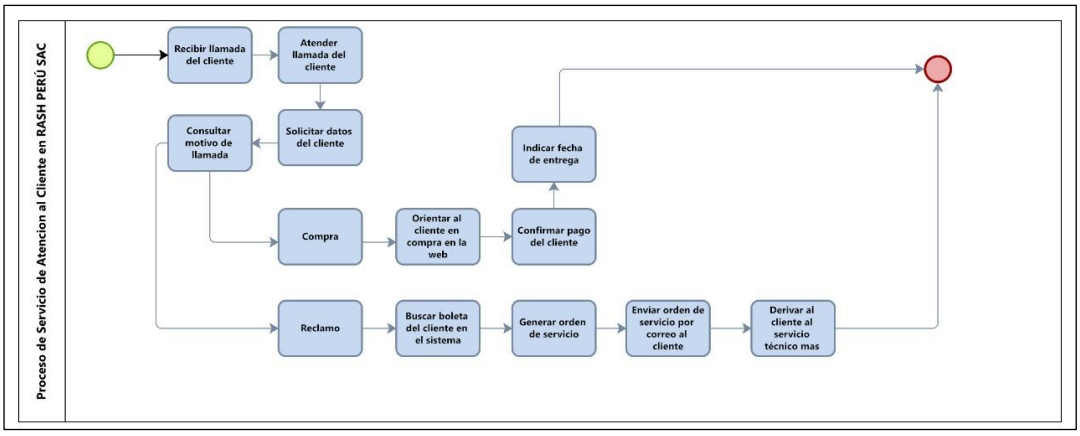


Figura 40, (PO-01) Servicio de atención al cliente.

Fuente, Elaboración propia.

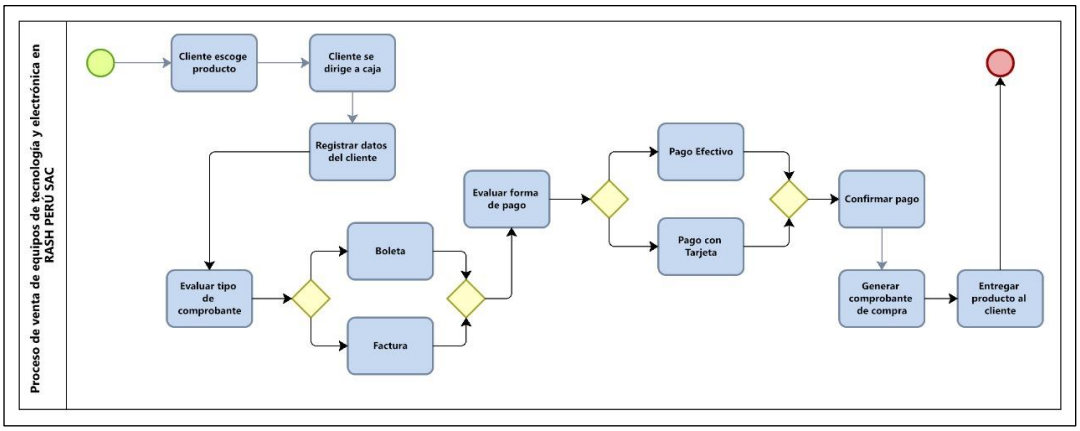


Figura 41, (PO-02) Venta de equipos de tecnología y electrónica.

Fuente, Elaboración propia.

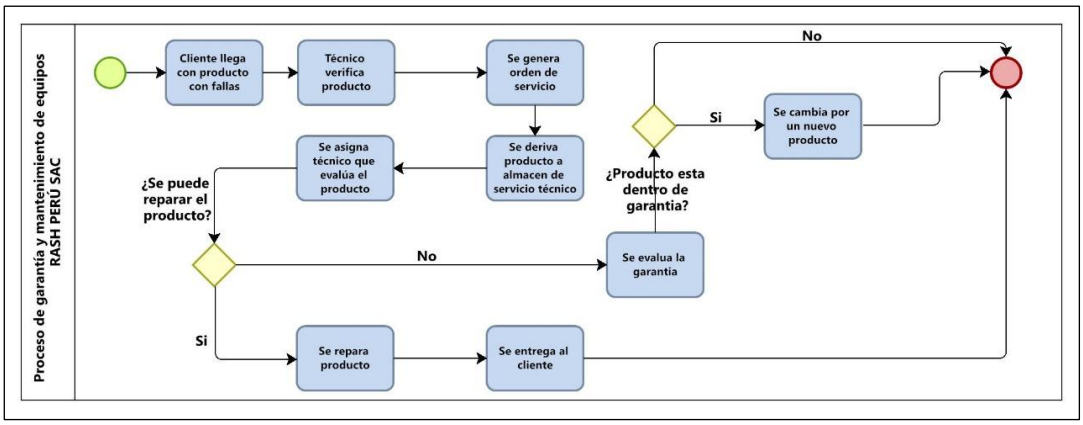


Figura 42, (PO-03) Servicio de garantía y mantenimiento de equipos.

Fuente, Elaboración propia.

Luego de especificar los procesos con mayor criticidad dentro de Rash Perú S.A.C, se procedió al levantamiento de un inventario de activos por área, para poder hacer un diagnóstico más preciso de los activos con lo que cuenta dicha compañía. El inventario por áreas se muestra a continuación:

En el área de Gerencia General se cuentan con los siguientes activos:

Tabla 43

Inventario de activos informáticos en Gerencia General.

CANTIDAD	PRODUCTO	MARCA	TIPO
1	PC DESKTOP CORE I7	LENOVO	HARDWARE.
1	IMPRESORA OFICCEJET PRO	HP	HARDWARE.
1	LAPTOP THINKPAD I7	LENOVO	HARDWARE.
1	ROUTER 4 PUERTOS	CISCO	HARDWARE.
1	IPAD PRO	APPLE	HARDWARE.
1	CELULAR	XIAOMI	HARDWARE.
1	TV FHD 50 “	SAMSUNG	HARDWARE.
2	CÁMARAS IP	HK VISION	HARDWARE.

Fuente, Elaboración propia.

En el área Comercial se cuentan con los siguientes activos:

Tabla 44

Inventario de activos informáticos en el Área Comercial

CANTIDAD	PRODUCTO	MARCA	TIPO
4	PC DESKTOP CORE I7	LENOVO	HARDWARE.
6	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
2	IMAC I5 1TB	APPLE	HARDWARE.
1	ROUTER 16 PUERTOS	CISCO	HARDWARE.
1	SWITCH	TP LINK	HARDWARE.
1	IMPRESORA MULTIFUNCIONAL C7100	XEROX	HARDWARE.
1	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
3	TV LED FHD 50”	AOC	HARDWARE.
12	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
3	CÁMARAS IP	HK VISION	HARDWARE.
2	UPS	CHICAGO DIGITAL	HARDWARE.
8	CELULARES	XIAOMI	HARDWARE.
2	TELÉFONOS ANEXO	AVAYA	HARDWARE.

Fuente, Elaboración propia.

En el área de Marketing se cuentan con los siguientes activos:

Tabla 45

Inventario de activos informáticos en el Área Marketing

CANTIDAD	PRODUCTO	MARCA	TIPO
1	PC DESKTOP CORE I7	LENOVO	HARDWARE.
3	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
3	IMAC I5 1TB	APPLE	HARDWARE.
1	ROUTER 16 PUERTOS	CISCO	HARDWARE.

1	SWITCH	TP LINK	HARDWARE.
1	IMPRESORA MULTIFUNCIONAL C7100	XEROX	HARDWARE.
1	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
1	TV LED FHD 50”	AOC	HARDWARE.
4	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
2	CÁMARAS IP	HK VISION	HARDWARE.
3	UPS	CHICAGO DIGITAL	HARDWARE.
6	CELULARES	XIAOMI	HARDWARE.
1	TELÉFONOS ANEXO	AVAYA	HARDWARE.

Fuente, Elaboración propia.

En el área de RR.HH. se cuentan con los siguientes activos:

Tabla 46

Inventario de activos informáticos en el Área RR.HH.

CANTIDAD	PRODUCTO	MARCA	TIPO
7	PC DESKTOP CORE I7	LENOVO	HARDWARE.
4	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
1	ROUTER 8 PUERTOS	CISCO	HARDWARE.
1	SWITCH 8 PUERTOS	TP LINK	HARDWARE.
1	IMPRESORA MULTIFUNCIONAL	XEROX	HARDWARE.
1	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
1	TV LED FHD 50”	AOC	HARDWARE.
7	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
2	CÁMARAS IP	HK VISION	HARDWARE.
6	CELULARES	XIAOMI	HARDWARE.
1	TELÉFONOS ANEXO	AVAYA	HARDWARE.

Fuente, Elaboración propia.

En el área Legal se cuentan con los siguientes activos:

Tabla 47

Inventario de activos informáticos en el Área Legal

CANTIDAD	PRODUCTO	MARCA	TIPO
1	PC DESKTOP CORE I7	LENOVO	HARDWARE.
2	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
1	ROUTER 4 PUERTOS	CISCO	HARDWARE.
1	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
1	TV LED FHD 50”	AOC	HARDWARE.
1	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
1	CÁMARAS IP	HK VISION	HARDWARE.
3	CELULARES	XIAOMI	HARDWARE.
1	TELÉFONOS ANEXO	AVAYA	HARDWARE.

Fuente, Elaboración propia.

En el área de Administración y Finanzas se cuentan con los siguientes activos:

Tabla 48

Inventario de activos informáticos en el Área de Administración y Finanzas.

CANTIDAD	PRODUCTO	MARCA	TIPO
7	PC DESKTOP CORE I7	LENOVO	HARDWARE.
5	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
1	ROUTER 8 PUERTOS	CISCO	HARDWARE.
1	SWITCH 8 PUERTOS	TP LINK	HARDWARE.
1	IMPRESORA MULTIFUNCIONAL	XEROX	HARDWARE.

1	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
1	TV LED FHD 50”	AOC	HARDWARE.
7	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
3	CÁMARAS IP	HK VISION	HARDWARE.
7	CELULARES	XIAOMI	HARDWARE.
2	TELÉFONOS ANEXO	AVAYA	HARDWARE.

Fuente, Elaboración propia.

En el área de Proyectos se cuentan con los siguientes activos:

Tabla 49

Inventario de activos informáticos en el Área de Proyectos

CANTIDAD	PRODUCTO	MARCA	TIPO
1	PC DESKTOP CORE I7	LENOVO	HARDWARE.
2	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
1	ROUTER 4 PUERTOS	CISCO	HARDWARE.
1	IMPRESORA MULTIFUNCIONAL L465	EPSON	HARDWARE.
1	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
1	CÁMARAS IP	HK VISION	HARDWARE.
3	CELULARES	XIAOMI	HARDWARE.
1	TELÉFONOS ANEXO	AVAYA	HARDWARE.

Fuente, Elaboración propia.

En el área de Logística se cuentan con los siguientes activos:

Tabla 50

Inventario de activos informáticos en el Área de Logística.

CANTIDAD	PRODUCTO	MARCA	TIPO
7	PC DESKTOP CORE I7	LENOVO	HARDWARE.

3	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
1	ROUTER 8 PUERTOS	CISCO	HARDWARE.
1	SWITCH 8 PUERTOS	TP LINK	HARDWARE.
1	IMPRESORA MULTIFUNCIONAL	XEROX	HARDWARE.
1	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
2	TV LED FHD 50”	AOC	HARDWARE.
7	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
4	CÁMARAS IP	HK VISION	HARDWARE.
8	CELULARES	XIAOMI	HARDWARE.
2	TELÉFONOS ANEXO	AVAYA	HARDWARE.
3	IMPRESORAS MATRICIALES LX-350	EPSON	HARDWARE.

Fuente, Elaboración propia.

En el área de Operaciones se cuentan con los siguientes activos:

Tabla 51

Inventario de activos informáticos en el Área de Operaciones.

CANTIDAD	PRODUCTO	MARCA	TIPO
5	PC DESKTOP CORE I7	LENOVO	HARDWARE.
7	LAPTOPS THINKPAD I7	LENOVO	HARDWARE.
2	IMPRESORA OFICCEJET PRO	HP	HARDWARE.
1	ROUTER 16 PUERTOS	CISCO	HARDWARE.
1	SWITCH 8 PUERTOS	TP-LINK	HARDWARE.
3	TV FHD 50”	AOC	HARDWARE.
8	CELULARES	XIAOMI	HARDWARE.
3	TELÉFONOS ANEXO	AVAYA	HARDWARE.
2	CÁMARAS IP	HK VISION	HARDWARE.

70	PC DESKTOP CORE I5	LENOVO	HARDWARE.
70	IMPRESORA MATRICIALES LX-350	EPSON	HARDWARE.
70	ROUTER 4 PUERTOS	CISCO	HARDWARE.
70	KITS DE SEGURIDAD C/4 CÁMARAS 1TB HHD	SECUR THAG	HARDWARE.
70	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
70	CELULARES	ALCATEL	HARDWARE.
40	PC DESKTOP CORE I5	LENOVO	HARDWARE.
40	IMPRESORA MATRICIALES LX-350	EPSON	HARDWARE.
40	ROUTER 4 PUERTOS	CISCO	HARDWARE.
40	KITS DE SEGURIDAD C/4 CÁMARAS 1TB HHD	SECUR THAG	HARDWARE.
40	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
40	CELULARES	SAMSUNG	HARDWARE.
60	PC DESKTOP CORE I5	LENOVO	HARDWARE.
30	IMPRESORA MATRICIALES LX-350	EPSON	HARDWARE.
30	IMPRESORAS LASERJET	HP	HARDWARE.
30	KITS DE SEGURIDAD C/8 CÁMARAS 1TB HHD	SECUR THAG	HARDWARE.
60	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
30	CELULARES Y5 2018	HUAWEI	HARDWARE.
30	ROUTER 8 PUERTOS	CISCO	HARDWARE.
30	REPETIDORES	TP LINK	HARDWARE.
30	PC DESKTOP CORE I7	LENOVO	HARDWARE.
10	IMPRESORA MATRICIALES LX-350	EPSON	HARDWARE.
10	IMPRESORAS LASERJET	HP	HARDWARE.
10	KITS DE SEGURIDAD C/8 CÁMARAS 2TB HHD FHD	SECUR THAG	HARDWARE.

30	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
30	CELULARES POCO 8	XIAOMI	HARDWARE.
30	ROUTER 16 PUERTOS	CISCO	HARDWARE.
10	REPETIDORES	TP LINK	HARDWARE.
20	CÁMARAS IP	HK VISION	HARDWARE.

Fuente, Elaboración propia.

En el área de TI se cuentan con los siguientes activos:

Tabla 52

Inventario de activos informáticos en el Área de TI

CANTIDAD	PRODUCTO	MARCA	TIPO
9	PC DESKTOP CORE I7	LENOVO	HARDWARE.
3	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
1	ROUTER 8 PUERTOS	CISCO	HARDWARE.
1	SWITCH 8 PUERTOS	TP LINK	HARDWARE.
1	IMPRESORA MULTIFUNCIONAL	XEROX	HARDWARE.
1	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
2	TV LED FHD 50”	AOC	HARDWARE.
12	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
3	CÁMARAS IP	HK VISION	HARDWARE.
11	CELULARES	XIAOMI	HARDWARE.
2	TELÉFONOS ANEXO	AVAYA	HARDWARE.
3	SERVIDORES SYSTEM X3250 M6	LENOVO	HARDWARE.
5	PC DESKTOP CORE I5	LENOVO	HARDWARE.
5	PC DESKTOP CORE I7	LENOVO	HARDWARE.
3	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
3	ROUTER 8 PUERTOS	CISCO	HARDWARE.
3	SWITCH 8 PUERTOS	TP LINK	HARDWARE.

1	IMPRESORA MULTIFUNCIONAL	XEROX	HARDWARE.
2	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
2	TV LED FHD 50”	AOC	HARDWARE.
5	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
3	CÁMARAS IP	HK VISION	HARDWARE.
9	CELULARES	XIAOMI	HARDWARE.
2	TELÉFONOS ANEXO	AVAYA	HARDWARE.
5	UPS	CHICAGO DIGITAL	HARDWARE.

Fuente, Elaboración propia.

En el área de Servicios se cuentan con los siguientes activos:

Tabla 53

***Inventario de activos informáticos en el Área de Servicios*.**

CANTIDAD	PRODUCTO	MARCA	TIPO
7	PC DESKTOP CORE I7	LENOVO	HARDWARE.
1	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
1	ROUTER 16 PUERTOS	CISCO	HARDWARE.
1	SWITCH 8 PUERTOS	TP LINK	HARDWARE.
1	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
2	TV LED FHD 50”	AOC	HARDWARE.
7	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
2	CÁMARAS IP	HK VISION	HARDWARE.
4	CELULARES	XIAOMI	HARDWARE.
3	TELÉFONOS IP	AVAYA	HARDWARE.
1	PROYECTOR	EPSON	HARDWARE.

Fuente, Elaboración propia.

En el área de E-Commerce se cuentan con los siguientes activos:

Tabla 54

Inventario de activos informáticos en el Área de E-Commerce

CANTIDAD	PRODUCTO	MARCA	TIPO
2	IMAC I5 1TB	APPLE	HARDWARE.
1	LAPTOP THINKPAD I 7	LENOVO	HARDWARE.
1	ROUTER 16 PUERTOS	CISCO	HARDWARE.
2	UPS	CHICAGO DIGITAL	HARDWARE.
1	IMPRESORA OFICCEPRO LASERJET	HP	HARDWARE.
12	TV LED FHD 50”	AOC	HARDWARE.
2	ESTABILIZADORES	CHICAGO DIGITAL	HARDWARE.
1	CÁMARAS IP	HK VISION	HARDWARE.
4	CELULARES	XIAOMI	HARDWARE.
1	TELÉFONOS ANEXO	AVAYA	HARDWARE.
1	TABLET 10”	SAMSUNG	HARDWARE.

Fuente, Elaboración propia.

Además de estos inventarios por área, se dispone del siguiente conjunto consolidado de licencias y SOFTWARE.:

Tabla 55

Inventario de licencias y SOFTWARE.

PRODUCTO	MARCA	TIPO
WINDOWS 10 PRO	MICROSOFT	SOFTWARE.
SQL SERVER 2012	MICROSOFT	SOFTWARE.
ADOBE PHOTOSHOP	ADOBE	SOFTWARE.
ADOBE ILLUSTATOR	ADOBE	SOFTWARE.
PREMIER PRO	ADOBE	SOFTWARE.
INDESING	ADOBE	SOFTWARE.
SAP 4 HANA/ERP	SAP	SOFTWARE.
ACEWAN	RASH	SOFTWARE.

OFISMART	OFISIS	SOFTWARE.
CIC (CENTRO DE INCIDENCIAS COOBOX	RASH	SOFTWARE.
FORTICLIENT	FORTINET	SOFTWARE.
ANTIVIRUS KAPERSKI	KAPERSKI	SOFTWARE.

Fuente, Elaboración propia.

Luego de haber realizado el diagnóstico previo se evidenció que, la problemática principal de la seguridad informática en la empresa Rash Perú S.A.C radica en la escasa o nula gestión de medidas preventivas para dicho tipo de seguridad, por lo que es necesario disponer de un SGSI basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa caso de estudio, para este caso específico, Rash Perú S.A.C.

Tabla 56

***Causas y efectos de la deficiente gestión de la seguridad informática en Rash Perú* S.A.C.**

Problemática	**Causas**	**Consecuencias**
Deficiente gestión de la seguridad informática en Rash Perú S.A.C	Desconocimiento de la peligrosidad de los ataques a la seguridad informática	Infiltración de SOFTWARE. maliciosos como Ransomware, Phishing, etcétera.
	No se codifica las cuentas de acceso	Pérdida de información valiosa
	Falta de sensibilización en cuanto a los riesgos a la seguridad informática	No se forman hábitos de preservación de la seguridad informática
	Falta de un plan de renovación de equipos para la continuidad operativa del negocio	eficiente gestión de activos informáticos
	Carencia de acuerdos basados en la confidencialidad	Pérdidas de información por la nula regulación de la confidencialidad

Fuente, Elaboración propia.

Para el desarrollo del SGSI se necesitó como soporte, hacer uso de una metodología para la gestión de los riesgos informáticos. Para ello se realizó una búsqueda de las metodologías existentes en la literatura científica que gestionen los riegos de la seguridad informática. Por esta razón, se buscaron investigaciones acerca de este tipo de metodologías, con lo cual se lograron distinguir los estudios enunciados a continuación:

Tabla 57

Estudios acerca de metodologías para la gestión de riesgos de la seguridad informática.

Nº	Autor	Año	Metodologías identificadas
1	Gritzalis et al.	2021	EBIOS, MEHARI, OCTAVE, IT-Grundschutz, MAGERIT, CRAMM, HTRA, NIST SP800, RiskSafe, CORAS, COBIT.
2	Acevedo & Satizábal	2016	OCTAVE, CORAS, Australian ST, NTC-ISO/IEC 27005, CRAMM, MAGERIT, NIST Risk Management Methodology for IT systems, IDB Methodology, NIST Malware Incident Prevention Methodology.
3	Macedo & Da Silva	2012	OCTAVE, MEHARI, MAGERIT, IT-Grundschutz, EBIOS, IRAM, SARA, SPRINT, ISO 27005, NIST SP800-30, CRAMM, MIGRA, MAR, ISAMM, GAO/AIMD-00-33, IT System Security Assessment, MG-2 and MG-3, Security Risk Management Guide, Dutch A&K Analysis, MARION, Austrian IT Security Handbook, Microsoft's security risk management guide, RiskIT.
4	Syalim et al.	2009	MEHARI, MAGERIT, NIST800-30, Microsoft's Security Management Guide

Fuente, Elaboración propia.

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

Tabla 58

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

Metodología	¿Es una metodología?	¿Identifica los riesgos de la SI?	¿SOFTWARE . libre?	¿Actualizado a la fecha?	Se puede utilizar herramienta de soporte?	¿Facilidad de uso?	¿Posee aplicabilidad en el Perú?	SUMATORIA
MAGERIT	Sí	Sí	Sí	Sí	Sí	Sí	Sí	07
OCTAVE	Sí	Sí	Sí	Sí	No	Sí	Sí	06
MEHARI	Sí	Sí	Sí	Sí	Sí	No	Sí	06
IT-Grundschutz	Sí	Sí	Sí	Sí	No	Sí	No	05
EBIOS	Sí	Sí	Sí	Sí	No	Sí	No	05
IRAM	Sí	Sí	No	Sí	No	Sí	No	04
SARA	Sí	Sí	No	No	No	No	No	02
SPRINT	Sí	Sí	No	No	No	No	No	02
ISO 27005	No	Sí	Sí	Sí	No	No	Sí	04
NIST SP800-30	No	Sí	Sí	Sí	No	No	Sí	04
CRAMM	Sí	Sí	No	Sí	No	No	Sí	04
MIGRA	Sí	Sí	No	Sí	No	No	No	03
MAR	No	No	Sí	Sí	No	No	No	02
ISAMM	Sí	Sí	No	No	No	No	No	02
GAO/AI D-00-33	No	Sí	Sí	No	No	No	No	02

IT System Security Assessment	No	Sí	No	No	No	No	No	01
MG-2 and MG-3	No	Sí	No	No	No	No	No	01
Security Risk Management Guide	No	Sí	No	No	No	No	No	01
Dutch A&K Analysis	Sí	Sí	No	No	No	No	No	02
MARION	Sí	Sí	No	No	No	No	No	02
Austrian IT Security Handbook	No	Sí	No	Sí	No	No	No	02
Microsoft's security risk management guide	No	Sí	Sí	Sí	No	No	No	03
RiskIT	No	No	Sí	No	No	No	No	01
Australian ST	No	No	No	No	No	No	No	00

IDB Methodology	Sí	Sí	No	No	No	No	No	02
HTRA	No	Sí	No	No	No	No	No	01
RiskSafe	No	Sí	No	No	No	No	No	01
CORAS	No	Sí	No	No	No	No	No	01
COBIT	No	No	No	Sí	No	Sí	Sí	03

Fuente. Adaptado de Macedo & Da Silva (2012)

De la tabla anterior se pudo determinar que, MAGERIT es la metodología con las mejores prestaciones para ser usada como soporte para la implementación del SGSI basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C dado que, obtuvo el mayor puntaje (07 puntos totales) en la tabla comparativa anterior por sus características de ser una metodología, identificar los riesgos asociados a la seguridad informática, es de SOFTWARE. libre, se encuentra actualizada a la fecha, puede emplearse con el uso de herramientas de Entorno de Análisis de Riesgos (EAR) como soporte, tiene facilidad de uso baja y, lo más importante, es que posee aplicabilidad en el Perú.

En cuanto a MAGERIT (por su acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), es una metodología española de uso común y código abierto para el marco de gestión de riesgos según las normas pertenecientes a la familia ISO/IEC 27k. MAGERIT, que inicialmente fue publicada en 1997, es una metodología de con alta facilidad de uso y con alta aplicabilidad, asimismo, su implementación logra brindar buenos resultados sobre los estados relacionados con los riesgos asumidos. Además, puede ser empleada a manera de soporte al momento de mejorar la toma de decisiones.

MAGERIT busca alcanzar los siguientes objetivos:

a. Hacer que los encargados de los sistemas de información tomen conciencia de los riesgos y la importancia de abordarlos de manera oportuna.
b. Proporcionar un enfoque sistemático para el análisis de estos riesgos.
c. Ayudar en la identificación y planificación de medidas adecuadas para controlar los riesgos.
d. Indirectamente, preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

MAGERIT, a la fecha actual, se encuentra en la versión 3, disponiendo de tres (03) libros, los cuales se muestran a continuación:

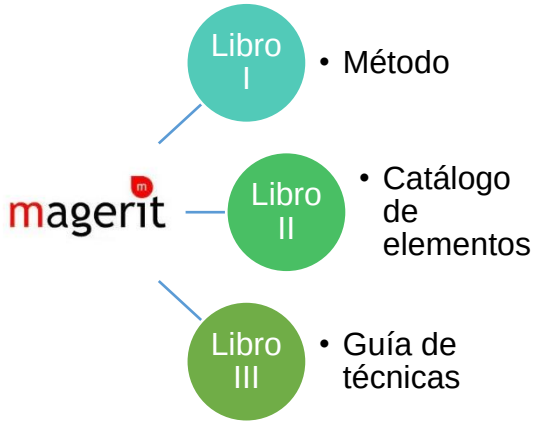


Figura 43, Documentación disponible en MAGERIT v.3

Fuente. Elaboración propia.

Tal y como puede visualizarse en la imagen anterior, MAGERIT posee los siguientes tres (03) libros según ENISA (2022) y que los describe de la siguiente manera:

a. El Libro I: presenta los pasos y tareas esenciales para llevar a cabo un proyecto de análisis y gestión de riesgos, incluyendo la descripción formal del proyecto, su aplicación en el desarrollo de sistemas de información y una serie de pistas prácticas junto con los fundamentos teóricos y otra información complementaria.

b. El Libro II: proporciona elementos y criterios estándar para los sistemas de información y el modelado de riesgos, tales como clases de activos, dimensiones de valoración, criterios de valoración, amenazas típicas y salvaguardas a considerar. También describe los informes que contienen los hallazgos y conclusiones, incluyendo el modelo de valor, el mapa de riesgos, la evaluación de salvaguardas, el estado de riesgos, el informe de deficiencias y el plan de seguridad, contribuyendo así a la uniformidad.

c. El Libro III: describe técnicas comúnmente utilizadas en proyectos de análisis y gestión de riesgos, como análisis tabular y algorítmico,

árboles de amenazas, análisis de costo-beneficio, diagramas de flujo de datos, diagramas de proceso, técnicas gráficas, planificación de proyectos, sesiones de trabajo y análisis Delphi. La metodología puede ser apoyada por el SOFTWARE. PILAR/EAR, que mejora su eficacia y potencialidades (siendo PILAR limitado a la Administración Pública Española, mientras que EAR es un producto comercial).

Como bien se ha podido observar anteriormente, MAGERIT brinda el soporte para la gestión de los riesgos asociados a la seguridad informática, que es *justamente* lo que se pretende proponer mediante la puesta en marcha del SGSI. Acerca de esto, el SGSI propuesto para RASH PERÚ S.A.C se encuentra basado en el Ciclo propuesto por el norteamericano William Edwards Deming, el mismo que permite relacionar sus cuatro (04) fases con la estructura de la norma ISO/IEC 27002. El Ciclo de Deming, es un modelo de mejora continua de la calidad que consta de una secuencia lógica de cuatro etapas claves: planificar, hacer, verificar y actuar. Para esta investigación, el ciclo de Deming nos permite específicamente:

a. Iniciar el nuevo proyecto de mejora de la seguridad informática
b. Desarrollar un diseño nuevo para el proceso de la seguridad informática.
c. Definir un proceso de trabajo repetitivo
d. Planificar la recopilación y el análisis de datos para verificar y priorizar los problemas o las causas fundamentales que afectan la seguridad informática.
e. Implementar cambios en materia de seguridad informática
f. Trabajar hacia la mejora continua de la organización haciendo énfasis en la seguridad informática

Por tanto, dicho SGSI queda establecido de la siguiente manera:

Figura 44. SGSI propuesto para RASH PERÚ S.A.C

Fuente. Elaboración propia.

A continuación, se especifican más a detalle cada una de las fases del SGSI propuesto para RASH PERÚ S.A.C:

a. Planificar (PLAN)

Describe la planificación aplicada a la RASH PERÚ S.A.C y el desarrollo de los lineamientos para cada procedimiento.

1. Contexto de la Organización: Sirve para determinar el propósito de la RASH PERÚ S.A.C y su contexto, con el fin de determinar las políticas de SI y los objetivos a seguir para el proceso de gestión de riesgos.

2. Liderazgo: Establece el liderazgo y compromiso de la alta dirección de RASH PERÚ S.A.C con respecto a la implementación del SGSI y destaca cómo debe determinar el compromiso, garantizando lo siguiente:

- Los objetivos y las políticas del SGSI están alineados con los objetivos de negocio de RASH PERÚ S.A.C.
- La disponibilidad de recursos para la implementación del SGSI (económicos, tecnológicos, humanos, etc.).
- Los roles y responsabilidades de todos los involucrados.

3. Planificación: Establecer los requisitos para la valoración, el tratamiento de los riesgos de seguridad y la planificación para obtenerlo.

   - Definir el enfoque de evaluación de riesgos: Metodología para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información
   - Determinar el nivel de riesgo en función de la probabilidad de ocurrencia y el impacto.

4. Soporte: Establece un proceso en el cual RASH PERÚ S.A.C debe asegurar recursos para el establecimiento, implementación y mejora del SGSI.

b. Implementar y operar (DO)

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

1. Definir plan de tratamiento de riesgos (RTP): Identificar acciones, recursos, responsabilidades y prioridades
2. Implementar RTP: una vez definida la meta, se implementan los objetivos de control identificados para esos procesos.
3. Implementar controles: Se aplican los controles ya establecidos para cada proceso.

4. Educación y conciencia: Todo el personal de RASH PERÚ S.A.C debe estar motivado sobre la importancia de aplicar el SGSI.
5. Gestión de operaciones del SGSI: Aplicar los procedimientos necesarios para gestionar el SGSI.

c. Auditar y verificar

Define los requisitos para medir y evaluar periódicamente el desempeño del SGSI.

1. Revisar el SGSI: se deben aplicar procedimientos de seguimiento y control para exponer errores e identificar brechas e incidentes de seguridad.
2. Medir la eficacia de los controles: implementar métodos de seguimiento para medir la eficacia de los controles estableciendo indicadores y métricas de gestión.
3. Revisar periódicamente la evaluación de riesgos: Influir en los cambios en la organización, la tecnología, los procesos y objetivos de negocio, las amenazas, la eficacia de los controles o el entorno de RASH PERÚ S.A.C.
4. Realizar periódicamente análisis internos: Sirven para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos establecidos por la norma ISO 27001.
5. Registrar acciones y eventos: Se debe registrar todo evento que pueda tener un impacto en el desempeño o en el SGSI.
6. Revisar periódicamente la eficacia del SGSI: en función de los resultados de las evaluaciones de seguridad.

d. Mantener y mejorar (ACT)

Establece el proceso de mejora del SGSI, a partir de las no conformidades identificadas en la RASH PERÚ S.A.C. Se deben establecer acciones para solucionarlos o para deshacerse de ellos.

1. Implementar las mejoras: Todas las Mejoras que se han propuesto en las fases anteriores deben ser implementadas.
2. Acciones correctivas: para resolver las no conformidades detectadas
3. Acciones preventivas: para evitar posibles no conformidades
4. Comprobar la eficacia de las acciones: las acciones y mejoras deben ser difundidas a todo el personal de RASH PERÚ S.A.C según el nivel de la jerarquía.

Posterior al levantamiento del inventario de activos por cada una de las áreas que conforman Rash Perú S.A.C, se procedió a hacer la valoración de los activos informáticos. Los activos se deben resguardar ya que poseen un valor para Rash Perú S.A.C, por lo tanto, es necesario protegerlos. Aquí se tomaron en consideración las cinco (05) características que tienen los activos para ser valorados según Chopra & Chaudhary (2020) que se encuentran especificados en la Figura 4 y que se muestran a continuación:

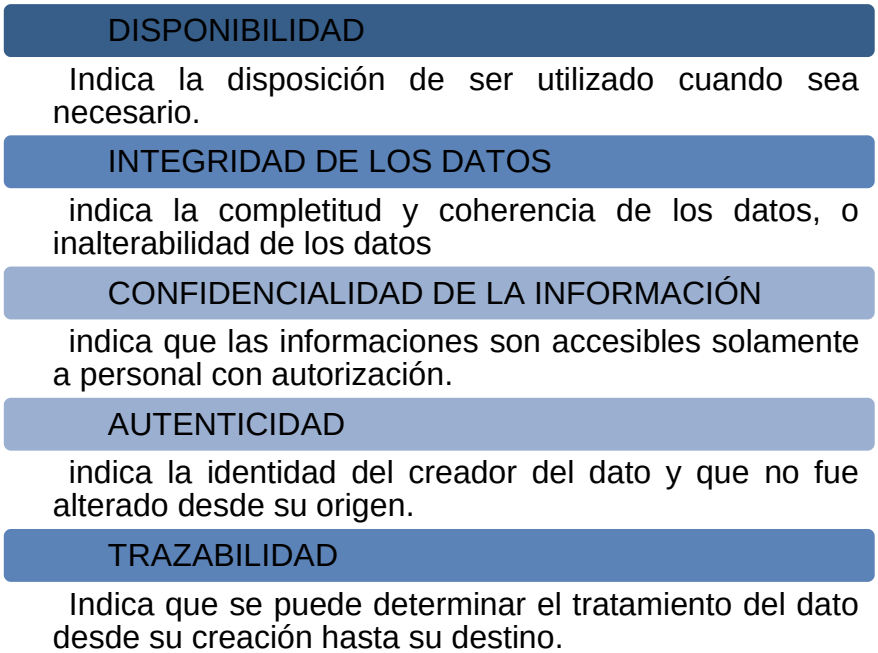


Figura 45. Características de los activos para ser valorados

Fuente. Chopra & Chaudhary (2020).

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

Tabla 59

Escala y cuadro de valores para activos

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

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

Tabla 60

Valoración de activos

Código	Categoría	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
VARP-01	HARDWARE.	Computador Desktop	10	10	10	10	10
VARP-02	HARDWARE.	Computador Portátil	10	10	10	10	10
VARP-03	HARDWARE.	Computador iMac	10	10	10	10	10
VARP-04	HARDWARE.	iPad Pro	10	10	10	10	10
VARP-05	HARDWARE.	Televisores Led FHD	05	05	05	05	05
VARP-06	HARDWARE.	Celulares	10	10	10	10	10
VARP-07	HARDWARE.	Impresora	06	06	06	06	06

VARP-08	HARDWARE.	Proyector	06	06	06	06	06
VARP-09	HARDWARE.	Cámaras IP	10	10	10	10	10
VARP-10	HARDWARE.	Router Alámbrico	10	10	10	10	10
VARP-11	HARDWARE.	Repetidor Wifi	10	10	10	10	10
VARP-12	HARDWARE.	Switch	10	10	10	08	08
VARP-13	HARDWARE.	Teléfonos IP	07	07	07	07	07
VARP-14	HARDWARE.	Kit De Seguridad De Cámaras	10	10	10	10	10
VARP-15	HARDWARE.	Estabilizadores	05	05	05	05	05
VARP-16	HARDWARE.	Ups	06	06	06	06	06
VARP-17	SOFTWARE.	Servidor Sistema X3250 M6	10	10	10	10	10
VARP-18	SOFTWARE.	Antivirus Kaspersky Corporativo	06	06	06	06	06
VARP-19	SOFTWARE.	SQL Server 2014	08	08	08	08	08
VARP-20	SOFTWARE.	SOFTWARE. Licencia Sistema Operativo	10	10	10	10	10
VARP-21	SOFTWARE.	SOFTWARE. De Edición De Videos	04	04	04	04	04
VARP-22	SOFTWARE.	SOFTWARE. De Edición De Imágenes	04	04	04	04	04
VARP-23	SOFTWARE.	SOFTWARE. SAP ERP	09	09	09	09	09
VARP-24	SOFTWARE.	SOFTWARE. VPN	08	08	08	08	08
VARP-25	SOFTWARE.	SOFTWARE. de Desarrollo Propio	07	07	07	07	07

VARP-26	SOFTWARE.	SOFTWARE. De Ofimática	06	06	06	06	06
VARP-27	SOFTWARE.	SOFTWARE. De Gestión CRM (OFISMART)	10	10	10	10	10

Fuente, Elaboración propia.

Tal y como se pudo visualizar en la tabla anterior, el promedio de las calificaciones de los Activos Esenciales y datos son MUY ALTOS, esto radica en su importancia y su trascendencia para el proceso de registro de datos en línea, por lo tanto, debe procurarse tener cero errores o en todo caso el error debe ser el más intrascendente posible.

3.5.1. Identificación de las amenazas

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

Tabla 61

Identificación de amenazas potenciales

Identificador	Descripción	Listado
N	Desastre natural	Fuego Inundación Terremoto Rayo
I	De origen industrial	Fuego Inundación Descarga eléctrica Polvo Vibración Fallas en los equipos Corte de energía Temperatura inadecuada Corte de suministros Degradación en almacenamiento
E	Errores no intencionados	Errores de usuario Errores de administrador Error de configuración Presencia de virus Sobrecalentamiento Borrado de información Ingeniería Social SOFTWARE. vulnerable Error de actualización de SOFTWARE. Error de mantenimiento e HARDWARE. Falta de recursos de HARDWARE. Pérdida de equipos Exceso de confianza Desecho de activos

		Manipulaciones de configuraciones
		Suplantaciones de identidades
		Abuso en acceso privilegiado
		Presencia de virus
		Mal uso de recursos
		Acceso sin autorización
		Negación de compromisos
A	Ataques intencionados	Interceptaciones en la comunicación
		Destrucción de información
		Borrado de información
		Mal uso del SOFTWARE.
		Mal uso del HARDWARE.
		Denegación de servicio
		Hurto
		Terrorismo
		Personal indispuesto
		Ingeniería Social
		Extorción

Fuente, Elaboración propia.

Topología de las amenazas

a. Amenazas de Tipo Internas

Imprudencias de seguridad:

A nivel mundial existen esquemas ineficientes de seguridad y es el usuario los puntos más vulnerables que amenaza el aseguramiento de las informaciones, cometiendo imprudencias en el uso de los equipos o dispositivos de cómputo.

Ejemplo:

i. Las instalaciones de SOFTWARE.s no autorizados.
ii. Archivos de emails adjuntos que han sido infestados por virus.
iii. Divulgación de informaciones sensibles a amistades, familiares etcétera (claves de acceso, identificadores de dispositivos).

Empleados deshonestos:

Se trata de usuarios internos que conocen la red y el funcionamiento de la misma.

Los usuarios que son poseedores de algún nivel de acceso a las redes por la misma necesidad de sus labores, ante una disconformidad pueden presentar quejas abusando de sus privilegios en beneficio propio o de terceros.

Los IP y Firewall son mecanismos que no son totalmente eficaces y efectivos en amenazas intrínsecas porque se conocen atajos y vulnerabilidades.

Espionaje corporativo:

Se realiza cuando terceros externos contactan personal de menor nivel o infiltran a proveedores eventuales con la finalidad de buscar un beneficio.

b. Amenazas de Tipo Externas

Amenaza Malware:

Es un tipo de amenaza que está aumentando con grandes capacidades de propagación: gusanos, virus, etcétera.

Esbozados para camuflarse y dar acompañamiento en el código de los programas benignos: troyanos, etcétera.

Bosquejados para abrir puertos y suministrar accesos a sistemas: *backdoors*, etcétera.

Se adjuntan y relacionan con los cuadros publicitarios: *spyware*, *adware*, *hijackers*.

Pueden ser capaces del robo de información personal: *keyloggers*, *stealers*.

Con atributos de comunicaciones automáticas por intermedio de vías telefónicas: *dialers*, etcétera.

Ataques o tareas distribuidas: *botnets*, etcétera. Sus riesgos potenciales son:

i. Phishing.
ii. Secuestros de ordenadores.
iii. Envenenamiento por DNS y el auto direccionar a web sites fraudulentos.
iv. Spams o envíos de correos electrónicos basuras.
v. Control y espionaje.
vi. Creación de *botnets*.
vii. *Exploits*.
viii. Ataques DDoS y DoS.

Ejemplo:

i. Vulnerabilidad con el uso de iTunes de Apple.
ii. Utilizar las herramientas del proyecto TOR.
iii. Usanza del programa secreto PRISM.

Amenaza Ingeniería Social:

Tipo de amenaza que consiste en la maniobra de individuos y de compañías suplantando identidades para adquirir un beneficio personal y que puede ser económico. Los riesgos son tremendamente peligrosos.

Ejemplo:

Cuando recibimos correos electrónicos solicitando información acerca de alguna cuenta generalmente bancaria.

Ofertas de trabajo falsas ofreciendo trabajos supuestamente bien asalariados y gratificados, pero que en realidad buscan víctimas potenciales para aprovecharse económica o moralmente.

Correos de caridad y solidaridad para beneficiar a posibles perjudicados o damnificados, muchas veces se solicita ayuda económica.

Suplantación de identidad a través de llamadas telefónicas, correos electrónicos o mensajería instantánea.

Amenaza Redes Sociales

Las principales amenazas relacionadas con la usanza de las redes sociales es que, dichas redes son controladas y gestionadas por compañías que, de manera asidua, logran hacer usanza inadecuada de las informaciones personales, los datos publicados en dichas redes sociales. Por ello es que, existen dos (02) problemas fundamentales en este aspecto:

i. Los usuarios, muchas veces, no sabe qué sucede con sus informaciones y quienes son los que acceden a los mismos.
ii. En redes sociales logran publicarse un sinfín de informaciones de naturaleza personal, que puede servir como incentivo a la delincuencia, por lo tanto, es un alto riesgo a la SI.

Asimismo, se han verificado diversas modalidades de difamaciones o calumnias y acosos a infantes u otros tipos de menores de edad.

Amenaza *Cloud Computing*:

En la actualidad, gran diversidad de compañías de los sectores privados está optando por los servicios y ventajas de la nube, el riesgo está en que la data o información está fuera de los dominios del propietario, es decir está en posesión de un tercero, convirtiéndose en una vulnerabilidad considerable.

El alojamiento de información fue el primer paso que despertó las ventajas administrativas y económicas de las empresas, actualmente se tiene también servidores de producción y contingencia en la nube.

i. Correos con la usanza de servicios tales como, verbigracia, Hotmail, Gmail, etcétera.
ii. Documentos con la usanza de servicios Google Docs. de Google.
iii. Documentaciones, informes, entre otros mediante la usanza de Dropbox.
iv. Visualización de videos en la usanza de YouTube.
v. Imágenes fotográficas en usanza de Instagram, Flickr, etcétera.

vi. Hojas de vida en la usanza de CompuTrabajo, Indeed, LinkedIn, etcétera.

3.5.2. Vulnerabilidades y métodos para su detección

Vulnerabilidad es la debilidad de cualquier tipo que envuelve la SI de los sistemas de información. Se agrupan en función de:

Diseño

a. Debilidad en diseños de protocolos de los que se hacen usanza en redes.
b. Políticas de SI inexistentes y/o deficiente.

Implementación

a. Errores de códigos en cuanto a programación.
b. En los sistemas informáticos se evidencian existencias de “puertas traseras”.
c. Descuidos por parte de proveedores y/o fabricantes.

Uso

a. Malas configuraciones de SI y TICS.
b. Falta de sensibilización sumado al desconocimiento de los colaboradores y responsables de oficina de informática respecto del tratamiento de información.
c. Disponibilidad de técnicas y herramientas que faciliten ataques físicos y cibernéticos.
d. Limitación del gobierno en sus políticas de aseguramiento de la información.

Vulnerabilidad del día cero:

Son aquellas vulnerabilidades que aún no son poseedoras de soluciones bien documentadas pero que, en realidad se conoce las maneras de explotarlas.

Vulnerabilidades cotidianas:

Vulnerabilidad de desbordamiento de buffer: Cuando un programa no controla la cantidad de datos que se copian en buffer, puede llegar a sobrepasarse la capacidad del buffer y los bytes que sobran se guardan en zonas de memoria adyacentes, lo que se puede aprovechar para ejecutar código que nos dé privilegios de administrador.

Vulnerabilidad de condición de carrera (race condition): Sucede cuando varios procesos acceden al mismo tiempo a un recurso compartido. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.

Vulnerabilidad de Cross Site Scripting (XSS): Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBScript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad, la víctima cree que está accediendo a una URL, pero en realidad está accediendo a otro sitio diferente.

Vulnerabilidad de denegación del servicio: Consiste en saturar la red para producir el colapso de un servicio o recurso con la finalidad de denegar el acceso a los colaboradores. Las pérdidas de conectividades de red por consumos del ancho de banda son también usuales cuando no se tiene los filtros necesarios para bloquear puertos innecesariamente abiertos.

Vulnerabilidad de ventanas engañosas (Window Spoofing). Las ventanas falaces hacen suponer al ganador de tal o cual cosa, con la finalidad que la víctima ingrese información personal. Otro tipo de ventanas es la que obtiene datos del equipo desktop o laptop para, posteriormente, desplegar ataques.

Cuentas con contraseñas débiles o sin contraseña: Asignación de usuarios con contraseñas débiles o por defecto constituyen una vulnerabilidad cotidiana en las instituciones donde existe abundante personal.

Insuficiente filtrado de los paquetes con direcciones de inicio y destino inadecuadas

Adulteración de dirección IP, método del que hacen usanza los atacantes para esconder sus huellas digitales en la web site.

Registro de eventos (*logging*) incompleto o inexistente:

Creación de registros (log) para un análisis minucioso con la finalidad de descubrir nuevas vulnerabilidades.

3.5.3. Tabla de amenazas y vulnerabilidades

Tabla 62

Tabla de amenazas y vulnerabilidades

Amenaza	Activo	Dimensión	Descripción	Vulnerabilidad
Fuego	W SI AUX	D	Riesgo de incendio ante un corto circuito	Sensores de humo no alertan Hay material inflamable No hay procedimiento de frente a un incendio Personal no capacitado
Inundación	HW SI	D	Riesgo de daño en los servidores	Sensores de aniegos no son revisados para probar su funcionalidad
Corte de energía	HW SI AUX	D	Riesgo de falta de energía para seguir operando	No hay procedimiento ante corte de energía. UPS no cuentan con buena autonomía. El grupo electrógeno no es probado frecuentemente.
Degradación en almacenamiento	SI	D	Riesgo de falta de espacio	Escaso mantenimiento del SOFTWARE. en los servidores Falta de aprovisionamiento de cintas de backup.
Manipulación de configuración	D SW HW COM	I C D A	Riesgo que la configuración de un activo sea inadecuada	No existe procedimiento ni SOFTWARE. para detectar intrusos en tiempo real. El nivel de las políticas de seguridad es muy alto (usuarios olvidan muy usualmente las contraseñas.
Suplantación de identidad	SW	C A I	Riegos de acceso privilegiado a personal no autorizado	Falta de políticas de auditoría de accesos. La política de uso de contraseñas no se revisa frecuentemente. El proceso de altas y bajas no es controlado en tiempo real.
Sabotaje digital	SW	D C I	Riesgo de acceso privilegiado a los servicios en línea.	Escasos programas de protección ante un ataque cibernético.

				Desconocimiento de nuevas herramientas de control y bloqueos. Falta de conciencia respecto del aseguramiento de las informaciones de programas en la Site Web
Abuso de acceso privilegiado	SW HW	C I	Riesgo de manipulación de la data para uso personal	No existe revisión periódica de derechos y permisos de usuario en la Data Base. No existe SOFTWARE. que alerte alguna modificación inadecuada en la Data Base.
Exceso de confianza	HW SW	D I C	Riesgo del uso de claves por terceros	El personal confía sus claves a personal de confianza. Se anotan claves y datos sensibles en *pos-its* a la vista de cualquier personal.
Denegación del servicio	HW SW	D	Riesgo de falta de algún recurso	Poco conocimiento en el uso de los cortafuegos. Falta de políticas. Tardanza en asignación de permisos a un usuario. Caídas de la red.
Hurto o robo	HW SW AUX COM	D C	Riesgo que se pueda utilizar claves en beneficio ajeno Riesgo de sustracción de información	No hay control estricto de dispositivos de almacenamiento. No hay inventario actualizado de equipos habilitados. Control inadecuado de personal que tienen acceso a los equipos de cómputos. Los sistemas de alarma de intrusos no son revisados para verificar su operatividad.
Desecho de activos	HW C SI	C	Riegos de entregar activos con información sensible	No hay políticas de desecho o proceso de baja de activos. No hay procedimiento de destrucción de información de activos incinerados y/o destruidos.

Fuente, Elaboración propia.

3.5.4. Gestión de Riesgos

Un riesgo es conceptualizado como aquella probabilidad de ocurrencia de un evento que dificulte a una organización o persona obtener un resultado esperado en el despliegue de un proyecto y/o negocio.

Tabla 63

Probabilidad de amenazas

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

Fuente, Elaboración propia.

Tabla 64

Impacto del nivel de riesgos

Valor	Impacto	Descripción
1	Insignificante	Impacta levemente en la operatividad del proceso
2	Menor	Impacta la operatividad del proceso
3	Medio	Impacta levemente la operatividad del marco proceso
4	Critico	Impacta levemente la operatividad de los procesos
5	Catastrófico	Impacta fuertemente en la operatividad de los procesos

Fuente, Elaboración propia.

Tabla 65

Nivel de riesgo

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

Fuente, Elaboración propia.

Tabla 66

Impacto vs Probabilidad

Probabilidad	**Impacto**				
Siempre	7	8	9	10	11
Muy frecuente	6	7	8	9	10
Frecuente	5	6	7	8	9
Normal	4	5	6	7	8
Poco Frecuente	3	4	5	6	7
Muy poco Frecuente	2	3	4	5	6
Nunca	1	2	3	4	5

Fuente, Elaboración propia.

3.5.5. **Matriz de Gestión de Riesgos**

Tabla 67

Matriz de gestión de riesgos

Cód.	Riesgo	Descripción	Causas	Consecuencias	ANALISIS DE RIESGOS					Dominio de la seguridad
					Valor	Probabilidad	(10) VALOR	Impacto	Severidad	
1	Compra de equipos sin las características mínimas requeridas para el tratamiento de la información.	1. Comprar SOFTWARE. que no cumple los requerimientos mínimos requeridos por Rash Perú S.A.C. 2. Comprar activos de comunicación (sw, router, etc.) inadecuados a las necesidades de Rash Perú S.A.C.	1. Desconocimiento de características actuales de los equipos. 2. Falta de revisión de las características solicitadas.	Pérdidas económicas. Denegación del sistema. Inestabilidad de los procesos.	20	Poco frecuente	2	Menor	40	A12 seguridad de las operaciones
2	Uso indebido de la información	Eventualidad de que la información confidencial, que se origine, proporcione o almacene en los sistemas de información, pueda ser accedida, manipulada y/o divulgada sin la debida autorización.	1. Insuficiente nivel de protección para acceder a la información. 2. Falta de conocimiento de las políticas de manejo de la información. 3. Actividades maliciosas por parte de terceros. 4. Acceso a información sin autorización. 5. Fraude cometido desde dentro de la organización.	Desconfianza del público usuario. Mala imagen, Toma de decisiones no adecuadas.	70	Frecuente	3	Medio	210	A9 control de acceso
3	Vulnerabilidad del sistema de información	Posibilidad de un acceso no autorizado por parte de un tercero al sistema de información de Rash Perú, con el objetivo de modificar, sustraer o dañar la información.	1. Nivel bajo de seguridad para el acceso a la información. 2. Seguridad perimetral inestable 3. Bugs en los sistemas de información. 4. Desconocimiento de los estándares para la implementación del aseguramiento de la información.	Pérdidas económicas. Inestabilidad de los procesos. Fuga de información	20	Poco frecuente	4	Critico	80	A9 control de acceso

4	Daños, deterioro o pérdida de los equipos informáticos	Posibilidad de que los recursos tecnológicos sufran daños, fallas o pérdidas tanto en su uso como en su almacenamiento.	1. Ausencia o mantenimiento inadecuado de los equipos de cómputo. 2. Calidad deficiente de los equipos de cómputo. 3. Uso inapropiado de los equipos de cómputo. 4. Falta de capacitación sobre el uso adecuado de los equipos de cómputo. 5. Insuficiente protección para los equipos de cómputo. 6. Amenaza de terrorismo. 7. Factores ambientales que pueden afectar el funcionamiento de los equipos de cómputo.	Equipos averiados. Mal uso de los recursos informáticos.	70	Frecuente	2	Menor	140	A11 seguridad física y ambiental
5	Ausencia y/o deficiencia en los SOFTWARE. y sistemas de información	Baja calidad en los resultados y/o estadísticas en los aplicativos que intervienen en el sistema.	1. Proceso complicado para la compra de activos. 2. Carencia o inadecuada gestión de mantenimiento de los recursos tecnológicos. 3. Deficiencia en la calidad de los recursos tecnológicos.	Elevación de las tasas en los servicios.	20	Poco frecuente	3	Medio	40	A14 adquisición, desarrollo y mantenimiento de sistemas
6	Inadecuada utilización de los recursos Web	Hace referencia a la inadecuada utilización de la página Web de Rash Perú S.A.C.	1. Ausencia de una cultura tecnológica arraigada en la organización. 2. Falta de capacitación en el uso de los sistemas y aplicaciones involucrados en el proceso.	Desinformación de los usuarios. Proceso de inscripción tradicional con la lentitud y riegos tradicionales.	80	Frecuente	2	Menor	160	A14 adquisición, desarrollo y mantenimiento de sistemas
7	Fallas en las comunicaciones	Posible denegación de los servicios de *networking* (internet, redes, intranet, servicio telefónico).	1. Servicio no disponible por parte del proveedor. 2. Mantenimiento insuficiente de los equipos y redes. 3.Deterioro de las redes de comunicación. 4. Fallas en las comunicaciones.	Acceso inoportuno a los servicios de inscripción y publicidad:	40	Normal	3	Critico	120	A13 seguridad de las comunicaciones

8	Fallas en el fluido eléctrico	Posible denegación de los servicios eléctricos	1. Variaciones en la corriente eléctrica. 2. Falta de salvaguardias para sobretensiones y/o cortes de energía no programados (Alimentación redundante). 3. Solución inadecuada de sistemas de energía ininterrumpida (UPS).	No prestar atención oportuna a los usuarios. Perjuicio económico para la institución	30	Poco frecuente	3	Crítico	90	A11 seguridad física y ambiental
9	Fracaso de eventos programados	Suspensión de actividades o eventos	1. Falta de difusión o escasa difusión de información. 2. Falta de interés por parte de los usuarios en temas de seguridad de la información.	Personal no capacitado. Frustración de los Gerentes ante incumplimiento de las metas.	90	Muy frecuente	3	Crítico	270	A13 seguridad de las comunicaciones
10	Humedad producida por sistemas de refrigeración inadecuados y/o filtraciones de agua	Daños en la infraestructura física (Servidores y demás activos dentro del datacenter).	1. Mal funcionamiento de los sistemas de aire de acondicionado. 2. Inadecuada protección del ambiente del datacenter frente a las amenazas ambientales.	Inestabilidad en los servicios registrales. Posible pérdida de información. Interrupción de procesos, daños físicos en los activos dependientes.	10	Muy poco frecuente	3	Crítico	30	A11 seguridad física y ambiental
11	Accesos no autorizados a las instalaciones del Área de Sistemas.	Ingreso de personas no autorizadas para la manipulación de equipos informáticos	1. Inadecuado control de acceso a las instalaciones 2 Puertas no aptas para la seguridad informática y de la información.	Pérdida de activos. Daños, manipulación, robos en la infraestructura Informática	50	Normal	3	Medio	150	A9 control de acceso

Fuente, Elaboración propia.

3.5.6. Tratamiento del Riesgo

Tabla 68

Matriz de tratamiento de riesgos

		EVALUACIÓN DE RIESGOS							
código	**Riesgo**	**Control**	**Descripción del Control**	**Tipo de Control**	**Está Documentado**	**Tipo de documento**	**aplicación**	**Eficacia del control**	**Frecuencia del control**
1	Compra de equipos sin las características mínimas requeridas para el tratamiento de la información.	Evolución de experto	Diagnóstico sobre ventajas y desventajas de las compras	Preventivo	SI	Procedimientos establecidos	SI	Alta	Cuando se presenta
2	Uso indebido de la información	Mejora de la estructura de usuarios por jerarquías. Difusión de políticas de gestión de la información. Supervisión continua de los sistemas de información. Implementación de procedimientos para la asignación de roles y accesos a los sistemas de información.	Establecimiento de roles en el sistema. Optimización de los controles en los sistemas de información	Preventivo	SI	Procedimiento de altas y bajas de acceso	SI	Alta	Mensual
3	Vulnerabilidad del sistema de información	Fortalecimiento de los equipos de seguridad perimetral. Procedimientos de control para la detección de vulnerabilidades en los sistemas de información. Aplicación de buenas prácticas para implementación de sistemas de información seguros.	Verificar que las políticas de Aseguramiento de la información estén funcionando adecuadamente de acuerdo con las normas internacionales ISO	Preventivo	SI	Normas de políticas de aseguramiento de la información	SI	Alta	Semanal
4	Daños, deterioro o pérdida de equipos informáticos	Mantener el material y los equipos asignados para el cumplimiento de las funciones	Inventarios frecuentes con reporte del estado actual de los equipos informáticos.	Preventivo	SI	Políticas de control de equipos.	SI	Alta	Semanal
5	Ausencia y/o deficiencia en los SOFTWARE. y sistemas de información	Determinar las características adecuadas	Brindar asesoría en la adquisición adecuada a los requerimientos de Rash Perú S.A.C	Preventivo	NO		SI	Alta	Cuando se presenta
6	Inadecuada utilización de los recursos Web	Capacitación y concientización	A través de la red de capacitadores, cursos y/o manuales de usuario	Preventivo	SI	Políticas de capacitación y concientización	SI	Alta	Cuando se presenta
7	Fallas en las comunicaciones	Verificación de las conectividades entre los activos comprendidos en el sistema	Monitoreo de performance de las redes de comunicaciones	Preventivo	NO		SI	Alta	Semanal

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

Fuente, Elaboración propia.

Tabla 69

Escala por tipo de control

Aplicación		Periodicidad		Producto	Eficacia	Valoración
Preventivo	4	Periódico	3	12	Alta	4
Preventivo	4	Permanente	2	8	Media	3
Preventivo	4	Ocasional	1	4	Baja	2
Correctivo	3	Periódico	3	9	Alta	4
Correctivo	3	Permanente	2	6	Media	3
Correctivo	3	Ocasional	1	3	Baja	2
Detectivo	2	Periódico	3	6	Media	3
Detectivo	2	Permanente	2	4	Baja	2
Detectivo	2	Ocasional	1	2	Baja	2
Inexistente	1	--		1	Inexistente	1

Fuente, Elaboración propia.

Tabla 70

Eficacia de control

Eficacia del Control	
ALTO	4
MEDIO	3
BAJO	2
INEXISTENTE	1

Fuente, Elaboración propia.

3.5.7. Cálculo del riesgo residual

Después de aplicar los controles, el riesgo que permanece se conoce como riesgo residual. Para calcular el nivel de exposición al riesgo, se divide el nivel de riesgo original por el nivel de eficacia del control asociado al riesgo

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

Tabla 71

Valoración del riesgo residual

Valoración de riesgo (residual)	
Nivel	Calificación
INACEPTABLE	> 30
IMPORTANTE	20 a 30
MODERADO	10 a 20
TOLERABLE	5 a 9.9
ACEPTABLE	< 5

Fuente, Elaboración propia.

3.5.8. Fase para el tratamiento del riesgo

Acción: Actividad a realizar.

a. Opciones de Posibles Tratamientos: Medidas a efectuar según la acción.
b. Resultado del Costo/Beneficio.

Tipo de Tratamiento:

a. Prevenir: Evitación por no iniciar o continuar la actividad que condujo al riesgo.
b. Aceptar: Aceptar o aumentar el riesgo para perseguir una oportunidad.
c. Evitar: Eliminación de la fuente de riesgo.
d. Mitigar: Cambio de probabilidad y / o consecuencias.
e. Transferir: Compartiendo el riesgo con otra parte.
f. Retener: Retención del riesgo mediante una decisión informada.

Responsable: Encargado de la actividad o tarea a realizar.

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

3.5.9. Selección de controles

¿Por qué usar la ISO 27002?

Se puede lograr una gran adaptabilidad a otros estándares de sistemas de gestión, como ISO 9001 e ISO 14001. El proceso de mejora continua del sistema de gestión de seguridad de la información se mantiene en curso. Se definen los requisitos para la documentación y almacenamiento de registros. Se lleva a cabo una evaluación de riesgos y se utilizan procedimientos de gestión en el modelo PHVA (Planificar, Hacer, Verificar y Actuar).

Tabla 72

Nuevos conceptos ISO 27002

Nuevo concepto actualizado	Explicación
Contexto	Entorno en el que opera la organización
Problemas, riesgos y oportunidades	Sustituye a la acción preventiva
Liderazgo	Requisitos de la gerencia
Comunicación	Requisitos para las comunicaciones internas y externas
Objetivos de seguridad	Los objetivos se encuentran fijos en cada nivel
Evaluación de riesgos	Identificación de activos, amenazas y vulnerabilidades
Propietarios de riesgos	Reemplaza propietarios de los activos
Plan de tratamiento	Eficacia de los controles
Controles	Se determinan durante el proceso de riesgos
Información documentada	Reemplaza los documentos y riesgos
Evaluación del desempeño	Cumple con el SGSI y la eficacia del plan de tratamiento de riesgos
Mejora continua	Planificar, hacer, verificar, actuar (PHVA)

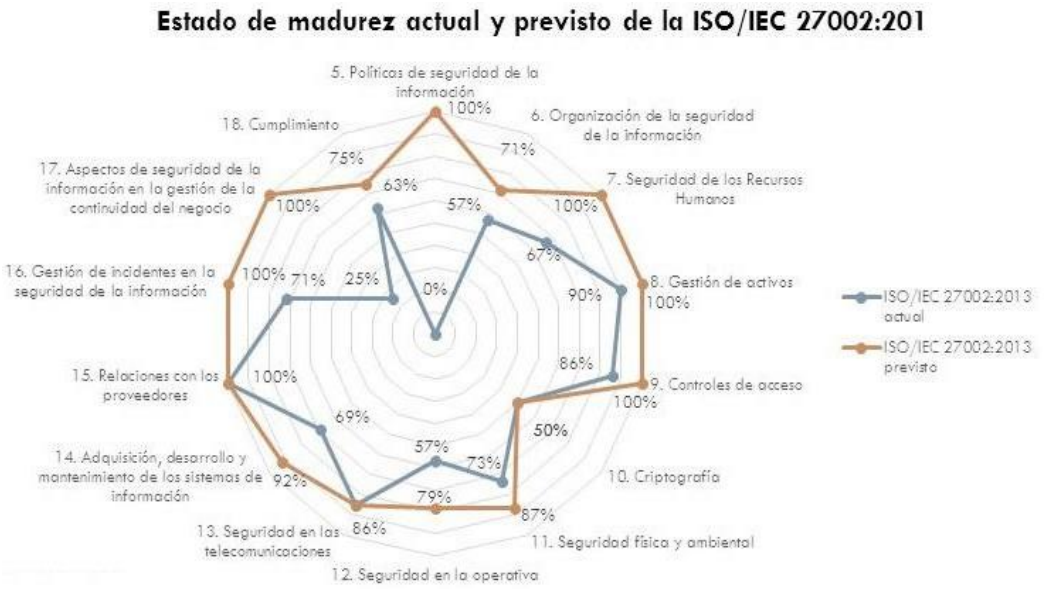


Figura 46. Estado de madurez actual Norma ISO/IEC 27002

3.5.10. Elección de la herramienta para implementación del SGSI

Se realizó un análisis de diversas alternativas de herramientas que se presentan en el mercado, solicitando demos y versiones de prueba, tales como SoftExpert, E-Pulpo, ISOTools SGSI y Securia SGSI, determinando a Securia SGSI como la herramienta alineada a la ISO 27002, de código abierto y de bajo costo, dicho aplicativo nos sirve de memoria ayuda y cubre el proceso implantación, puesta en funcionamiento, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) basados en la norma internacional ISO 27002. Por ser de código abierto se cuenta con apoyo de los desarrolladores interesados en el aplicativo, así como con manuales de implementación y uso en español.

A continuación, muestra de la descripción y las interfaces de las herramientas para SGSI:

Herramienta AWRisk:

AWRisk es un SOFTWARE. que se adapta a las necesidades específicas de la organización y permite automatizar los procesos de gestión de riesgos en diversos contextos, incluyendo la seguridad de la información (SGSI), la protección de datos personales (LPDP 29733), PCI, SOX, OHSAS 18000, calidad con ISO 9000, NIST, continuidad de negocio con ISO 22000, gestión de proyectos e ISO 27018 para empresas en la nube, entre otros.

En la pantalla, se muestra el menú principal, donde se pueden identificar los renglones a los que se le presta servicio:

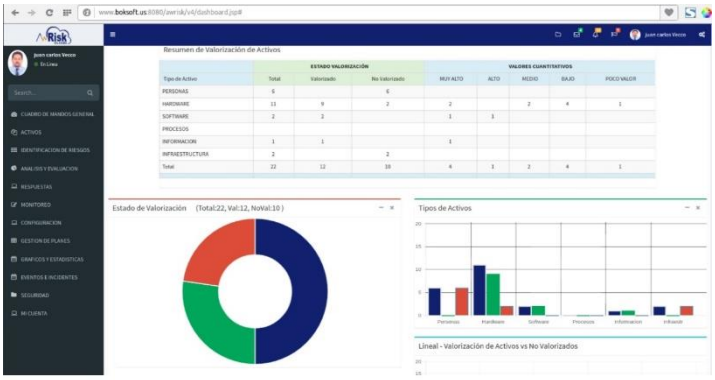


*Figura 47***,** Interfaz Estado de herramienta AWRisk.

Fuente, Elaboración propia.

Herramienta ePULPO:

Esta herramienta, es una combinación de SOFTWARE. libre y desarrollos de de gestión para las diferentes metodologías: LOPD-LOPD-ENS- SGSI (ISO 27001)-ITIL (ISO 20000) PCI, entre otros. Su forma de organización es como rompecabezas, con el fin de hacer uso de herramientas de código abierto. En la pantalla siguiente, se visualiza el menú principal, que se compone de conectores de aplicaciones para el caso que no existía ningún SOFTWARE. de código abierto que respondiera a las necesidades de la organización.

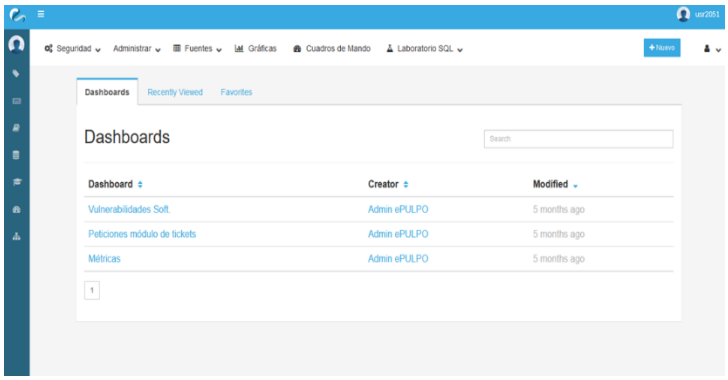
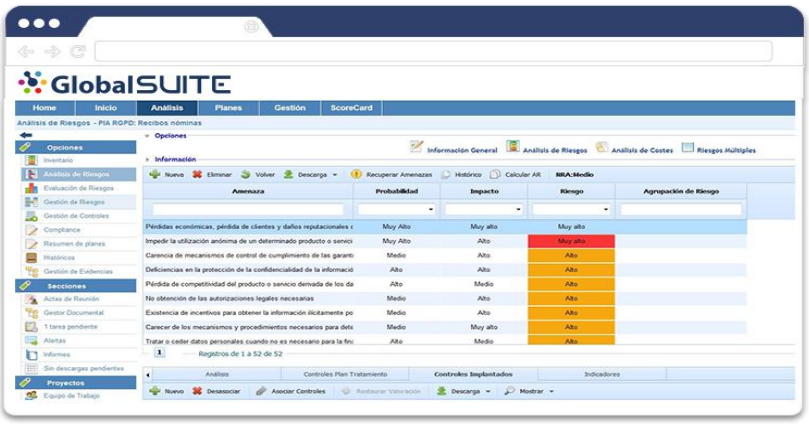


Figura 48, Interfaz Estado de herramienta ePULPO.

Fuente, Elaboración propia.

Herramienta Global Suite

Esta herramienta, actúa como un SOFTWARE. de gestión que mantiene y despliega normas, leyes y estándares internacionales, como ISO 22301, ISO 27001, ISO 31000, ISO 20000, protección de infraestructuras críticas, de datos y mejores prácticas. En la figura 49, se muestra su interfaz, donde se presentan las distintas opciones de gestión de



riesgos.

Figura 49, Interfaz herramienta Global SUITE.

Fuente, Elaboración propia.

Herramienta Seguridad SGSI

Esta herramienta integral, automatiza el proceso de implantación, puesta en marcha, mantenimiento y mejora continua de los Sistemas de Gestión de la Seguridad de la Información (SGSI), sus lineamientos son mucho mas específicos ya que son conforme a la norma ISO 27001.

En la pantalla siguiente, se muestra la creación de un SGSI, donde se visualiza, tablas, índices, foráneos, entre otros.

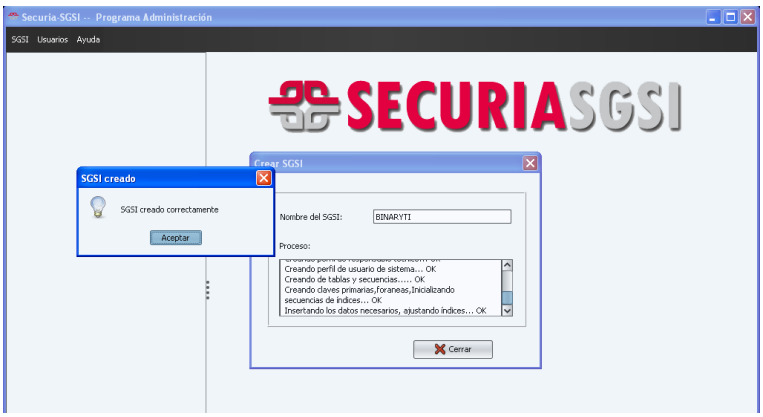


*Figura 50***,** Interfaz herramienta Seguridad SGSI.

Fuente, Elaboración propia.

Herramienta ISOTools

Esta herramienta, automatiza el proceso de gestión, bajo su plataforma de planificación estratégica de la organización, impulso de competitividad a largo plazo, facilita el control para la toma de decisiones,

y proporciona buenas prácticas, para la mejora continua de los procesos. Además, forma parte del pacto mundial de las naciones unidas.

En la interfaz, se puede apreciar la estructura de los tipos de elementos, activo, amenaza, vulnerabilidad.

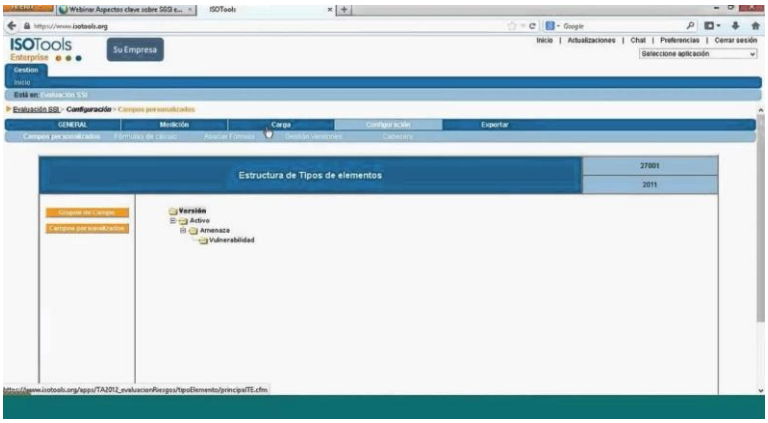


Figura 51, Interfaz herramienta ISOTools

Fuente, Elaboración propia.

3.5.11. Mejoras al aseguramiento de la información

3.5.11.1. Aplicación de salvaguardas

Según Magerit, las salvaguardas permiten hacer frente a las amenazas. Con el avance tecnológico e informático, las técnicas varían:

a. Aparecen nuevas tecnologías y desaparecen las tecnologías antiguas, pero el principio y finalidad es la misma.
b. Los tipos de activos se renuevan, aparecen o cambian y todos deben ser considerados.
c. Los atacantes se modernizan y evolucionan hacia nuevas estrategias de ataques.
d. Así mismo evoluciona el catálogo de salvaguardas disponibles, vistos desde nuevos ámbitos territoriales informáticos.

Protección de los datos / información

a. Respaldo permanente de los datos (Backus).
b. Aseguramiento de la integridad de la información.
c. Técnicas de cifrado en el tratamiento de la información.
d. Uso más frecuente de firmas electrónicas, con las respectivas cualidades de seguridad.
e. Uso de servicios de fechado electrónico (*time stamping*, o sellado de tiempo).

Protección de los servicios

a. Asegurar la disponibilidad de los servicios (principio de alta disponibilidad)
b. Aceptación y puesta en marcha de los servicios.
c. Asignación de perfiles de seguridad a los empleados y recursos.
d. Explotación S.CM Gestión de cambios (mejoras y sustituciones).
e. Protección de servicios, aplicaciones web, alojamiento en la nube y correos electrónicos.
f. Protección de directorios locales y virtuales.
g. Protección de servidores Controlador de nombres de dominio (DNS).
h. Servicios de teletrabajo.
i. Servicio de telefonía voz sobre IP.

Existen 2 tipos de funciones tipificados para salvaguardar los servicios:

a. Los servicios o funciones preventivos se enfocan en la vulnerabilidad de un activo antes de que se produzca una agresión, lo que disminuye la probabilidad de que la amenaza se materialice (aunque no la posibilidad en general, que es independiente del activo amenazado). Estos servicios se encargan de reducir tanto las amenazas involuntarias como las intencionales realizadas por seres humanos.

Las funciones o servicios curativos o restablecedores tienen como objetivo reducir la gravedad del impacto una vez que ha ocurrido la

agresión. Estos servicios pueden aplicarse a amenazas de cualquier tipo. En contraste, las funciones preventivas actúan antes de que ocurra la agresión y buscan reducir la vulnerabilidad y la potencialidad de materialización de la amenaza, independientemente del tipo de activo amenazado y si la amenaza es involuntaria o intencional.

Función Salvaguarda preventivo

Magerit implementa este mecanismo para actuar directamente sobre las vulnerabilidades de los sistemas, generalmente sobre el factor humano previniendo y disuadiendo para tomar conciencias de las consecuencias de una agresión intencional o involuntaria sobre los activos de la empresa.

Un ejemplo concreto es la implementación de controles de acceso. Si se detectan y previenen posibles infracciones, es posible que se desaliente a los posibles delincuentes. Además, la aplicación adecuada de la ley puede ser crucial para reducir el riesgo potencial.

Función Salvaguarda curativo y restablecedor

Este tipo de mecanismo actúa sobre el impacto ocasionado en el área afectada y trata de disminuir la gravedad del ataque.

Por ejemplo, si se detecta un problema de integridad en una información debido a un desequilibrio, se toman medidas para detener la circulación de esa información y verificar las fuentes. La detección curativa, o monitoreo del impacto, debe llevarse a cabo antes de tomar medidas para restaurar los sistemas de seguridad, ya que a menudo las amenazas no se detectan o se detectan demasiado tarde para tomar medidas efectivas de restauración.

El arqueo de las cajas es un buen ejemplo de esta salvaguarda detectora.

Estrategias para la conservación de documentos digitales

Preservación de la tecnología. - La propuesta de David Bearman tiene como objetivo la creación de museos cibernéticos o informáticos que recojan tanto el HARDWARE. como el SOFTWARE. que ya no se utiliza.

Conversión. - Margaret Hedstrom sugiere que, para preservar objetos digitales sin perder su funcionalidad, se deben utilizar formatos que

cumplan con estándares no propietarios y que puedan ser exportados. Por otro lado, Jeff Rothenberg defiende la emulación de la tecnología, lo que implica recrear la apariencia y funcionalidad original de un objeto digital mediante el uso de emuladores de SOFTWARE. obsoleto. Finalmente, la migración consiste en la transferencia periódica de materiales digitales de una configuración de HARDWARE. / SOFTWARE. a otra o a la siguiente generación de tecnología.

Consejos de buenas prácticas para protegerse de las amenazas y vulnerabilidades.

- Mantener estricto control de contraseñas y políticas de cuentas de acceso.
- Vigilar el estricto cumplimiento en la separación de funciones y privilegios para la asignación de acceso a la información sensible.
- Evitar la facilidad en los procesos de visto bueno a la hora de otorgar permisos.
- Practicar la rotación de tareas constantemente.
- Ser muy exigentes en la selección y formación del personal que administra los sistemas de la institución.
- Capacitar y concientizar periódicamente en temas de sensibilización de aseguramiento de la información para todos los empleados.
- Realizar evaluaciones de riesgos en el Sistema de Intermediación Digital con regularidad incluyendo pruebas de transgresiones internas y externas al sistema al menos una vez al año.
- Seleccionar y aplicar los objetivos de los controles del Anexo A de la ISO/IEC 27001:2013 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Utilizar una metodología efectiva como MAGERIT para el análisis y gestión de riesgos.
- Acciones de defensa activa e inmediata contra códigos maliciosos.

- Desactivar el acceso a los sistemas inmediatamente después de culminada su situación contractual con los empleados y proveedores en general.
- Asegurar que los *backup* cumplan con los requisitos primordiales de seguridad de la información.
- Supervisar y responder inmediatamente a todas las acciones sospechosas en sistemas y comportamiento de empleados, especialmente si son administradores o personal de apoyo.
- Integrar la ISO/IEC 27001 con otras ISO, compatibles con el objetivo de ser parte de un proceso de certificación.
- Evitar el uso generalizado del usuario administrador del sistema para el acceso a servidores o para validar un acceso.
- Realizar la adecuada configuración de las cuentas de usuario, estableciendo permisos y contraseñas robustas.
- Utilizar SOFTWARE. legal licenciado y controlar constantemente su actualización.

Implementación de tecnología "Facephi" como alternativa para evitar el fraude por robo de identidad.

El proceso de identificación implica comparar los rasgos biométricos del usuario (1:N). En términos generales, el sistema verifica la identidad del usuario basándose en su patrón facial. Para ello, el patrón facial extraído se compara con la base de datos completa de usuarios del sistema. Si se encuentra una coincidencia, se identifica al usuario correspondiente cuyo patrón almacenado se asemeja más al patrón extraído durante el proceso de verificación.

Ventajas:

a. Tecnología 100% propietaria
b. HARDWARE. de bajo costo y fácil implementación
c. Patrón de 6Kb, no almacena imágenes del usuario
d. Patrón encriptado, no permite realizar ingeniería inversa sobre el patrón.
e. Rapidez del proceso en 38 mili segundos (detección. Extracción y *matching*)

f. Capacidad de comparación de 80,321 rostros por segundo.
g. Tecnología inteligente, la imagen no se afecta por el paso del tiempo o cambio de rostro.
h. No intrusivo, reconoce la cara a distancia.

Monitoreo de la red

Principales características de las herramientas y métodos:

a. Transmitir alertas de manera efectiva.

b. Conectar y colaborar con servidores externos.

c. Presentar datos de manera clara y fácil de usar en la interfaz.

d. Adaptarse de manera flexible a herramientas y SOFTWARE. específicos.

e. Proporcionar una API para permitir el acceso a sistemas externos.

f. Detectar dispositivos automáticamente.

g. Integrarse con bases de datos.

h. Ser compatible con múltiples dispositivos.

i. Escalar eficientemente con el crecimiento del sistema.

j. Soportar diversos protocolos de adquisición de datos.

k. Mantener la seguridad en todas las operaciones.

l. Integrarse con máquinas virtuales.

m. Integrar HARDWARE. adicional.

n. Permitir el control remoto del sistema.

o. Realizar un inventario de HARDWARE. y SOFTWARE..

p. Proporcionar información de geolocalización.

q. Monitorear sistemas en la nube.

Aplicación de código hash, a los certificados digitales utilizando

Este proceso implica convertir todo el certificado digital en un valor numérico o cadena de datos. Además, en este sistema criptográfico, cada usuario debe tener un par de claves:

Clave privada: La clave privada es un elemento de seguridad que debe ser cuidadosamente protegido por su dueño y no debe ser compartido con nadie más. Es un componente crítico en un sistema criptográfico y su pérdida o compromiso puede poner en riesgo la seguridad de los

datos protegidos por dicha clave. Por lo tanto, es importante que el propietario tome medidas adecuadas para asegurar la confidencialidad de su clave privada.

Clave pública: La clave pública, por otro lado, será compartida por todos los usuarios del sistema criptográfico y se utiliza para cifrar los mensajes o datos que se quieren transmitir. La pareja de claves funciona de manera complementaria: lo que se cifra con una clave solo puede ser descifrado con la otra clave correspondiente. Las claves son generadas mediante algoritmos matemáticos complejos que hacen virtualmente imposible calcular una clave a partir de la otra en un tiempo razonable.

Dispositivos físicos para gestión y custodia de claves

En la actualidad, se han establecido normas para evaluar los niveles de seguridad de los dispositivos criptográficos que combinan HARDWARE. y SOFTWARE., como los HSM. El National Institute of Standards and Technology (NIST) ha desarrollado un estándar conocido como Federal Information Processing Standard (FIPS) que permite establecer el nivel de seguridad ofrecido por estos dispositivos. Este estándar es considerado como una guía para los organismos gubernamentales o sujetos a regulaciones muy estrictas, y se divide en cuatro niveles que gradúan el nivel de seguridad de los dispositivos evaluados. A continuación, se detallan los niveles:

Nivel 1: Es el más básico y solo requiere el uso de un algoritmo criptográfico y una función de seguridad reconocidos. En este nivel, no hay requisitos de seguridad física.

Nivel 2: Además de cumplir con los requisitos del nivel anterior, se exige la implementación de medidas de seguridad físicas que permitan detectar manipulaciones en el dispositivo que puedan posibilitar un acceso no autorizado a las claves manejadas en el mismo. Estas medidas pueden ser sellos que se rompan cuando se accede al dispositivo que almacena las claves en claro o a los parámetros críticos

de seguridad del dispositivo. Estos parámetros se almacenan sin cifrar en los registros del criptoprocesador y se utilizan para generar las claves.

Nivel 3: Además de cumplir con los requisitos del nivel 2, en el nivel 3 se exige que el dispositivo no solo detecte accesos no autorizados, sino que también responda a ellos y evite el uso no autorizado o la modificación del módulo. Por ejemplo, un dispositivo de nivel de seguridad 3 debería detectar automáticamente si se abre y, como medida de seguridad, borrar los parámetros de seguridad críticos para inutilizar el acceso no autorizado y proteger la confidencialidad de las claves almacenadas.

Nivel 4: En el nivel 4, se deben mantener los requisitos de seguridad de los niveles anteriores, pero también se agregan nuevos requisitos. Además de tener mayor capacidad para detectar intrusiones físicas, el dispositivo también debe ser capaz de detectar condiciones ambientales inadecuadas, como humedad, temperatura o tensión, que podrían afectar su funcionamiento. De esta manera, se puede garantizar que se manejen estas contingencias para preservar la confidencialidad de la información almacenada en el dispositivo. Cabe señalar que cualquier HSM que se utilice para implementar una PKI debe tener al menos un certificado FIPS-2, lo que implica cumplir con los requisitos de seguridad del nivel 3.

3.5.11.2. Estrategias de mayor relevancia

3.5.11.2.1. Estrategia de “Defensa en Profundidad”

El término "defensa en profundidad" se originó en el ámbito militar, específicamente en la época en la que las ciudades eran fortalezas. Actualmente, este concepto se ha trasladado al campo de la seguridad de la información. La definición de este término se centra en la implementación de una estrategia global y dinámica que coordina varias líneas de defensa en todo el sistema de información, cubriendo su profundidad. De esta manera, se busca proteger el sistema de información de posibles ataques, implementando una

serie de medidas defensivas en varias capas para dificultar el avance de un atacante

Objetivo. - El propósito de esta estrategia es retrasar el progreso del oponente mediante la implementación de múltiples capas de defensa en lugar de una sola línea defensiva fuerte. Al tener varias líneas de defensa, se busca dificultar el avance del oponente y, en caso de que logre superar una capa de defensa, encontrarse con otra capa que le dificulte aún más el progreso. De esta manera, se aumenta la probabilidad de detección del atacante y se brinda al defensor más tiempo para ajustar y fortalecer las defensas en áreas vulnerables.

En el ámbito de la seguridad de redes, se utiliza una técnica conocida como defensa en profundidad, la cual se basa en la implementación de varias capas de defensa en la red. Esta estrategia de seguridad permite que si un atacante logra vulnerar una capa de defensa, se tope con otra capa de medidas de seguridad, lo que dificulta su avance. Gracias a la existencia de estas capas de defensa, se pueden evitar ataques directos a sistemas y datos críticos, además de aumentar la posibilidad de detección de un atacante y darle al defensor más tiempo para ajustar las defensas en las áreas necesarias en caso de un ataque continuo.

Las capas de las posiciones defensivas en defensa en profundidad son las siguientes:

Datos. - El objetivo principal de un atacante, incluyendo la información de servicios del Directorio activo, las bases de datos, documentos y más.

Aplicación. - El SOFTWARE. que maneja los datos, este el objetivo principal del atacante.

Host. - Las computadoras que utilizan las aplicaciones.

Red interna. - La red en la infraestructura de TI de la empresa.

Perímetro. - La red que conecta la infraestructura de TI de la empresa a otra red externa, con socios o con Internet.

Física. - Los aspectos visibles en informática: discos duros, las computadoras-servidores, conmutadores de red, etc.

Conocimiento de políticas y procedimientos. - Los fundamentos generales que ejercen la estrategia de seguridad de la empresa. Esta capa es primordial, sin ella, fallaría toda la estrategia.

3.5.11.2.2. Plan de capacitación y concientización

A. Introducción

La implementación de un Sistema de Gestión de Seguridad de la Información se implementa en una institución para proteger los activos esenciales, es por ello que se debe tener al personal informado y capacitado en temas referidos al aseguramiento de la información para mantener los estándares de nivel de seguridad. La ISO 27002 nos ayuda con sus dominios y controles y debemos conocerlo para mantenerlo.

B. Justificación

Según las encuestas y entrevistas realizadas al personal relacionado con el uso de la plataforma electrónica Sistema de Intermediación Digital, se hizo necesario la elaboración de un plan de capacitación y concientización respecto de acciones en el puesto de trabajo referido al aseguramiento de la información.

Se realizó un ejercicio de jerarquización para priorizar las acciones de capacitación:

a. Necesidades de una persona.
b. Necesidades que tiene un grupo.
c. Necesidades de un puesto de trabajo
d. Necesidades que requieren atención inmediata.
e. Necesidades que requieren solución a futuro.
f. Necesidades que exigen instrucción sobre la marcha.
g. Necesidades que precisan instrucción fuera del trabajo.

h. Necesidades que la empresa puede resolver por sí misma.
i. Necesidades que requieren contratar a capacitadores externos.

C. Objetivos

a. Evitar que se haga mal uso de las herramientas de HARDWARE. y SOFTWARE. asignado a los servidores registrales y notariales.
b. Detectar anticipadamente los riesgos y amenazas que comprometen la seguridad de los activos de la institución.
c. Proteger los activos de la institución al que tiene acceso el personal registral y notarial a través del conocimiento de los métodos y controles de la ISO 27002.

D. Estrategias de capacitación

- **Capacitación en el puesto:** Se utiliza con personal nuevo, el cual es adiestrado por un personal antiguo, es decir la capacitación es parte de su labor y el aprendizaje es con eventos reales.
- **Conferencias:** las más utilizadas para alcanzar a un gran número de empleados, se puede ayudar con la entrega de manuales, fichas, procedimientos, etc.
- **Juegos de roles:** importante cuando el personal tiene que cubrir otro rol dentro de la institución.
- **Técnicas audiovisuales:** se utiliza para orientar al empleado a través de videos, diagramas, audios, etcétera.
- **Aprendizaje programado:** Técnica que permite al empleado a retroalimentarse.
- **Simulaciones:** Se realiza en el mismo puesto de trabajo o en ambientes de pruebas.

E. Programación

- **Manejo de contraseñas:** Se tuvo en cuenta las políticas de seguridad según las normas internacionales, consejos de

buenas prácticas según ITIL y COBIT, tips para cambio de contraseñas.

- **Correo electrónico:** Consejos de buenas prácticas para el acceso a correos desconocidos, ventajas y virtudes de algunos proveedores de servicio gratuito o pagado.
- **Código malicioso:** Uso de técnicas para detección y eliminación de código malicioso, herramientas más utilizadas.
- **Sistema de Intermediación Digital:** Se detalla el proceso de inscripción, función de los actores y recomendación para la seguridad de las herramientas que intervienen en este proceso.
- **Usurpación de identidad:** Aclarar el concepto de usurpación de identidad, leyes que rigen la acción del delito, técnicas para de protección frente a dicha amenaza.
- **Ciclo de vida del SOFTWARE.:** Concientizar acerca de la necesidad de las actualizaciones en los aplicativos y SOFTWARE. utilizado en las terminales de red, así como la necesidad de hacer buen uso e informar respecto de la funcionalidad de estos.
- **Principio de escritorio limpio:** Concientizar acerca de la ventaja y precauciones para evitar el robo de información sensible, manteniendo el escritorio libre de papeles y material con anotaciones varias.
- **Control de accesos:** Conocer las distintas técnicas y herramientas utilizadas para el acceso a los sistemas informáticos y áreas restringidas. Concientizar respecto de los niveles de acceso.
- **Ingeniería social:** Conocer los mecanismos de defensa para afrontar las amenazas de los atacantes, tomar conciencia que el eslabón más débil es el usuario.
- **Redes sociales:** Conocer las diferentes herramientas que actualmente existen para la comunicación y transferencia de datos en la red internet. Conocer los peligros a los que estamos expuestos al conectarnos al internet.

- **Informática en la nube:** Conocer los diferentes proveedores que existen en la nube y son ofertados para proveer de espacio para almacenamiento u operatividad de sistemas completos de una institución.
- **Ciberseguridad:** Conocer las distintas técnicas y herramientas para proteger nuestros activos de los ciberataques. Aquí se habla del concepto de seguridad digital e identificar los riesgos y amenazas actuales.
- **Talleres de entrenamiento:** En 3 distintos temas de mayor incidencia en los centros de labores.

Asimismo, en cuanto a la validación del SGSI basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en Rash Perú SAC, se precisó evaluar dicho modelo por expertos. Por lo que en primer lugar se debió de diseñar el instrumento de recolección de datos, como, la ficha de juicio de expertos, la cual contempló diez (10) indicadores como puede visualizarse a continuación:

ASPECTOS DE VALIDACIÓN

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

VALORACIÓN: _____

OPINIÓN DE APLICABILIDAD: _____

Lugar y fecha: Chiclayo, ____ abril del 2012.

*Figura 52***,** Indicadores considerados en la Ficha de Juicio de Expertos.

Fuente, Elaboración propia.

Posterior a ello, se procedió a solicitar la evaluación crítica de tres (03) expertos que vean la viabilidad del SGSI basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en Rash Perú SAC, el mismo que fue desarrollado por el investigador. Para ello, fue necesario que dichos expertos posean las siguientes características:

- Tener Grado Académico en Ingeniería de SOFTWARE. o Ingeniería de Sistemas o Ingeniería Informática.
- Tener postgrado conforme con la Gestión de TI
- Tener conocimientos probados en procesos de seguridad de la información y/o seguridad informática en la gestión pública o privada
- Tener experiencia profesional mayor a 10 años en labores asociadas a Ingeniería de SOFTWARE., Ingeniería de Sistemas o Ingeniería Informática.

Luego de determinar cuáles son los criterios, se pudo establecer comunicación con tres (03) expertos cumplían con las características necesarias para la evaluación de dicho modelo. Los expertos que fueron tomados en cuenta se muestran en la siguiente tabla:

Tabla 73

Expertos para validación del modelo propuesto

Nº	Nombres y Apellidos del Experto	Grado Académico
1	Ruiz Gómez Woolder	Doctor (c) en Ingeniería de Sistemas e Informática
2	Huerta Michiline Carlos Antonio	Maestro en Dirección de Sistemas y Tecnologías de la Información
3	Quenema Moron Carlos Alfonso	Maestro (c) en Dirección de Sistemas y Tecnologías de la Información

Fuente. Elaboración propia.

Consecuente a la selección de los expertos, se continuó con la comunicación con cada uno de ellos a través del uso de correo electrónico, en los cuales se adjuntó la Ficha de Juicio de Expertos. Luego de que los expertos culminaron con la solicitud de validación, se procede a la recepción de las "Ficha de Juicio de Expertos" con los resultados. Estas fichas se encuentran en el **¡Error! No se encuentra el origen de la referencia.**. A continuación, se muestran las valoraciones brindadas por los expertos:

Tabla 74

Resultados de valoración por juicio de expertos

Nº	Experto	Promedio por experto	Nivel de Aceptación del Modelo
1	Experto 01	95.00	
2	Experto 02	93.50	94.50%
3	Experto 03	95.00	

Fuente. Elaboración propia.

Como se pudo ver en la anterior tabla, el SGSI basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en Rash Perú SAC se valoró con un porcentaje de aceptación de 94.50 en una escala del 1 al 100, por lo que se consideró como "Muy Buena".

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones.

Se concluye del objetivo específico 1 que el estado actual de la seguridad informática en Rash Perú SAC, el valor promedio del Re-test fue de 69.90% y el valor promedio Post-test fue de 14.00%. Además, el valor mínimo del re-test fue 50%, el valor máximo es 88%, y el valor mínimo de la post-test es 0% y el máximo es 27%; evidenciándose deficiencias tales como, poco conocimiento en políticas de seguridad, no aseguramiento del acceso de personal autorizado, se carecían de procedimientos para la eliminación de accesos de usuarios, no se venían firmando acuerdos de confidencialidad, eran defectuosos los procedimientos de destrucción de data en equipos sensibles, no desarrollaba capacitación y concientización en seguridad informática.

Se concluye del objetivo especificó 2 desarrolló un sistema de gestión de seguridad informática fundamentado en la Norma ISO/IEC 27002 para la empresa caso de estudio, para lo cual se realizó un ranking de metodologías existentes para la gestión de los riesgos llegando a determinar a MAGERIT como la de mejores prestaciones, y sumada con, el soporte del Ciclo de Deming, pudo establecer un sistema de cuatro fases bien definidas. En la que se evidenció que el nivel de significancia en el Re-test fue de 0,265 y para el Post-test, 0,108. Por lo cual se determina que el indicador se ajusta a una distribución normal o paramétrica ($P > 0.05$).

Se concluye del objetivo específico 3 que se validó mediante juicio de expertos el sistema de gestión de la seguridad informática diseñado previamente para la empresa Rash Perú SAC mediante dicha técnica, de modo que los expertos emitieron su veredicto favorable con un promedio de 94.50 de aprobación, determinándose que dicho sistema de gestión poseía los requerimientos necesarios de la gestión de la información.

Se concluye objetivo específico 4 que al ejecutar una prueba piloto del sistema de gestión de la seguridad informática en la empresa RASH PERÚ SAC, resultados mostraron que el nivel de significancia en el Re-test fue de

0,265 y para el Post-test, 0,108. Por lo cual se determina que el indicador se ajusta a una distribución normal o paramétrica (P > 0.05). utilizando políticas, controles y procedimientos que fueron diseñados previamente y que evidenciaron mejoras en cuanto al nivel de la seguridad de la información, riesgos de la información y programas de capacitación y concientización en dicho caso de estudio.

Se concluye del objetivo específico 5 que los resultados obtenidos posteriores a la implementación del SGSI el valor promedio del Re-test fue de 52.60% y el valor promedio Post-test fue de 11.40%. Además, el valor mínimo del re-test fue 40%, el valor máximo es 70%, y el valor mínimo del post-test es 0% y el máximo es 22%. obteniéndose mejoras significativas en el 100% de los indicadores establecidos, tales como, nivel de seguridad de equipos, nivel de políticas de control de accesos, nivel de protección de datos, etcétera.

4.2. Recomendaciones.

Se recomienda a Rash Perú SAC que hay que realizar mejoras continuas a fin de minimizar los riesgos ante las amenazas que se muestra en aumento en los distintos aspectos del avance tecnológico, implementando para ese fin, el presente SGSI que se ha desplegado en esta investigación pues se encuentra enmarcado en un estándar de rigor internacional.

Se recomienda a futuros investigadores en seguridad de la información, hacer usanza del instrumento de recolección de datos elaborado en esta investigación pues se encuentra fundamentada en las dimensiones de la gestión de la seguridad de la información y en las características propias de la ISO/IEC 27002.

Se recomienda a los directivos de diversas empresas de este sector retail que, aprovechando el alto nivel de validez de los expertos acerca del SGSI propuesto en esta investigación, se implemente en su totalidad en sus representadas para comprobar de forma práctica la total eficacia de las políticas de seguridad definidas.

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

Se recomienda que se debe realizar auditorías externas y internas para verificar que las políticas de SI se aplican de acuerdo a las normas vigentes.

REFERENCIAS

Acevedo, N., & Satizábal, C. (2016). Risk management and prevention methodologies: a comparison. *Sistemas & Telemática, 14*(36), 39-58. Obtenido de https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/view/2214

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), 1-15. Obtenido de https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*(1), 1-10. Obtenido de https://www.sciencedirect.com/science/article/pii/S0167404820302765

Alvarado, G., & Sánchez, M. (2021). *Information security in the process of system and product development through the implementation of security controls based on ISO 27002:2015 in the company BITNESS CORP S.A.C., 2020.* Lima: Universidad Peruana Unión. Obtenido de https://repositorio.upeu.edu.pe/handle/20.500.12840/4660

Anderson, R., Barton, C., B¨ohme, R., Clayton, R., Gañán, C., Grasso, T., . . . Vasek, M. (2019). *Measuring the Changing Cost of Cybercrime.* Cambridge: Cambridge University. Obtenido de https://www.repository.cam.ac.uk/handle/1810/294492

Angraini, A., Alias, R., & Okfalisa, C. (2019). Information Security Policy Compliance: Systematic Literature Review. *The Fifth Information Systems International Conference 2019* (págs. 1216-1224). Surabaya: Procedia Computer Science. Obtenido de https://www.sciencedirect.com/science/article/pii/S1877050919319465

Aquino, M., Huallpa, J., Huillcen, H., Carpio, E., & Plaomino, F. (2020). Implementation of an Information Security Management System Based on the ISO/IEC 27001: 2013 Standard for the Information Technology Division. *The International Conference on Advances in Emerging Trends and*

Technologies (págs. 264-272). Cham: Springer. Obtenido de https://link.springer.com/chapter/10.1007/978-3-030-63665-4_21

Arafat, M. (2018). Information security management system challenges within a cloud computing environment. *ICFNDS '18: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (págs. 1-6). Amán: Association for Computing Machinery. Obtenido de https://dl.acm.org/doi/abs/10.1145/3231053.3231127

Atencio, E. (2019). *Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú.* Cerro de Pasco: Universidad Nacional Daniel Alcides Carrión. Obtenido de http://repositorio.undac.edu.pe/handle/undac/1474

Barlette, Y., & Fomin, V. (2008). Exploring the suitability of IS security management standards for SMEs. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (págs. 308-308). Hawái: IEEE. Obtenido de https://ieeexplore.ieee.org/document/4439013

Bisell, K., LaSalle, R., & Cin, P. (6 de Marzo de 2019). *Ninth Annual Cost of Cybercrime Study*. Obtenido de Accenture: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Bravo, M., & Yoo, S. (2019). Developing an Information Security Management System for Libraries Based on an Improved Risk Analysis Methodology Compatible with ISO/IEC 27001. *The International Conference on Advances in Emerging Trends and Technologies* (págs. 371-379). Cham: Springer. Obtenido de https://link.springer.com/chapter/10.1007/978-3-030-32033-1_34

Brito, D. (2017). Definición del riesgo empresarial y principales tipos. *Universidad y Sociedad*(10(1), 269-277. doi:http://rus.ucf. edu.cu/index.php/rus

Calder, A. (2011). *Implementing Information Security based on ISO 27001/ISO 27002* (Primera ed.). Nueva York: Van Haren Publishing.

Carrasco, D. (2016). *Metodología de la investigación científica (2.a ed.).* San Marcos E.I.R.L. Obtenido de https://www.academia.edu/26909781/Metodologia_de_La_Investigacion_Cientifica_Carrasco_Diaz_1_

Carrillo, Á., Sánchez, M., & Villalobos, J. (2017). *Plan Nacional de Ciencia, Tecnología e Innovación para el desarrollo del sector de las Tecnologías de la Información y las Comunicaciones (TIC).* Bogotá: Ministerio de las TIC. Obtenido de https://minciencias.gov.co/sites/default/files/plan-ctei-tic-2017-2022_0.pdf

Carvajal, D., Cardona, A., & Valencia, F. (2019). A proposal for the management of the information security applied to a Colombian public entity. *Entre Ciencia e Ingeniería, 13*(25), 68-76. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S1909-83672019000100068

Cassetto, O. (30 de Julio de 2019). *Information Security (InfoSec): The Complete Guide*. Obtenido de Exabeam: https://www.exabeam.com/information-security/information-security/

Chopra, A., & Chaudhary, M. (2020). *Implementing an Information Security Management System* (Primera ed.). Nueva York: Apress.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117. Obtenido de https://dl.acm.org/doi/abs/10.1145/1290958.1290971

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2019). From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance. *ESORICS 2019 International Workshops* (págs. 238-257). Ciudad de Luxemburgo: Springer. Obtenido de https://link.springer.com/chapter/10.1007/978-3-030-42048-2_16

Disterer, G. (2017). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(2), 92-100. Obtenido de https://www.scirp.org/journal/paperinformation.aspx?paperid=30059

ENISA. (2022). *MAGERIT*. Obtenido de European Union Agency for Cybersecurity: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html

Erazo, M. (2011). Rigor científico en las prácticas de investigación cualitativa. *Ciencia, Docencia y Tecnología, 22*(42), 107-136. Obtenido de https://www.redalyc.org/articulo.oa?id=14518444004

ESAN. (06 de 11 de 2013). *Los riesgos que se pueden controlar.* Obtenido de https://www.esan.edu.pe/conexion-esan/riesgos-controlar

Espinoza, C. (2014). *Metodología de la investigación tecnológica: Pensando en sistemas* (Segunda ed.). Huancayo: Soluciones Gráficas S.A.C.

Fathurohman, A., & Witjaksono, R. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering, 1*(1), 1-11. Obtenido de http://bcsee.org/index.php/bcsee/article/view/analysis-and-design-of-information-security-management-system-ba

FBI. (17 de Marzo de 2021). *FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics*. Obtenido de FBI National Press Office: https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

Ferreira, A. (2020). *Implementação de um Sistema de Gestão de Segurança da Informação em Conformidade com a ISO/IEC 27001.* Coímbra: Universidade de Coimbra. Obtenido de https://estudogeral.sib.uc.pt/handle/10316/94643

Fonseca, O., Rojas, A., & Florez, H. (2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG International Journal of Computer Science, 48*(2), 213-222. Obtenido de http://www.iaeng.org/IJCS/issues_v48/issue_2/IJCS_48_2_01.pdf

Fuentes, R. (2020). *Information Security Management System based on the ISO/IEC 27003 Standard for the National University of Cajamarca.* Lambayeque: Universidad Nacional Pedro Ruiz Gallo. Obtenido de https://repositorio.unprg.edu.pe/handle/20.500.12893/9097

Gomm, R. (2008). *Social Research Methodology: A Critical Introduction* (Segunda ed.). Hampshire: Macmillan International Higher Education.

Gritzalis, D., Stergiopoulos, G., Vasilellis, E., & Anagnostopoulou, A. (2020). Readiness Exercises: Are Risk Assessment Methodologies Ready for the Cloud? En G. Tsihrintzis, & M. Virvou, *Advances in Core Computer Science-Based Technologies: Papers in Honor of Professor Nikolaos Alexandris* (Primera ed., págs. 109-128). Cham: Springer.

Huayamave, R. (2018). *Implementation of an information security management system (ISMS) applied to the assets of the construction company Coetecorpza SA, based on the ISO 27002 standard.* Guayaquil: Escuela Superior Politécnica del Litoral. Obtenido de https://www.dspace.espol.edu.ec/xmlui/handle/123456789/43622

Irwin, L. (22 de Julio de 2021). *ISO 27001 vs. ISO 27002: What's the difference?* Obtenido de IT Governance UK Blog: https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002

ISO. (2013). *ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements.* Ginebra: ISO/IEC International Standards Organization. Obtenido de https://www.iso.org/standard/54534.html

ISO. (2013). *ISO/IEC 27002:2013: Information technology - Security techniques - Code of practice for information security controls.* Ginebra: ISO/IEC International Standards Organization. Obtenido de https://www.iso.org/standard/54533.html

Jassim, N., Al-Zahir, B., & Khazraji, A. (2022). Diagnosing the current Information Systems Security Department in the Information Technology Department according to the international standard (ISO/IEC 27001:2013). *Journal of Management Information & Decision Sciences, 25*(2), 1-8. Obtenido de https://www.abacademies.org/articles/diagnosing-the-current-information-systems-security-department-in-the-information-technology-department-according-to-the-internati-13146.html

Kaplan, R., & Norton, D. (2009). *The Balanced Scorecard* (Tercera ed.). Barcelona: Ediciones Gestión 2000.

Kilian, D. (2007). Einführung in Informationsmanagementsysteme (II): BSI-Standards und Vergleich. *Datenschutz und Datensicherheit-DuD, 31*(1), 49-52. Obtenido de https://link.springer.com/article/10.1007/s11623-007-0015-2

Latorre, E., Castro, K., & Potes. (2018). *Las TIC, las TAC y las TEP: Innovación educativa en la era conceptual.* Bogotá: Universidad Sergio Arboleda. Obtenido de

https://repository.usergioarboleda.edu.co/bitstream/handle/11232/1219/TIC%20TAC%20TEP.pdf

Leiva, R. (2017). *Design of an Information Security Management System based on the ISO/IEC 27001 and ISO/IEC 27002 Standards to protect the information assets in the medicine supply process of the Lambayeque Health Network 2015.* Lambayeque: Universidad Nacional Pedro Ruiz Gallo. Obtenido de https://repositorio.unprg.edu.pe/handle/20.500.12893/1019

Macedo, F., & Da Silva, M. (2012). *Comparative study of information security risk assessment models.* Lisboa: Universidade Técnica de Lisboa. Obtenido de https://fenix.tecnico.ulisboa.pt/downloadFile/395139415147/

Martins, J. (26 de 10 de 2022). *Planificación estratégica para empresas.* Obtenido de https://asana.com/es/resources/strategic-planning

Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. *2020 International Conference on Information Technologies (InfoTech)* (págs. 1-5). Varna: IEEE. Obtenido de https://ieeexplore.ieee.org/document/9211066

Namakforoosh, M. (2000). *Metodología de la Investigación* (Segunda ed.). Ciudad de México: Limusa.

Ochoa, V. (23 de Noviembre de 2020). *Siete nuevos centros comerciales se preparan para operar en el 2021*. Obtenido de Diario Gestión: https://gestion.pe/economia/empresas/estos-son-los-siete-nuevos-centros-comerciales-se-preparan-para-operar-en-2021-noticia/

Ozdemir, Y., Basligil, H., Alcan, P., & Kandemirli, B. (2017). Evaluation and comparison of COBIT, ITIL and ISO27K1/2 standards within the framework of information security. *International Journal of Technical Research and Applications, 11*(1), 22-24. Obtenido de https://www.researchgate.net/publication/339435225

Peltier, T. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management* (Primera ed.). Boca Ratón: CRC Press.

PriceWaterhouseCoopers. (2021). *Organisations' cyber security strategies need to be rethought*. Obtenido de PwC: https://www.pwc.dk/da/publikationer/2021/cybercrime-survey-2020-en.html

Proença, D., & Borbinha, J. (2018). Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001. *International Conference on Business Information Systems* (págs. 102-114). Cham: Springer. Obtenido de https://link.springer.com/chapter/10.1007/978-3-319-93931-5_8

Qusef, A., Arafat, M., & Al-Taher, S. (2018). Organizational management role in information security management system. *ICFNDS '18: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (págs. 1-8). Amán: Association for Computing Machinery. Obtenido de https://dl.acm.org/doi/abs/10.1145/3231053.3231064

Raza, M. (26 de Noviembre de 2019). *Introduction to Information Security Management Systems (ISMS)*. Obtenido de BMC Blogs: https://www.bmc.com/blogs/introduction-to-information-security-management-systems-isms/

Richardson, R. (2008). *CSI computer crime and security survey.* Orlando: Computer Security Institute. Obtenido de https://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSIsurvey2008.pdf

Riek, M., Bohme, R., & Moore, T. (2017). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 261-273. Obtenido de https://ieeexplore.ieee.org/document/7056466

Risco, E. (2021). *Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021.* Lima: Universidad César Vallejo. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/63424

Rodríguez, J. (2010). *Administración de pequeñas y medianas empresas* (Sexta ed.). Ciudad de México: Cengage Learning.

Rodríguez, J., Rojas, A., & Mejía, C. (2018). Methodological model based on Gophish to face phishing vulnerabilities in SME. *2018 ICAI Workshops (ICAIW)* (págs. 1-6). Bogotá: IEEE. Obtenido de https://ieeexplore.ieee.org/document/8555006

Rodriguez, L., Cruzado, C., Mejía, C., & Alarcón, M. (2020). Application of ISO 27001 and its influence on the information security of a Peruvian private company. *Propósitos y Representaciones, 8*(3), 1-11. Obtenido de

http://www.scielo.org.pe/scielo.php?pid=S2307-79992020000400011&script=sci_arttext

Salah, J. (2017). *Modelo de Gobierno y Gestión de TI basado en la estrategia de Gestión del Riesgo para la Secretaría de Educación de Magdalena Caso de estudio: macroproceso Gestión de la Cobertura.*

Sandelowski, M. (2000). Combining Qualitative and Quantitative Sampling, Data Collection, and Analysis Techniques in Mixed-Method Studies. *Research in nursing & health, 23*(3), 246-255. Obtenido de https://onlinelibrary.wiley.com/doi/abs/10.1002/1098-240X(200006)23:3%3C246::AID-NUR9%3E3.0.CO;2-H

Seeba, M., Matulevičius, R., & Toom, I. (2021). Development of the Information Security Management System Standard for Public Sector Organisations in Estonia. *24th International Conference on Business Information Systems* (págs. 355-366). Hannover: TIB Open Publishing. Obtenido de https://www.tib-op.org/ojs/index.php/bis/article/view/43

Solano, G. (2020). *Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en la empresa Udersol en Costa Rica.* [Tesis de pregrado, Universidad Latina de Costa Rica]. Obtenido de https://repositorio.ulatina.ac.cr/handle/20.500.12411/293?locale=es

Susanto, H., & Almunawar, M. (2018). *Information Security Management Systems* (Primera ed.). Boca Raton: Apple Academic Press.

Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. *2009 International Conference on Availability, Reliability and Security* (págs. 726-731). Fukuoka: IEEE. Obtenido de https://ieeexplore.ieee.org/document/5066554

Szczepaniuk, E., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security, 90*(1), 1-11. Obtenido de Computers & Security: https://www.sciencedirect.com/science/article/pii/S0167404819302469

Tribunal Constitucional del Perú. (2020). *El Hábeas Data en la actualidad* (Primera ed.). Lima: Doctrina Constitucional.

Tsakalidis, G., & Vergidis, K. (2019). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49*(4), 710-729. Obtenido de https://ieeexplore.ieee.org/document/7936557

Tunggal, A. (17 de Octubre de 2021). *What is Information Security?* Obtenido de UpGuard: https://www.upguard.com/blog/information-security

Whitman, M., & Mattord, H. (2021). *Principles of Information Security* (Séptima ed.). Boston: Cengage Learning.

Yoseviano, H., & Retnowardhani, A. (2018). The use of ISO/IEC 27001:2009 to analyze the Risk and Security of Information System Assets: case study in XYZ, Ltd. *2018 International Conference on Information Management and Technology (ICIMTech)* (págs. 21-26). Yakarta: IEEE. Obtenido de https://ieeexplore.ieee.org/document/8528096

ANEXOS

Anexo 1

Resolución de aprobación del proyecto de investigación

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0957-2021/FIAU-USS

Pimentel, 15 de octubre de 2021

VISTOS:
El Acta de reunión N°2209-2021 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante Oficio N°0334-2021/FIAU-IS-USS de fecha 25 de septiembre de 2021, y;

CONSIDERANDO:

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

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

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

Que, según documentos de vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerda aprobar la modificación de los temas de Tesis a cargo de los egresados que se detallan en el anexo de la presente Resolución.

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

SE RESUELVE:

ARTÍCULO 1°: MODIFICAR, el tema de la Tesis perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de los egresados del Programa de estudios de **INGENIERÍA DE SISTEMAS** según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: MODIFICAR, la Resolución de Facultad con la que se asigna Asesor especialista y/o Jurado evaluador en el extremo del tema de la tesis quedando tal como se detalla en el anexo de la presente Resolución.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Mg. Victor Alexci Tuesta Monteza
Decano (e) / Facultad De Ingeniería, Arquitectura Y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

MBA. Maria Noelia Sialer Rivera
Secretaria Académica / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Cc: Interesado, Archivo

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0957-2021/FIAU-USS

Pimentel, 15 de octubre de 2021

ANEXO

N°	AUTOR(ES)	TEMA DE TESIS ACTUAL	TEMA DE TESIS ANTERIOR	RESOLUCIÓN PREVIA
1	LIZANA FERNANDEZ MICHAEL KENNETH	MODELO DE ELICITACIÓN DE REQUERIMIENTOS PARA MEJORAR LA CAPTURA DE REQUERIMIENTOS DE SOFTWARE EN UNA EMPRESA DE DESARROLLO DE SOFTWARE	APLICACIÓN DE MODELO DE INGENIERÍA DE REQUERIMIENTOS PARA MEJORAR LA CAPTURA DE REQUERIMIENTOS DE SOFTWARE EN EL HOSPITAL REGIONAL DE LAMBAYEQUE	0951-2017-FIAU/USS
2	MORON PEREDO KRISTOPHER RENZO	DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC	DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC – LIMA 2017	2017-II
3	FERNANDEZ RAMOS ROY GABRIEL	ANALISIS Y DISENO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA NTP – ISO/IEC 27001:2014 EN LA EMPRESA CONSULTORA N&V ASESORES SAC	UNA REVISIÓN DE LA LITERATURA ACERCA DE LOS TIPOS DE ATAQUES Y MÉTODOS DE DETECCIÓN DE PHISHING	1359-2020/FIAU-USS

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

Anexo 2

Carta de aceptación de la institución para la recolección de datos

Coolbox
Tecnología & Electrónica

Magdalena del Mar, 09 de abril del 2018

Sres.

UNIVERSIDAD SEÑOR DE SIPÁN

Presente.

Por medio de la presente nos es grato saludarlos y dirigirnos a ustedes con la finalidad de constatar que el Sr. MORON PEREDO KRISTOPHER RENZO, identificado con DNI 46642368 y Código Universitario 2130816021, en su condición de estudiante del X ciclo de la Escuela Académica Profesional de Ingeniería de Sistemas en la Universidad Señor de Sipán, utilice datos e informaciones para fines exclusivos de elaboración de su tesis denominada "DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC". La misma que viene desarrollando para obtención del Título Profesional de Ingeniero de Sistemas en dicha casa de estudios superiores.

Se extiende la presente constancia, a solicitud de la parte interesada para los fines que estime conveniente.

Atentamente,

Coolbox
RASH PERU S.A.C.
Aldo Mongilardi Fuchs
GERENCIA DE GESTION HUM...

RASH PERÚ S.A.C.
Av. Salaverry 3310 Lima 17 – Perú
(511) 264-2600 / Fax (511) 264-2558
www.coolbox.pe

Anexo 3

Instrumentos de recolección de datos - Ficha de Juicio de Expertos

VALIDACIÓN DE JUICIO DE EXPERTOS
INSTRUMENTO DE INVESTIGACIÓN

Título de la investigación:

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC

Autor:

Bach. Moron Peredo Kristopher Renzo

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú SAC.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: _____

1.2. Grado Académico y Profesión: _____

1.3. Áreas de Experiencia Profesional: _____

1.4. Institución donde labora: _____

1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC.**

II. VALIDACIÓN

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

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

ASPECTOS DE VALIDACIÓN

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

VALORACIÓN: _____

OPINIÓN DE APLICABILIDAD: _____

Lugar y fecha: Chiclayo, ____ abril del 2022.

Anexo 4

Instrumentos de recolección de datos – Cuestionario

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Encuesta

Introducciones: Lea cuidadosamente cada pegunta y conteste marcando con el número según criterio. El cuestionario es completamente anónimo, con el fin que sus respuestas sean lo más sinceras y honestas posible.

Criterios:

No Cumple = 0

Cumple Parcial = 1

Cumple = 2

Ítems	Cumple Criterio	Observaciones
1. ¿El nivel de seguridad de los equipos es óptimo para operar con el OFISMART?		
2. ¿Existe una política o procedimiento para la gestión de claves de cifrado?		
3. ¿Se dispone de un procedimiento para la gestión de cambio?		
4. ¿Existe una política de control de accesos debidamente documentada y se revisa constantemente?		
5. ¿Con la finalidad de reducir alteraciones y/o modificaciones sin autorización o hacer mal uso de la información o servicios, las funciones y las responsabilidades son separados o segregados?		

6. ¿Los controles aseguran que los usuarios sólo tienen acceso a los recursos de la red a los cuales han sido autorizados a utilizar según sus funciones?		
7. ¿Existe un procedimiento para garantizar que los accesos de los usuarios sean eliminados al finalizar el vínculo laboral, contractual o cambio de puesto de trabajo?		
8. ¿Todos los empleados y proveedores firman acuerdos de confidencialidad y no divulgación?		
9. ¿Existe procedimientos para la destrucción de la data contenida en equipos sensibles cuando estos sean dados de baja?		
10. ¿Existe una política sobre el uso de técnicas criptográficas para el tratamiento de la información transmitida en el OFISMART?		
11. ¿Los datos y/o documentos se encuentran protegidos contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales del negocio?		
12. ¿Se dispone de planes y equipamiento para la continuidad operativa del servicio del OFISMART?		
13. ¿Se realiza capacitación integral en temas de seguridad de la información a los empleados y usuarios del OFISMART?		
14. ¿Se elabora publicidad de concientización respecto a temas de seguridad de la información?		

Fuente. Elaboración propia.

Anexo 5

Consentimiento informado

DECLARACIÓN DE CONSENTIMIENTO INFORMADO

Fecha _____

Yo, _____, identificado (a) con DNI _____, por medio del presente documento doy consentimiento para mi participación en la investigación: "DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC", la cual dirige el docente de la Escuela Académica Profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán, Mg. Ing. Mejía Cabrera Heber Iván, por medio del alumno, Moron Peredo Kristopher Renzo, estudiante del X ciclo de la carrera profesional en mención de dicha casa de estudios.

Se me ha informado acerca de las características del estudio y he recibido garantía de que, los datos personales que se revelen al encargado de realizar la investigación, serán estrictamente confidenciales, además de que los procederes a evaluar no son perjudiciales a la integridad de mi persona.

_____

Firma del Usuario

Nombre: _____

DNI: _____

Cargo: _____

Anexo 6

Resultados individuales de Juicio de Expertos

Experto 01

VALIDACIÓN DE JUICIO DE EXPERTOS
INSTRUMENTO DE INVESTIGACIÓN

Título de la investigación:

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC

Autor:

Bach. Moron Peredo Kristopher Renzo

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú SAC.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: **RUIZ GÓMEZ WOOLDER**

1.2. Grado Académico y Profesión: **Ms. Ing. de Sistemas con mención en T.I.**

1.3. Áreas de Experiencia Profesional: **Seguridad Informática, Redes e Infraestrucutura de T.I.**

1.4. Institución donde labora: **DIGEMID - MINSA**

1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC.**

II. VALIDACIÓN

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

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

ASPECTOS DE VALIDACIÓN

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

VALORACIÓN: 950

OPINIÓN DE APLICABILIDAD: MUY BUENA PROPUESTA

Lugar y fecha: Lima, 25 de Abril del 2022.

Woolder Ruiz Gómez
DNI: 10647620

VALIDACIÓN DE JUICIO DE EXPERTOS
INSTRUMENTO DE INVESTIGACIÓN

Título de la investigación:

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC

Autor:

Bach. Moron Peredo Kristopher Renzo

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú SAC.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: HUERTA MICHILINE, CARLOS ANTONIO

1.2. Grado Académico y Profesión: MAESTRO EN DIRECCION DE SISTEMAS Y TECNOLOGIA DE LA INFORMACION / INGENIERO DE SISTEMAS

1.3. Áreas de Experiencia Profesional: SISTEMAS Y TECNOLOGIAS DE LA INFORMACION

1.4. Institución donde labora: ZINC INDUSTRIAS NACIONALES S.A.

1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC.**

II. VALIDACIÓN

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

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

ASPECTOS DE VALIDACIÓN

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

VALORACIÓN: 935

OPINIÓN DE APLICABILIDAD: MUY BUENA PROPUESTA

Lugar y fecha: Lima, 25 de abril del 2022.

Carlos Alberto Huerta Michiline

DNI: 10173116

VALIDACIÓN DE JUICIO DE EXPERTOS
INSTRUMENTO DE INVESTIGACIÓN

Título de la investigación:

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC

Autor:

Bach. Moron Peredo Kristopher Renzo

Objetivo:

El objetivo del presente instrumento es someter a evaluación el presente Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú SAC.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: QUENEMA MORON CARLOS ALFONSO

1.2. Grado Académico y Profesión: INGENIERO INFORMÁTICO

1.3. Áreas de Experiencia Profesional: GESTION DE PROYECTOS / JEFATURA DE DESARROLLO SOFTWARE

1.4. Institución donde labora: UNIVERISIDAD PRIVADA DEL NORTE

1.5. Nombre del instrumento motivo de evaluación: **VALIDACIÓN DE EXPERTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27002 PARA MEJORAR EL NIVEL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RASH PERÚ SAC.**

II. VALIDACIÓN

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

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

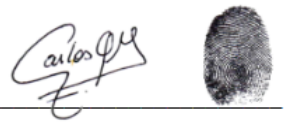
ASPECTOS DE VALIDACIÓN

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

VALORACIÓN: 950

OPINIÓN DE APLICABILIDAD: MUY BUENA PROPUESTA

Lugar y fecha: Lima, 25 Abril del 2022.



DNI - 25856663

Anexo 7

Declaración de Aplicabilidad

Sec.	Objetivo	Control	Justificación de exclusión	Aplicación SI/NO	Adopción a RASH PERÚ SAC
5	**Políticas de seguridad de la información**				
5:1	**Directrices establecidas por la dirección para la seguridad de la información**				
5.1.1	**Políticas para la seguridad de la información**	Existen políticas de seguridad de la información, que son publicadas y divulgadas por la alta gerencia a los colaboradores y partes externas		Si	Se elaboró e implementó el documento de Política y procedimientos para la gestión de la seguridad informática en Rash Perú SAC.
5.1.2	**Revisión de las políticas para seguridad de la información**	Se deben de tener procedimientos para la revisión periódica en intervalos planificados de las políticas de la seguridad de la información.		Si	Se elaboró e implementó el documento de Política y Procedimientos para la gestión de la seguridad informática en Rash Perú SAC, en el cual se determina el periodo de revisión de la política.
6	**Organización de la seguridad de la información**				
6:1	**Organización interna.**				
6.1.1	**Roles y responsabilidades para la seguridad de información**	Se deben definir y asignar responsabilidades de acuerdo a las políticas de seguridad de la información.		si	Se elaboró e implementó el documento de Política y Procedimientos para la gestión de la seguridad informática en Rash Perú SAC, en el cual se determinan los roles y responsabilidades respecto a la seguridad de la información. En los procedimientos
6.1.2	**Separación de deberes**	Se deben separar los deberes y las áreas de responsabilidad, de esta forma se evita el uso indebido de los activos de la organización.		si	Los procesos de RASH PERÚ SAC se han segregado.

6.1.3	**Contacto con las autoridades**	Se debe contemplar el mantener contacto permanente con autoridades reguladoras seguridad de la información.	La organización no tiene contacto con autoridades reguladoras de los procesos de negocio.	no	
6.1.4	**Contacto con grupos de interés especial**	Es importante que el encargado de la seguridad informática este en contacto permanente con grupos de interés, buscando la cooperación y coordinación relacionadas con la seguridad informática.	No representa un riesgo crítico para la empresa.	no	
6.1.5	**Seguridad de la información en la gestión de proyectos**	La seguridad de la información se debe tratar en cualquier proyecto.	No representa un riesgo crítico para la empresa.	no	
6:2	**Dispositivos móviles y teletrabajo.**				
6.2.1	**Política para dispositivosmóviles**	Se deben aplicar políticas para eluso adecuado de dispositivos móviles, su uso inadecuado representa grandes riesgos		si	Se diseñó e implemento una Política para dispositivos móviles (RPS-P18)
6.2.2	**Teletrabajo**	La Cía. no posee empleos bajo la modalidad de teletrabajo		si	Se diseñó e implemento una política para el Acceso remoto (RPS-P13)
7	**Seguridad de los recursos humanos**				
7:1	**Antes de asumir el empleo.**				
7.1.1	**Selección**	Se deben realizar una exhaustiva comprobación de los antecedentes del personal como empleados, contratistas, terceros con el fin de saber su procedencia, referencias personales, judiciales.		si	Se diseñó la política de seguridad de los RRHH.

7.1.2	**Términos y condiciones del empleo**	Se debe diseñar un documento que permita a los empleados, contratistas y terceros firmar cláusulas de confidencialidad con la organización, manejo adecuado de recursos tecnológicos	si	Se diseñó el documento Acuerdo de Confidencialidad el cual estipula que la información que corresponde a los procesos internos RASH PERÚ SAC y información de los clientes, son de carácter confidencial y la divulgación de estos conlleva castigos penales, así como la ruptura de la relación con RASH PERÚ SAC. **(RPS-P03)**
7:2	**Durante la ejecución del empleo.**			
7.2.1	**Responsabilidades de la dirección**	Se debe exigir a los empleados, contratistas y terceros el cumplimiento a cabalidad de las políticas de seguridad de la información implementada.	si	Se diseñó la política para el uso correcto de la información. **(RPS-P03)**
7.2.2	**Toma de conciencia, educación y formación en la seguridad de la información**	Se debe capacitar a todo el personal en aspectos relacionados con la seguridad de la información	si	El personal de RASH PERÚ SAC es sensibilizado respecto a temas de seguridad de la información. (Plan de concientización y capacitación).
7.2.3	**Proceso disciplinario**	Se deben establecer políticas sobre sanciones que se aplicarán a quienes incumplan con lo descrito en las políticas de seguridad	si	Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determinan las penalidades sobre el incumplimiento de la política.
7:3	**Terminación o cambio de empleo**			
7.3.1	**Terminación o cambio de responsabilidades de empleo**	Se debe informar a losempleados en los casos dondelas responsabilidades y deberesque les fueron asignados duranteel empleo, los cobijan auncuando se realice una terminación o cambio de contrato	si	Se diseñó un procedimiento de gestión de usuarios (P-RPS-01)

8	**Gestión de activos**			
8:1	**Responsabilidad por los activos**			
8.1.1	**Inventario de activos**	Se debe contar con un inventario detallado de los activos que posee la Cía.	si	Se identificó y clasificó los activos de los procesos relevantes de la Org. teniendo como resultado el Inventario de Activos informáticos
8.1.2	**Propiedad de los activos**	Además de la implementación del control anterior, se debe identificar en custodia de quien se encuentra actualmente	si	El inventario de activos diseñado tiene información actualizada del propietario (responsable) del activo.
8.1.3	**Uso aceptable de los activos**	Debe existir una cláusula donde los empleados se comprometan a realizar un uso aceptable de los activos de la organización	si	Se diseñó e implementó la política de Gestión de Activos en la que se establece el uso que los empleados le deben dar a los activos. (RPS-P01)
8.1.4	**Devolución de activos**	Se debe establecer un proceso para la devolución de los activos para cuando los empleados cambien de puesto o cuando se termine su contrato	si	se diseñó e implemento la política general de gestión de activos (RPS-P01)
8:2	**Clasificación de la información**			
8.2.1	**Clasificación de la información**	Se debe establecer un procedimiento que permita clasificar la información de acuerdo a su valor	no	
8.2.2	**Etiquetado de la información**	La información debe estar debidamente rotulada, además esta rotulación se debe clasificar de acuerdo con el valor que representa la información para la empresa	no	
8.2.3	**Manejo de activos**	Se debe contar con procedimientos que ayuden en el adecuado manejo que se le debe dar a un activo	no	
8:3	**Manejo de medios**			
8.3.1	**Gestión de mediosremovibles**	Se deben establecer políticassobre el correcto manejo que sele deben dar a los mediosremovibles, puesto que estos	si	Se diseñó e implementó la política específica de Gestión de Activos en la que se establece que los medios

		sonnecesarios en el desarrollo de laslabores diarias.dar a un activo		removibles deben ser inhabilitados en todas las computadoras de Rash Peru SAC
8.3.2	**Disposición de los medios**	Protección de la información cuando los medios sean destinados a labores diferentes a las actuales, se podría hablar de un procedimiento de eliminación de información en estos casos.	no	
8.3.3	**Transferencia de medios físicos**	Definir procedimientos que permitan que la información almacenada en estos no sea divulgada, modificada o eliminada.	no	
9	**Control de acceso**			
9:1	**Requisitos del negocio para control de acceso**			
9.1.1	**Política de control de acceso**	Establecer políticas que permitan el acceso a la información de acuerdo con privilegios establecidos según sus funciones	si	Se diseñó e implementó la Política Específica de Gestión de Accesos.
9.1.2	**Política sobre el uso de los servicios de red**	Definir el acceso a la red para el desarrollo de funciones que les fueron asignadas.		Se diseñó e implemento la política para el uso correcto de Internet
9:2	**Gestión de acceso de usuarios**			
9.2.1	**Registro y cancelación del registro de usuarios**	Todos los usuarios con acceso a sistema de información deben estar registrados, también se debe dar de baja a los que no formen parte de la organización o no hagan uso del sistema.	si	El personal que cesa de la empresa se le debe retirar los accesos a los sistemas de información en un periodo oportuno. **P-RPS-01**
9.2.2	**Suministro de acceso de usuarios**	Implementar un procedimiento que permita a los usuarios del sistema acceder al sistema o negar el acceso a este cuando se considere necesario.	si	Se diseñó e implemento la política de uso correcto de contraseñas. **RPS-P10**
9.2.3	**Gestión de derechos de acceso privilegiado**	Se deben establecer privilegios de acceso a la información de	si	Existe una revisión periódica de accesos otorgados en el sistema Ofismart, acewan y Cic

		acuerdo al desempeño de sus funciones.			
9.2.4	**Gestión de información de autenticación secreta de usuarios**	Esta información sólo debe ser accesada por personal con privilegios especiales		si	Sólo personal autorizado tiene acceso a la Gestión de Accesos en los sistemas de información.
9.2.5	**Revisión de los derechosde acceso de usuarios**	Monitoreo de privilegios asignados a usuarios con el fin de identificar si son adecuados para el desarrollo de sus funciones.		si	Se cubre con el procedimiento P-RPS-01 y la política RPS-P02
9.2.6	**Retiro o ajuste de los derechos de acceso**	Se debe dar de baja o modificar los privilegios de acceso a la información en caso de traslado del usuario o retiro de la organización.		si	Se cubre con el procedimiento P-RPS-01 y la política RPS-P02
9:3	**Responsabilidades de los usuarios**				
9.3.1	**Uso de la información de autenticación secreta**	Se deben crear perfiles para el acceso a información considerada de suma importancia para la empresa		si	Se cubre con el procedimiento P-RPS-01 y la política RPS-P02
9:4	**Control de acceso a sistemas y aplicaciones**				
9.4.1	**Restricción de acceso Información**	Restringir el acceso a la información por parte de personal no autorizado.		si	Los activos físicos críticos se encuentran en un ambiente restringido al público. **RPS-P08**
9.4.2	**Procedimiento de ingreso seguro**	Se deben establecer procedimientos que restrinjan el acceso a la información a personal no autorizado		si	Se cubre con la política de uso correcto de contraseñas. **RPS-P10**
9.4.3	**Sistema de gestión de contraseñas**	Se deben establece políticas de gestión de contraseñas como caducidad, bloqueo después de un número de intentos, y parámetros para creación de contraseñas seguras.		si	Se cubre con la política de uso correcto de contraseñas. **RPS-P10**
9.4.4	**Uso de programas utilitarios privilegiados**	Restringir el uso de programas utilitarios ya que pueden violentar la seguridad de las contraseñas.	No representa un riesgo crítico para la empresa.	no	

9.4.5	**Control de acceso a códigos fuente de programas**	Políticas de acceso al código fuente, sólo con acceso por el personal autorizado.	No aplica a la empresa.	no	
10	**Criptografía**				
10:1	**Controles criptográficos**				
10.1.1	**Política sobre el uso de controles criptográficos**	Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad de la información		si	por buscar
10.1.2	**Gestión de llaves**	Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad y no repudio de la información		si	Las tablas de información confidencial son encriptados a nivel de base de datos.
11	**Seguridad física y del entorno**				
11:1	**Áreas seguras**				
11.1.1	**Perímetro de seguridad física**	Se debe establecer un perímetro de tal forma que los sitios donde se encuentren los activos tengan accesos restringido		si	se cubre con la política para el acceso físico RPS-P04
11.1.2	**Controles físicos de entrada**	Se debe restringir el acceso a sitios seguros como centro de cableado, ubicación del servidor, espacios donde se encuentre información confidencial, estos sitios deben permanecer con llave.		si	En Rash Perú SAC las áreas restringidas están señalizadas. con acceso restringido a personal autorizado.
11.1.3	**Seguridad de oficinas, recintos e instalaciones**	Restringir el acceso a personal no autorizado, las áreas deben estar demarcadas dando aviso que son sitios restringidos		si	En Rash Perú SAC las áreas restringidas están señalizadas.
11.1.4	**Protección contra amenazas externas y ambientales**	Se debe contar con detectores de humo y humedad, ubicación de extinguidores en sitios estratégicos, cuartos técnicos con aire acondicionado, adquisición de pólizas contra robo y desastres naturales		si	En Rash Perú SAC se han implementado medidas de seguridad ante amenazas internas como extintores, alarmas, luminarias ante falta de electricidad, etc.

11.1.5	**Trabajo en áreas seguras**	Se deben preservar los sitios donde se encuentren activos valiosos con el fin de protegerlos contra daños intencionados		no	
11.1.6	**Áreas de despacho y carga**	Se deben designar sitios especiales para carga y despacho, lo recomendable es que estén aislados de los denominados sitios seguros o restringidos		no	
11:2	**Equipos**				
11.2.1	**Ubicación y protección de los equipos**	Los equipos deben estar ubicados en sitios seguros, de esta forma se protege contra robo, accesos no autorizados.		si	se cubre con la política RPS-P04
11.2.2	**Servicios de suministro**	Se debe contar con un adecuado suministro y respaldo de energía	Se cuentan con procedimientos de continuidad de negocio.	no	
11.2.3	**Seguridad del cableado**	Se debe proteger el cableado eléctrico y de datos de posibles daños como interceptaciones con el fin de causar daño.	No representa un riesgo crítico para la empresa.	no	
11.2.4	**Mantenimiento de equipos**	Se debe contar con mantenimiento preventivo y correctivo en períodos de tiempo establecidos, con el fin de evitardaños en HARDWARE., actualizaciónde SOFTWARE..			Se diseñó e implemento el procedimiento de mantenimiento preventivo(P-RPS-02) y el procedimiento de mantenimiento correctivo (P-RPS-03)
11.2.5	**Retiro de activos**	Se debe definir un procedimiento que autorice el retiro de activos de la empresa tales como equipos de cómputo, SOFTWARE..		si	Se diseñó e implemento una política para el retiro de activos
11.2.6	**Seguridad de equipos y activos fuera de las instalaciones**	Aplicar la misma seguridad que se realiza a los equipos dentro de la empresa		si	Se diseñó procedimiento para el cuidado de los activos fuera de la empresa
11.2.7	**Disposición segura o reutilización de equipos**	Se debe proteger la información confidencial de equipos en		si	Se diseñó e implemento la Política de equipo sin uso (RPS-P12)

		desuso o cuando son dados de baja.			
11.2.8	**Equipos de usuario desatendidos**	Establecer políticas para equipos cuando los usuarios no están presentes, evitando así el acceso no autorizado o robo de información.		si	Se diseñó e implemento la Política de equipo sin uso (RPS-P12)
11.2.9	**Política de escritorio limpio y pantalla limpia**	Definir procedimientos para que los escritorios estén libres de papeles, medios de almacenamiento que puedan permitir filtración de información, además políticas de pantallas limpias.		si	Los escritorios deben permanecer libre de documentos con información confidencial.
12	**Seguridad de las operaciones**				
12:1	**Procedimientos operacionales y responsabilidades**				
12.1.1	**Procedimientos de operación documentados**	Los procedimientos deben estar documentados y puestos al alcance de todos, también manuales de operaciones específicas			Las políticas y documentación propia de la empresa en lo que respecta a procesos de negocio se encuentran en una carpeta compartida al cual toda la organización tiene acceso.
12.1.2	**Gestión de cambios**	Establecer políticas donde los cambios sean realizados por personal autorizado, además deben quedar soportados para llevar un control para evitar contratiempos.	No representa un riesgo crítico para la empresa.	no	
12.1.3	**Gestión de capacidad**	Se debe realizar un monitoreo de los recursos de tal forma que no afecten la operación, algunos pueden ser capacidad de banda ancha, circuitos des calibrados que afecten el fluido eléctrico, equipos lentos.	No representa un riesgo crítico para la empresa.	no	

12.1.4	**Separación de losambientes de desarrollo,pruebas y operación**	Los ambientes de desarrolloprueba y operación deben estaraislados, con restricciones deacceso con el fin de evitarcambios o modificaciones noautorizadas.	no aplica para la empresa	no	
12:2	**Protección contra códigos maliciosos**				
12.2.1	**Controles contra códigos maliciosos**	Los equipos de cómputo deben contar con SOFTWARE. contra código malicioso, el cual se debe actualizar constantemente con el fin actualizar parches que mitiguen las nuevas vulnerabilidades.		si	Se diseñó e implemento la política de protección contra SOFTWARE. malicioso.
12:3	**Copias de respaldo**				
12.3.1	**Respaldo de información**	Se debe realizar respaldo de la información, además se deben realizar pruebas para comprobar que estos cumplen con las políticas de respaldo		si	Se diseñó e implemento la política de copias de respaldo. **RPS-P05**
12:4	**Registro y seguimiento**				
12.4.1	**Registro de eventos**	Se debe llevar un control de los eventos con el fin de establecer procedimientos que ayuden a repararlos o eliminarlos definitivamente, con el fin de que no se vuelvan a presentar	No representa un riesgo crítico para la empresa.	no	
12.4.2	**Protección de la información de registro**	Se debe proteger la información de registro de personal no autorizado, sólo el administrador o encargado será quien pueda tener acceso a estos, se deben realizar copias de logs.	No representa un riesgo crítico para la empresa.	no	

12.4.3	**Registros del administrador y del operador**	Todas las tareas que desarrollen el administrador y el operador del sistema de información deben estar registradas, además se debe realizar un respaldo de estos registros.		si	RPS-P05 - Política de copias de respaldo
12.4.4	**sincronización de relojes**	Los relojes de los dispositivos que intervienen en el procesamiento de información deben estar sincronizados.	No representa un riesgo crítico para la empresa.	no	
12:5	**Control de SOFTWARE. operacional**				
12.5.1	**Instalación de SOFTWARE. en sistemas operativos**	La instalación de SOFTWARE. debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas.		si	RPS-P09 - Política de uso de SOFTWARE. y procedimiento P-RPS-05
12:6	**Gestión de la vulnerabilidad técnica**				
12.6.1	**Gestión de lasvulnerabilidades técnicas**	Se deben establecer procedimientos que minimicen las vulnerabilidades a que están expuestos los activos tecnológicos.		si	Se utilizan los procedimientos preventivos y correctivos
12.6.2	**Restricciones sobre la instalación de SOFTWARE.**	La instalación de SOFTWARE. debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas.		si	RPS-P09 - Política de uso de SOFTWARE.
12:7	**Consideraciones sobre auditorias de sistemas de información**				
12.7.1	**Información controles de auditoría de sistemas**	Se deben establecer procedimientos que permitan el buen uso de las herramientas de auditoría a los sistemas, pero siempre procurando minimizar la interrupción del servicio a causa de estas.	No representa un riesgo crítico para la empresa.	no	
13	**Seguridad de las comunicaciones**				
13:1	**Gestión de la seguridad de las redes**				

13.1.1	**Controles de redes**	Se deben instalar dispositivos o SOFTWARE. que permita controlar el acceso a la red como Firewall, Id, autenticación para su ingreso.		si	procedimiento P-RPS-07
13.1.2	**Seguridad de los servicios de red**	Establecer controles de acceso, acuerdos de servicio en su utilización, monitoreo constante para detectar intrusos		si	procedimiento P-RPS-07
13.1.3	**Separación en las redes**	Es necesario loa separación de las redes como la intranet de la red con acceso a internet, para lo cual se debe implementar un DMZ	No representa un riesgo crítico para la empresa.	no	
13:2	**Transferencia de información**				
13.2.1	**Políticas y procedimientos de transferencia de información**	Se deben establecer todas las políticas que sean necesarias para proteger la información en el momento de ser transferida (intercambio de información), permitiendo integridad y confidencialidad.	No aplica a la empresa.	no	
13.2.2	**Acuerdos sobre transferencia de información**	Se deben establecer controles que permitan respetar acuerdos de intercambio o transferencia de información	No aplica a la empresa.	no	
13.2.3	**Mensajería electrónica**	Deben existir controles sobre el uso adecuado de la mensajería electrónica, para ello se deben instalar programas que detecten antivirus y spam, además se debe capacitar sobre correos sospechosos, también políticas del uso adecuado de los recursos, en este caso uso del correo electrónico sólo para el desarrollo de las funciones asignadas.		si	RPS-P07 - Política para el uso del correo empresarial

13.2.4	**Acuerdos de confidencialidad o de no divulgación**	Se deben cumplir las políticas de confidencialidad de la información, las cuáles fueron aceptadas en el momento de la firma del contrato.	si	RPS-P03 - Política para el uso correcto de la Información
14	**Adquisición, desarrollo y mantenimientos de sistemas**			
14:1	**Requisitos de seguridad de los sistemas de información**			
14.1.1	**Análisis y especificación de requisitos de seguridad de la información**	Las especificaciones de requisitos se deben tener en cuenta cuando se vaya a realizar un cambio, implementar un nuevo S. información.	no	
14.1.2	**Seguridad de servicios de las aplicaciones en redes publicas**	Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información	no	
14.1.3	**Protección de transacciones de los servicios de las aplicaciones**	Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información	no	
14:2	**Seguridad en los procesos de desarrollo y soporte**			
14.2.1	**Política de desarrollo seguro**	Es importante establecer políticas de código seguro en el desarrollo de SOFTWARE., es aquí donde se deben implementar procedimientos de seguridad como paso de variables por cabecera, sesiones, entre otros, los cuáles deben blindar el sistema de información para evitar vulnerabilidades	no	

14.2.2	**Procedimientos de controlde cambios en sistemas**	Todos los cambios que se realicen a los programas se deben documentar y quedar registrados, se deben establecer procedimientos	si	RPS-P09 - Política de uso de SOFTWARE.
14.2.3	**Revisión técnica de las aplicaciones después de cambios en la plataforma de operación**	Se deben realizar pruebas a las aplicaciones que han sido modificadas, con el fin de evitar alteraciones en la prestación del servicio o mal funcionamiento a causa del desarrollo.	si	RPS-P09 - Política de uso de SOFTWARE.
14.2.4	**Restricciones en los cambios a los paquetes de SOFTWARE.**	Los cambios o modificaciones que se le realizan a las aplicaciones deben estar restringidos con el fin de evitar fallas no deseadas.	no	
14.2.5	**Principios de construcción de sistemas seguros**	Establecer procedimientos y políticas que permitan la construcción de aplicaciones seguras	no	
14.2.6	**Ambiente de desarrollo seguro**	Los ambientes de desarrollo deben estar aislados y contar con las medidas de seguridad en control de acceso a la información e instalaciones	no	
14.2.7	**Desarrollo contratado externamente**	Cuando se adquieran sistemas externos, realizar seguimiento, es necesario validarlos antes de ponerlos en funcionamiento	no	
14.2.8	**Pruebas de seguridad de sistemas**	Someter los sistemas a pruebas para identificar vulnerabilidades, se podrían hacer pruebas de hacking ético.	no	
14.2.9	**Prueba de aceptación de sistemas**	Someter los sistemas a pruebas para identificar vulnerabilidades, se podrían hacer pruebas de hacking ético.	no	
14:3	**Datos de prueba**			
14.3.1	**Protección de datos de prueba**	Hay que tener cuidado con los datos que se van a ingresar para realizarle pruebas a la aplicación, esto	no	

		con el fin de evitar alguna fuga de información importante.		
15	**Relación con los proveedores**			
15:1	**Seguridad de la información en las relaciones con los proveedores**			
15.1.1	**Política de seguridad de lainformación para lasrelaciones conproveedores**	Igual que con los usuarios de la organización, proveedores se deben establecer acuerdos de confidencialidad, control de acceso a la información, seguridad física, intercambio deinformación entre otros para nover afectada la seguridad de lainformación.	No representa un riesgocrítico para la empresa.	no
15.1.2	**Tratamiento de la seguridad dentro de los acuerdos con proveedores**	Definir acuerdos de confidencialidad	No representa un riesgo crítico para la empresa.	no
15.1.3	**Cadena de suministro de tecnología de información y comunicación**	Se deben establecer acuerdos que permitan mitigar los riesgos de la seguridad de la información derivados de la cadena de suministro.	No representa un riesgo crítico para la empresa.	no
15:2	**Gestión de la prestación de servicios con los proveedores**			
15.2.1	**Seguimiento y revisión de los servicios de los proveedores**	Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.		no
15.2.2	**Gestión de cambios en los servicios de proveedores**	Se debe contar con otras alternativas de proveedores que permitan la continuidad del servicio en caso de cambio de proveedor		no
16	**Gestión de incidentes de seguridad de la información**			
16:1	**Gestión de incidentes y mejoras en la seguridad de la información**			

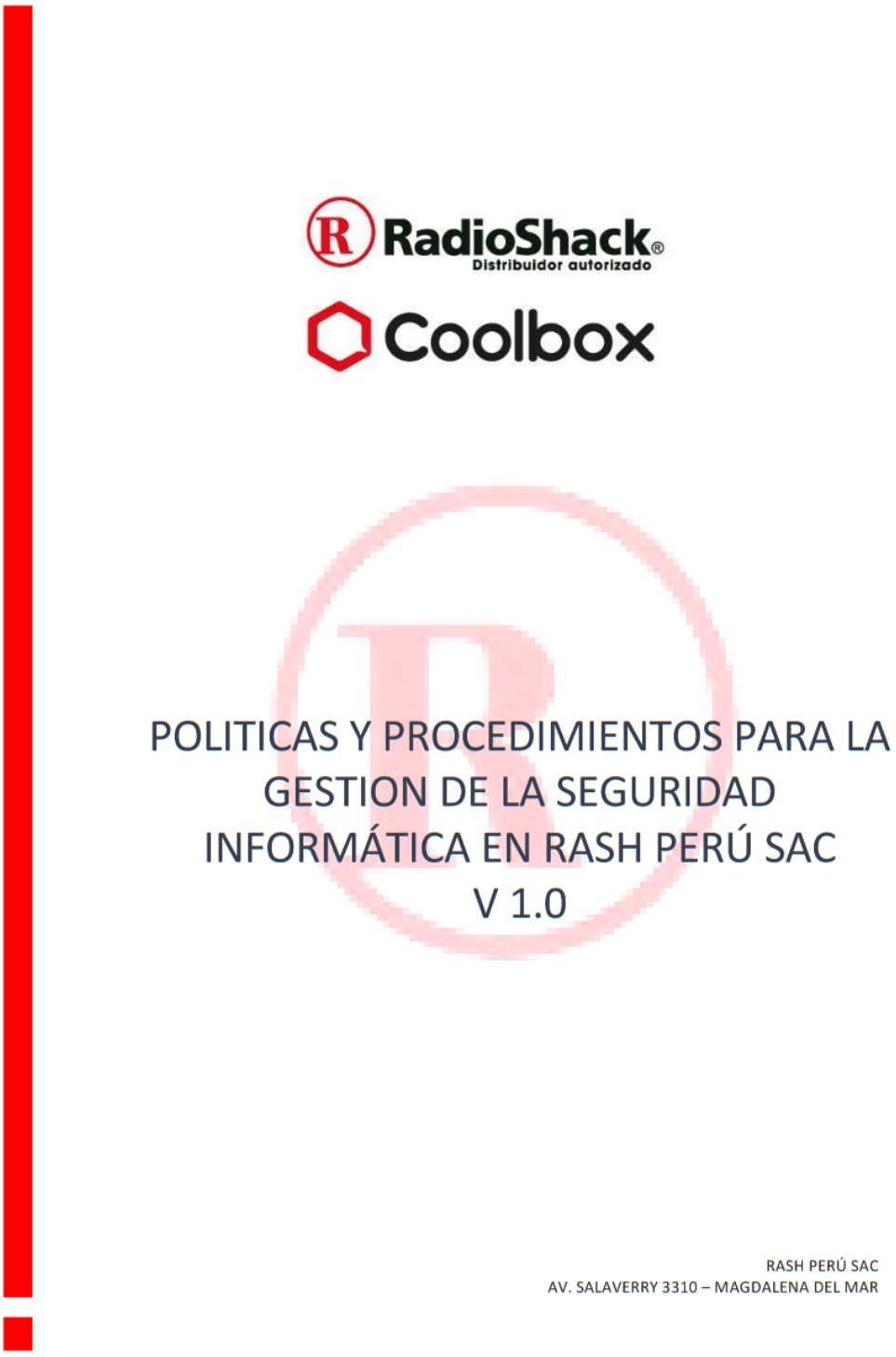
16.1.1	**Responsabilidad y procedimientos**	Definir procedimientos que permitan una reacción rápida ante problemas generados por causa de la seguridad de la información.		si	Se diseñó e implementó el documento de Política de Gestión de Incidentes en él se especifica el plan de respuesta ante los incidentes de seguridad de la información. **RPS-P14**
16.1.2	**Reporte de eventos de seguridad de la información**	Se debe informar sobre eventos generados a causa de seguridad de la información con el fin de documentar la solución, es necesario llevar un registro de estos.		si	Los incidentes de seguridad de la información será registrados en el documento lógico "Incidentes de Seguridad de la Información" lo que permitirá trazabilidad.
16.1.3	**Reporte de debilidades de seguridad de la información**	Informar oportunamente sobre eventos generados, con el fin de identificar recurrencias y debilidades.		si	se diseñó la política RPS-P14
16.1.4	**Evaluación de eventos de seguridad de la información y decisiones sobre ellos**	Cada vez que se presente unevento se seguridad de lainformación es importante evaluarsi será considerado como unincidente o no.	Todos los eventos seránconsiderados incidentes,por lo que no se harádistinción.	no	
16.1.5	**Respuesta a incidentes de seguridad de la información**	Se debe establecer un proceso que permita facilitar la atención del incidente.		si	Se diseñó procedimiento para la gestión de incidentes P-RPS-04
16.1.6	**Aprendizaje obtenido de los incidentes de seguridad de la información**	La experiencia que se ha adquirido en resolver los incidentes, es pieza fundamental para reducir el impacto que pueda causar este incidente a la seguridad.		si	Se diseñó procedimiento para la gestión de incidentes P-RPS-04
16.1.7	**Recolección de evidencia**	Definir un procedimiento para documentar los incidentes de tal forma que exista una evidencia.		si	Se creo un documento en drive, en la cual se registraran los incidentes que se den en la organización.
17	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**				
17:1	**Continuidad de seguridad de la información**				

17.1.1	**Planificación de la continuidad de la seguridad de la información**	Definir políticas que permita la gestión de la continuidad del negocio, aunque la organización presente una crisis	si	
17.1.2	**Implementación de la continuidad de la seguridad de la información**	Implementar procedimientos que permitan la continuidad del negocio ante situaciones imprevistas que podrían causar retrasos en la operación.	si	Se diseñó e implementó el documento de Política de Gestión de Incidentes, la cual cuenta con procedimiento que permite la continuidad del negocio ante eventos que limiten el funcionamiento.
17.1.3	**Verificación, revisión y evaluación de la continuidad de la seguridad de la información**	Realizar revisiones a los procedimientos implementados para la gestión de la continuidad del servicio para determinar si son efectivos.		
17:2	**Redundancias**			
17.2.1	**Disponibilidad de instalaciones de procesamiento de información.**	Es necesario establecer redundancias en las instalaciones donde se procesa la información con el fin de que no se vea afectada la disponibilidad de la información.	si	En respuesta al riesgo se diseñó implementó el documento de Política de Gestión de Copias de Respaldo
18	**Cumplimiento**			
18:1	**Cumplimiento de requisitos legales y contractuales**			
18.1.1	**Identificación de la legislación aplicable y de los requisitos contractuales**	Definir el marco legal con el cual se debe regir la seguridad de la información.		
18.1.2	**Derechos de propiedad intelectual**	Cumplir a cabalidad las políticas de derechos de propiedad intelectual, SOFTWARE. patentado.	no	
18.1.3	**Protección de registros**	Procedimiento que permita la custodia de los registros en situaciones de robo, modificación o divulgación.	si	Se han determinado controles preventivos que aseguran la seguridad de los registros.

18.1.4	**Privacidad y protección de datos personales**	Cumplir con las políticas de la protección de datos personales	si	Se han determinado controles preventivos que aseguran la seguridad de los registros.
18.1.5	**Reglamentación de controles criptográficos**	Cumplir con las normas relacionadas con controles criptográficos	si	Se diseñará una política de controles criptográficos en la v2.0 del documento de políticas.
18:2	**Revisiones de seguridad de la información**			
18.2.1	**Revisión independiente de la seguridad de la información**	Se debe revisar periódicamente el SGSI, estas revisiones deben ser adicionales a las establecidas en las políticas de seguridad de la información.	no	
18.2.2	**Cumplimiento con las políticas y normas de seguridad**	La dirección debe revisar los cumplimientos de las políticas de seguridad de la información establecidas de acuerdo con su área de responsabilidad.	no	
18.2.3	**Revisión del cumplimiento técnico**	Se deben revisar que todo el personal conoce y cumple con las políticas de seguridad de la información	si	Se debe realizar revisiones anuales al sistema de gestión de seguridad de la información.

Anexo 8

Políticas y procedimientos de gestión de la seguridad informática



RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
Política general de la seguridad de la información	

La Política de Seguridad Informática es el compromiso de la alta dirección y de los colaboradores de la compañía RASH PERÚ SAC con respecto a la protección de los activos informáticos que soportan los procesos de la compañía y declaran su apoyo a la implementación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27002.

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

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

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

RASH PERÚ SAC procura dar cumplimiento a normatividades y leyes creadas para proteger la información y los activos informáticos.

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P01 - Política general de gestión de activos	

El área de TI debe disponer de un inventario de los activos informáticos de RASH PERÚ SAC y mantenerlo actualizado.

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

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

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

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

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

Una vez finalizado el contrato de trabajo, el empleado deberá hacer entrega de los implementos informáticos al área de TI, para que este genere un formato donde quede constancia de la entrega de estos y se haga revisión de su estado,

a su vez, el área de TI validando lo anterior, procederá a firmar el formato de devolución de activos.

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

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

Los equipos informáticos asignados son para el uso exclusivo de las labores y para almacenamiento de información dentro de RASH PERÚ SAC.

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

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

RadioShack Distribuidor autorizado / Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P02 - Política de seguridad de los recursos humanos	

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

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

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

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

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

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

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P03 - Política para el uso correcto de la Información	

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

Todo desarrollo realizado por los colaboradores de RASH PERÚ SAC será propiedad intelectual de la empresa.

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

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

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
	RPS-P04 - Política para el Acceso físico

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

RASH PERÚ SAC deberá disponer de cámaras de vigilancia para monitorear eventos de seguridad.

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

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

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

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P05 - Política de copias de respaldo	

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

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

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

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

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

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

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

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

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

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

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P06 - Política para el uso correcto del internet	

El acceso a internet es un recurso para contribuir a actividades laborales como accesos a portales de proveedores, portales bancarios, portales gubernamentales entre otros según las necesidades del cargo y funciones desempeñadas.

El acceso a redes sociales no es permitido a excepción de la persona encargada del manejo comercial y promocional de la empresa.

Los empleados autorizados para el uso de Internet, no podrán descargar, copiar, instalar software que necesiten de licenciamiento y que puedan generar sanciones a la empresa por derechos de autor.

El área de TI, definirá niveles de acceso a internet aplicado a los usuarios, bloqueando accesos a sitios web que sean categorizados como inapropiados a través del Fortigate y en caso de que se requiera algún permiso especial debe ser autorizado por la Gerencia de su área en la que labora.

Los usuarios son responsables de las actividades que se realicen desde sus equipos hacia internet, por eso la importancia de cuidar sus sesiones.

Cada usuario es responsable de cualquier evento no deseado que se provoque al intentar acceder a algún sitio no autorizado.

Los empleados autorizados para el uso de Internet deben reportar al área de Sistemas, cualquier anomalía que pueda afectar la seguridad de los activos informáticos de la compañía.

El área de TI debe programar la descarga de las actualizaciones del sistema operativo en horas que no afecte las actividades del negocio.

Para ingreso a portales bancarios digitar la URL y verificar que sea establezca conexión segura a través de HTTPS y usando el token proporcionado por la entidad bancaria.

Los usuarios por seguridad no deben guardar credenciales cuando se los pregunte el navegador utilizado al ingresar a algún sitio.

Solicitar reporte mensual al proveedor de servicios móviles, el consumo de datos de los equipos de los colaboradores con el fin de monitorear el uso.

RadioShack / Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P07 - Política para el uso del correo empresarial	

El correo empresarial deberá ser creado por el área de TI para los empleados autorizados por la Gerencia de las El áreas en las que labora.

Todos los mensajes tanto enviados o recibidos por medio de correo electrónico empresarial pertenecen a RASH PERÚ SAC y está podrá acceder a ellos cuando lo requiera.

El correo empresarial solo será utilizado con propósitos laborales.

Es responsabilidad del empleado evitar que su cuenta de correo electrónico sea utilizada por terceros.

El área de TI debe supervisar que todos los correos empresariales creados deben configurársele la firma digital del empleado que hará uso.

No se permite el envío de spam a clientes con fines comerciales

Será sancionado el uso del correo empresarial para cometer acciones ilícitas.

El empleado es responsable de cualquier archivo adjunto que envíe a terceros a través del correo empresarial.

El empleado debe ser precavido con la descarga de archivos adjuntos que reciba de terceros a través del correo empresarial.

Es responsabilidad del empleado archivar los mensajes de correos electrónicos para efectos de soportar ante terceros en caso de requerirse.

El área de TI definirá el tamaño del buzón de acuerdo a las actividades que desempeñará el empleado y a la capacidad del Hosting contratado.

Ningún usuario tiene información de la cuenta de correo electrónico empresarial, ya que esta se entrega configurada en el Outlook del equipo asignado.

El área de TI debe tener un inventario sobre las cuentas de correos creados y sus respectivas contraseñas.

El área de TI debe utilizar contraseñas seguras basadas en la política de gestión de contraseñas.

El área de TI será la encargada de crear y administrar las cuentas de correo de Gmail para la configuración de las cuentas de Google Play Store de los smartphones.

Los usuarios no podrán configurar cuentas de correos personales en los celulares asignados por la empresa.

El área de TI podrá desactivar las cuentas de correo que no demuestren su uso durante más de dos (2) meses consecutivos.

El área de RRHH deberá informar al área de TI sobre los usuarios que saldrán a vacaciones o licencias de trabajo, para desactivar temporalmente las cuentas y configurar un mensaje de respuesta automática, con el fin de evitar que los buzones de mensajes se llenen y bloqueen las demás cuentas.

Las cuentas de correo serán desactivadas después de 7 días hábiles a partir de la fecha en la cual la persona termine su vinculación con la empresa.

El área de TI deberá crear medidas de control en el Fortigate y en el servidor de correos para filtrar correos maliciosos con contenidos perjudiciales.

RadioShack / Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P08 - Política de seguridad en el Data center	

RASH PERÚ SAC debe disponer de un área restringida para la ubicación de los activos informáticos críticos que soportan la infraestructura tecnológica del sistema de información.

Este centro de datos debe tener un sistema de refrigeración por aire acondicionado que mantenga la temperatura adecuada, las tomas eléctricas deben estar debidamente organizadas e instaladas.

El área de TI debe garantizar que todos los activos informáticos ubicados dentro del centro de datos estén protegidos con UPS, el cual permita un tiempo considerable mientras se restablece la energía o se realice un apagado correcto.

Dentro del centro de datos se prohíbe comer o beber.

En el centro de datos no debe almacenarse papelería, materiales inflamables o combustibles que generen riesgo de propagación de fuego.

Las puertas del centro de datos deben permanecer cerradas. La Gerencia de TI será la responsable de las llaves del sitio.

Cuando se realicen mantenimientos dentro del centro de datos por parte de terceros, deberán ser supervisadas por el área de TI.

Debe controlarse y vigilarse el acceso al centro de datos, ya que contiene los activos informáticos críticos.

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P09 - Política de uso de software	

No está permitido la descarga ni instalación de software sin autorización previa del área de TI, con el fin de evitar piratería y sanciones de tipo legal para RASH PERÚ SAC

El área de TI deberá mantener inventariada las licencias con sus respectivos soportes de compra y medios de instalación

El área de TI deberá velar por la vigencia de las licencias del software adquiridos.

Es responsabilidad del área de TI, instalar el software necesario para cada equipo de cómputo del empleado de RASH PERÚ SAC.

En caso de fallas del software y se solicita mantenimiento correctivo en el cual se repare o se actualice deberá quedar registrado en la hoja de vida del equipo de cómputo donde se presentó.

El área de TI deberá supervisar los mantenimientos correctivos, en caso de formateo de un equipo, suministrar al técnico los medios de instalación, licencias y exigir no realizar ningún tipo de instalación de software pirata o instalaciones sin autorización previa.

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P10 - Política de uso correcto de contraseñas	

Es responsabilidad de cada empleado hacer buen uso de las cuentas de usuario asignadas sea para acceso al equipo, acceso remoto o sistemas informáticos de la empresa, evitando compartir el uso de las cuentas, ni dejando en evidencia los datos de acceso que puedan ser usados por otra persona.

El área de TI inicialmente asignará la contraseña al empleado, pero deberá configurarse de tal manera que solicite ser inmediatamente cambiada en el primer inicio de sesión, cumpliendo con algunos parámetros de seguridad:

- Tener mínimo ocho caracteres.
- La contraseña debe estar compuesta por caracteres: mayúsculas, minúsculas, alfanuméricos y algún carácter especial.
- La contraseña no debe ser igual o parecida a la anterior.

El área de TI debe definir una política para que le exija al empleado el cambio de contraseña cada 30 días, el sistema debe informarle al empleado al inicio de sesión cumplido los días pactados.

El área de TI no restablecerá la contraseña a un usuario, a menos que este mismo lo solicite y se identifique a sí mismo.

Se deberán cambiar las contraseñas en caso de que exista o haya algún indicio de una posible vulnerabilidad del sistema.

Si al superar cinco intentos consecutivos al acceder a una cuenta de usuario de equipo o al sistema sin éxito, la cuenta se bloqueará por motivos de seguridad en la cual tendrá que intervenir El área de TI.

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P11 - Política de protección contra software malicioso	

Es responsabilidad del área de TI gestionar el licenciamiento del antivirus que brinde protección contra software malicioso.

El área de TI debe instalar en cada equipo de cómputo y servidores el software antivirus.

Es responsabilidad El área de TI monitorear desde la consola del antivirus las actividades anormales que se presentan para mitigar los riesgos.

Los empleados deben reportar fallas si el antivirus informa alguna falla o detección de virus.

Los empleados deberán analizar previamente con el antivirus el medio de almacenamiento como USB antes de abrir los archivos contenidos para evitar riesgos de seguridad a RASH PERÚ SAC.

No está permitido el uso de medios de almacenamiento virtual que no estén previamente autorizados por el área de TI.

Cualquier sospecha de anomalías en el equipo asignado a causa de infección de virus, deberá ser informado inmediatamente al área de TI para la revisión y solución de la amenaza.

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P12 - Política de equipo sin uso	

El área de TI debe garantizar que todos los equipos de cómputo estén configurados de tal forma que cuando detecte el sistema periodos de inactividad del empleado, después del tiempo establecido se bloquee la sesión del usuario y requiera de datos de accesos para iniciar sesión.

Es responsabilidad del empleado al realizar pausas activas o alejarse del puesto de trabajo, bloquear la sesión para evitar suplantación de identidad, sabotajes o robo de información.

Los usuarios no deben utilizar el sistema de una sesión que no sea la asignada.

El usuario deberá asumir parte de las responsabilidades en su sesión de usuario en caso de algún incidente ya sea por préstamo de credenciales o por no bloquear su sesión.

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P13 - Política de Acceso remoto	

El servicio de acceso remoto solo será habilitado a usuarios con fines laborales.

El servicio de acceso remoto debe permitir solo acceso al sistema de información de la empresa y a archivos compartidos en la intranet.

El área de TI debe definir un canal seguro para la conexión de usuarios externos a través de la configuración y asignación de datos de acceso a los empleados mediante la VPN de la empresa.

El área de TI deberá configurar políticas en el servidor donde se conectan los usuarios remotos para que después de determinado tiempo de inactividad o detección de usuarios desconectados, las sesiones se cierren completamente evitando el consumo de recursos por procesos activos en el servidor sin utilizarse.

El área de TI deberá gestionar licencias de usuarios remotos necesarios para el acceso al servidor de Terminal.

Está prohibido utilizar herramientas de soporte remoto como Anydesk, Team viewer, Zoom, etc. Solo se podrán utilizar con autorización y supervisión de el área de TI.

El área de TI debe garantizar la disponibilidad del servicio de internet a los usuarios remotos para que accedan al sistema.

RadioShack Distribuidor autorizado Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P14 - Política de gestión de incidentes	

RASH PERÚ SAC, debe establecer procedimientos para la gestión y tratamiento de incidentes de seguridad de los activos informáticos, con el fin de detección temprana y prevención de incidentes, crear una bitácora de incidentes con su respectiva solución para ir documentando los planes de acción ante determinada incidencia y auditar la respuesta de incidentes para una mejora continua.

Los empleados están obligados a reportar a el área de TI situaciones sospechosas o anómalas que puedan considerarse como incidencias de seguridad informática. A su vez el área de TI deberá analizar y valorar la incidencia reportada y comunicarla a la Gerencia de TI. En última instancia el Gerente evaluará la incidencia y tomará acciones sancionando al implicado o recurrir ante las autoridades competentes.

Toda la información referente a los incidentes reportados, debe ser manejada con discreción y confidencialidad.

RadioShack / Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
	RPS-P15 - Política de Escritorio Limpio

RASH PERÚ SAC ha implementado esta Política de Escritorio Limpio para aumentar la seguridad física en las instalaciones.

Esta política garantiza que la información confidencial y los materiales sensibles se guarden fuera de la vista cuando no se utilicen o cuando el espacio de trabajo esté desocupado.

Esta política establece los requisitos básicos para mantener un espacio de trabajo limpio, donde la información sensible y confidencial sobre los empleados, clientes, proveedores y propiedad intelectual de RASH PERÚ SAC esté protegida.

La política se aplicará a todos los empleados, contratistas y afiliados de RASH PERÚ SAC.

Los empleados deben asegurar toda la información sensible/confidencial en su espacio de trabajo al final de la jornada laboral y cuando se espera que estén fuera de su espacio de trabajo por un período de tiempo prolongado. Esto incluye tanto la información electrónica como la impresa.

Los puestos de trabajo informáticos/portátiles deben bloquearse (cerrar la sesión o apagarse) cuando estén desatendidos y al final de la jornada laboral. Los dispositivos portátiles, que permanezcan en la oficina durante la noche deben apagarse y guardarse.

Los dispositivos de almacenamiento masivo como, unidades USB o discos duros externos deben tratarse como material sensible y guardarse bajo llave cuando no se utilicen.

Los materiales impresos deben retirarse inmediatamente de las impresoras. La impresión de copias físicas debe reservarse para momentos de absoluta necesidad.

Los documentos deben verse, compartirse y gestionarse electrónicamente siempre que sea posible.

Todos los documentos delicados y la información restringida deben depositarse en los contenedores designados para su destrucción.

Las contraseñas no deben anotarse ni guardarse en ningún lugar de la oficina.

Es responsabilidad de cada Gerencia la de designar un encargado que vigile y verifique que se genere el cumplimiento de las políticas mencionadas.

RadioShack / Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P16 - Política de destrucción de Datos	

El área de TI es responsable de gestionar todas las actividades de conservación y destrucción de datos de la empresa. Otros departamentos, como el de Finanzas y Contabilidad, Operaciones y Recursos Humanos, también son responsables de proporcionar al departamento de TI sus requisitos de conservación y destrucción de datos.

El área de TI es responsable de desarrollar, ejecutar y probar periódicamente los procedimientos de conservación y destrucción de datos cumpliendo con los estándares industriales apropiados para la retención y destrucción de datos.

RASH PERÚ SAC desarrollará planes integrales de retención y destrucción de datos de acuerdo con las buenas prácticas de gestión de datos definidas por las normas establecidas.

Los planes de conservación y destrucción de datos deberán abordar los datos electrónicos almacenados en soportes electrónicos como CD, unidades de disco duro, unidades de disco de estado sólido, cintas magnéticas y otros soportes adecuados.

También deberán abordar los datos almacenados en soportes no electrónicos (por ejemplo, archivos en papel, microfichas).

Los planes de conservación y destrucción de datos se referirán a los sistemas de información electrónicos (por ejemplo, servidores, enrutadores, conmutadores) y a sus componentes (por ejemplo, cableado y conectores, fuentes de alimentación, bastidores de almacenamiento) y a otros activos que estén actualmente fuera de producción o que esté previsto que se retiren gradualmente de los entornos de producción.

Los planes de destrucción de datos establecerán los parámetros para la destrucción de los datos electrónicos (por ejemplo, sobreescritura, reformateo, desmagnetización, borrado basado en el firmware, destrucción física de los soportes de datos), de los datos no electrónicos (por ejemplo, destrucción de copias impresas) y de los sistemas y componentes (por ejemplo, servicios de destrucción de terceros).

Los planes de retención y destrucción de datos se revisarán y probarán periódicamente en un entorno adecuado para garantizar que los datos, las bases de datos, los soportes, los sistemas y otros elementos relevantes puedan ser retenidos o destruidos y que la dirección y los empleados de <nombre de la empresa> comprendan cómo deben ejecutarse los planes, así como sus funciones y responsabilidades.

Todos los colaboradores de RASH PERÚ SAC deben conocer el programa de retención y destrucción de datos y sus propias funciones y responsabilidades.

Los planes de retención y destrucción de datos y otros documentos se mantendrán actualizados y reflejarán las circunstancias existentes y cambiantes.

RadioShack / Coolbox	Versión 1.0
	Autor: Kristopher Renzo Moron Peredo
	Fecha: 02/05/2022
RPS-P17 - Política de capacitación y concientización	

RASH PERÚ SAC entiende que las personas son a menudo la mayor amenaza (intencionada o inadvertida) para la seguridad de la información sensible. Por ello, todos los usuarios de los sistemas de información deben ser conscientes de los riesgos de seguridad asociados a sus actividades.

Aquellas personas con responsabilidades significativas en materia de seguridad deben recibir la formación adecuada para llevar a cabo las tareas y responsabilidades relacionadas con la seguridad de la información que se les asignen.

Esta política se aplica a todos los empleados de RASH PERÚ SAC y a sus sistemas.

Todos los empleados y cualquier persona que acceda a los sistemas de informáticos deben entender cómo proteger la triada de la información.

El área de TI se asegurará de que todos los empleados reciban formación sobre seguridad y privacidad durante el proceso de contratación y antes de acceder a cualquier sistema de RASH PERÚ SAC.

Esta formación refleja la concienciación común sobre seguridad y privacidad específica del entorno de la compañía, incluyendo, pero sin limitarse a ello, el acceso físico, las áreas restringidas, los incidentes potenciales, cómo informar de los incidentes, las mejores prácticas con ordenadores portátiles y cómo detectar una estafa de phishing.

Además de la formación inicial en materia de seguridad que se imparte en la orientación para nuevas contrataciones, todos los empleados deben realizar un

curso de concienciación en materia de seguridad y privacidad y aprobar la prueba posterior en un plazo de 30 días tras la contratación y o renovación.

Rash Perú Sac proporcionará formación continua a través de las actividades del Equipo de Concienciación y Formación, las capacitaciones se darán mensualmente sobre temas seleccionados, también se proporcionará información a través de carteles en áreas designadas en toda la instalación y artículos semanales publicados en la página de intranet interna.

Rash Perú Sac también llevará a cabo una formación de actualización anual para todos los empleados y siempre que haya cambios significativos en el entorno.

Esta política se revisará anualmente o cada vez que se produzcan cambios significativos en el entorno.

PROCEDIMIENTOS

RASH PERÚ SAC describe los siguientes procedimientos con el fin de apoyar los procesos que ayudan a mejorar y proteger los activos informáticos.

P-RPS-01 - Gestión de usuarios.

La creación, modificación y eliminación de usuarios requiere atención óptima y oportuna para que todo colaborador inicie sus actividades sin ningún inconveniente hasta el cese de su vínculo laboral, es en esta fase en la que se debe de bloquear las cuentas asociadas al usuario, impidiendo de esta manera delitos informáticos como fuga o robo de información.

Objetivo. Establecer los lineamientos para gestionar usuarios.

Alcance. El procedimiento de gestión de usuario, indica los pasos a seguir

Para la óptima gestión de cuentas y accesos de los empleados de RASH PERÚ SAC para el uso de sus sistemas de informáticos.

Responsabilidades:

a. Coordinador de TI.
   - Vigilar el cumplimiento del procedimiento.
   - Asignar cuentas de usuarios para los diferentes accesos según rol.
   - Mantener registro de inventario de cuentas creadas e historial de cambios de usuarios.

b. Líder de calidad.
   - Solicitar e informar al área de TI la vinculación y desvinculación de empleados que tengan designados equipos de cómputo y acceso al sistema.

c. Usuario.
   - Cumplir con los acuerdos de confidencialidad.
   - No compartir credenciales de cuentas de usuarios asignadas.

Descripción.

I. La líder de calidad informa al área de TI sobre dar de alta o baja al usuario a través de un correo electrónico. La solicitud debe indicar datos básicos del empleado como número de documento de identificación, nombre completo, cargo y el área en la que desempeña funciones.

II. Si corresponde a solicitud de creación de nuevo usuario, se debe contar adicionalmente con datos como teléfono, dirección, correo electrónico, así como rol que desempeñará para definir el perfil de la cuenta de usuario. Los datos deben enviarse completos para procesar la solicitud.

III. Seguidamente se dan permisos de acceso a la red, se asigna usuario y licencia para el uso del OFISMART, ACEWAN, CIC, también se asigna un correo empresarial y si es usuario remoto se crea una VPN con la que podrá conectarse.

IV. Se envía un correo electrónico de respuesta al líder de calidad informando de las cuentas y perfiles creados. Se envía a la cuenta de correo electrónico proporcionada los datos de acceso a los sistemas. Adicional a ello, Se adjunta copia del manual de políticas de seguridad de la empresa.

V. Si la solicitud corresponde a un usuario que será dado de baja, se debe de informar la fecha en la que la cuenta ya no tendrá más acceso a los sistemas de la empresa.

VI. Se envía correo electrónico al líder de calidad indicando que se procedió a realizar la baja del usuario.

P-RPS-02 - Mantenimiento Preventivo.

Los activos informáticos correspondientes a hardware y software requirieren de un mantenimiento trimestral, con el fin de alargar la vida útil de los equipos y evitar fallos de los equipos, logrando prevenir las incidencias antes de que estas ocurran.

Objetivo. Crear un cronograma anual de mantenimiento preventivo de los activos informáticos de la empresa que soportan los datos y aplicarlo, con el fin de protegerlos y mantenerlos en condiciones aptas para garantizar el buen funcionamiento y rendimiento del sistema de información.

Alcance. Este procedimiento es aplicable para cubrir el servicio de mantenimiento preventivo de los activos informáticos y de redes que sean de propiedad de la empresa y correspondan a la sede Principal de RASH PERÚ SAC.

Responsabilidades

a. Coordinador de TI.

- Verificar el cumplimiento del procedimiento.
- Supervisar la ejecución de los mantenimientos preventivos en las fechas estipuladas y bajo las condiciones en las que se contrató el servicio con el proveedor.
- Revisar y firmar los reportes de mantenimiento
- Verificar registros de las actividades y observaciones realizados en la hoja de vida de cada activo informático.

b. Soporte TI.

- Cumplir con el soporte programado.
- Utilizar los implementos de protección necesarios para realizar las actividades de mantenimiento.
- Informar de cualquier novedad que evidencie en los activos informáticos a el Coordinador TI

- Registrar y documentar las actividades realizadas en las hojas de vida de los activos e informes de soporte.

Descripción.

I. El área de TI deberá acordar junto con el proveedor contratado de los mantenimientos, la programación anual de los mantenimientos preventivos. El contrato deberá incluir, frecuencia de mantenimientos, sedes las cuales se le harán mantenimiento, cantidad de equipos por sedes, recomendaciones de utilización de implementos de protección necesarios para la realización de las actividades, entregar mensualmente copias del pago de seguridad social y demás parafiscales del técnico encargado y si la actividad a realizar lo requiere deberá certificar curso de altura.

II. Elaborar y publicar programa general de mantenimientos preventivos, para que los usuarios estén atentos a la fecha correspondiente a su equipo.

III. Informa a los usuarios y a los proveedores sobre la realización de actividades programadas de mantenimiento preventivo.

IV. En el momento de realización de los mantenimientos preventivos por parte del proveedor, darle las indicaciones y recomendaciones necesarias sobre las actividades a realizar como:

- Limpieza física de los equipos, si hay algún equipo en garantía no destapar.
- Limpieza de software: borrado de temporales, análisis del antivirus, revisión de instalación de software no autorizado.
- Revisión lógica: ejecución de Scandisk, desfragmentación del disco.
- Actualizaciones pendientes de software.
- Revisión de batería de UPS
- Registrar en cada orden de mantenimientos, la fecha, número de equipo, serial del equipo, actividades realizadas dentro en cada equipo, novedades, fallas encontradas.

V. El área de TI deberá supervisar la jornada de mantenimientos, para verificar el trabajo realizado en cada equipo, dando su aprobación en cada orden de mantenimiento.

VI. En caso de que el técnico encuentre una falla y sea necesario reemplazar algún componente, como por ejemplo la batería de la UPS, deberá registrarlo e informarle a El área de TI.

VII. El área de TI hará las cotizaciones pertinentes referentes a la parte afectada y si es de cambio urgente, presentará las necesidades a la Gerencia de TI para que apruebe la asignación de presupuesto.

P-RPS-03 - Mantenimiento Correctivo.

El mantenimiento correctivo se origina inesperadamente a causa de una falla o avería en un activo informático por tal motivo no se puede considerar como una actividad planificable, en caso de falla en hardware puede representar costos por cambio o reparación del componente.

Objetivo. Realizar mantenimiento correctivo de los activos informáticos de la empresa, que soportan los datos con el fin reparar daños y reestablecer el buen funcionamiento del mismo.

Alcance. Este procedimiento es aplicable para cubrir el servicio de mantenimiento correctivo de los activos informáticos y de redes que sean de propiedad de la empresa y correspondan a la sede Principal de RASH PERÚ SAC.

Responsabilidades

a. Coordinador TI.

- Vigilar el cumplimiento del procedimiento.
- Supervisar las actividades realizadas por el técnico que brinda el soporte, enviado por el proveedor contratado.
- Analizar la valoración del activo dada por el técnico para tomar decisiones.
- Gestionar la compra de la pieza o activo averiado con el Gerente.
- Verificar que el activo que presenta fallas quede funcional.
- Asegurarse de que el registro de las actividades realizadas haya quedado detallado en la hoja de vida del activo informático afectado.

b. Soporte TI

- Atender el soporte de acuerdo a los niveles de atención contratadas.

- Utilizar los implementos de protección necesarios para realizar las actividades de mantenimiento.
- Informar de cualquier novedad que evidencie en los activos informáticos a la Coordinador TI para cambio de partes.
- Registrar y documentar las actividades realizadas en la hoja de soporte.

c. Usuario.

- Informar el mal funcionamiento del activo informático.
- Describir las acciones que estaba realizando en el momento de presentar la falla.
- Realizar pruebas sobre el activo para confirmar solución de falla.

Descripción.

I. El área de TI deberá descartar fallas de primer nivel, con el fin de resolver. Si es algo crítico, solicitar el servicio de mantenimiento correctivo al proveedor. Llamando a la línea de soporte, para que se agende el servicio según la prioridad que se le asigne.

II. Registrar en la orden de mantenimientos, la fecha, número de equipo, serial del equipo, actividades realizadas dentro en cada equipo, novedades, fallas encontradas.

III. En caso de que el técnico encuentre una falla y sea necesario reemplazar algún componente, como por ejemplo la batería de la UPS, deberá registrarlo e informarle al área de TI.

IV. El área de TI hará las cotizaciones pertinentes referentes a la parte afectada y si es de cambio urgente, presentará las necesidades a la Gerencia de TI para que apruebe la asignación de presupuesto.

V. El área de TI deberá supervisar la jornada de mantenimientos, para verificar el trabajo realizado en cada equipo, dando su aprobación en la orden de mantenimiento.

VI. Evaluar el servicio prestado para garantizar la calidad de este.

P-RPS-04 – Procedimiento de Gestión de Incidentes.

La gestión de incidentes consiste en resolver de manera rápida y eficaz, cualquier evento causante de interrupción parcial o total de las actividades realizadas por un activo informático, comprometiendo la confidencialidad, integridad, disponibilidad, autenticidad o confiabilidad de la información.

Objetivo.

Definir responsables que atiendan los incidentes y garanticen la operatividad del negocio, la continuidad y la disponibilidad del servicio.

Establecer el seguimiento que se debe aplicar a los incidentes de seguridad de la información para ser analizados y clasificados.

Aplicar salvaguardas adecuadas a los incidentes en la empresa y operaciones de negocio con el fin de mitigar el impacto causado.

Llevar bitácora de incidencias ocurridas, las cuales incrementa las oportunidades de prevenir las ocurrencias de futuros incidentes.

Alcance. Este procedimiento contempla desde la detección y reporte de Incidentes por parte del usuario, hasta el seguimiento que le dé el responsable de la gestión de incidentes: recepción, análisis de Incidentes, rastreo de ataque, custodia de evidencia, recuperación de datos o sistemas afectados, restauración de la información y registro en bitácora para manejo de incidentes futuros.

Responsabilidades

a. Coordinador TI.
- Vigilar el cumplimiento del procedimiento.
- Bloquear conexiones de red del equipo afectado para evitar replicas.
- Resolver la incidencia y solicitar apoyo al proveedor si es necesario.
- Documentar las incidencias para prevenir futuras amenazas.

b. Usuario.
- Informar incidente inmediatamente a El área de TI.
- Describir las acciones que estaba realizando en el momento de presentar la falla.

- Seguir indicaciones y recomendaciones dadas por la coordinara de sistemas.

Descripción.

I. En el momento en que se detecte comportamientos extraños en el funcionamiento de un equipo o servicio prestado en RASH PERÚ SAC, el usuario tiene la obligación de informar inmediatamente al coordinador de TI, el cual validará el incidente e informará al Gerente de TI si el impacto es alto.

II. A continuación, se detallarán indicaciones de cómo debe proceder el coordinador de TI ante un incidente:

- Desconectar el equipo afectado para aislarlo de la red.
- El usuario responsable del equipo afectado debe brindar información y el apoyo que requiera el área de TI para realizar el levantamiento de información.
- El área de TI determinará el origen y destino de la incidencia.
- Analizar el impacto causado en el equipo o sistemas involucrados.
- Etiquetar y poner en custodia la evidencia
- Identificar y aplicar el tratamiento o solución al incidente
- Documentar el Incidente en una bitácora, teniendo en cuenta aspectos como:
  - Fecha
  - Equipo afectado
  - Responsable del equipo
  - Resumen del incidente
  - Acciones realizadas.
  - Evidencias recopiladas
  - Observaciones.
  - Recomendaciones
  - Tratamiento de la incidencia.

III. Si el incidente tiene probabilidad de replicarse en otros equipos, el coordinador de TI implementará las mismas medidas preventivas en los demás equipos.

IV. El área de TI tiene el deber de reportarle al gerente los incidentes presentados si es de alto impacto en el mismo instante o si es de medio o bajo luego de solucionarlo.

V. El área de TI deberá dar recomendaciones a los usuarios si es necesario realizar capacitación sobre las medidas preventivas.

VI. Los usuarios responsables de los equipos involucrados deben acatar las medidas correctivas indicadas por la coordinadora.

VII. Una vez concluido el proceso de descartes de incidentes o restauración del equipo, El área de TI restablecerá las conexiones de red al equipo.

P-RPS-05 - Actualización de Sistemas Operativos y Software.

Los fabricantes de software constantemente están liberando nuevas versiones, parches de actualizaciones aplicadas a sistemas operativos, aplicaciones, controladores de hardware, antivirus para corregir fallas de seguridad, mejoras o corrección de errores para mitigar vulnerabilidades.

Objetivo.

Definir los lineamientos para llevar a cabo procesos de actualización y

cambios en los sistemas operativos y software.

Alcance.

El procedimiento contempla indicaciones para efectuar actualizaciones y cambios en los sistemas operativos y software autorizados por la Gerencia de TI y el coordinador TI.

Responsabilidades

a. Coordinador TI.

- Controlar el cumplimiento del procedimiento.
- Mantenerse informada de actualizaciones y mejoras de sistemas operativos y software.
- Tener un ambiente de pruebas para las actualizaciones.

- Programar horarios de actualizaciones para no afectar la operatividad de actividades.
- Informar y solicitar autorización a Gerencia de TI para programación de actualizaciones críticas.
- Realizar pruebas de migraciones en ambiente de pruebas antes de pasar a producción.
- Documentar cambios de sistemas operativos y software para control y seguimiento.
- Solicitar generación de licencias en caso de necesitarse.

b. Proveedor de software.

- Proveer repositorios para descarga de instaladores de actualizaciones.
- Proveer información sobre mejoras y versiones.
- Proveer licencias.
- Ofrecer acompañamiento y canales de soporte

c. Gerente de TI.

- Dar apoyo y autorización a El área de TI para la realización de actualizaciones.
- Coordinar la seguridad de las instalaciones para trabajar en actualizaciones en días no laborables.

Descripción.

Sistemas Operativos de Servidores

I. Se deberá abrir una ventana de mantenimiento para programar la actualización del sistema operativo de los servidores. Debido a que para este proceso se requiere el reinicio del servidor, debe programarse en horario que no afecte la actividad laboral.

II. Algunas actualizaciones pueden generar incompatibilidades con las aplicaciones, por lo tanto, es necesario revisar e investigar sobre los parches liberados por los fabricantes antes de cualquier cambio.

Sistemas Operativos de PC

I. Para no afectar el ancho de banda de internet, es necesario configurar en los equipos que el horario para realizar las actualizaciones del sistema

operativo se haga en un horario determinado que no afecte las actividades laborales del empleado y evitar que estas no se descarguen en todos los equipos simultáneamente. Por tal motivo no se deben dejar automáticas sino programarse.

Software de los servidores.

I. Para actualizaciones de firmware o sistema de algún hardware como el Fortigate, es necesario tener respaldo de la configuración del equipo y programar una ventana de mantenimiento ya que este equipo soporta toda la administración de la red de RASH PERÚ SAC, así que debe ejecutarse en horas fuera de la jornada normal.

II. En cuanto a Actualizaciones de la consola del Antivirus, es necesario recurrir al uso de la consola para que primero se descargue en el servidor donde se administra la consola y luego se programe su distribución a los demás equipos de cómputo en un horario establecido que no afecte el rendimiento de la red, aunque esto no genera interrupción de las actividades se evidencia lentitud en los equipos, por lo que se recomienda hacerlo en horarios laborales no muy concurridos por clientes.

P-RPS-06 - Operaciones del Centro de Datos.

Es necesario disponer de un sitio seguro y con condiciones adecuadas para establecer un Centro de Datos, en el cual se ubiquen y protejan los activos informáticos más críticos que soportan la infraestructura tecnológica para el funcionamiento del sistema de información y las comunicaciones de RASH PERÚ SAC. Este centro de datos debe estar acondicionado para que la operatividad de la empresa no se interrumpa.

Objetivo.

Establecer las normas para crear y mantener el centro de datos de la empresa que contenga los activos informáticos críticos de RASH PERÚ SAC

Alcance.

El procedimiento contempla las acciones a implementar para el buen funcionamiento del centro de datos de la empresa en la Sede principal.

Responsabilidades

a. Coordinador TI.
- Verificar el cumplimiento del procedimiento.
- Controlar el Centro de Datos de la empresa
- Supervisar el acceso al centro de datos.
- Asegurar que los activos ubicados en el centro de datos operen correctamente
- Hacer un chequeo semanalmente de las condiciones del centro de datos para corregir, mejorar y aplicar cambios necesarios.
- Programar y supervisar mantenimientos preventivos de los equipos.

b. Gerencia de TI.
- Brindar recursos financieros para mantener las condiciones óptimas del centro de datos de RASH PERÚ SAC.

Descripción.

I. El procedimiento describe medidas que se deben aplicar para el centro de datos que debe crear RASH PERÚ SAC.

II. Suministro eléctrico y Sistema de alimentación ininterrumpida

III. Dentro del centro de datos se resguardan los activos informáticos más importantes que soportan la infraestructura tecnológica del sistema de información y comunicaciones de RASH PERÚ SAC, en caso de fallo del suministro eléctrico, el sistema de alimentación ininterrumpida (UPS) entra a jugar un papel importante para mantener la disponibilidad de los activos como servidores, equipos de redes y comunicaciones.

IV. Las UPS deben cubrir todos los activos informáticos ubicados en el centro de datos previniendo el riesgo ante un corto o fluctuaciones de energía, no solo la caída de la conexión con los servidores generando pérdida de información y de trabajo sino viéndose afectado los componentes lógicos y físicos de los activos.

V. Se debe realizar una estimación de la duración del tiempo de descarga de las baterías de la UPS para proveer el tiempo con el que se dispone para guardar documentos abiertos y realizar un apago correcto de los equipos para protegerlos de daños, en caso donde el corte de energía eléctrica sobrepasa el tiempo de disponibilidad de la UPS.

Sistema de Aire acondicionado

I. Mantener una temperatura adecuada es fundamental dentro del centro de datos, ya que las temperaturas generadas por los equipos y por las condiciones climáticas de la ciudad de Cúcuta resultan bastantes altas y pueden ocasionar problemas a los activos informáticos que se encuentren resguardados en el centro de datos.

II. Si se presentan fallas en el sistema de aire acondicionado, la coordinadora de sistemas deberá aplicar medidas para mejorar las condiciones de temperatura y controlar el nivel de temperatura, solicitar soporte urgente con el proveedor de mantenimiento de aires acondicionados y si es necesario considerar apagar los equipos mientras se da una solución inmediata.

Canal de Internet, red MPLS y Central telefónica.

I. Al presentar caídas del servicio de internet, MPLS o telefonía, afecta las actividades de RASH PERÚ SAC, denegando la conexión con las demás sedes en especial con las tiendas donde las transacciones de venta migran en tiempo real, esto genera una desfase en la migración de la información creando duplicidad de documentos en algunos casos; el bloqueo de accesos a los portales de proveedores para realizar pedidos de mercancía; cese en el envío de cotizaciones y documentos a través de internet, las cuales están siendo solicitadas con urgencia por clientes, Por lo tanto, se deberán tomar medidas preventivas como otro canal de internet para contingencia y configuradas las IP públicas del servidor como plan opcional cuando la red MPLS no esté disponible; tener disponibles varias líneas celulares para solventar el problema de telefonía fija.

II. Los equipos propiedad de terceros correspondientes a los servicios subcontratados no deberán ser manipulados internamente, a menos que lo solicite el proveedor. En caso de fallos se deberá reporta a las líneas de atención para soporte, garantizando el cumplimiento de los niveles de atención contratados.

III. Se deberá supervisar y dar información necesaria a los proveedores de los servicios subcontratados con el fin de dar una rápida solución a alguna falla.

Equipos de redes y comunicaciones

I. Los equipos propiedad de terceros correspondientes a los servicios subcontratados no deberán ser manipulados internamente, a menos que el proveedor lo exija para apoyar en caso de soporte remoto o indique las instrucciones telefónicamente.

II. Se deberá realizar copias de respaldos del Fortigate, con el objeto de respaldar las políticas creadas y las demás configuraciones ante una falla del dispositivo. En caso de avería de este activo debe disponerse de un plan de contingencia debido a que este equipo soporte toda la administración de la red LAN, WAN y WIFI.

P-RPS-07 - Seguridad de Redes.

Los usuarios de RASH PERÚ SAC., para acceder al sistema de información o archivos compartidos, utiliza varios servicios ofrecidos por la administración de la red. Por tal motivo, es necesario establecer medidas que aseguren la integridad, confidencialidad y disponibilidad de la información.

Objetivo.

Definir lineamientos para controlar la seguridad de las redes y proteger la transmisión de la información al utilizar los servicios de red.

Alcance.

El procedimiento establece medidas para RASH PERÚ SAC.

Responsabilidades

a. Coordinador TI.
- Supervisar el cumplimiento del procedimiento.
- Administrar las redes de RASH PERÚ SAC.
- Brindar soporte a usuarios con respecto al acceso a redes de la empresa.
- Asegurar el cumplimiento de los servicios subcontratados de Internet, telefonía y Red MPLS.
- Monitorear las redes de comunicaciones.

b. Usuarios.
- Proteger las claves de acceso y sesiones a las redes que esté autorizado de RASH PERÚ SAC.

Descripción

Administración de la red y de equipos de conectividad

I. El tipo de encriptación aplicada para la contraseña de red WIFI debe ser de WPA2-PSK (AES).
II. Los equipos de red y comunicaciones no deberán tener claves por defecto de fábrica, están deberán asignársele una clave segura.
III. Solo El área de TI podrá tener acceso y a la administración de los equipos de red que sean propiedad de RASH PERÚ SAC.
IV. Deberán contemplarse en los mantenimientos preventivos.

Administración de la red privada virtual

I. El área de TI deberá crear un canal seguro, utilizando una red privada virtual (VPN) para accesos remotos al sistema de información de RASH PERÚ SAC.
II. Se debe establecer horarios y duración de la conexión remota a los servidores para uso del sistema de información.

Administración de acceso inalámbrico (WIFI)

I. La administración del WIFI es responsabilidad del área de TI y solo el tendrá la clave de acceso para acceder a la red inalámbrica de RASH PERÚ SAC.
II. Proveedores, clientes o visitantes a la empresa, tendrán acceso a la red WIFI, solo en casos donde el coordinador de TI haya dado previa autorización y se conectarán a una red aislada para visitantes.
III. El área de TI deberá cambiar la contraseña y el nombre de la red WIFI con frecuencia para evitar accesos no autorizados, el nombre de la red no deberá ser algo que identifique la empresa como tal, para pasar desapercibida, pero si se deberá usarse como tipo de seguridad WPA2-PSK (AES) para cifrar contraseñas.
IV. Dentro de la configuración del Fortigate, siendo este el dispositivo que libera las direcciones a las conexiones WIFI, deberá mantener reservadas las direcciones para los dispositivos inalámbricos autorizados identificados a través de sus direcciones MAC, nombre de usuario y dirección IP.

Seguridad del cableado de red de datos

I. Todo equipo de cómputo incluyendo equipos portátiles de RASH PERÚ SAC, tendrá asignado una dirección IP estática por red cableada, configurada desde el Fortigate, con el fin de acceder más ágilmente y tener mayor estabilidad de conexión.
II. Solo se habilitará la red inalámbrica a equipos autorizados y que la requieran para movilidad del equipo.

P-RPS-07 - Monitoreo de Redes.

Los ataques a las redes son muy frecuentes y su transcendencia depende de los controles y mecanismos que se apliquen para monitorear y mantener la seguridad de ellas, pudiéndose detectar oportunamente la amenaza y tomar acciones para minimizar el impacto sobre los activos de información de RASH PERÚ SAC.

Objetivo.

Implementar lineamientos para el monitoreo de redes y servicios

Alcance.

El procedimiento contempla el monitoreo de redes y servicios asociados a la Sede Principal de RASH PERÚ SAC y a las tiendas.

Responsabilidades

a. Coordinador TI.

- Asegurar el cumplimiento del procedimiento.
- Monitorear el tráfico de la red y servicios utilizando herramientas confiables que garanticen la optimización de la red.
- Configurar alertas sobre las aplicaciones de monitoreo para facilitar la administración de la red y los servicios.

Descripción

RASH PERÚ SAC cuenta con un dispositivo para proteger la red local y servicios como correo electrónico, control de navegación entre otros. Este dispositivo es un Fortigate, el cual administra toda la red, asigna direccionamiento DHCP, monitorea y bloquea tráfico de red entrante y saliente según las políticas de configuración establecidas.

I. Para acceder y monitorear la red desde el Fortigate es necesario tener datos del usuario administrador, conocimientos de redes y otros conocimientos necesarios para el manejo de la interfaz.

II. Es indispensable realizar copias de respaldos del Fortigate, con el objeto de respaldar las políticas creadas y las demás configuraciones ante una falla del dispositivo.

III. En caso de avería de este activo se requiere de un plan de contingencia debido a que este equipo soporte toda la administración de las redes disponibles en RASH PERÚ SAC.

IV. Se deberá analizar con frecuencia los puertos, protocolos y servicios habilitados e identificar si están siendo usados, de lo contrario deshabilitarlos para evitar explotación de vulnerabilidades.

V. Se debe configurar desde el Fortigate el análisis de los protocolos IMAP y POP, aplicando filtros que ayuden a detectar y bloquear correos maliciosos.

VI. Para mayor control en la seguridad, se requiere analizar frecuentemente los logs de eventos proporcionados por Windows para el caso de los servidores o equipos y aplica también para los dispositivos como el Fortigate, con el fin de revisar la ocurrencia de eventos que puedan perjudicar los sistemas y activos de información.

Anexo 9

Evidencias Fotográficas

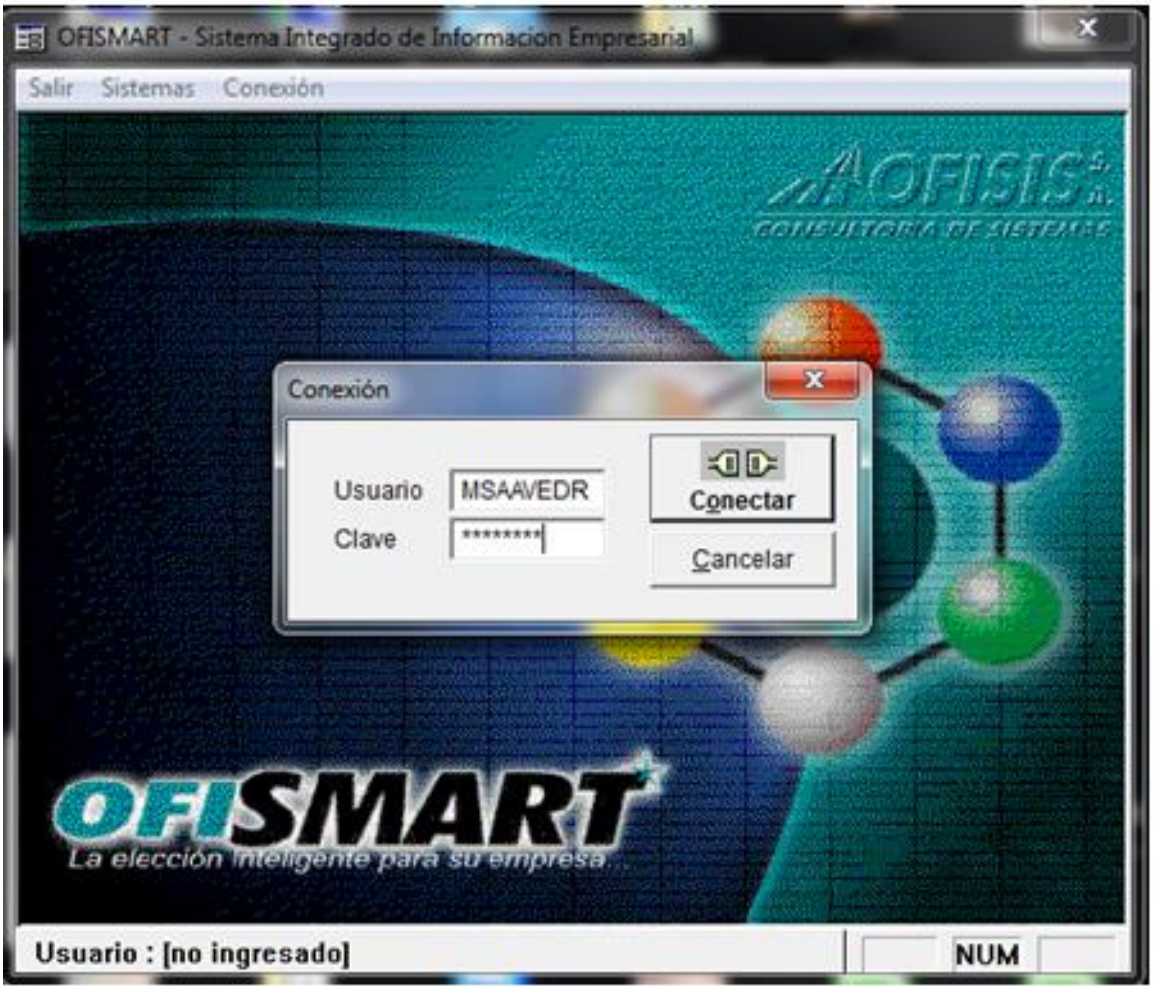


Figura 53. Acceso al Sistema OFISMART

Fuente. Elaboración propia.

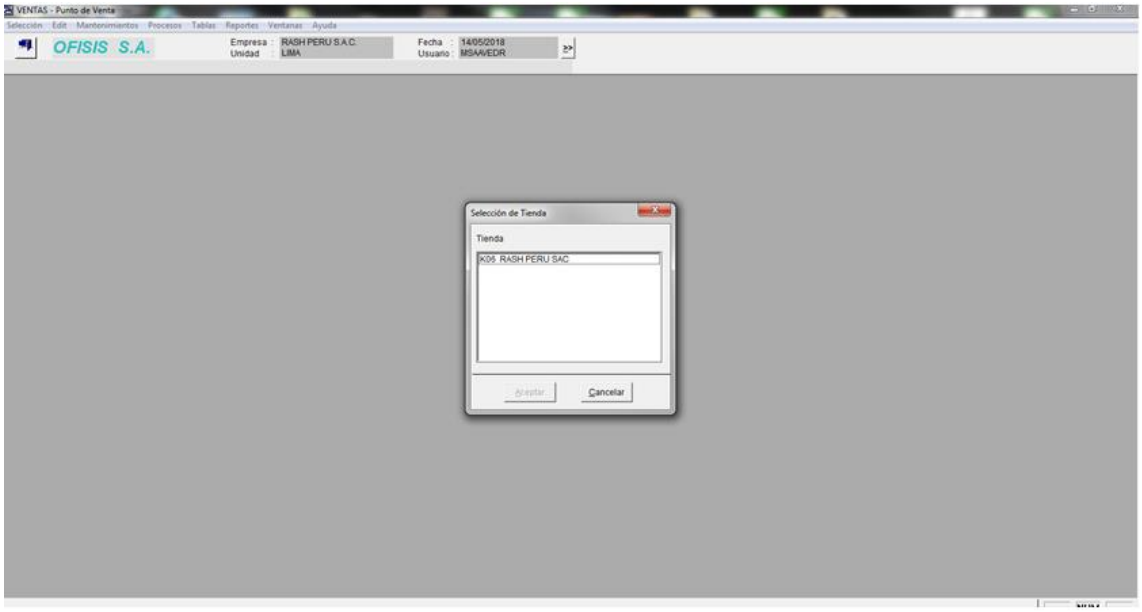


Figura 54. Selección de tienda

Fuente. Elaboración propia.

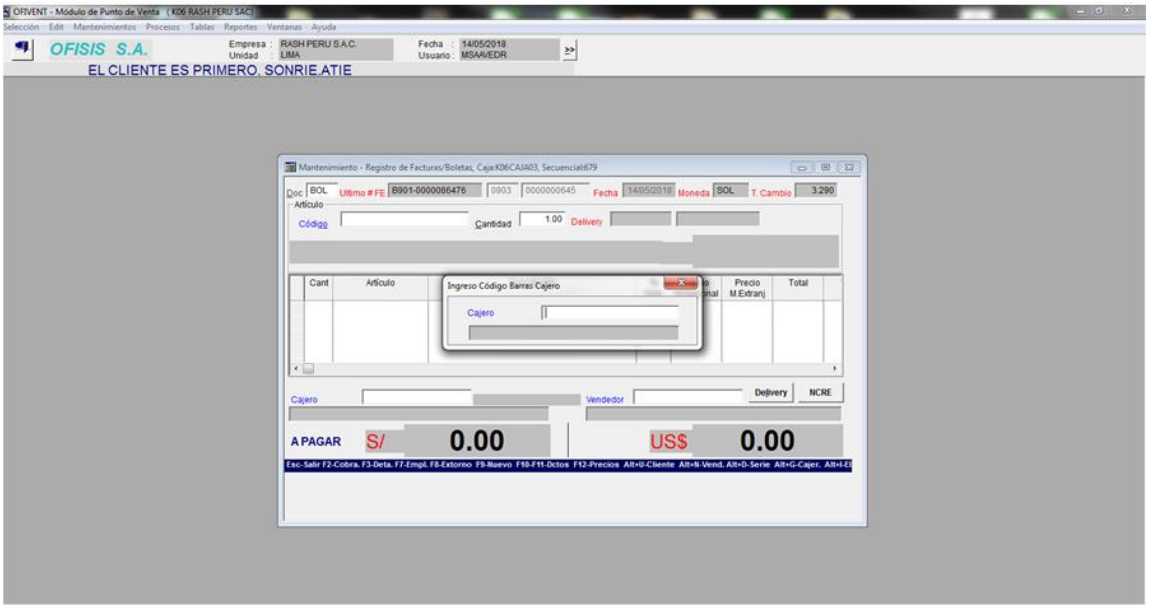


Figura 55. Pantalla de cobro

Fuente. Elaboración propia.

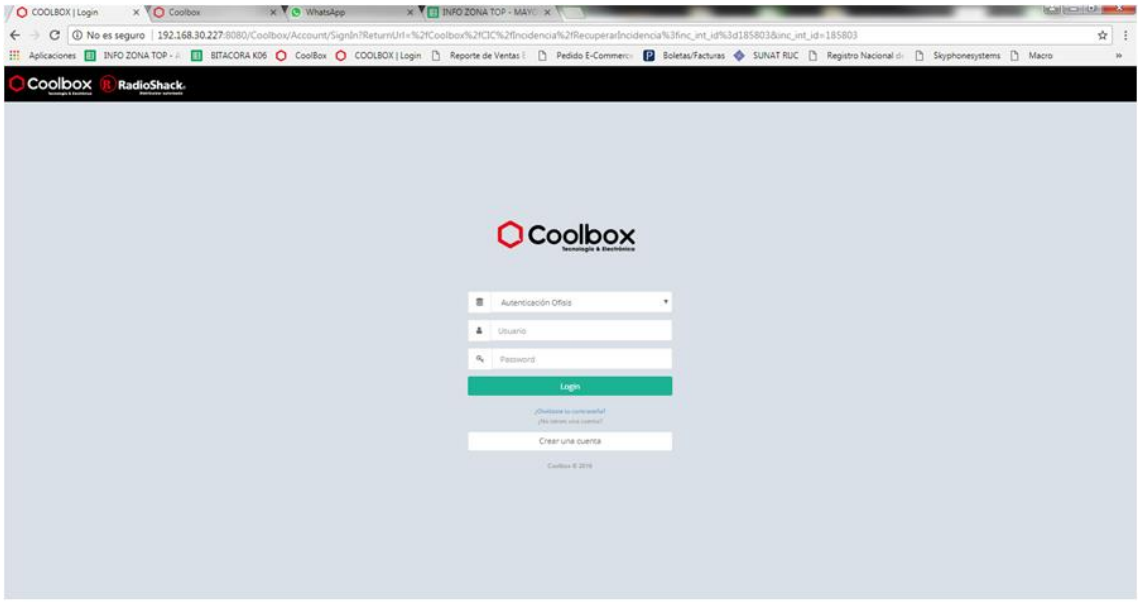


Figura 56. Interfaz de acceso al sistema

Fuente. Elaboración propia.

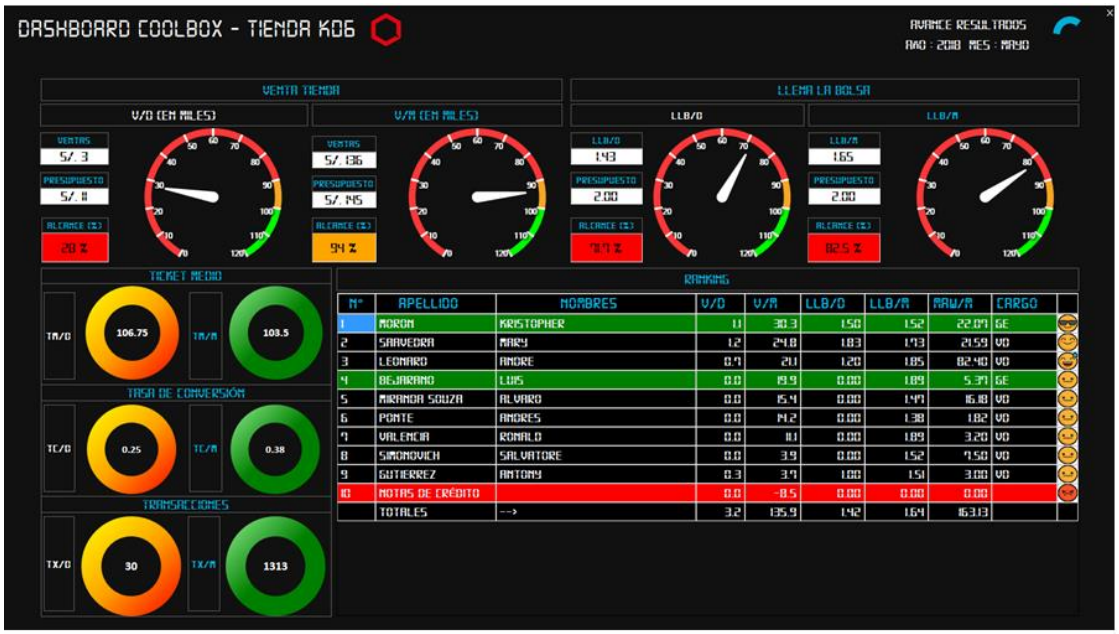


Figura 57. Dashboard Coolbox - Rash Perú SAC

Fuente. Elaboración propia

Figura 58. Interfaz principal

Fuente. Elaboración propia.

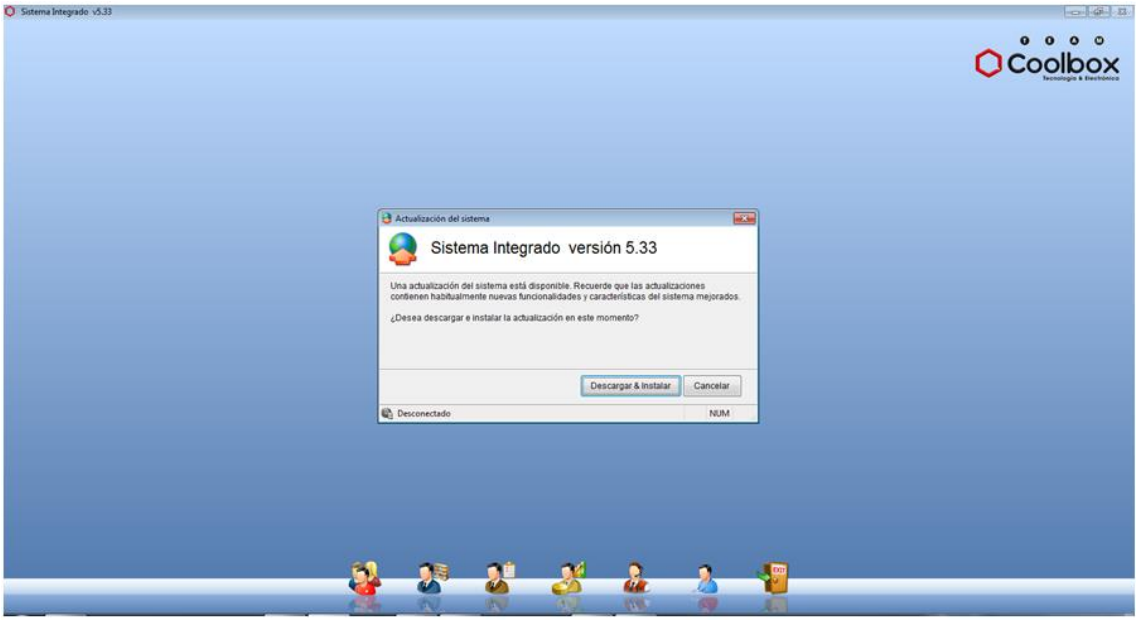


Figura 59. Mensaje de bienvenida al OFISMART

Fuente. Elaboración propia.

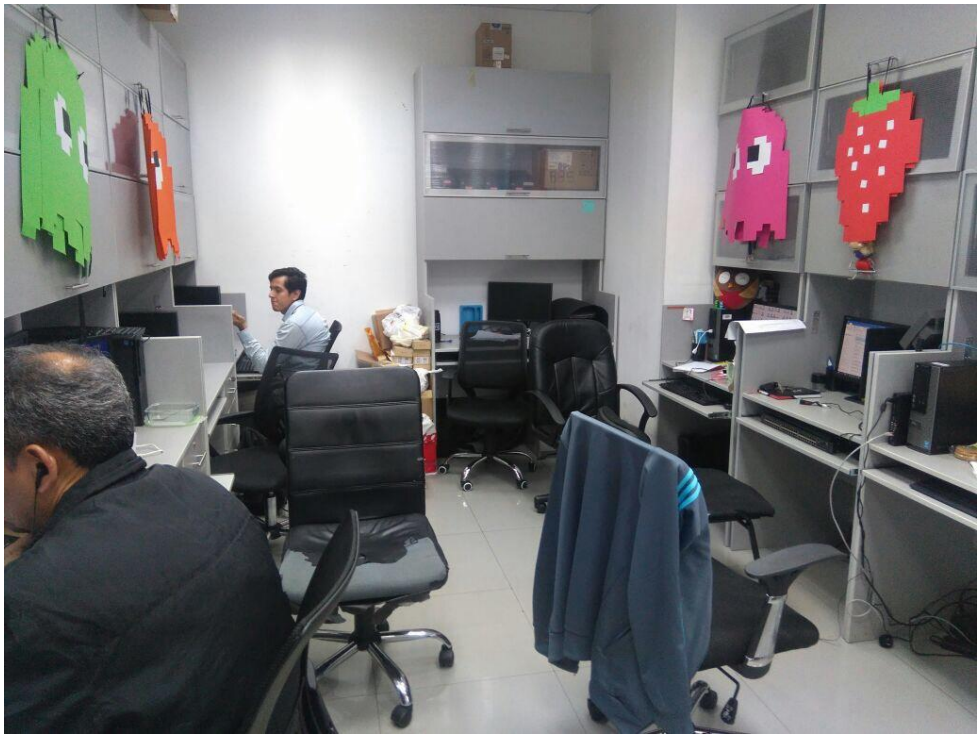


Figura 60. Evidencia fotográfica durante inventario de activos

Fuente. Elaboración propia.

Figura 61. Evidencia fotográfica durante visita a instalaciones

Fuente. Elaboración propia.

Anexo 10

Tabla comparativa de herramientas de soluciones existentes.

Herramienta	AWRisk	ePULPO	GlobalSUITE	SecuriaSGSI
Proveedor	AtixWorld Systems	Ingenia	GlobalSUITE Solutions	CEEI
Denominación	Herramienta	Herramienta	Herramienta	Herramienta
¿Qué cubre?	Implementación de SGSI	Implementación de SGSI	Implementación de SGSI	Implementación de SGSI
Funciones	Gestión integral de TI y SI	Gestión integral de TI y SI	Gestión integral de TI y SI	Gestión integral de TI y SI
Módulos Funcionales	06 módulos	08 módulos	06 módulos	04 módulos
Servicios	Implantación, Formación y Mantenimiento	Implantación, Formación, Mantenimiento, Asistencia Técnica Especializada 24/7, desarrollos específicos y la posibilidad de integrarse con otros componentes de la compañía.	Implantación, Formación y Mantenimiento	Implantación
Página Web	https://www.awrisk.com/	https://ingenia.es/pe/productos/epulpo/	https://www.globalsuitesolutions.com/	http://www.binaryti.com/2012/02/securia-sgsi.html

Fuente. Elaboración propia.

Anexo 11

Módulos del SGSI Rash Perú SAC

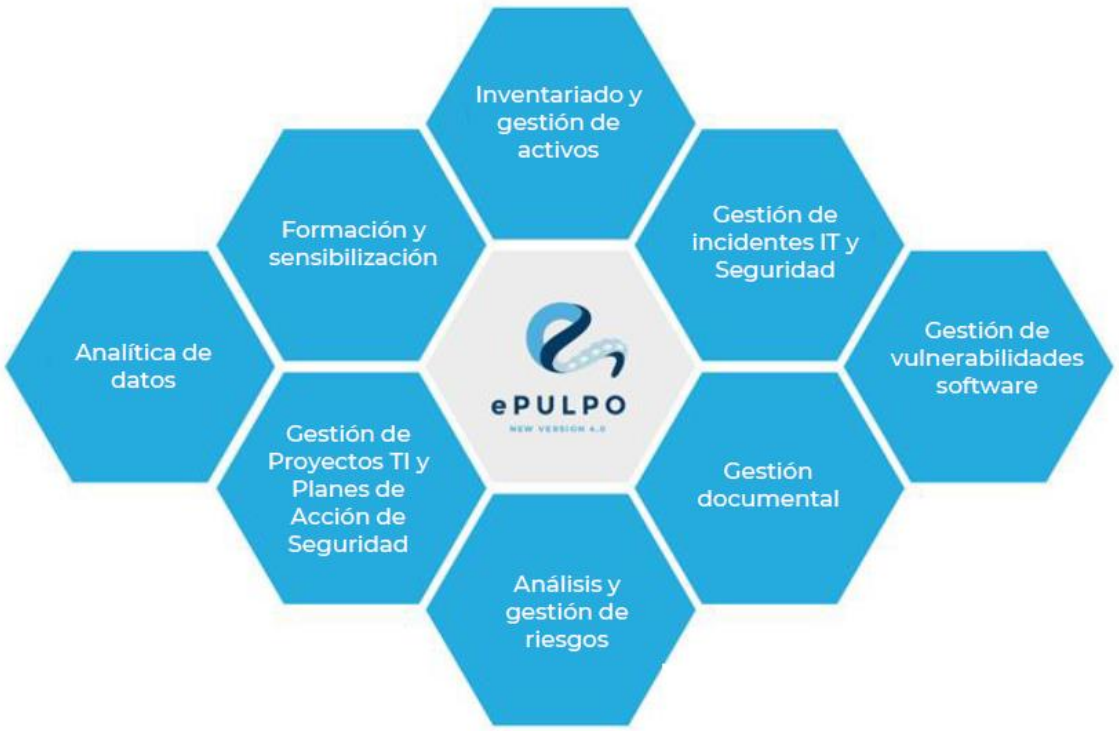


Figura 62. Módulos del SGSI según ePULPO

Fuente. Elaboración propia.

Inventariado y gestión de activos

- Activo: cualquier elemento que tiene valor para la organización. ePULPO permite gestionar cualquier tipo de activo.
- Inventariado automático de hardware y software: agente y descubrimiento SNMP
- Otros tipos de activos como la información que gestiona la organización, servicios, procesos, etc pueden ser inventariados manualmente o importados de forma masiva vía csv
- Relacionar entre sí los activos, establecer sus contratos, proveedores,...

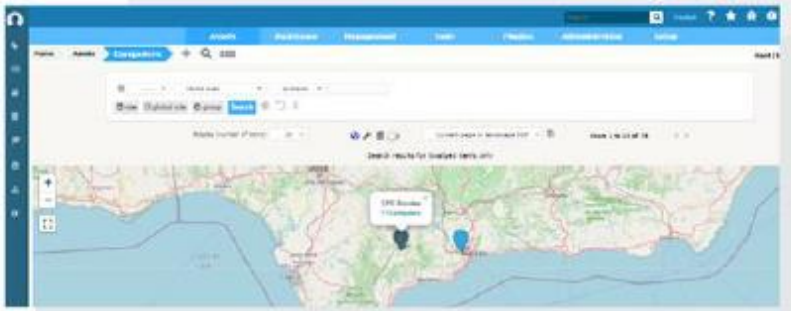


Figura 63. Módulo Inventariado y gestión de activos

Fuente. Elaboración propia.

Gestión de incidentes IT y Seguridad

- Creación y gestión de incidentes de seguridad (también de los datos personales) y peticiones IT.
- Las peticiones pueden estar asociadas a activos específicos del inventario de la organización.
- Notificación por email para usuarios finales y técnicos a lo largo de todo el ciclo de vida de la petición.
- Asignación automática de peticiones a técnicos de acuerdo a reglas personalizadas.
- Portal de servicios para peticiones de clientes, proveedores y usuarios.

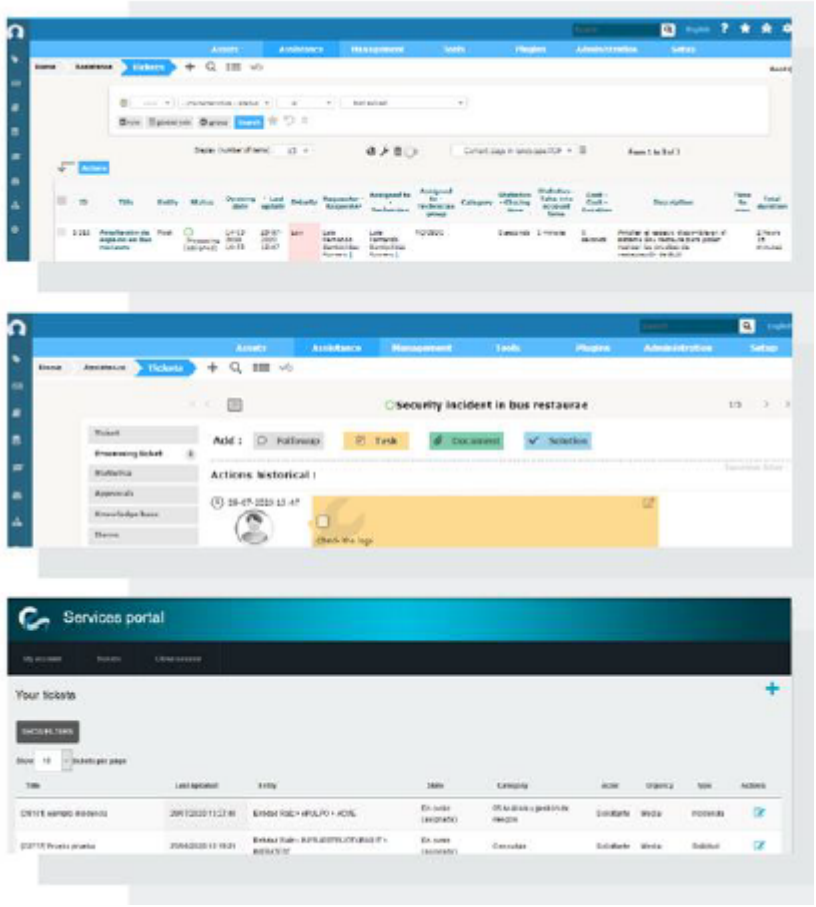


Figura 64. Módulo Gestión de incidentes IT y seguridad

Fuente. Elaboración propia.

Gestión de vulnerabilidades software

- Gestión automatizada de identificación de vulnerabilidades del software inventariado de la organización.
- Vulnerabilidades clasificadas según nomenclatura CVE (Common Vulnerabilities and Exposures).
- Visualización de vulnerabilidades en formato listado y cuadro de mandos.
- Las vulnerabilidades identificadas pueden ser gestionadas para su resolución desde el módulo de gestión de peticiones de ePULPO.

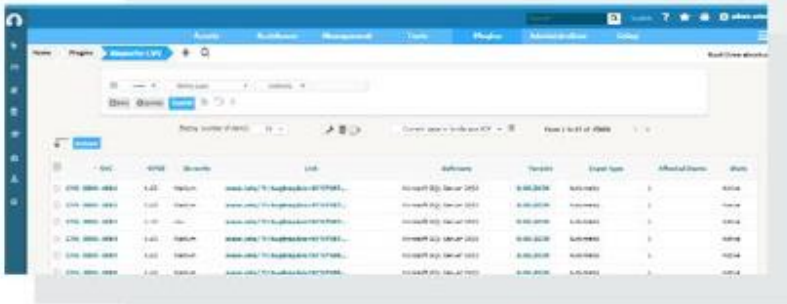


Figura 65. Módulo Gestión de vulnerabilidades SOFTWARE.

Fuente. Elaboración propia.

Gestión documental

- Repositorio centralizado para almacena y gestionar todo tipo de documentos generados de forma externa o por cualquiera de los módulos que componen ePULPO.
- Definición de responsabilidades y accesos a los espacios documentales a usuarios y grupos.
- Tramitación de documentos mediante flujos documentales.
- Localización rápida de documentos mediante búsqueda por contenidos o metadatos.
- Versionado de documentos.

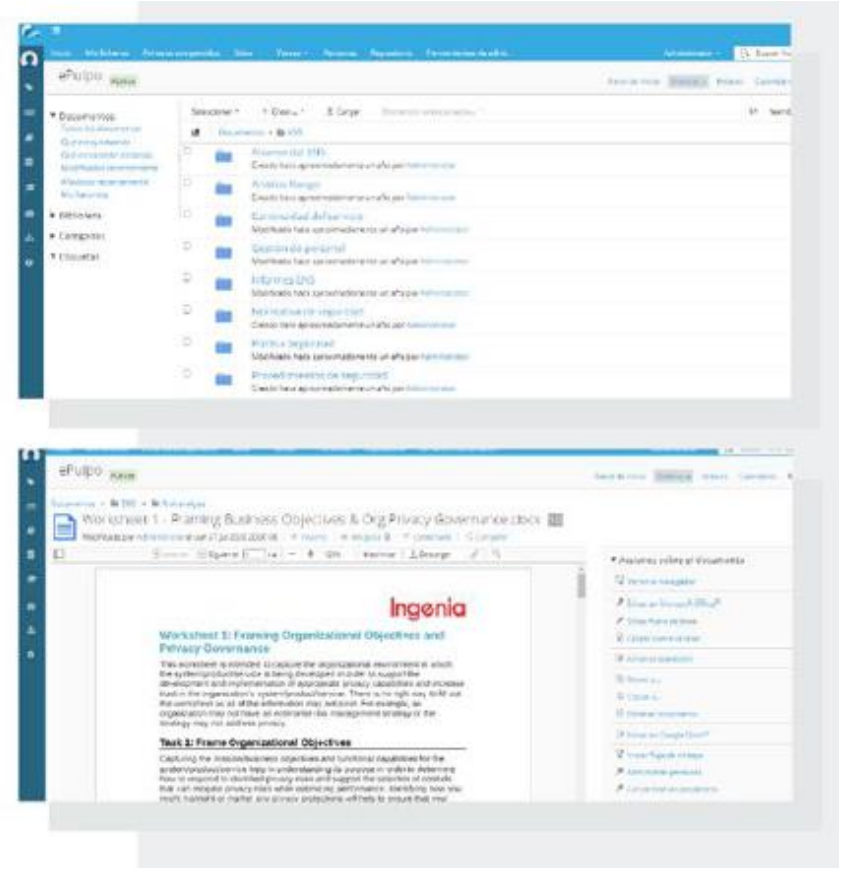
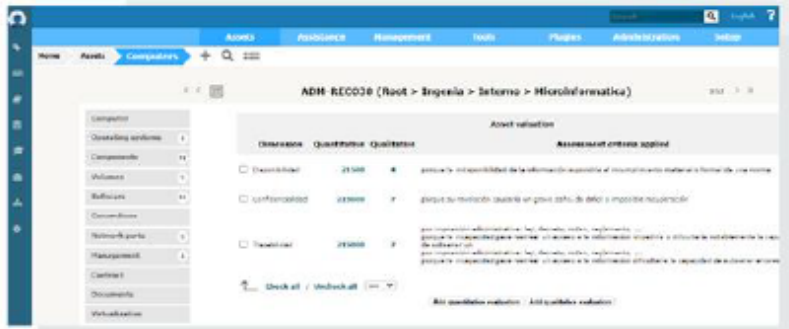


Figura 66. Módulo Gestión documental

Fuente. Elaboración propia.

Análisis y gestión de riesgos

- ePULPO se integra con PILAR, herramienta basada en la metodología MAGERIT para realizar el análisis y la gestión de riesgos.
- Fuente de datos única. PILAR carga la información de activos del módulo de gestión de activos.
- Incluye información que requiere PILAR como dependencias, valoraciones, dominios de seguridad, clases de activos y capas/grupos.
- Permite establecer qué activos debe cargar PILAR.
- Incluye las actividades de tratamiento como activos que pueden ser incluidos en el AGR.
- Proyecto de análisis de riesgos realizado en PILAR, queda almacenado en ePULPO.
- Nuevo módulo de riesgos . ePULPO 4.1



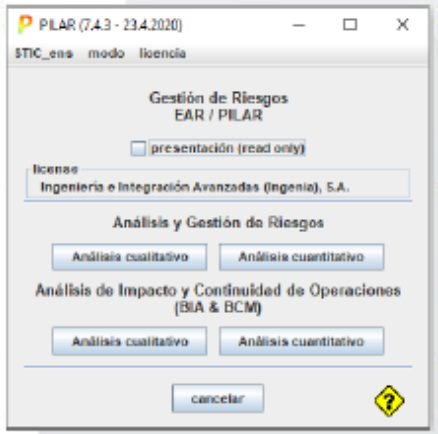


Figura 67. Módulo Análisis y gestión de riesgos

Fuente. Elaboración propia.

Gestión de planes de acción

- Gestión de tareas, tiempos o avance de un plan de acción.
- Asiste al gestor de proyectos para planificación y ejecución de planes, asignación de recursos a tareas, seguimiento y análisis de carga de trabajo.
- Gestión de costes y presupuestos del proyecto.
- Diagrama de Gantt.
- Metodología ágil - Pizarra Kanban para organizar y asignar las tareas.

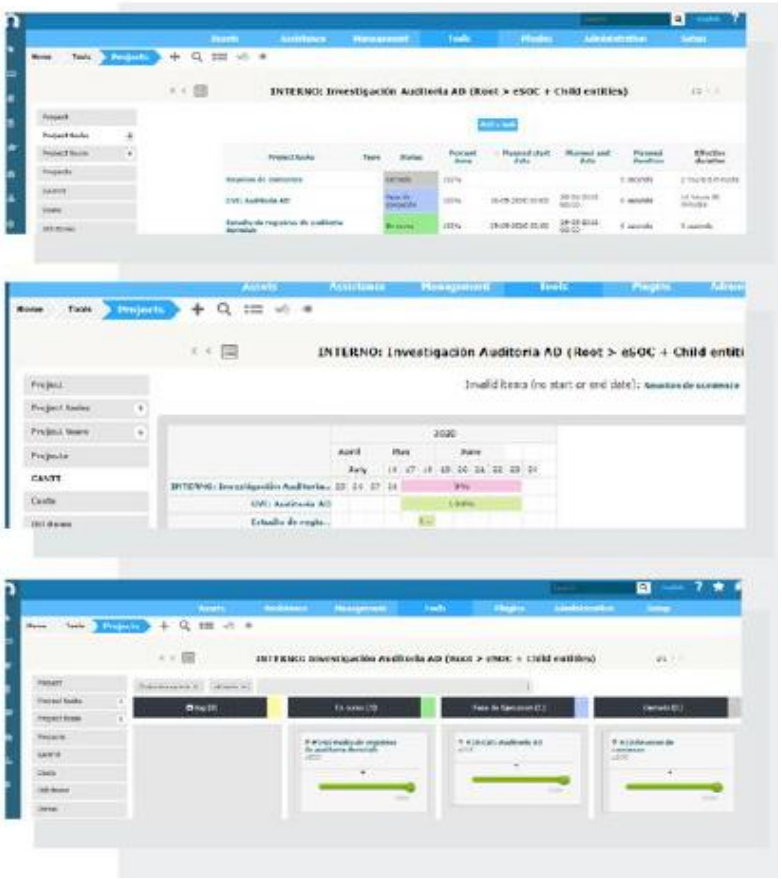


Figura 68. Módulo Gestión de Proyectos TI y Planes de Acción de Seguridad

Fuente. Elaboración propia.

Analítica de datos

- Módulo de Inteligencia de Negocios (BI) que facilita y agiliza la toma de decisiones.
- Analiza los datos que gestiona ePULPO internamente y de fuentes externas.
- Proporciona información relevante en tiempo real
- Cuadros de mandos personalizables con un conjunto de informes personalizados para comunicación con responsables de negocios, auditores, reguladores u otros interesados

Figura 69. Módulo Analítica de Datos

Fuente. Elaboración propia.

Formación y sensibilización

- Plataforma formativa que dispone de funcionalidades para el desarrollo de los cursos y para la interacción de los participantes en la acción formativa.
- Permite acreditar ante un tercero (auditor, entidad certificadora) que se han llevado las acciones de formación según las normativas o requisitos que apliquen.
- Herramientas: Glosarios, tareas o acciones concretas a realizar por los alumnos, cuestionarios, encuestas, taller, chat, etc.

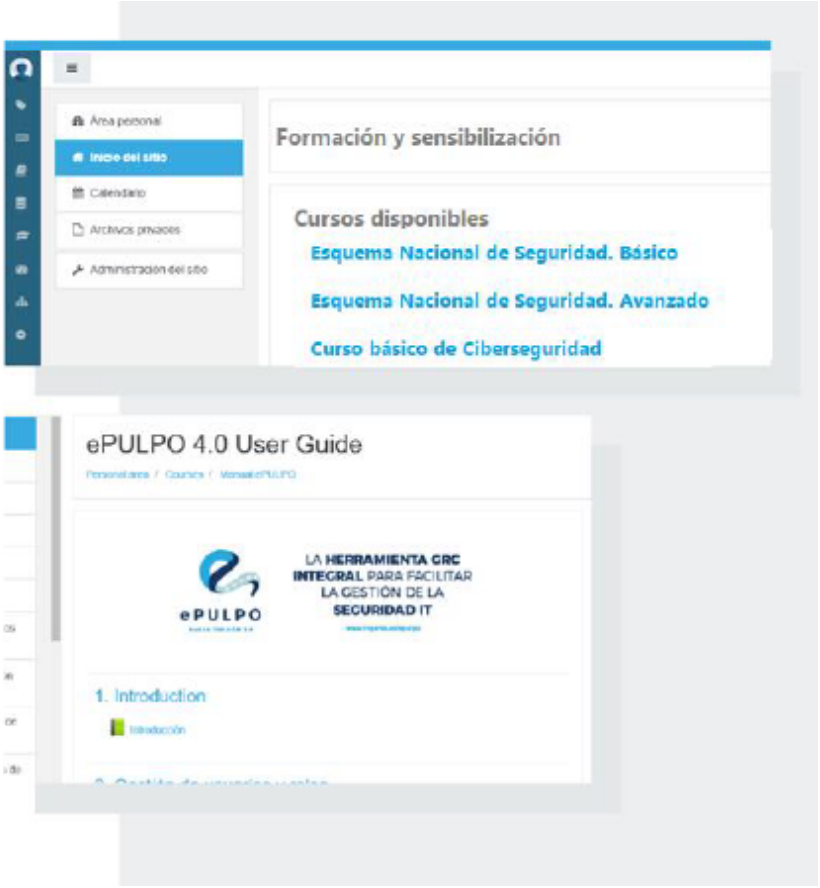


Figura 70. Módulo Formación y sensibilización

Fuente. Elaboración propia.

Anexo 12

Niveles de prioridad Módulos del SGSI Rash Perú SAC

ID	Descripción	Prioridad	Estimación	Persona Asignada
M1	Inventariado y gestión de activos	Muy Alta	5	Moron Peredo Kristopher Renzo
M2	Gestión de incidentes IT y Seguridad	Muy Alta	5	Moron Peredo Kristopher Renzo
M3	Gestión de vulnerabilidades software	Muy Alta	5	Moron Peredo Kristopher Renzo
M4	Análisis y gestión de riesgos	Muy Alta	5	Moron Peredo Kristopher Renzo
M5	Gestión documental	Alta	2	Moron Peredo Kristopher Renzo
M6	Gestión de planes de acción	Muy Alta	4	Moron Peredo Kristopher Renzo
M7	Analítica de datos	Alta	2	Moron Peredo Kristopher Renzo
M8	Formación y sensibilización	Alta	2	Moron Peredo Kristopher Renzo

Figura 71. Módulos del Sistema de Gestión de Seguridad de la Información

Fuente. Elaboración propia.

Anexo 13

Interfaz del SGSI Rash Perú SAC

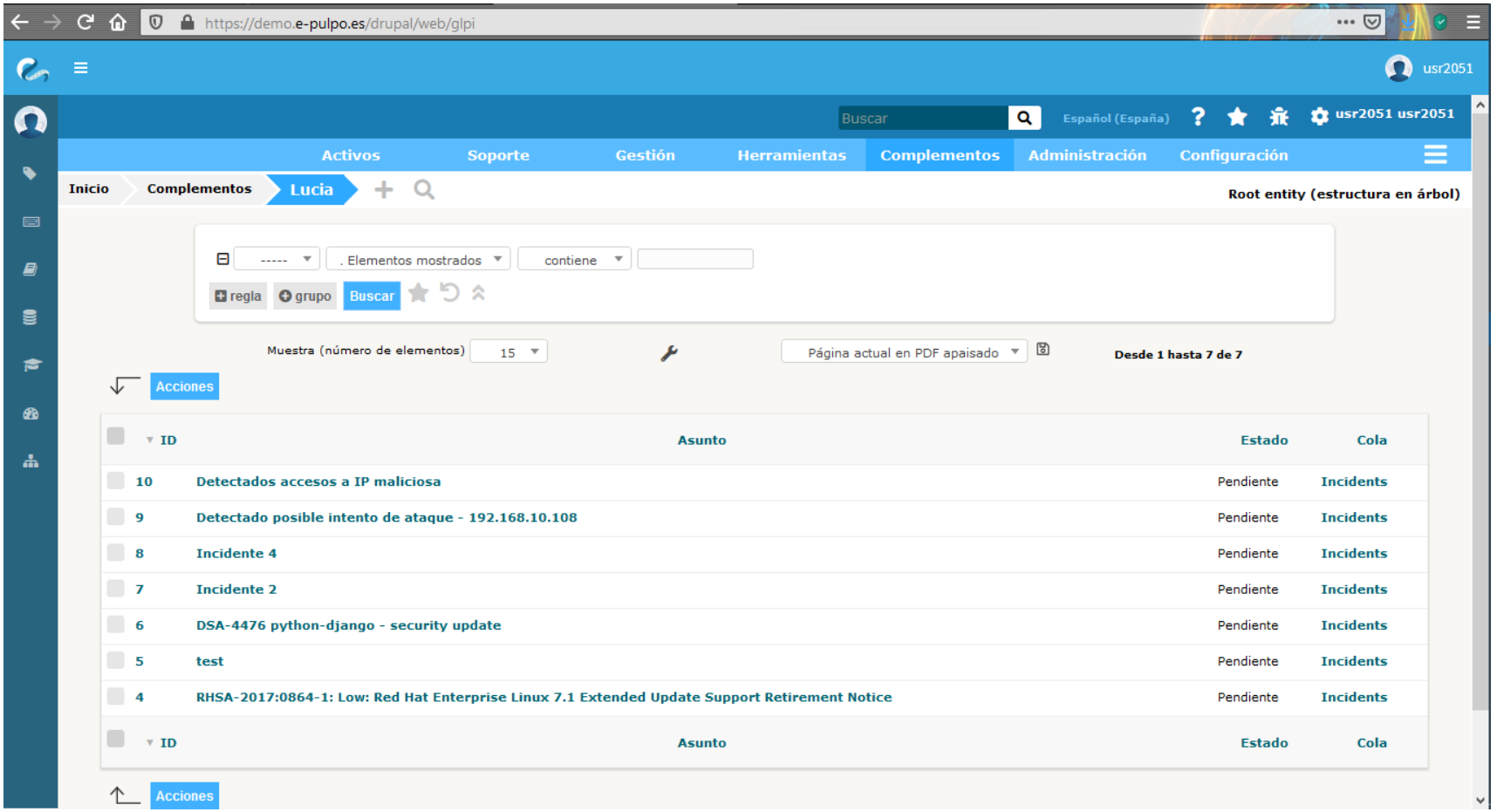


Figura 72. Gestión de activos y tickets

Fuente. Elaboración propia.

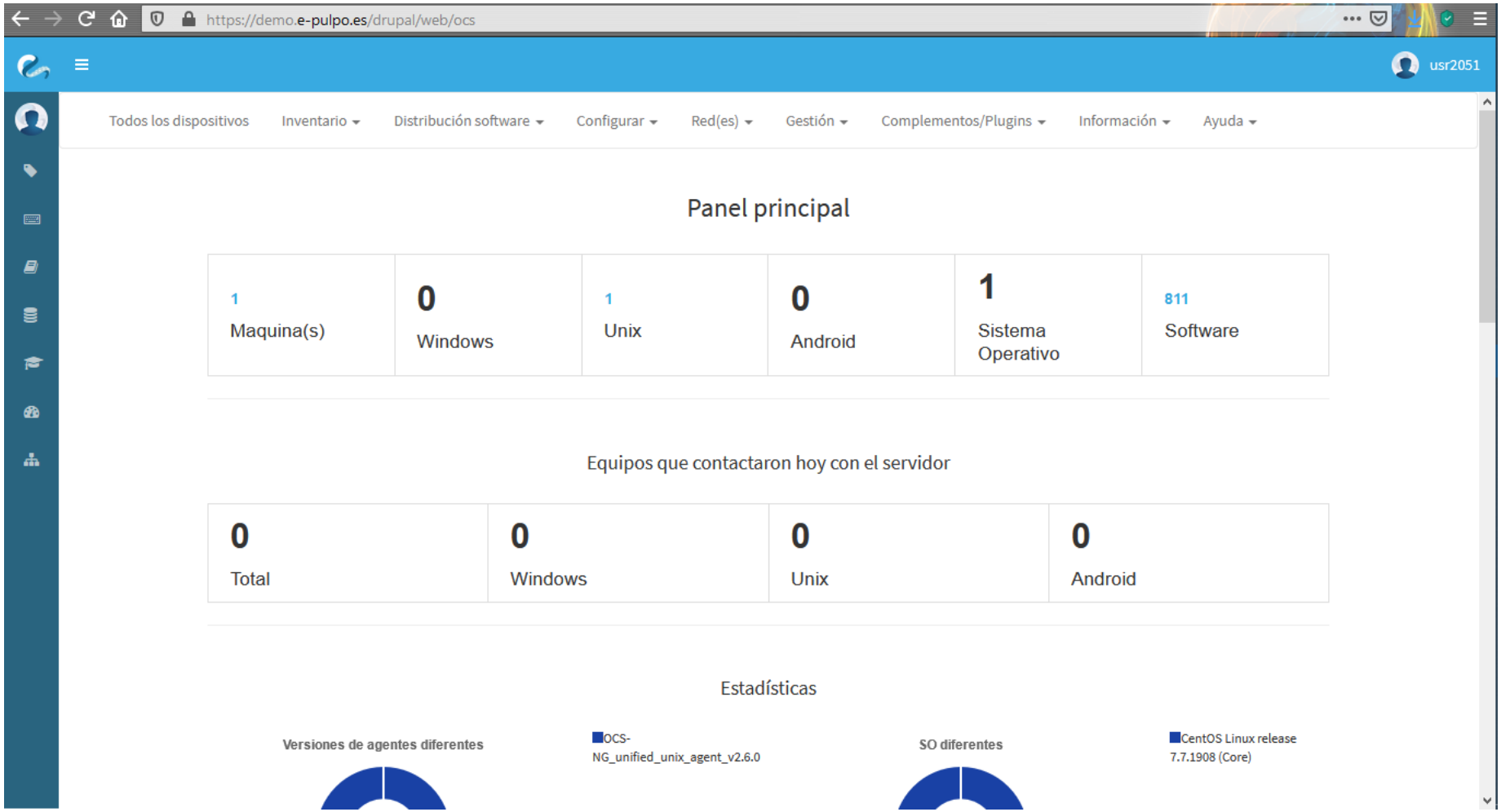


Figura 73. Gestión de inventario mediante agentes

Fuente. Elaboración propia.

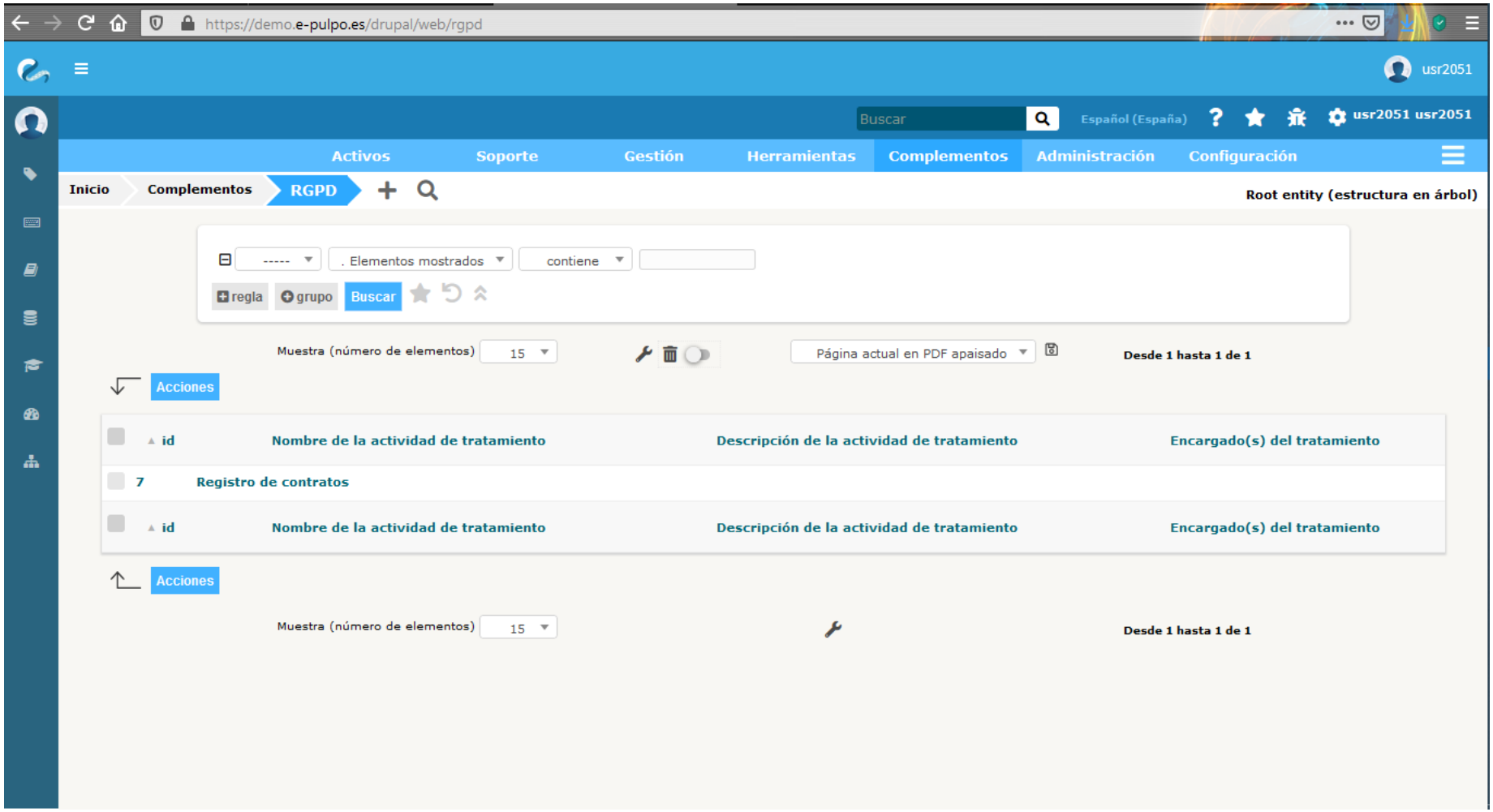


Figura 74. Registro de actividades de tratamiento de incidencias

Fuente. Elaboración propia.

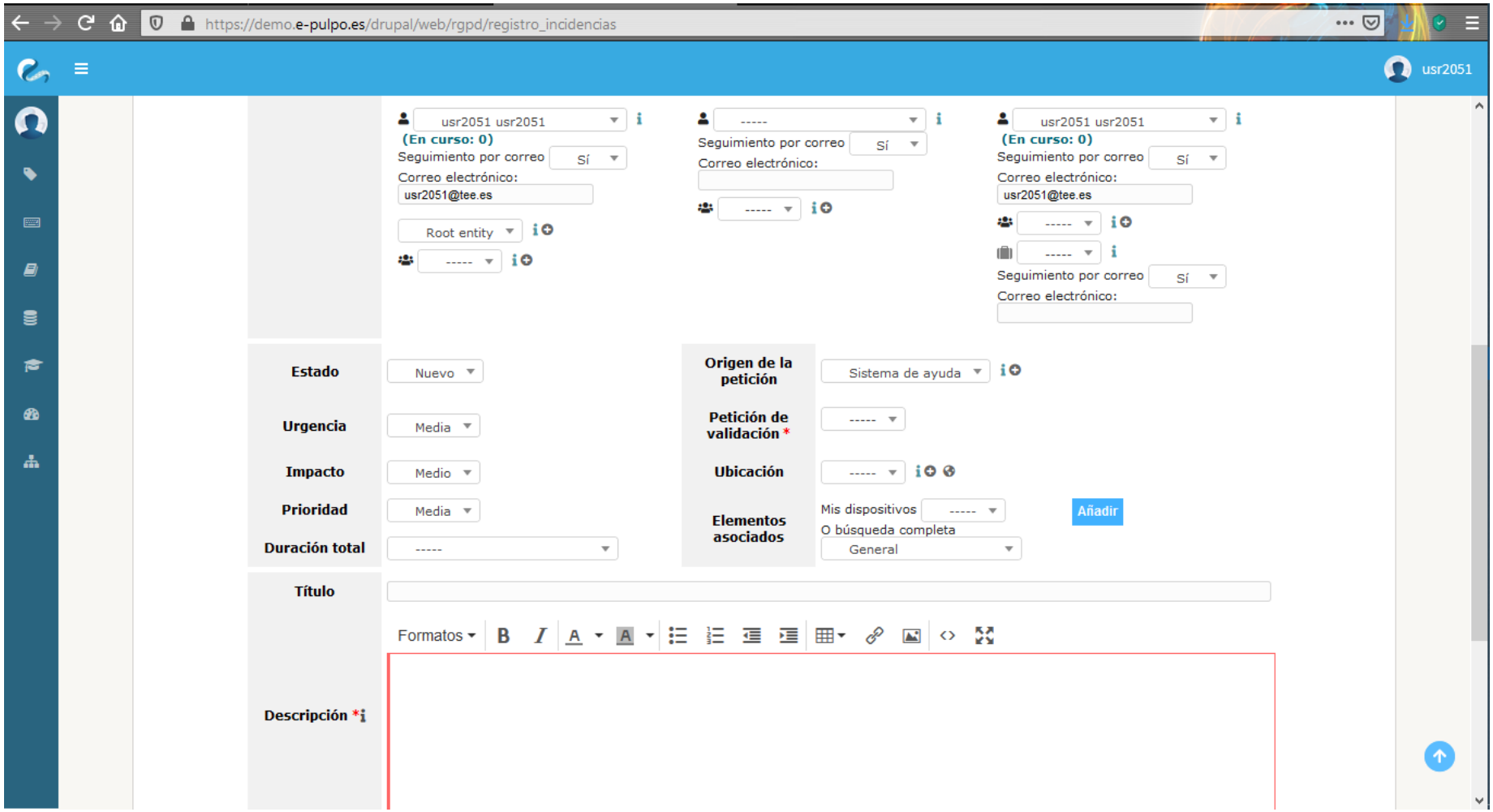


Figura 75. Registro de incidencias

Fuente. Elaboración propia.

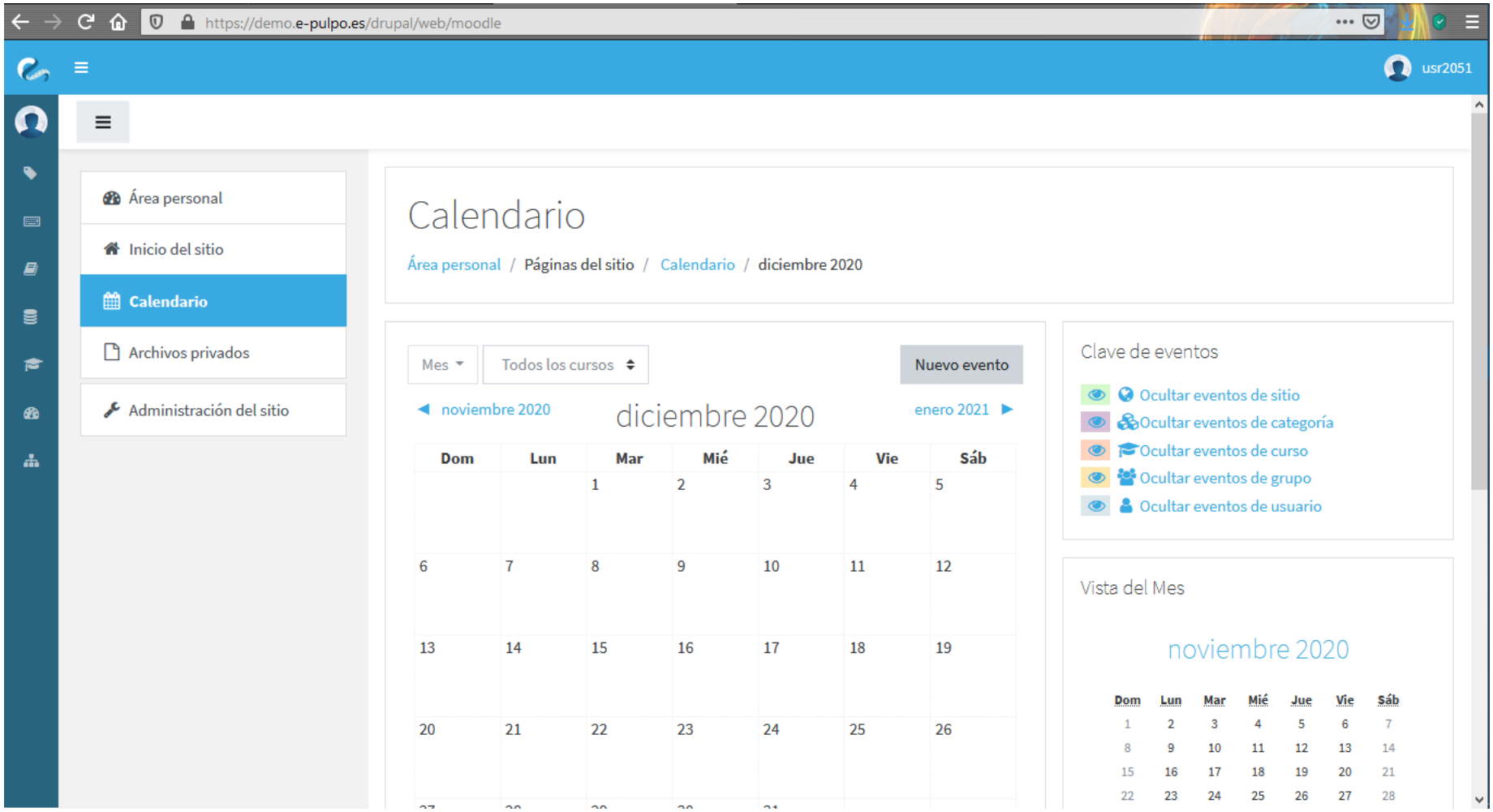


Figura 76. Calendario de formación y concientización

Fuente. Elaboración propia.

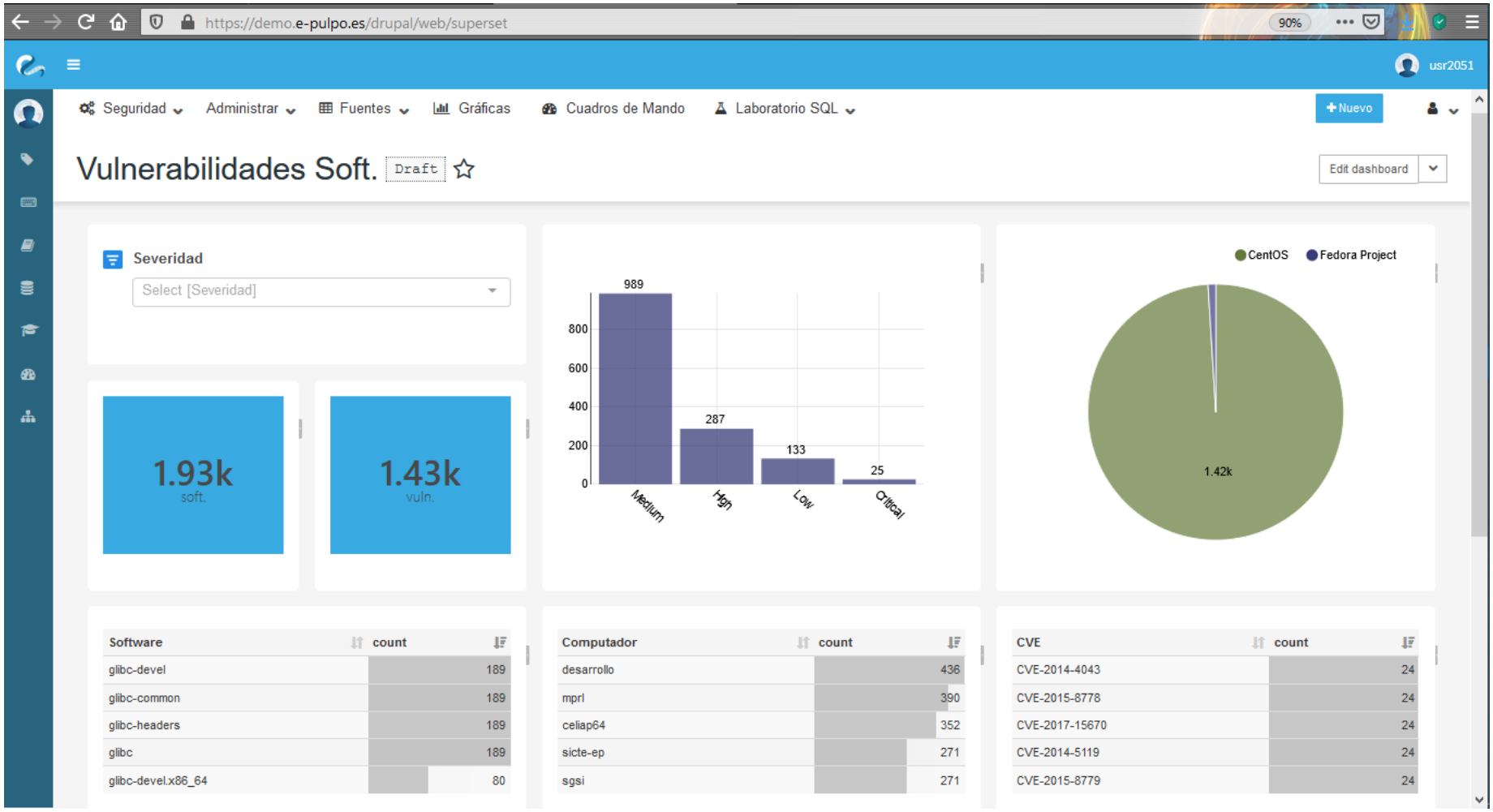


Figura 77. Dashboard de vulnerabilidades de SOFTWARE.

Fuente. Elaboración propia.

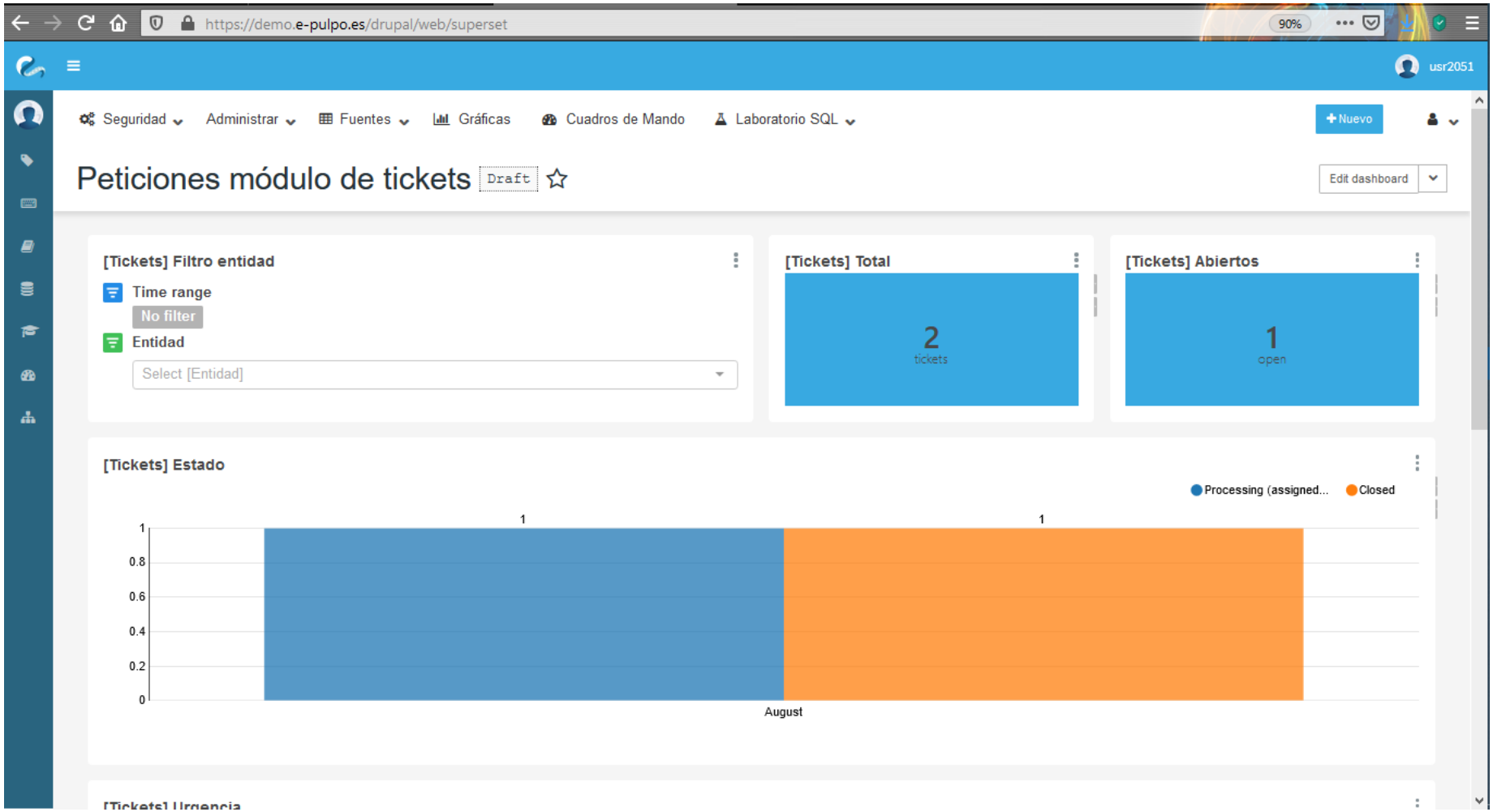


Figura 78. Peticiones de módulo de tickets

Fuente. Elaboración propia.

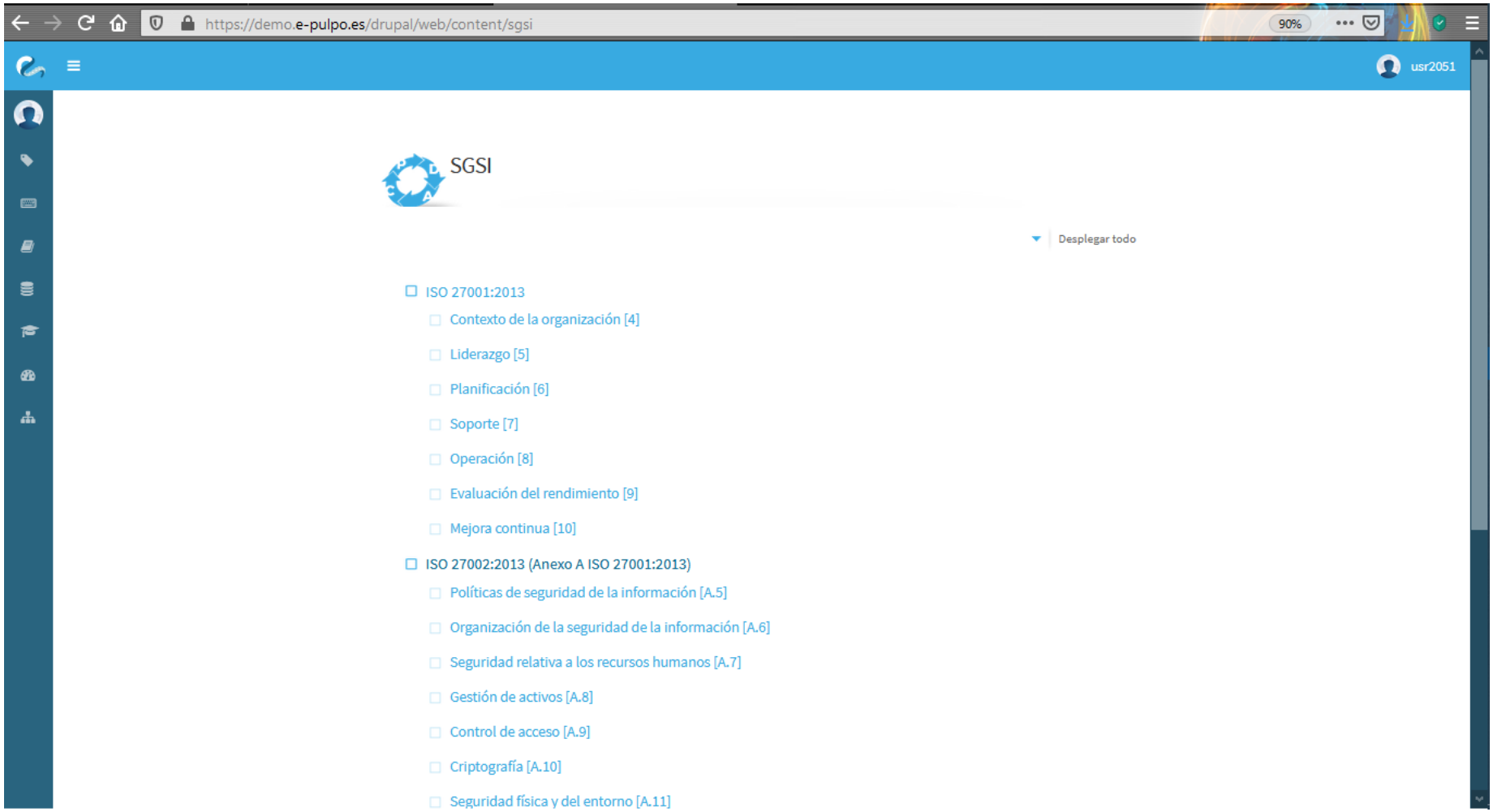


Figura 79. Documentación adicional por parte de la herramienta ePULPO

Fuente. Elaboración propia.

Anexo 14. Fichas de registro test

Investigador				
Empresa				
Dirección				
Fecha de inicio	**02/07/2022**			
Fecha de terminación	**21/07/2022**			
Variable	Formula			
Reportes		$ANA = \frac{RANA}{TAD} \times 100$		
Indicador	Medida			
seguridad de la información (TEST)	Porcentaje	Donde: ANA: seguridad de la información TAD: Total de Accesos seguridad de la información RANA: Reporte de Accesos seguridad de la información		
ÍTEM	**FECHA**	**RANA**	**TAD**	**ANA %**
1	02/07/2022	**13**	**20**	**65**
2	03/07/2022	**10**	**18**	**56**
3	04/07/2022	**15**	**20**	**75**
4	05/07/2022	**10**	**19**	**53**
5	06/07/2022	**13**	**18**	**72**
6	07/07/2022	**15**	**17**	**88**
7	08/07/2022	**10**	**20**	**50**
8	09/07/2022	**11**	**18**	**61**
9	10/07/2022	**15**	**19**	**79**
10	11/07/2022	**13**	**20**	**65**
11	12/07/2022	**10**	**17**	**59**
12	13/07/2022	**16**	**18**	**89**
13	14/07/2022	**13**	**19**	**68**
14	15/07/2022	**10**	**20**	**50**
15	16/07/2022	**15**	**22**	**68**
16	17/07/2022	**10**	**17**	**59**
17	18/07/2022	**10**	**18**	**56**
18	19/07/2022	**15**	**17**	**88**
19	20/07/2022	**13**	**17**	**76**
20	21/07/2022	**16**	**17**	**94**
	TOTAL	**253**	**371**	
	PROMEDIO			**68**

Fichas de registro test

Investigador				
Empresa				
Dirección				
Fecha de inicio	**01/02/2022**			
Fecha de terminación	**20/02/2022**			
Variable	Formula			
Reportes		$ANA = \frac{RANA}{TAD} \times 100$		
Indicador	Medida			
seguridad de la información (RE-TEST)	Porcentaje	ANA: seguridad de la información TAD: Total de Accesos seguridad de la información RANA: Reporte de Accesos seguridad de la información		
ÍTEM	**FECHA**	**RANA**	**TAD**	**ANA %**
1	01/08/2022	**15**	**20**	**75**
2	02/08/2022	**14**	**18**	**78**
3	03/08/2022	**13**	**20**	**65**
4	04/08/2022	**14**	**19**	**74**
5	05/08/2022	**10**	**18**	**56**
6	06/08/2022	**15**	**17**	**88**
7	07/08/2022	**14**	**20**	**70**
8	08/08/2022	**10**	**17**	**59**
9	09/08/2022	**15**	**18**	**83**
10	10/08/2022	**14**	**19**	**74**
11	11/08/2022	**10**	**20**	**50**
12	12/08/2022	**15**	**19**	**79**
13	13/08/2022	**14**	**18**	**78**
14	14/08/2022	**10**	**17**	**59**
15	15/08/2022	**14**	**20**	**70**
16	16/08/2022	**13**	**18**	**72**
17	17/08/2022	**10**	**18**	**56**
18	18/08/2022	**10**	**19**	**53**
19	19/08/2022	**14**	**17**	**82**
20	20/08/2022	**13**	**17**	**77**
	TOTAL	**257**	**369**	
	PROMEDIO			**70**

Anexo 15

Fichas de registro pos test.

Investigador				
Empresa				
Dirección				
Fecha de inicio	**01/03/2022**			
Fecha de terminación	**20/03/2022**			
Variable	Formula			
Reportes		$ANA = \frac{RANA}{TAD} \times 100$		
Indicador	Medida			
seguridad de la información (POST-TEST)	Porcentaje	ANA: seguridad de la información TAD: Total de Accesos seguridad de la información RANA: Reporte de Accesos seguridad de la información		
ÍTEM	**FECHA**	**RANA**	**TAD**	**ANA %**
1	01/09/2022	2	15	13
2	02/09/2022	3	14	21
3	03/09/2022	1	10	10
4	04/09/2022	0	10	0
5	05/09/2022	2	10	20
6	06/09/2022	3	14	21
7	07/09/2022	4	15	27
8	08/09/2022	2	12	17
9	09/09/2022	1	11	9
10	10/09/2022	1	10	10
11	11/09/2022	3	15	20
12	12/09/2022	0	14	0
13	13/09/2022	0	13	0
14	14/09/2022	1	10	10
15	15/08/2022	3	11	27
16	16/09/2022	2	10	20
17	17/09/2022	1	10	10
18	18/09/2022	1	10	10
19	19/09/2022	3	14	21
20	20/09/2022	2	14	14
	TOTAL	35	247	
	PROMEDIO			**14**

Fichas de registro test

Investigador				
Empresa				
Dirección				
Fecha de inicio	**02/07/2022**			
Fecha de terminación	**21/07/2022**			
Variable	Formula			
Reportes		$\mathbf{EBMD} = \frac{\mathbf{EMBDNR}}{\mathbf{TMDD}} \times \mathbf{100}$ Donde: EBMD: Riesgo de la información TMDD: Total de Riesgo de la información : Eliminar, Manipular, Borrar Datos No reconocidos		
Indicador	Medida			
Eliminar, manipular, borrar, datos (TEST)	Porcentaje			
ÍTEM	**FECHA**	**EMBDNR**	**TMDO**	**EBMD%**
1	02/07/2022	10	20	50
2	03/07/2022	15	25	60
3	04/07/2022	10	20	50
4	05/07/2022	13	22	59
5	06/07/2022	10	23	43
6	07/07/2022	10	24	42
7	08/07/2022	11	25	44
8	09/07/2022	15	20	75
9	10/07/2022	10	20	50
10	11/07/2022	10	25	40
11	12/07/2022	13	20	65
12	13/07/2022	10	25	40
13	14/07/2022	10	20	50
14	15/07/2022	10	20	50
15	16/07/2022	13	22	59
16	17/07/2022	11	23	48
17	18/07/2022	11	23	48
18	19/07/2022	10	20	50
19	20/07/2022	10	20	50
20	21/07/2022	10	20	50
	TOTAL	233	439	
	PROMEDIO			51

Anexo 16

Fichas de registro re-test

Investigador				
Empresa				
Dirección				
Fecha de inicio	**01/08/2022**			
Fecha de terminación	**20/08/2022**			
Variable	Formula			
Reportes		$\mathbf{EBMD} = \frac{\mathbf{EMBDNR}}{\mathbf{TMDD}} \times \mathbf{100}$ Donde: EBMD: Riesgo de la información TMDD: Total de Riesgo de la información : Eliminar, Manipular, Borrar Datos No reconocidos		
Indicador	Medida			
Eliminar, manipular, borrar, datos (RE-TEST)	Porcentaje			
ÍTEM	**FECHA**	EMBDNR	TMDO	EBMD%
1	01/08/2022	15	22	68
2	02/08/2022	10	23	43
3	03/08/2022	14	24	58
4	04/08/2022	10	22	45
5	05/08/2022	10	20	50
6	06/08/2022	10	25	40
7	07/08/2022	14	20	70
8	08/08/2022	15	24	63
9	09/08/2022	10	20	50
10	10/08/2022	10	22	45
11	11/08/2022	10	23	43
12	12/08/2022	14	24	58
13	13/08/2022	10	20	50
14	14/08/2022	10	22	45
15	15/08/2022	15	27	56
16	16/08/2022	14	25	56
17	17/08/2022	10	20	50
18	18/08/2022	14	26	54
19	19/08/2022	10	22	45
20	20/08/2022	15	24	63
	TOTAL	240	455	
	PROMEDIO			**53**

Anexo 17

Fichas de registro postest

Investigador				
Empresa				
Dirección				
Fecha de inicio	**01/09/2022**			
Fecha de terminación	**20/09/2022**			
Variable	Formula			
Reportes		$EBMD = \frac{EMBDNR}{TMDD} \times 100$		
Indicador	Medida			
Eliminar, manipular, borrar, datos (POST-TEST)	Porcentaje	Donde: EBMD: Riesgo de la información TMDD: Total de Riesgo de la información : Eliminar, Manipular, Borrar Datos No reconocidos		
ÍTEM	**FECHA**	**EMBDNR**	**TMDO**	**EBMD%**
1	01/09/2022	3	22	14
2	02/09/2022	5	23	22
3	03/09/2022	4	24	17
4	04/09/2022	1	22	5
5	05/09/2022	0	20	0
6	06/09/2022	2	25	8
7	07/09/2022	4	20	20
8	08/09/2022	2	24	8
9	09/09/2022	3	20	15
10	10/09/2022	1	22	5
11	11/09/2022	5	23	22
12	12/09/2022	0	24	0
13	13/09/2022	2	20	10
14	14/09/2022	2	22	9
15	15/09/2022	3	27	11
16	16/09/2022	5	25	20
17	17/09/2022	3	20	15
18	18/09/2022	5	26	19
19	19/09/2022	0	22	0
20	20/09/2022	2	24	8
	TOTAL	52	455	
	PROMEDIO			**11**

Anexo 18

Fichas de registro test

Investigador				
Empresa				
Dirección				
Fecha de inicio	**01/07/2022**			
Fecha de terminación	**21/07/2022**			
Variable	Formula			
Reportes		$VI = \frac{VINE}{VID} \times 100$		
Indicador	Medida	VI: control informático		
control informático (TEST)	Porcentaje	VINE: total controles informáticos VID: total controles aplicados en el día		
ÍTEM	**FECHA**	**TEBMDS**	**EBMDR**	**EBMD %**
1	02/07/2022	**3**	**10**	**30**
2	03/07/2022	**5**	**10**	**50**
3	04/07/2022	**4**	**8**	**50**
4	05/07/2022	**3**	**9**	**33**
5	06/07/2022	**5**	**10**	**50**
6	07/07/2022	**4**	**8**	**50**
7	08/07/2022	**5**	**7**	**71**
8	09/07/2022	**4**	**9**	**44**
9	10/07/2022	**5**	**8**	**63**
10	11/07/2022	**5**	**7**	**71**
11	12/07/2022	**4**	**9**	**44**
12	13/07/2022	**5**	**9**	**56**
13	14/07/2022	**5**	**7**	**71**
14	15/07/2022	**4**	**9**	**44**
15	16/07/2022	**5**	**9**	**56**
16	17/07/2022	**5**	**10**	**50**
17	18/07/2022	**5**	**8**	**38**
18	19/07/2022	**4**	**7**	**71**
19	20/07/2022	**5**	**10**	**40**
20	21/07/2022	**5**	**8**	**50**
	TOTAL	**87**	**172**	
	PROMEDIO			**51**

Anexo 19

Fichas de registro Pre-test

Investigador				
Empresa				
Dirección				
Fecha de inicio	**01/08/2022**			
Fecha de terminación	**20/08/2022**			
Variable	Formula			
Reportes		$VI = \frac{VINE}{VID} \times 100$		
Indicador	Medida	VI: control informático		
control informático (RE-TEST)	Porcentaje	VINE: total controles informáticos VID: total controles aplicados en el día		
ÍTEM	**FECHA**	**TEBMDS**	**EBMDR**	**EBMD %**
1	01/08/2022	6	8	75
2	02/08/2022	4	10	40
3	03/08/2022	6	9	67
4	04/08/2022	5	10	50
5	05/08/2022	4	10	40
6	06/08/2022	3	9	33
7	07/08/2022	4	10	40
8	08/08/2022	4	10	40
9	09/08/2022	5	8	63
10	10/08/2022	4	10	40
11	11/08/2022	4	9	44
12	12/08/2022	4	10	40
13	13/08/2022	4	10	40
14	14/08/2022	3	8	38
15	15/08/2022	6	10	60
16	16/08/2022	4	9	44
17	17/08/2022	3	10	30
18	18/08/2022	5	8	63
19	19/08/2022	4	10	40
20	20/08/2022	5	9	56
	TOTAL	87	187	
	PROMEDIO			**47**

Anexo 20

Fichas de registro pos test

Investigador				
Empresa				
Dirección				
Fecha de inicio	**01/09/2022**			
Fecha de terminación	**20/09/2022**			
Variable	Formula			
Reportes		$VI = \frac{VINE}{VID} \times 100$		
Indicador	Medida			
control informático (POST-TEST)	Porcentaje	VI: control informático VINE: total controles informáticos VID: total controles aplicados en el día		
ÍTEM	**FECHA**	**TEBMDS**	**EBMDR**	**EBMD %**
1	01/09/2022	1	8	13
2	02/09/2022	2	9	22
3	03/09/2022	1	9	11
4	04/09/2022	1	7	14
5	05/09/2022	1	9	11
6	06/09/2022	0	8	0
7	07/09/2022	0	7	0
8	08/09/2022	0	8	0
9	09/09/2022	0	7	0
10	10/09/2022	1	8	13
11	11/09/2022	1	8	13
12	12/09/2022	1	8	13
13	13/09/2022	1	9	11
14	14/09/2022	2	7	29
15	15/09/2022	0	8	0
16	16/09/2022	0	8	0
17	17/09/2022	2	7	29
18	18/09/2022	2	8	25
19	19/09/2022	2	9	22
20	20/09/2022	1	8	13
	TOTAL	19	160	
	PROMEDIO			**12**