FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

"IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO IEC/27002, PARA OPTIMIZAR LA GESTIÓN EN LA CORTE SUPERIOR DE JUSTICIA DE LIMA"

Trabajo de suficiencia profesional para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autor:
Ruben Eduardo Rumiche Huamani

Asesor:
Mg. Ing. Jorge Alfredo Bojórquez Segura

Lima - Perú

2021

DEDICATORIA

A Dios

Por permitirme despertar cada día, por darme la dicha de tener a mis padres con vida, por haberme regalado dos hijos maravillosos, por darme la oportunidad de tener una buena pareja y compañera quién día a día me anima a seguir adelante, por darme aliento, fuerza, salud, perseverancia, paciencia, y, sobre todo, siempre estar conmigo en los momentos difíciles que me tocó afrontar desde que la conocí.

A mis padres,

Quienes siempre confiaron en mí, me supieron inculcar buenos valores, me enseñaron que la vida no es fácil, y que hay que luchar mucho para alcanzar las metas, por qué siempre están pendientes de mí, así sea ya un niño grande para ellos, por la vida que me dieron.

A los profesores.

Quienes, con sus excelentes conocimientos, paciencia y consejos, supieron llegar a los alumnos y en mí persona, siempre fueron motivos y ejemplos a seguir.

Ya que fueron y serán un gran aporte para todos aquellos que deseen alcanzar sus sueños, aprendiendo de sus conocimientos y experiencias en sus carreras y también en sus vidas.

A mis hermanos y amigos.

Mis hermanos, quienes fueron ellos los que día a día estuvieron dándome aliento y consejos para no declinar ante el reto universitario, mis amigos quienes, con su apoyo moral y académico, siempre supieron apoyarme.

El autor

AGRADECIMIENTO

Un profundo agradecimiento a todas las personas que me apoyaron, moral, académica y económicamente en este gran reto que emprendí años atrás cuando inicié la carrera universitaria. A mis compañeros de trabajo, quienes sabiendo el arduo trabajo que desarrollo en mi centro laboral, se dieron tiempo para cubrirme y darme espacios para desarrollar las tareas de algunos cursos.

A las personas que me apoyaron con sus buenos consejos, cuando se enteraban que me encontrara estudiando, ya que gracias a ese entusiasmo que mostraban, me animaban a llegar a la meta trazada.

A la Universidad Privada del Norte, la cual me dio la oportunidad de retomar los estudios y completar mi formación profesional, dando opción a los adultos que trabajamos, avanzar académicamente para el bien personal, de la sociedad, y ser un ejemplo para los jóvenes, que nunca es tarde para estudiar

Tabla de contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El trabajo de investigación realizado en la Corte Superior de Justicia de Lima, tuvo la intención de conocer los riesgos y vulnerabilidades y posteriormente tuvo el objetivo de implementar un plan de Seguridad Informática en la institución, tomando como referencia la norma internacional ISO IEC 27002:2013, la cual encierra políticas y lineamientos que permitirá mejorar el nivel y establecer una cultura en la seguridad de la información.

Para obtener mejores resultados sobre la situación tecnológica, se utilizó la técnica de encuesta para reunir información por las constantes fallas de los sistemas informáticos, a fin de evaluar la necesidad de implementar un plan de seguridad informática.

El resultado de dicha encuesta es que no se aplica una política interna en la seguridad informática, así como no cuenta con controles permanentes en el parque informático y desconocimiento en el uso de la norma ISO 27002:2013.

Las vulnerabilidades y riesgos que se presentan en los sistemas de información que administra la Corte Superior de Justicia de Lima, son muy frecuentes, y se espera que, cumpliendo con políticas y estrategias adecuadas, se podrá afrontar cualquier eventualidad o ataque futuro, siendo conscientes de la importancia que representa la información en toda institución pública o privada.

Palabras claves:

Seguridad de la información, ISO 27002, SGSI, Seguridad Informática.

ABSTRACT

The research project carried out at the Corte Superior de Justicia de Lima, intend to know risks and vulnerabilities and the subsequent objective of implementing a Computer Security plan in the institution, taking as reference the international standard ISO IEC 27002: 2013, that contains policies and guidelines that will improve the level and establish a culture of information security.

To obtain better results on the technological situation, the survey technique was used to gather information for the frequent failures of the computer systems, in order to evaluate the need to implement a computer security plan.

The result of this survey shows that the internal policy on computer security is not applied, as well as it does not have permanent controls in the computer park and unawareness in the use of ISO 27002: 2013.

The vulnerabilities and risks that arise in the information systems managed by the Corte Superior de Justicia de Lima are very frequent and it is expected that fulfilling with appropriate policies and strategies, any eventuality or future attack can be faced, being aware of the importance of information in any public or private institution.

KEY WORD:

Security of the information, ISO 27002, SGSI, Informatic security.

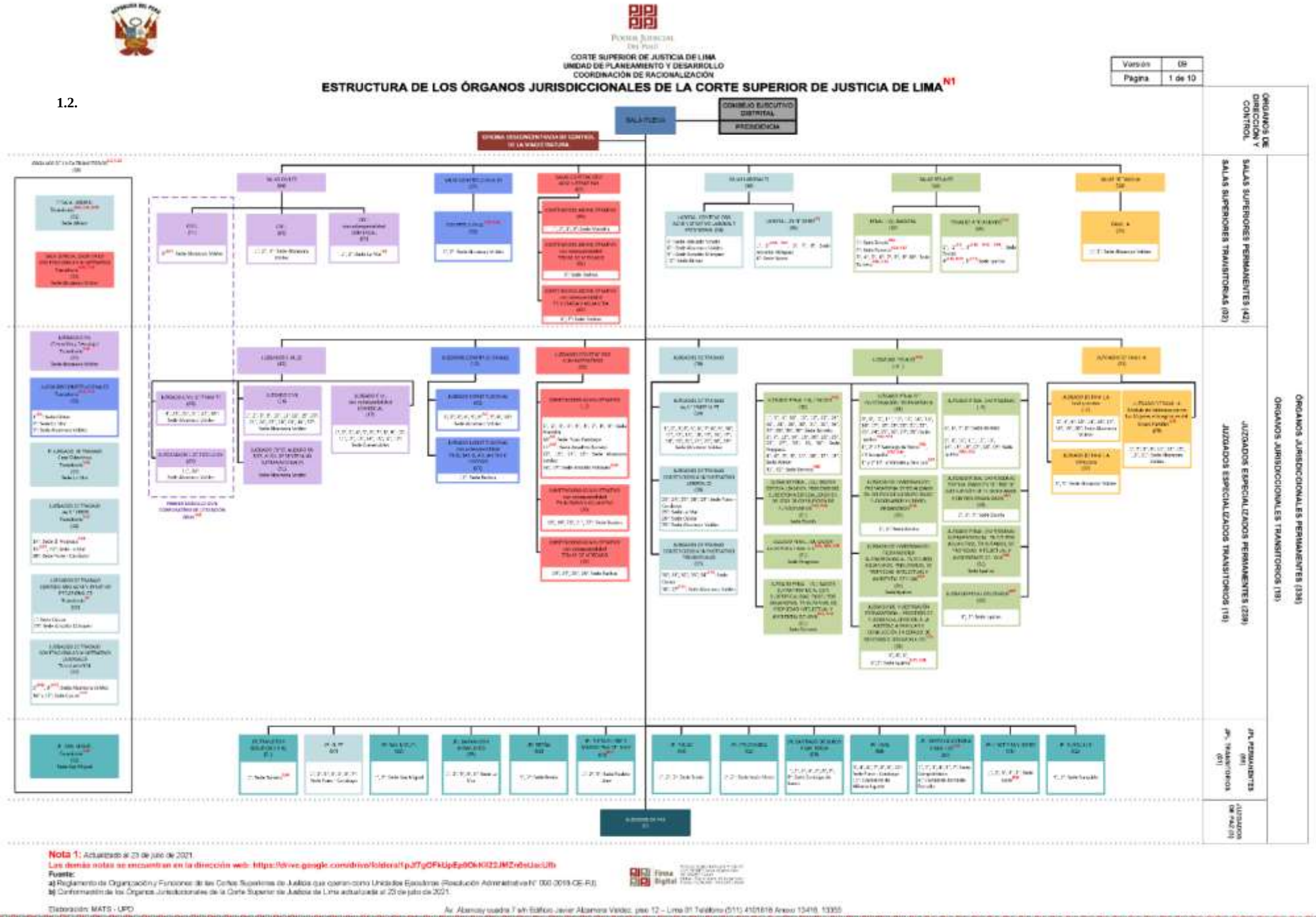
CAPÍTULO I.

1.1. Introducción

La Corte Superior de Justicia de Lima, es la corte más grande e importante del Perú, esto es, porque abarca la mayor cantidad de personal que la conforman y por ende, la mayor carga procesal de país, tiene un entorno laboral con alta presión y con profesionales de gran nivel, desplegados en las áreas jurisdiccionales y administrativas, esto amerita un trabajo de investigación como integrante del equipo de informática al que pertenezco, con una experiencia profesional en el área de más de ocho años, y con los permisos correspondientes de parte de las autoridades administrativas, en búsqueda de determinar el nivel de seguridad de la información, invocando para esto, la norma ISO IEC /27002 , con la cual se busca optimizar la gestión en esta entidad judicial.

El trabajo de investigación tuvo la problemática que por el estado de emergencia que se viene atravesando, se priorizo el trabajo remoto en gran parte de los trabajadores de la entidad judicial, con lo cual en muchos aspectos se vulnera la seguridad informática ya que todos los usuarios utilizan en VPN de conexión con una contraseña universal exponiendo la información a ataques mal intencionados de parte de terceros o personal de la institución.

1.2.



Fuente. (ROF . Corte Superior de Justicia de Lima – 2018)

1.3. ORGANIGRAMA ESTRUCTURAL – CORTE SUPERIOR DE JUSTICIA QUE OPERA COMO UNIDAD EJECUTORA

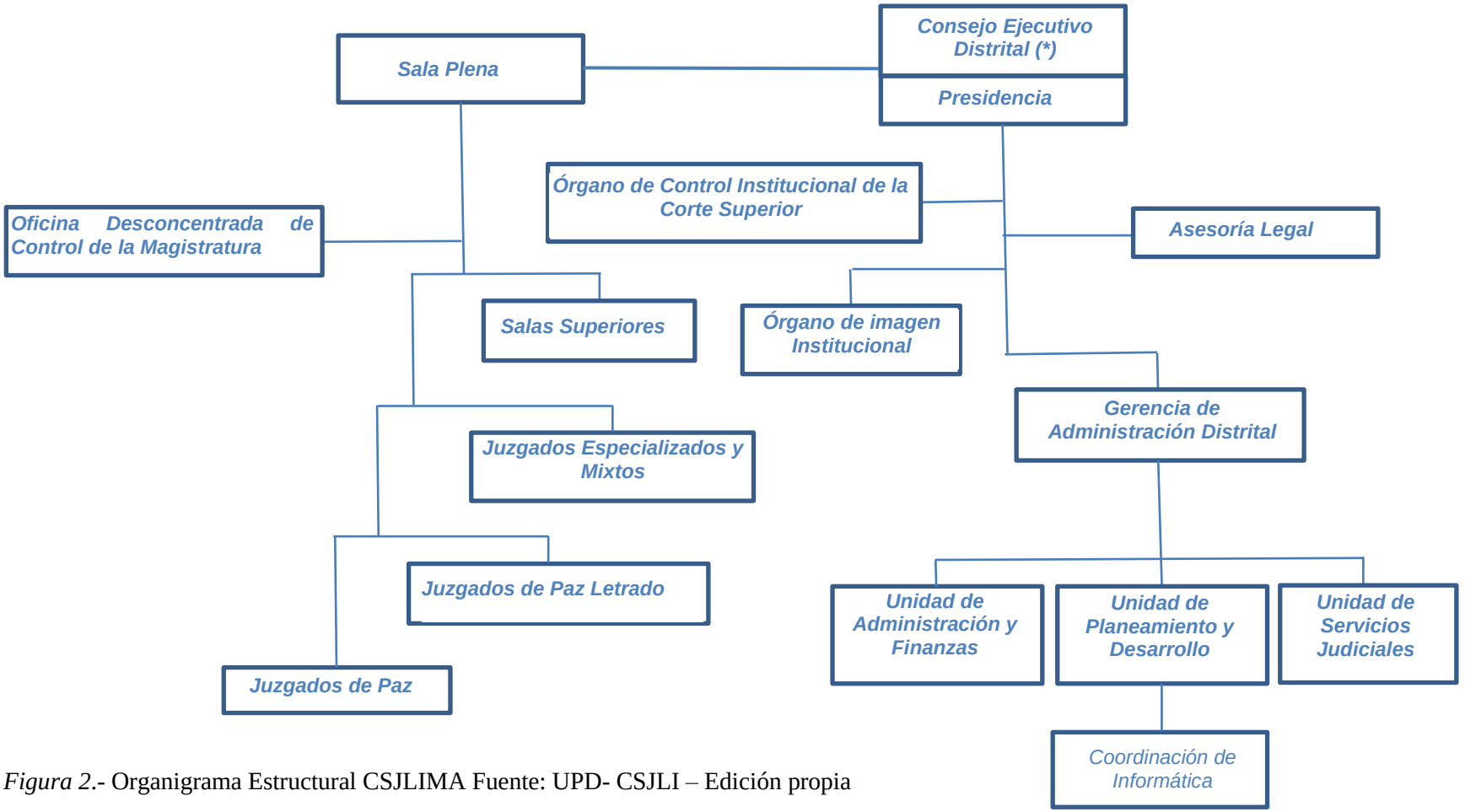


Figura 2.- Organigrama Estructural CSJLIMA Fuente: UPD- CSJLI – Edición propia

1.1. Realidad problemática

La Corte Superior de Justicia de Lima creada el 22 de diciembre de 1824, fue denominada Alta Cámara por el libertador Don José de San Martín y es una de las 34 cortes a nivel nacional que conforman el Poder Judicial del Perú, y es de acuerdo a la constitución y las leyes, la institución que tiene como función administrar justicia a través de sus órganos jurisdiccionales, y de acuerdo a la ley orgánica del Poder Judicial serían los siguientes:

1.- La Corte Superior de Justicia de Lima, la cual comprende:

- Salas Superiores
- Juzgados de Primera Instancia o especializados, y
- Juzgados de Paz Letrado

Dicha ley define los derechos y deberes de los magistrados, el cual sus funciones es de administrar justicia; de los justiciables, que aquellos que están siendo juzgados o quienes están solicitando justicia, y de los trabajadores jurisdiccionales cuya función es brindar apoyo a la labor de los integrantes de la magistratura.

El levantamiento de información realizado en la sede principal a las diferentes dependencias de la Corte Superior de Justicia de Lima, sobre las quejas de los trabajadores y usuarios finales que es el público justiciable, se basa que la red de área local (LAN) y la red de área extendida (WAN), en varias ocasiones pierda el enlace, o el SIJ (Sistema de Integración Judicial) se cuelgue, ocasionando congestión en colas del público en general, y si la caídas son por un periodo prolongado, provoca la incomodidad de más de 5,000 usuarios que trabajan en la Corte Superior de Justicia de Lima; y no solo el malestar del público en general, si no también que se podría presentar ataques informáticos ya sea a través de virus informático, ingeniería social, códigos de inyección SQL, correos maliciosos o mal intencionados al correo institucional u otro tipo de ataque informático; lo

cual sumado al mal uso de las herramientas informáticas por algunos colaboradores que laboran en la institución, y por la actual pandemia que atraviesa el mundo con el COVID 19, la seguridad de los equipos se volvió más vulnerable, ocasionando en muchos casos, pérdida de información involuntaria y/o provocadas, logrando con esto un peligro latente y diario en la red, equipos e información de la institución.

Frente a esta realidad existente se desprende la importancia de que como entidad que administra justicia, se reduzca las posibles caídas del Sistema de red, así también las vulnerabilidades a los sistemas informáticos de la institución.

Un plan de mejoras de seguridad y de buenas prácticas bien estructuradas y adecuadamente desplegadas es una solución rápida, confiable y efectiva para la protección de los activos de cualquier empresa pública o privada.

El presente proyecto de investigación se titula **"Implementación de un plan de Seguridad Informática basado en la norma ISO IEC 27002, para optimizar la gestión en la Corte Superior de Justicia de Lima"**.

Con el uso de esta norma la cual está orientada a administrar y ordenar la gestión de las empresas de los distintos ámbitos, se buscará reunir la información necesaria para implementar un plan de seguridad informática de acuerdo a la norma ISO/IEC:27002, para proteger los activos de la información y otorgar una mitigación del riesgo a los usuarios de la Corte Superior de Justicia de Lima del Poder Judicial del Perú.

Según Knapp, et al (2009), En el contexto internacional existen varios modelos estandarizados relacionados con la seguridad de la información tales como ISO 27002, OSSTMM, COBIT, entre otros; mecanismos basados en software para la implantación de un SGSI, los cuales son muy genéricos y globales. (ver tabla 1).

Tabla 1.- *Contratación de los Sistemas de apoyo a SGSI existentes*

Herramienta	BABEL	E-PULPO	MEYCOR COBIT KP	SECUWARE SECURITY	GLOBALSGSI	GXSGSI	GAP ISO 27001	SECURIA SGSI
Creador	ÁRTICA	INGENIA	DATASEC	SECUWARE	AUDISEC	SIGEA	SIGEA	SECURIA
Licencia	Open Source	GNU GPL v2	Comercial	Comercial	Comercial	Comercial	Comercial	GPL v2
Sistemas operativos en los que funciona	GNU/Linux, IBM AIX, Sun Solaris, OpenSolaris, SPARC, Windows	GNU/Linux	Windows	Windows	Windows	Windows	Windows	GNU/Linux, Windows
Estándares de seguridad	SOX/LOPD, ISO 27001, COBIT	ITIL, LOPD, ENS, ISO 27001, ISO 27002, ISO 20000	ISO I27001, COBIT, ISO 27002, ISO 20000, COSO I, COSO II	Ninguno. Suite empresarial para proteger la información en el puesto de trabajo.	ISO 27001	UNE 71502, ISO 27001	ISO 27001, ISO 27002	ISO 27001
Gestión documental	✓	✓	✓	×	✓	×	×	✓
Gestión de incidencias	✓	✓	✓	×	✓	✓	×	✓
Auto-evaluación de controles	✓	×	✓	×	✓	×	×	✓

Fuente: Sistema de administración de controles de Seguridad Informática basado en la ISO/IEC 27002 - Diana C. Franco - César D. Guerrero (2013)

1.4. Antecedentes

1.4.1. Antecedentes Nacionales

Celis (2018) Plan de seguridad de la información aplicado a la central hidroeléctrica Carhuaquero.

Resumen: La presente investigación surge como alternativa de solución frente al problema de seguridad de la información que tiene la Unidad de Producción Hidráulica de la referida organización. El Plan de Seguridad compromete la organización de los procesos de la citada Unidad, puesto que la correcta gestión de seguridad de la información puede marcar la diferencia entre la eficacia y la inoperancia. En cuanto a la metodología utilizada debemos señalar que después de una sutil comparación con las ya existentes en este campo, se optó por aquella denominada MAGERIT; la misma que permitió el análisis y gestión de riesgos. También, se utilizó la herramienta EAR-PILAR que ayudó en la toma

de las mejores decisiones frente al problema de seguridad de la información. Finalmente, después de haber recogido información fidedigna producto de una exhaustiva investigación, se concluyó que el Sistema de Gestión de Seguridad de la Información (SGSI) es un soporte importante que ayuda a organizar los procesos, controles y salvaguardas de la Unidad de Producción Hidráulica de la Central Hidroeléctrica Carhuaquero; y al mismo tiempo hace posible mantener la información bajo medidas de seguridad, garantizando su integridad, confidencialidad y autenticidad.

Escalante (2018) Conflictos entre la gobernabilidad y la soberanía en organizaciones multilaterales: estudio de la implementación de políticas de seguridad informática entre los años 2004 - 2016 en la Unión Europea

Resumen: El presente trabajo estudia y analiza las causas de la inexistencia de políticas públicas comunitarias en la Unión Europea que garanticen de manera eficaz la seguridad y gobernabilidad informática tanto de los países miembros como de la organización comunitaria en sí. Los espacios cibernéticos e informáticos y sus aplicaciones en nuestra vida diaria van en continuo progreso y aumento, cada vez más espacios de nuestra vida cotidiana y, por ende, ciudadana se ven penetrados por el desarrollo tecnológico, cibernético e informático. Esto también supone la participación del Estado como usuario y regulador en su contexto nacional como en el espacio internacional. El fenómeno tecnológico y su impacto en la política viene siendo analizado en espacios académicos focalizados y la bibliografía especializada en la materia, escaza aún, por ejemplo, ya analiza el uso de herramientas de inteligencia artificial para la definición de la política exterior de los Estados a la par de que actualmente se vienen creando unidades especializadas en las fuerzas armadas de diferentes países ya que se considera al

ciberespacio como un área de desarrollo militar como ya lo son el aire, mar y tierra. En ese contexto, en el que se vienen trasladando temas propios del denominado “highpolitics” al ciberespacio y sus implicancias, ¿por qué la Unión Europea no ha podido diseñar e implementar políticas públicas comunitarias y eficaces que garanticen la seguridad y gobernabilidad informática? La presente tesis hace un breve recuento del estado de la cuestión en la materia, así como una revisión cualitativa de los planes y regulaciones comunitarias existentes, así como del estado de avance y desarrollo de la materia en los países hegemónicos y relevantes en el proceso de toma de decisiones en la Unión Europea (Alemania, Francia y Reino Unido). Los resultados principales obtenidos en la presente investigación, a la luz de la tradición realista de las relaciones internacionales, muestran que la interacción de los intereses nacionales de los países impide un desarrollo comunitario en la materia y, paradójicamente, los expone a mayores vulnerabilidades. Estos intereses se basan en las diferentes concepciones de seguridad que tengan los países como en variables identitarias que tienen un rol trascendente en la determinación de políticas e intereses nacionales y en el cómo se armonizan o no con las políticas e intereses comunitarios.

Huanca (2018) La falsa percepción en la seguridad de los sistemas informáticos

Resumen: El presente trabajo aborda temas de seguridad e inseguridad en los sistemas informáticos, debido a la incertidumbre sobre la percepción de seguridad existente. Se espera cumplir con la con la confidencialidad, integridad y disponibilidad de la información según ISO 27001, esto se aplica en diversos escenarios de desarrollo de software en forma empírica, estos requerimientos toman mayor valor en la administración de datos de entidades públicas y privadas, debido a que la ausencia de la seguridad en los

sistemas desestabiliza el orden social global. El presente trabajo se asocia a un grupo de Mypes muestreadas, en el cual se evidencia la inseguridad, debido al modo de desarrollo de sus procesos para el aseguramiento de la información. En cuanto al método se evaluaron cuatro tratamientos tecnológicos en dos factores fijos midiendo así el grado se seguridad e inseguridad en las Mypes a través del Diseño Factorial Completamente al Azar. Los cuatro tratamientos han sido aplicados al grupo muestral, buscando así identificar diferencias entre los tratamientos. En cuanto a los resultados y según el planteamiento de la hipótesis general, la prueba de Análisis Factorial Univariante resultó no significativo P-valor > nivel se significancia, lo que conlleva a indicar como conclusiones que no es suficiente suministrar tratamientos tecnológicos físicos y lógicos a las Mypes muestreadas, esto si el personal que los dirige no tiene solvencia académica requerida para el desarrollo adecuado de los protocolos de seguridad, planes de gestión tecnológica y sistemas de gestión de seguridad de la información, las cuales contribuyen en el aseguramiento de la información.

Sandoval (2019) Modelo de buenas prácticas aplicando ISO 27002 para gestión de incidencias de la red Wncor.

Resumen: La presente investigación dio respuesta al problema general "¿De qué manera el modelo de buenas prácticas aplicando ISO 27002 mejorará la gestión de incidencias de la red Wncor?", el objetivo general fue "Implementar un modelo de buenas prácticas aplicando ISO 27002 para mejorar la gestión de incidencias de la red Wncor; y la hipótesis general que se contrastó fue "La Implementación un modelo de buenas prácticas aplicando ISO 27002 mejorará la gestión de incidencias de la red Wncor." El método de investigación fue el científico, el tipo de investigación fue aplicada, el nivel de investigación fue correlacional, el diseño de la investigación fue pre experimental, se

trabajó con una población que fue de 500 usuarios de los cuales se tomó un muestreo probabilístico de 40 usuarios. Finalmente se llegó a la conclusión general: Con la implementación del modelo de buenas prácticas aplicando ISO 27002 mejoró la gestión de incidencias de la red Wncor.

Palomino (2017) Buenas Prácticas en Seguridad de la Información Basada en ISO 27002 en la Asociación Para el Desarrollo Empresarial en Apurímac – ADEA

Resumen: En el presente informe de experiencia profesional se describe un proyecto de implementación de buenas prácticas en seguridad de la información basada en ISO 27002, para la Asociación para el Desarrollo Empresarial en Apurímac – Andahuaylas y Chincheros. Dicha entidad ofrece varios servicios, siendo el más importante de ellos el rubro de servicios financieros, donde hace uso de herramientas tecnológicas para la automatización de sus procesos, por lo cual actualmente tiene alta dependencia de la misma. En dicho contexto, se procedió a realizar la identificación del estado actual de la seguridad de la información, mediante la verificación de los objetivos de control de la norma ISO 27002 en ADEA, además se tuvo que hacer uso de los niveles de madurez del CMMI, haciendo un modelo que esquematice mejor el objetivo del proyecto.

García & Del Águila (2017) Análisis e implementación de la seguridad de la información del centro de datos de la Universidad Nacional de la Amazonía Peruana bajo la norma ISO 27002.

Resumen: Mediante la elaboración del análisis de seguridad de la información y seguridad informática basada en la norma ISO/IEC 27002, el presente trabajo tuvo como finalidad conocer las vulnerabilidades a las que está expuesta la información por la falta de

aplicación de controles de seguridad. El análisis estuvo dirigido al centro de datos de la oficina general de informática de la UNAP, teniendo como objetivo principal el estudio de seguridad en los procesos críticos. A través de reuniones, revisión de documentación, consultas, observación, encuestas y ejecución de entrevistas con directivos que poseen un amplio conocimiento del negocio, se logró identificar los riesgos actuales a los que se exponen los datos tanto físicos, lógicos y sistemas de procesamiento de información. La ejecución del análisis de riesgos da a conocer el nivel de impacto que tendría la ocurrencia de las amenazas identificadas en cada activo de la información que pueden afectar datos relevantes utilizados o resultantes de la ejecución de las actividades propias del negocio. Los resultados obtenidos dan a conocer que, para minimizar los riesgos existentes, es necesario implementar controles de seguridad, lo cual ayuda a fortalecer tres aspectos importantes: la confidencialidad, integridad y disponibilidad de la información. Pero los resultados también muestran la importancia del compromiso y trabajo en equipo que debe tener la institución.

Cortez (2018) Plan de seguridad informática basado en la norma ISO 27002 para mejorar la gestión tecnológica del colegio carmelitas – Trujillo

Resumen: El presente trabajo de investigación titulado “Plan de Seguridad Informática basado en la Norma ISO 27002 para mejorar la Gestión Tecnológica del Colegio Carmelitas – Trujillo”, se ha realizado con la finalidad de mejorar la gestión tecnológica en los aspectos de seguridad informática (hardware, software, operaciones y servicios), que forma parte a su vez de la seguridad de la información.

Entre los objetivos específicos planteados para esta tesis se tuvo: gestionar de manera segura todos los activos de la institución, controlar los accesos a los recursos informáticos

de la institución, definir políticas de cifrado, establecer la seguridad física y ambiental en toda la institución, establecer la seguridad en las operaciones del negocio, establecer la seguridad en las telecomunicaciones y definir medidas adecuadas para la adquisición, desarrollo y mantenimiento de los sistemas de información..

El diseño de la investigación ha sido No Experimental, Transversal debido que la recolección de datos se realizará en un único momento. El esquema del diseño de investigación fue descriptivo simple. La metodología utilizada para el desarrollo de la presente tesis se basa en el uso de los controles de seguridad a nivel operativo de la norma internacional ISO 27002:2013, los cuales corresponden a un plan de seguridad informática propiamente dicho. Los controles de seguridad seleccionados fueron: gestión de activos, control de accesos, cifrado, seguridad física y ambiental, seguridad en las operaciones, seguridad en las telecomunicaciones y adquisición, desarrollo y mantenimiento de los sistemas de información.

En cuanto a los logros obtenidos, éstos se encuentran plasmados en las conclusiones de la presente tesis, donde cada uno de ellos permite observar, medir y cuantificar el cumplimiento de los objetivos planteados al inicio de la presente investigación.

Gavidia (2018) Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte.

Resumen: Esta tesis tiene por objetivo mejorar el nivel de seguridad física y lógica de la información del área de TI de la Unión Peruana del Norte. En conjunto con la norma ISO/IEC 27002:2013, se utilizó el Framework Objetivos de Control para la información y tecnologías relacionadas (COBIT). Se implementó una metodología de elaboración propia,

para el desarrollo del proyecto, la cual se complementó en 5 fases. Cada fase contó con la aprobación de especialistas en el tema para corroborar la veracidad de la implementación, además, cada fase contiene actividades para desarrollar y cumplir con la mejora en seguridad. En la fase 1 se desarrolló el compromiso con la organización para la implementación del proyecto. En la fase 2 y 5 se realizó la evaluación preliminar y la evaluación final. En la fase 3 se desarrolló el análisis de acuerdo a lo que menciona la norma ISO/IEC: 27005 para la identificación y medición de riesgos, que abarca sobre la identificación de activos, amenazas y vulnerabilidades. En la fase 4 se realizó la implementación de los controles seleccionados de la ISO/IEC 27002:2013. La implementación de los controles de la ISO/IEC 27002:2013 permite mejorar el nivel de seguridad de la información del área de Tecnologías de Información (TI) de la Unión Peruana del Norte (UPN), permitiendo que el área de TI cumpla con el objetivo trazado para el desarrollo y beneficio de la organización, haciendo que la información se encuentre protegida y segura en su uso, almacenamiento, procesamiento y distribución.

López (2015) Sistema de Control basado en COBIT para la certificación SOX. Caso: AFP en Perú.

Resumen: La tesis tiene como objetivo establecer un marco de trabajo estándar y homologado en la organización para la gestión de tecnología, así como también de la gestión de riesgos tecnológicos, con la finalidad de implementar controles que permita la certificación Ley Sarbanes-Oxley (SOX). Para ello, el estudio se aplica a una Empresa Administradora de Pensiones (AFP) y a través del método del test al área de tecnología se busca detectar la situación actual de gobierno TI. La investigación considera tres pilares fundamentales para la implementación de SOX: Cobit (Guía a seguir sobre trabajo de

dominios y procesos), ISO 27002 (buenas prácticas a seguir sobre seguridad de la Información) e Itil (InformatiónTechnologyInfraestructure Library proporciona un planteamiento sistemático para la provisión de servicios de TI con calidad). Finalmente, se realiza una autoevaluación para poder mantener los controles en el tiempo.

Martínez (2014) Controles de seguridad para reducir la cantidad de incidencias de seguridad de la información del año 2012 en el servicio de administración tributaria de Huancayo.

Resumen: La Tesis titulada "Controles de Seguridad para reducir la cantidad de incidencias de seguridad de la información del año 2012 en el servicio de Administración Tributaria de Huancayo" se realizó principalmente con la finalidad de preservar la seguridad de los activos de información en sus 3 dimensiones (la confidencialidad, integridad y disponibilidad) mediante la implementación de mecanismos apropiados de seguridad frente a eventos externos e internos que podrían materializarse como incidentes causando daños. El Servicio de Administración Tributaria de Huancayo como institución gubernamental hace el uso de la información en su estado digital y físico, el mismo que se encuentra soportada por los recursos de tecnologías de información, recursos humanos, infraestructura física, servicios de terceros, entre otros. Por ende, la información que es considerada como uno de los activos más importantes de la organización debe ser preservada y protegida de las amenazas que al materializarse como incidencias podrían comprometer la seguridad. En tal sentido, dentro del presente trabajo se realizó el análisis de riesgos para identificar a los activos de información que necesitan ser protegidos, las amenazas que acechan, el impacto que causaría la materialización de una amenaza, las vulnerabilidades de los activos, y el nivel de riesgo al que se encuentran expuestos.

Finalmente, en base a la ISO/IEC 17799(27002):2005 "Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información", la institución implementó cierta cantidad de controles de seguridad, para mitigar el nivel de riesgo de los activos y reducir las incidencias registradas, que de lo contrario podrían dificultar el normal funcionamiento de la organización.

1.4.2. Antecedentes Internacionales

Franco, D. C., & Guerrero, C. D. (2013). Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002.

Resumen: La gestión de la seguridad de la información es un factor cada vez más determinante en la competitividad de las organizaciones. La gestión del riesgo y el aseguramiento de la información se apoyan en la aplicación de normas internacionales como el estándar ISO/IEC 27002. El proceso de implementación de la norma y su gestión permanente se facilita a través del uso de software que en la actualidad es mayoritariamente comercial. La restricción de idioma, poca documentación y limitada disponibilidad de software abierto que se ajuste a requerimientos particulares de organizaciones en el contexto latinoamericano, limita la aplicación de la norma y la efectividad de su uso. Este artículo presenta una plataforma web abierta denominada SGCSI que permite apoyar la gestión de controles de seguridad de la información de acuerdo con el estándar ISO 27002. Tras la evaluación comparativa del uso de la plataforma por parte de expertos y aprendices en seguridad, se pudo evidenciar su efectividad en la auditoría sobre el cumplimiento de los 32 objetivos de control establecidos por la norma.

Valencia & Orozco (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000.

Resumen: Se propone una metodología de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la familia de normas de la ISO/IEC 27000, con énfasis en la interrelación de cuatro normas fundamentales a través de las cuales se desarrollan las actividades requeridas para cumplir con lo establecido en la ISO/IEC 27001, los controles de seguridad presentados en la ISO/IEC 27002, el esquema de riesgos de la ISO/IEC 27005 y los pasos recomendados en la ISO/IEC 27003. Se genera como resultado un proceso metodológico que da respuesta al cómo abordar un proyecto de este nivel de importancia en el contexto actual de las organizaciones y basado en estándares internacionales. Este proceso metodológico representa un aporte a los profesionales que emprenden esta labor, y que buscan un método para una implementación exitosa de un SGSI.

Ramos, Y., Urrutia, O., Bravo, A., & Ordoñez, D. (2017, July). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002: 2013 para la Cooperativa Codelcauca.

Resumen: El desarrollo del presente proyecto denominado “Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la cooperativa CODELCAUCA”, tiene como objetivo principal la adopción e implementación de políticas de seguridad de la información teniendo en cuenta la norma 27002:2013, las cuales servirán como guía para proporcionar herramientas que

contribuyan a mejorar la gestión de la información obtenida, generada o procesada en CODELCAUCA., la política de seguridad facilitará la adopción de lineamientos necesarios para garantizar la seguridad de la información teniendo las directrices establecidas en los objetivos de control 5.1.1 y 5.1.2 relacionados con políticas de seguridad y sustentados en los objetivos de la empresa. Teniendo en cuenta este planteamiento se tendrá presente los procesos y procedimientos, como: registro de incidencias, respaldo de la información, registro de incidencias, respaldo de la información, mantenimiento de equipos y copias de seguridad. Para los cuales se partirá teniendo en cuenta los criterios relacionados con política de seguridad, gestión de activos, control de acceso, seguridad física y ambiental, seguridad relacionada con el personal, teniendo en cuenta los dominios establecidos en el anexo A de la NTC ISO/IEC 27001:2013. Finalmente hay que destacar que este trabajo se desarrolla entre la Institución Universitaria Colegio Mayor del Cauca y el la Cooperativa Codelcauca, en un proceso de integración de la academia con el sector productivo de la ciudad de Popayán.

Aliaga Flores, L. C. (2013). Diseño de un sistema de gestión de seguridad de información para un instituto educativo.

Resumen: En el transcurrir de las últimas décadas, el tema de la seguridad de información se ha convertido en un aspecto vital en la gestión de las organizaciones. Conforme van saliendo a la luz incidentes de seguridad que afectan a grandes empresas internacionalmente reconocidas, la sociedad cada vez más va tomando conciencia de la importancia y el valor que representa la información. Estas incidencias ocurrieron con mayor frecuencia en la década del 2000 con los famosos “Wikileaks”, los cuales, entre otros informes, publicaron diversos documentos de gobiernos de distintos países con

contenido muy confidencial. Frente a esta realidad, se observa que el no contar con un programa de seguridad de información que brinde las garantías necesarias para la información en cualquier organización, en medio de un mercado tan competitivo como el actual, representa una desventaja considerable frente a empresas del mismo rubro que sí trabajan el tema dentro de su cultura organizacional. Esta desventaja podría traer pérdidas muy graves, tales como la pérdida de un número importante de clientes o de acuerdos laborales con otras empresas, lo cual afectaría principalmente la parte financiera de la organización, y finalmente podría, si las pérdidas llegan a ser críticas, llevar a la quiebra al negocio. En el caso de instituciones educativas, se puede observar que éstas aún no toman a la seguridad de información como prioridad. Así como también se observa que no existe una cultura de seguridad transversal en dichas entidades. Si bien es cierto que aún no existe una regulación del Ministerio de Educación, no se tendría que esperar que el tema se regule para que recién tomar acción en el establecimiento de controles para mitigar o reducir los riesgos a los que la información de estas entidades está expuesta. Bajo este contexto, el presente proyecto brinda como alternativa el diseño de un Sistema de Seguridad de Información (SGSI) para una institución educativa de nivel superior, tomando la realidad de una entidad educativa local. La presente tesis se enfoca en proteger la información de los procesos principales de esta institución educativa siguiendo normas internacionales vigentes.

Tasinchana, C., & Maribel, S. (2017). Análisis e Implantación de la norma ISO/IEC 27002: 2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo.

Resumen: En el proyecto de investigación se presenta la experiencia obtenida en la aplicación de técnicas a fin de obtener información acerca de la norma ISO/IEC 27002:2013 en las organizaciones gubernamentales donde el objetivo es desarrollar habilidades que beneficie a la infraestructura tecnológica y humana dentro de la edificación protegiendo la seguridad de la información. Por lo que se llevó a cabo un análisis de encuestas, entrevistas para obtener los efectos que causan el manejo de la información sin una estrategia planificada de tal manera que, los resultados deben ajustarse a los estándares utilizados en la investigación para mejorar el rendimiento del personal que labora dentro de la organización; Se realizó un análisis dentro de la infraestructura tecnológica de la Institución donde se observó muchas falencias en cuanto al manejo de la información y mediante la investigación se estableció un plan estratégico para corregirlas y con esto lograr impulsar los controles de seguridad para que sean integrados acorde a las necesidades de la organización.

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas

Resumen: La seguridad informática permite a las organizaciones proteger sus recursos financieros, sistemas de información, reputación, situación legal, y otros bienes tangibles e intangibles. El objetivo principal de este trabajo es desarrollar un modelo de simulación que permita evaluar el nivel óptimo de seguridad que deben tener las organizaciones considerando aspectos relacionados con la reducción del riesgo y la obtención de beneficios empresariales. La técnica empleada para la construcción del modelo fue dinámica de sistemas, la cual permite modelar y analizar el comportamiento de sistemas complejos en el corto, mediano y largo plazo. El modelo fue construido con el software

"POWERSIM", que es un ambiente integrado para la construcción y utilización de modelos de simulación de negocios. Con el desarrollo del modelo se concluye que, si las organizaciones no cuentan con un plan director que guíe los esfuerzos de protección de los activos, por mucho dinero que inviertan en seguridad nunca alcanzarán niveles de seguridad satisfactorios.

Suárez, D., & Fontalvo, A. Á. (2017). Una forma de interpretar la seguridad informática.

Resumen: La seguridad informática actualmente forma parte de los grandes negocios en materia de tecnología y seguridad en las empresas. Debido a que hoy en día se reflejan distintos tipos de ataques y amenazas al acceso de la información de las organizaciones, es necesario crear medidas y procesos que contrarresten estos peligros que afectan los recursos funcionales de las entidades. Por eso, se requiere la disposición de diferentes mecanismos de seguridad que van relacionados con varios tipos de recursos tanto humanos como tecnológicos que ayudan a garantizar una muy buena seguridad en las empresas. El recurso humano entonces, se convierte en un elemento fundamental a la hora de definir pautas de seguridad que garanticen la robustez de un sistema de información. La seguridad de la información es un tema de nunca acabar y que por tal motivo la actualización de los distintos recursos y procesos que se identifiquen día a día es sumamente importante para minimizar los riesgos en el ámbito de seguridad de las organizaciones.

Infante Moro, A., Infante Moro, J. C., Martínez López, F. J., & García Ordaz, M. (2016). Percepción de la importancia de la seguridad informática en la industria

hotelera española. El turismo y la experiencia del cliente: IX jornadas de investigación en turismo.

Resumen: Ante un mundo empresarial cada vez más dependiente de las Tecnologías de la Información y las Comunicaciones (TIC), es conveniente que la seguridad informática tenga un hueco importante en estas empresas para el buen funcionamiento de las mismas. Por este motivo, este artículo analiza esta área, pero en el sector hotelero, un sector que hoy día no se puede concebir sin el uso de las TIC. Este estudio analiza la percepción (por parte de las empresas) de la seguridad informática en el sector hotelero español a través de encuesta en 2 periodos, con un horizonte temporal de 10 años, y utilizando como marco comparativo el sector empresarial español en general. Obteniendo como resultados, la mayor concienciación por esta seguridad informática en el sector hotelero a lo largo del tiempo, ya que, en el primer periodo temporal, la diferencia entre este sector y las empresas españolas en general era bastante amplia.

Haro, C. A. R. (2015). La Seguridad Informática. Ciencia Unemi,

Resumen: Las tendencias actuales sobre tecnologías y sus avances, han dado una serie de facilidades a las personas, tanto en lo laboral como en lo particular, el hogar, lo social, las comunicaciones, etc. permitiendo crear entornos participativos más amplios. La conciencia en el uso de estas tecnologías donde la información que se proporciona es cada vez mayor, sugeriría un cambio de paradigma sobre los hábitos de relacionamiento con los demás. Inicialmente, la idea de una Aldea Global era solamente una teoría que afirmaba que algún día todas las personas podrían estar comunicadas a escala mundial, y no es sino gracias a las redes sociales, que actualmente se tiene acceso a una Aldea Digitalmente Global, pero

¿bajo qué términos y con qué tipo de consecuencias? En las empresas, un programa de seguridad de la información es un plan para mitigar los riesgos asociados con el procesamiento de la misma, ante lo cual la innovación permanente es la clave para mantenerla; poder ir un paso adelante de aquellos que pretenden sustraerla. El presente artículo pretende enfatizar conceptos poco tratados que ayuden en la administración de información a uno de los eslabones más débiles en la cadena de la seguridad: el factor humano.

CAPÍTULO II.

2.1. Marco Teórico

Se hizo la evaluación del parque informático en la Corte Superior de Justicia de Lima, encontrando que por la antigüedad de sus equipos y por la falta de presupuesto, no se ha tomado las previsiones de renovación de estos bienes, habiendo sido la oficina de Informática, específicamente la oficina de Soporte Técnico, quien se dedicó a tratar de implementar con partes de equipos ya sin uso y en algunos casos, reciclados y apoyar en el funcionamiento a los órganos jurisdiccionales, así como administrativos. Asimismo, no se cuenta en los órganos de Paz Letrados los cuales se ubican en los distritos aledaños al centro de Lima, con servidores que administren los usuarios, razón por la cual, en esos juzgados, como en los demás, se implementó un único usuario de inicio de sesión, el cual adquirió perfil de administrador y esto ocasionó que cualquier usuario pueda alterar la configuración de sus computadoras. Por otro lado, también se identificó que un gran número de trabajadores de la institución, que no tienen conocimiento básico en lo que concierne a seguridad de la información ni de la seguridad informática, y en muchos casos, se niegan a aprender el funcionamiento del Windows 7 y 10 y sus utilitarios respectivos razón por la cual, el factor humano es uno de los principales riesgos que exponen la seguridad informática.

Bajo este concepto y luego de la investigación, se piensa implementar un Plan de Seguridad Informática lo cual ayude a la institución a buscar y optar por buenas soluciones y estrategias de seguridad, basándose en los parámetros de la norma ISO 27002:2013, con lo cual se busca establecer mejores controles y buscar solución a las vulnerabilidades con que cuenta la entidad judicial.

Objetivos de la Seguridad Informática

***Figura 3*.- Los 3 pilares de la Seguridad Informática**

Fuente: Giancarlo Gómez Articulo "Los Objetivos de la Ciberseguridad" 2018-CAEN

Sistema de Gestión de la Seguridad de la Información (SGSI)

Su denominación en el inglés "Information Security Management System" (ISMS) lo cual es un conjunto de políticas utilizadas por la ISO/IEC 27001 aprobadas en el año 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission, la cual especifica los requisitos para implementar, establecer, mantener, operar, mejorar, revisar y hacer seguimiento a la seguridad de la información.

2.1.1. Sistema de Gestión

Herramienta, políticas, procedimientos, guías y recursos asociados que le permiten a las empresas u organizaciones mejorar los objetivos y un mejor desempeño en forma ordenada.

El sistema de gestión está compuesto de cuatro grandes conceptos, conocidos como el circulo de Deming, lo cual permite establecer grandes mejoras en los procesos de la empresa.

Figura 4.- Círculo de Deming

Fuente. Instituto de Seguridad y Bienestar Laboral

2.1.2. Norma ISO/IEC 27001:2013

Es un conjunto de lineamientos que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Estos requisitos describen el comportamiento esperado del Sistema de Gestión una vez que esté en pleno funcionamiento. ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un SGSI. Estos requerimientos describen el comportamiento previsto de un SGSI una vez que es completamente operacional. El estándar no es una guía paso a paso sobre cómo construir o crear un SGSI. Javier-Elizabeth., Luna-Henry (2019) Propuesta de guía metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC en la seguridad de la información de la Municipalidad Provincial de Recuay – 2015 (p.30)

2.1.3. Norma ISO/IEC 27002:

Palomino (2017) Buenas prácticas en seguridad de la información basada en ISO 27002 en la asociación para el desarrollo empresarial en Apurímac – ADEA.

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2013 del estándar describe los siguientes catorce dominios principales:

1. Políticas de seguridad.
2. Organización de la seguridad de la información.
3. Seguridad de los recursos humanos.
4. Gestión de los activos.
5. Control de accesos.
6. Criptografía.
7. Seguridad física y ambiental.
8. Seguridad de las operaciones.

   Procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.
9. Seguridad de las comunicaciones.

   Gestión de la seguridad de la red; gestión de las transferencias de información.
10. Adquisición de sistemas, desarrollo y mantenimiento.

    Requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.
11. Relaciones con los proveedores.

    Seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.
12. Gestión de incidencias que afectan a la seguridad de la información.

    Gestión de las incidencias que afectan a la seguridad de la información; mejoras.

13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio.

Continuidad de la seguridad de la información; redundancias.

14. Conformidad.

Conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación

2.1.4. Seguridad de la Información

La Seguridad de la Información "Tiene como propósito, reducir riesgos hasta un nivel que sea aceptable para los interesados, en mitigar amenazas latentes. Puesto que la información podemos tenerla en distintas formas y estados, se requiere implantar medidas de protección adecuadas de acuerdo con su importancia y criticidad, sin importar su forma y estado. Este es precisamente el ámbito de la Seguridad de la información. (2015) Giancarlo Gómez, Profesor de Ciberseguridad de Post grado del Centro de Altos Estudios Nacionales CAEN.

Figura 5.- Propiedades fundamentales de la Seguridad (Fuente: Infosegur)

2.1.5. Seguridad Informática

Aguilera, P. (2011). Redes seguras (Seguridad informática). Se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

El objetivo fundamental de la seguridad informática no es la protección de los sistemas, sino la reducción de los riesgos y el soporte a las operaciones del negocio para lo cual ha de cubrir los siguientes campos: la seguridad de las personas, de la información, de las comunicaciones y de los sistemas. Para ser efectiva, la seguridad debe estar integrada en los procesos de la empresa y no estar relegada meramente a ciertas aplicaciones técnicas.

Sánchez, R. M. (2007). Análisis de riesgos en seguridad informática caso UNMSM

2.1.6. Objetivo de la Seguridad Informática

Este término encierra dos conceptos los cuales son los siguientes:

Seguridad: Es la confianza que adquiere un sistema o información que esté protegido ante cualquier peligro, amenaza o vulnerabilidad que afecten sus tres pilares los cuales son disponibilidad, confiabilidad e integridad.

Informática: Conjunto de conocimientos sistematizados y técnicos que hacen posible el tratamiento automático de la información por medio de la computadora.

Veites, A. G. (2001). Enciclopedia de la seguridad Informática 2da Edición. Alfaomega, afirma que "dados los conceptos de las palabras Seguridad e Informática, se puede decir que Seguridad Informática es la garantía de que los procesos llevados a cabo para el tratamiento de la información se mantengan aislados, en lo posible, de las amenazas que puedan afectar la integridad, disponibilidad y confiabilidad de la información"

2.1.7. Ingeniería Social

Ingeniería social utiliza la influencia y la persuasión para engañar a la gente convenciéndolos de que el ingeniero social es alguien que no es, o por la manipulación. Como resultado, el ingeniero social es capaz de tomar aprovecharse de la gente para obtener información con o sin el uso de tecnología. Ediciones RAMA – Kevin Mitcnik libro: El arte de la Intrusión (2008).

2.1.8. Políticas de Seguridad de la Información

Las políticas de seguridad informática surgen como una herramienta mediante la cual se pretende concientizar a los miembros de una institución acerca de la importancia y la sensibilidad de la información y de los servicios críticos que permiten a la organización desarrollarse y mantenerse en su sector de negocios, fijando los mecanismos y procedimientos que las empresas deben adoptar para salvaguardar sus sistemas y la información que estos contienen. Sánchez Sánchez, R. M. (2007). Análisis de riesgos en seguridad informática caso UNMSM.

2.1.9. Amenazas

La amenaza como causa potencial de un incidente que puede causar daños a un sistema de información o a una organización (UNE 71504:2018). Giancarlo Gómez Profesor de Ciberseguridad de Post grado de ESAN.

- Identificación de las amenazas
- De origen natural
- Del entorno (de origen industrial)
- Defecto de las aplicaciones
- Causadas por las personas de forma accidental
- Causadas por las personas de forma deliberada
- Intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente

Figura 6.- Tipos de Amenazas - Fuente: Alberto G. Alexander 2007

2.1.10. Vulnerabilidad

Se denomina vulnerabilidad a toda debilidad, defecto o falla de un sistema que puede ser aprovechada por una amenaza, riesgo, o más detalladamente a las debilidades de los activos o de sus medidas de protección que faciliten a atacantes en comprometer la seguridad, confidencialidad, integridad y disponibilidad de datos o información de una empresa o institución.

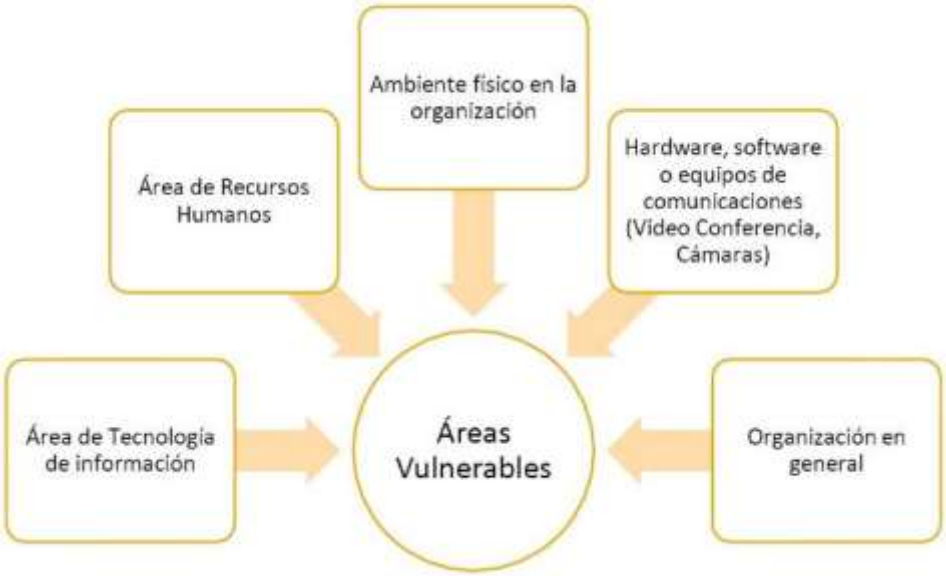


Figura 7.- Áreas Vulnerables (fuente: Moreno 2008)

2.1.11. Activo

Es considerado activo de una empresa o institución al conjunto de bienes, derechos y otros recursos de los que es propietaria una entidad privada o pública, por ejemplo, muebles, oficinas, equipos informáticos, información de datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos, también se incluyen aquellos de los que esperamos tener un beneficio futuro. Los Activos adoptaran un valor monetario cada uno, esta valoración dependerá de diferentes criterios y según la situación en la que puedan encontrarse.

2.1.12. Riesgo

Según Lozano Aldave (2017) Riesgo es el grado de exposición de un activo que permite la materialización de una amenaza. (P.16)

El riesgo es un término en el mundo de la informática cuando hay una exposición o posibilidad de pérdida de información o datos, por atentados o amenazas a los sistemas de la información.

2.1.13. Análisis de riesgos

Areitio (2008), manifiesta lo siguiente:

"El análisis de riesgos es un proceso consistente en identificar los peligros que afectan la seguridad, determinar su magnitud e identificar qué áreas necesitan salvaguardas. La valoración de riesgos es el resultado del proceso del análisis de riesgos."

En otro sentido, indica que para tratar de minimizar los efectos de un problema de seguridad se realiza el denominado análisis de riesgos, término que hace referencia al proceso necesario para responder a tres cuestiones básicas de la seguridad en una organización, que es saber qué se quiere proteger, contra quién o qué se quiere proteger y cómo se va a proteger, para lo cual existen dos enfoques básicos para realizar el análisis de riesgos, uno cualitativo y otro cuantitativo.

Desde otro punto de vista, en España, el Ministerio para las Administraciones Públicas (MAP, 2012) afirma lo siguiente: "Si el sistema aspira a una certificación en temas de seguridad de la información, el análisis de riesgos es un requisito previo que exigirá el evaluador. Es la fuente de información para determinar la relación de controles pertinentes para el sistema y que por tanto deben ser inspeccionados"

Alcance del Proyecto de investigación

Alcance temporal

Teniendo en consideración los factores internos y externos en el lugar a desarrollar la investigación, el trabajo fue desarrollado entre los meses de marzo a setiembre del año 2021, y las partes interesadas y sus expectativas, se ha definido el alcance del proyecto de investigación en:

Alcance geográfico

El presente proyecto de investigación se desarrollará en la Sede Principal de la Corte Superior de Justicia de Lima que es el Edificio Javier Alzamora Valdez, sede con mayor cantidad de usuarios distribuidos entre personal jurisdiccional y administrativo; específicamente en las áreas administrativas llámese, gerencia de administración, logística, recursos humanos, y la unidad de planeamiento y desarrollo.

Alcance Social

Las personas que participan en la presente investigación es el jefe de Informática de la Unidad de Planeamiento y Desarrollo, el Coordinador de Redes, el Coordinador de Soporte tecnológico, y la jefa de la Unidad de Planeamiento y Desarrollo de la Corte Superior de Justicia de Lima.

La Institución, Corte Superior de Justicia de Lima considerando los factores internos y externos y sus partes se ha definido el alcance del proyecto de investigación, en capacitación y buenas prácticas del uso de las normas de seguridad para un óptimo funcionamiento en los procesos de los diferentes sistemas administrativos, correos

electrónicos y servicios informáticos, desde su sede ubicada en el distrito, provincia y departamento de Lima.

Limitaciones

- Este proyecto, se limitará a la sede principal la cual es el edificio Javier Alzamora Valdez, en sus áreas administrativas de Gerencia de Administración, Logística y Contabilidad.
- Debido a las políticas de confidencialidad de la entidad estatal, no se publicará información como planos, o ubicación de cámaras de seguridad, ya su ubicación es estratégica.
- Por el estado de emergencia que atraviesa el país desde el mes de marzo del año 2019, el personal se encuentra dividido en personal vulnerable (quienes hacen labores remotas), personal mixto (trabajo Inter diario) y personal presencial, siendo estos últimos, quienes se encuentra en constante interacción con los equipos físicos de la institución. Razón por la cual, no hay un 100% de usuarios capacitados o con conocimiento de esta implementación.

2.1.14. Justificación del proyecto de investigación

Dado la problemática que presenta la Seguridad Informática de la Corte Superior de Justicia de Lima se realizó la propuesta de diseñar un plan de mejoras y buenas prácticas a la seguridad informática usando la norma ISO 27002.

Es muy importante la investigación ya que con ello se pretende mejorar la seguridad, mitigando los riesgos y vulnerabilidades, tener un mayor control y rendimientos de los servicios informáticos.

Justificación de conveniencia

La presente investigación es un tema conveniente para la institución, ya que aplicando una implementación de las normas y buenas prácticas se evitaría las posibles caídas del sistema, así como también el ataque al correo institucional y la página web, y la mala manipulación de los sistemas por parte de los usuarios. Por otra parte, la seguridad del centro de datos y del acervo documentario merecen una especial atención al respecto. La Corte Superior de Justicia de Lima tiene actualmente muchas vulnerabilidades de ambos tipos tecnológicos y políticos, pero al poner en control las políticas de seguridad usando la norma estándar ISO 27002:2013 será un gran paso.

Justificación de relevancia social.

La presente investigación tiene una relevancia social, y al ser un poder del estado que imparte justica a los ciudadanos, se evitaría largas colas y atención óptima a los justiciables, al tener un sistema y servicios informativos más óptimos posibles. El presente proyecto de investigación beneficiará a miles de ciudadanos tales como (abogados, público en general, otros poderes del estado que comparten información) y sobre todo proyección a brindar un mejor servicio a la ciudadanía, para así la Corte Superior de Justicia de Lima recupere el prestigio como Poder del Estado.

2.2. Formulación del problema

¿De qué manera la implementación de un plan de Seguridad Informática basado en la ISO 27002, optimiza la gestión en la Corte Superior de Justicia de Lima?

2.2.1. Problemas Específicos

1.- ¿Cómo se analiza los objetivos y políticas de la norma ISO 27002:2013?

2.- ¿Cómo se identifica los riesgos sobre los activos definidos en la norma ISO 27002:2013?

3.- ¿En qué medida se identifican los riegos que hay en los controles de los activos?

4.- ¿Cómo determinar la implementación de un plan de seguridad informática, para optimizar la gestión en la Corte Superior de Justicia de Lima?

2.3. Objetivos

2.3.1. Objetivo general

Implementar de un Plan de Seguridad Informática basado en la norma técnica ISO 27002, para optimizar la gestión en la Corte Superior de Justicia de Lima.

2.3.2. Objetivos específicos

1.- Analizar los objetivos y políticas de la norma ISO 27002:2013.

2.- Identificar los riesgos sobre los activos definidos en la Norma 27002:2013.

3.- Identificar los riesgos que hay en los controles de los activos.

4.- Determinar la implementación de un plan de seguridad informática, para optimizar la gestión en la Corte Superior de Justicia de Lima.

2.4. Hipótesis

"La implantación de un Plan de Seguridad Informática basado en la norma ISO 27002, optimizará la gestión en la Corte Superior de Justicia de Lima".

2.4.1. Hipótesis general

La implementación de un Plan de Seguridad Informática, basado en la norma ISO 27002, optimizará la gestión en la Corte Superior de Justicia de Lima.

2.4.2. Hipótesis específicas

1. Objetivos, y políticas de la norma 27002 se usará para las mejoras de la seguridad informática
2. Los riesgos sobre los activos que son identificados por la Norma 27002 mejorará la seguridad informática en la institución judicial
3. En gran medida se incrementan los riesgos en la seguridad informática por no implementar controles sobre los activos.
4. La implementación de un plan de seguridad informática, optimizará la gestión en la Corte Superior de Justicia de Lima

2.5. MATRIZ DE CONSISTENCIA

Tabla 2.- ***Matriz de Consistencia***

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES
PROBLEMA GENERAL: ¿De qué manera la implementación de un Plan de Seguridad Informática basado en la norma ISO 27002, optimiza la gestión en la Corte Superior de Justicia de Lima?	**OBJETIVO GENERAL:** Implementar un Plan de Seguridad Informática basado en la norma técnica ISO 27002, para optimizar la gestión en la Corte Superior de Justicia de Lima	**HIPOTESIS GENERAL:** La implementación de un Plan de Seguridad Informática basado en la norma ISO 27002, optimizará la gestión en la Corte Superior de Justicia de Lima.	**VARIABLES INDEPENDIENTES** Implementación de un Plan de Seguridad Informática La implementación del Sistema de Gestión de Calidad ayuda a la organización a estandarizar los procesos operativos y generar oportunidades de mejora continua. (Rodríguez, 2018).	D1.- Ejecutar las buenas prácticas de la norma ISO 27002 D2.- Establecer control de los equipos D3.- Mejora continua.
PROBLEMAS ESPECÍFICOS **1.-** ¿Como se implementa un plan de seguridad informática para mejorar la seguridad de la información? 2.- ¿Como se implementa un plan de seguridad informática para mitigar los riesgos y control de los equipos? 3.- ¿Como se implementa un plan de seguridad informática para mejorar la política de seguridad?	**OBJETIVOS ESPECÍFICOS:** 1.- Determinar cómo se implementa un plan de seguridad informática para mejorar la seguridad de la información. 2.- Determinar cómo se implementa un plan de seguridad informática para mitigar los riesgos y control de los equipos. 3.- Determinar cómo se implementa un plan de seguridad informática para mejorar la política de seguridad.	**HIPÓTESIS ESPECÍFICAS:** 1.- Implementa un plan de seguridad informática para mejorar la seguridad de la información 2.- Implementa un plan de seguridad informática para mitigar los riesgos y control de los equipos 3.- Implementa un plan de seguridad informática para mejorar la política de seguridad? .	**VARIABLES DEPENDIENTES** Optimizar la gestión en la Corte Superior de Lima Optimizar el servicio que brindan y el rendimiento de una empresa competitiva, es fundamental evaluar las técnicas actuales y la tecnología disponible para desarrollar sistemas que brinden eficiencia y eficacia de la gestión de servicio. (González, M. A., & Vásquez, L. M. 2013)	D1.- Seguridad de la información. D2.- Mitigar riesgos. D3.- Políticas de seguridad.

CAPÍTULO III.

3.1. Descripción de la Experiencia

La carrera profesional como trabajador de la Corte Superior de Justicia de Lima, se inicia en el mes de junio del año 1997, donde a través de un concurso público, logré ocupar una de las plazas administrativas en el archivo de esta Corte, en julio de 1999 soy rotado a la Secretaría General de la Presidencia hasta el año 2007, donde desempeño funciones administrativas y a finales del año 2012 y luego de regresar de una licencia laboral de 5 años donde, tuve la oportunidad de laborar en la alta dirección de 2 ministerios del Poder Ejecutivo, me incorporo a la oficina de Coordinación de Informática, y en el transcurso de unos pocos meses, logro ocupar el cargo de Encargado de Soporte Técnico de la Corte Superior de Justicia de Lima, encargo que tuvo en principio cerca de 50 trabajadores en toda la jurisdicción, pero luego de las conversiones en otras cortes del país y reducción del ámbito territorial, actualmente se cuenta con el 50% del personal de Soporte Técnico.

Como trabajador de la oficina de informática y estudiante de la Universidad Privada del Norte, me llevó a investigar las vulnerabilidades que existen en el tema informático en mi institución, lo cual me motivó a realizar el tema de esta investigación, y buscar a través de la norma ISO 27002, optimizar la gestión en la seguridad informática de esta institución pública.

3.2. METODOLOGÍA

Tipo de investigación

El tipo de investigación es aplicativa, con la cual se estima dar solución a la seguridad de la información que ha sido en varias oportunidades afectada por falta de políticas de seguridad informática basándose para tal efecto en lo indicado por la norma ISO 27002:2013. El tipo de investigación aplicada tiene como referencia la información o investigación básica, que no es otra cosa que las experiencias logradas en otras investigaciones y su base está en resolver problemas del día a día. Este tipo de investigación busca utilizar los conocimientos u experiencias de otras áreas, con la finalidad de implementar una solución más idónea.

Población y muestra (Materiales, instrumentos y métodos)

Se pretende implementar la elaboración de un plan de seguridad informática de acuerdo a la norma ISO en su versión 2013 (ISO 27002:2013) la cual se compone de 14 áreas de control como siguen (ISO Tools Excellence, 2016), pero no todas se ejecutarán en la institución.

1. Políticas de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Seguridad relativa a los recursos humanos.
4. Gestión de activos.
5. Control de acceso.
6. Criptografía.
7. Seguridad física y del entorno.
8. Seguridad de las operaciones.

9. Seguridad de las comunicaciones.

10. Adquisiciones, desarrollo y mantenimiento de los sistemas de información.

11. Relación de proveedores.

12. Gestión de incidentes de seguridad de la información.

13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio.

14. Cumplimiento.

Tabla 3.- ***Objetivos de Control y Controles ISO 27002:2013***

ÍTEMS	DOMINIOS	OBJETIVOS DE CONTROL
1	Política de seguridad de la información	1.1 directrices de gestión de la seguridad de la información
2	Organización de la seguridad de la información	2.1 organización interna 2.2 los dispositivos móviles y el teletrabajo
3	Seguridad relativa a los recursos rumanos	3.1 antes del empleo 3.2 durante el empleo 3.3 finalización del empleo o cambio en el puesto de trabajo
4	Gestión de activos	4.1 responsabilidad sobre los activos 4.2 clasificación de la información 4.3 manipulación de los soportes
5	Control de acceso	5.1 requisitos de negocio para el control de accesos 5.2 gestión de acceso de usuario 5.3 responsabilidades del usuario 5.4 control de acceso a sistemas y aplicaciones
6	Criptografía	6.1 controles criptográficos
7	Seguridad física y del entorno	7.1 áreas seguras 7.2 seguridad de los equipos
8	Seguridad de las operaciones	8.1 procedimientos y responsabilidades operacionales 8.2 protección contra el software malicioso (malware) 8.3 copias de seguridad 8.4 registros y supervisión 8.5 control del software en explotación 8.6 gestión de la vulnerabilidad técnica 8.7 consideraciones sobre la auditoria de sistemas de información
9	Seguridad de las comunicaciones	9.1 gestión de la seguridad de redes 9.2 intercambio de información
10	Adquisición, desarrollo y mantenimiento de los sistemas de información	10.1 requisitos de seguridad en sistemas de información 10.2 seguridad en el desarrollo y en los procesos de soporte 10.3 datos de prueba
11	Relación con proveedores	11.1 seguridad en las relaciones con proveedores 11.2 gestión de la provisión de servicios del proveedor
12	Gestión de incidentes de seguridad de la información	12.1 gestión de incidentes de seguridad de la información y mejoras
13	Aspectos de seguridad de la información para la gestión de la continuidad del negocio	13.1 continuidad de la seguridad de la información 13.2 redundancias
14	Cumplimiento	14.1 cumplimiento de los requisitos legales y contractuales 14.2 revisiones de la seguridad de la información

Fuente: Enunciado adoptado por la Norma ISO 27002:2013 (AENOR, 2015)

3.3. Variables de Estudio

- **Independiente**

  Implementación de un Plan de Seguridad Informática basado en la norma ISO 27002.

- **Dependiente**

Optimizar la gestión en la Corte Superior de Justicia de Lima.

3.4. POBLACIÓN Y MUESTRA

3.4.1. Población

"Una población es un Conjunto de todos los casos que concuerdan con determinadas especificaciones "(p. 174). Print Book: (2014) Hernández Sampieri - Metodología de la investigación.

En qué grado se aplica la norma 27002 para mejorar la seguridad informática en la Corte Superior de Justicia de Lima que es un aproximado de 5,000 usuarios con equipos de cómputos cada uno. Pero dado que nuestro estudio de investigación se delimita a la población de la Sede Principal de la Corte Superior de Justicia de Lima que es el Edificio Javier Alzamora Valdez con aproximadamente 1800 usuarios en las diferentes áreas administrativas y jurisdiccionales. Dada la coyuntura actual que el mundo viene atravesando con la pandemia del COVID 19, la población es limitada por las restricciones dictadas por el gobierno.

3.4.2. Muestra

Print Book: (2014) Hernández Sampieri - Metodología de la investigación. Una muestra es, en esencia, un subgrupo de la población. Digamos que es un subconjunto de elementos que pertenecen a ese conjunto definido en sus características al que llamamos población. (p. 175).

Después de haber definido el área de la institución, se toma la muestra que corresponde a un total de 40 personas en la primera etapa, y 44 personas en la segunda etapa, que serán encuestadas del 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.

3.5. Técnicas e instrumentos de recolección y análisis de datos.

Se trata de las técnicas que se usará para la recolección de información, en algunos casos son estudios ya realizados lo cual es una fuente para recopilar información.

Para esta recolección de datos se deberá revisar la documentación de diferente índole, manuales, informes, planes de seguridad, con la finalidad de proporcionar mayor información sobre las políticas de seguridad informática con que cuenta la institución.

Print Book: (2014) Hernández Sampieri - Metodología de la investigación.
“Recolectar los datos implica elaborar un plan detallado de procedimientos que nos conduzcan a reunir datos con un propósito específico” (p. 198).

Para realizar la planificación de esta investigación diseñamos instrumentos de medición los cuales nos permitirán producir datos sobre resultados finales o parciales, cuantitativos, para esto utilizaremos:

3.5.1. Instrumentos

Print Book: (2014) Hernández Sampieri - Metodología de la investigación.

"Un instrumento de medición recurso que utiliza el investigador para registrar información o datos sobre las variables que tiene en mente" (p. 245).

Para la presente investigación se usará el instrumento de validez de constructo o construcción de variable medida, que tiene lugar dentro de una hipótesis, teoría o modelo teórico, (Hernández (2014, p 203), la validez, la confiabilidad y la objetividad no deben tratarse de forma separada.

3.5.2. Cuestionario

Print Book: (2014) Hernández Sampieri - Metodología de la investigación.

El cuestionario es un conjunto de preguntas respecto de una o más variables que se van a medir (p. 217)

El instrumento para recolectar los datos para la presente investigación es el cuestionario, en que se tendrá preguntas abiertas y cerradas (mixtas) donde se usará escalas para medir las actitudes.

La Unidad de informática de la Corte Superior de Justicia de Lima, está dividido en tres sub áreas que son: el área de Sistemas, de Redes y comunicaciones de datos y área de Soporte Tecnológico; para medir las actitudes y conocimientos a los profesionales que trabajen en las tres áreas, teniendo en cuenta actitudes y conocimientos de la seguridad Informática se usará el método más conocido para medir por escalas las variables que constituyen actitudes es: el método de escalamiento de Likert.

Escalamiento de Likert, según Hernández en su libro metodología de la investigación nos dice "es un conjunto de ítems que se presentan en forma de afirmaciones para medir la reacción del sujeto en tres, cinco o siete categorías" (p. 238).

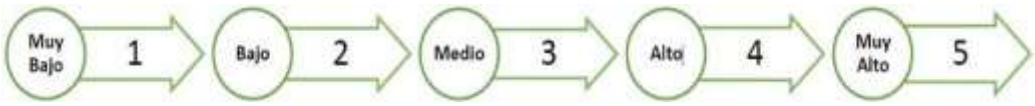


Figura 8.- ***Escala de Likert (Fuente. Alberto G. Alexander 2007)***

Su propósito tiene como objetivo evaluar los conocimientos de las personas encuestadas, con una encuesta de 12 preguntas y un cuestionario de 19 preguntas, se requiere obtener información actual de la problemática de La Corte Superior de Justicia de Lima en cómo se encuentra la situación de la Seguridad Informática, Políticas, conocimientos de la norma 27002, el estado de los equipos y los procesos realizados en el área de TI, para después poder analizar los datos obtenido y hacer su medición de confiabilidad y validez, para la obtención de los resultados y así poder hacer mejoras diseñando un plan de aumentar o hacer nuevas políticas de la seguridad de la información usando la norma ISO 27002.

Entrevista:

La Encuesta y el cuestionario se realizarán a 20 profesionales del área de TI, tomando como referencia las preguntas del cuestionario realizado de la encuesta, donde se busca conocer los conceptos que tienen con respecto a la seguridad informática

3.6. Procedimiento

Para el desarrollo de la presente Tesis titulada. "Implementación de un Plan de Seguridad Informática, basado en la norma ISO 27002, para optimizar la gestión de la Corte Superior de Justicia de Lima, se investigó material académico en los buscadores científicos como Scielo, Redalyc, Google Académico, Alicia Concytec y Cybertesis, con temas relacionados con Seguridad Informática, enfocándose en la norma ISO 27002:2013, así como el uso de herramientas como cuestionarios a personal de informática para tener conocimiento tecnológico, así como a las demás jefaturas de la Corte Superior de Justicia de Lima, para medir el conocimiento de la seguridad informática en la institución.

Estando a la investigación teórica realizada se determinó que la implementación del Plan de Seguridad, se ejecutará en 2 etapas, la primera será para el análisis, diagnóstico y recojo de datos lo cual se llevó a cabo a través de un cuestionario (anexo 1), asimismo, se observó in-situ el desarrollo de las labores de los trabajadores, la forma de uso de los equipos informáticos, de la información que utilizan y del conocimiento de los mismos, asimismo se realizó las siguientes tareas:

Tabla 4.- ***Procedimiento - Fase Diagnóstico***

FASE DIAGNÓSTICO			
TAREA	**INTERESADOS**	**Actividades a Desarrollar**	**Resultados**
Revisión de documentos de gestión de la CSJL	Jefe de Informática, jefa de la oficina de Seguridad, jefe del área de redes y comunicaciones	Reunión con dichos funcionarios, a fin de exponer la idea del proyecto del Plan de implementación de Seguridad informática basada en la norma ISO 27002	Aprobación y apoyo para dicha labor brindando información a través de cuestionarios.
Evaluación de los puntos indicados en la norma ISO 27002	Gestor del proyecto, jefe de informática y de la oficina de seguridad	Usando el Check list se realizó la verificación sobre el cumplimiento de cada objetivo indicado en la ISO 27002	Archivo check list de manera equilibrada en la medición de resultados.
Informe del estado situacional de las jefaturas	Gestor del proyecto, jefe de informática y de la oficina de seguridad, jefes de área	Se elevó informe a las jefaturas, indicando el estado situacional de la seguridad de la información	Informe del estado situacional de la seguridad de la información de la CSJLI

En esta primera etapa de diagnóstico se realizaron diferentes actividades, logrando buenos resultados, los cuales se indican a continuación:

Reuniones virtuales y presenciales, con personal con conocimiento en el tema, así como con los encargados de las áreas, a los cuales se les expuso las ideas de la implementación de un plan de seguridad informática en la institución, estableciendo buenas prácticas de acuerdo a lo que se indica en la norma ISO 27002, con estas reuniones se logró obtener información muy importante sobre el estado situacional de los equipos informáticos, en lo que respecta a software y hardware, seguridad de los ambientes donde se ubican y/o almacenan así como el nivel de conocimiento de parte de los trabajadores, con lo que respecta a la seguridad de la información.

Mediante el uso de cuestionarios se llegó a obtener información básica y con eso se elaboró un informe situacional invocando los parámetros de la norma ISO 27002.

En lo que respecta al tema estructural, donde se encuentran ubicados los centros de datos, seudos servidores, switchs y la exposición de las redes, en la primera etapa de diagnóstico, se encontró exposición de los mismos, los cuales podrían ser manipulados por cualquier usuario interno o externo, sin falta de seguridad, como puertas, candados, ausencia de cámaras de seguridad, y personal de vigilancia, no encontró equipos UPS.

Asimismo, los equipos de cómputo que son utilizados por los usuarios finales, no cuentan con accesos seguros, siendo transitables para todo el personal, no existe dispositivo de control biométrico para el control del tránsito en los pisos, y en muchos casos, no tienen usuarios o contraseñas para iniciar el equipo.

Tabla 5.- ***Procedimiento - Fase Planificación***

FASE PLANIFICACIÓN			
TAREA	**INTERESADOS**	**Actividades a Desarrollar**	**Resultados**
Calendarización de actividades a desarrollar	Jefe de Informática, jefa de la oficina de Seguridad, jefe del área de redes y comunicaciones	Se agenda actividades para la realización de la implantación del plan de seguridad	Se cuenta con una estructura y plan inicial del trabajo.
Determinación de los materiales necesarios	Gestor del proyecto, jefe de informática y de la oficina de seguridad	Se solicita a las áreas interesadas, materiales para proceder con la implementación	Archivo check list de manera equilibrada en la medición de resultados.
Difusión del Plan a desarrollar	Gestor del proyecto, jefe de informática y de la oficina de seguridad, jefes de área	Se presento el plan estratégico del proyecto, dando a conocer la importancia que encierra.	Informe con el plan de las acciones a tomar por parte de las distintas jefaturas.

Luego del diagnóstico efectuado, se planificó realizar la implementación de un plan de seguridad informática de acuerdo a lo establecido en previas reuniones con personal comprometido a esta labor, utilizando entre los recursos, difusión de esta implementación, para tener las facilidades de estudio llevado a cabo en la etapa 1, así como, presentación de informes y la manera

como se deberá ejecutar el plan de acción para salvaguardar la seguridad informática en la institución.

Se planificó evaluar y de ser el caso, reemplazar equipos informáticos con funcionamiento defectuoso, debido a la a ausencia de UPS (sistema de alimentación ininterrumpida), se evaluará la compra de dichos equipos que son de vital importancia, cuando suceda, caída o fallas eléctricas, ya que, por su sistema de funcionamiento por baterías, podría darle el tiempo necesario, para guardar la información que se encuentre en proceso, cuando suceda un falla o corte eléctrico.

Por otro lado, la planificación se efectuará tomando en cuenta lo indicado por la norma ISO 2002:2013, los cuales definen, los siguientes puntos;

- Políticas de seguridad de la información, a través de documentación que se logre emitir, se garantizaran los tres pilares de la seguridad de la información, tales como, la confidencialidad, integridad y disponibilidad, esto debe llevarse a cabo a través documentos circulares, correos electrónicos y demás medios de difusión donde se indique la importancia de la seguridad en las actividades desarrolladas por los colaboradores de la institución.
- La organización de la seguridad de la información, se deberá realizar, grupos de trabajo, los cuales deberán desarrollar estrategias de seguridad de la información, donde se incluya a los de dispositivos móviles, así como a los bienes informáticos que se encuentran haciendo teletrabajo.
- Seguridad relativa a los recursos humanos, el personal nuevo deberá ser capacitado a través, de cartillas y la entrega de material informativo, sobre la importancia de la seguridad informática y de la información, asimismo deberá ser supervisado y

evaluado periódicamente por personal encargado del cumplimiento de dicho punto y cuando el trabajador finalice su vínculo con la institución o sea rotado a otra dependencia judicial.

- Gestión de activos, se deberá establecer una supervisión permanente de los bienes materiales u objetos físicos de la institución, con esto se tiene con precisión el conocimiento del ciclo de vida de los activos institucionales, lo cuales deben ser renovados cuando ya hayan cumplido su ciclo de vida útil.
- Control de acceso, el acceso a los terminales o equipos de cómputo, se deberá crear el uso obligatorio de contraseñas de inicio de sesión y el cambio periódico de las claves que son utilizadas para acceder a los distintos sistemas que interactúan los trabajadores judiciales. Asimismo, se sugiere se implementen controles de acceso por piso utilizando para esto, controles biométricos.
- Criptografía. Establecer mejores controles criptográficos, ya que se detectó que este software Forticlient, el cual es utilizado para realizar trabajo remoto, cuando se encuentra activo, sirve de puente a la red de la institución, pero a su vez, gran cantidad de usuarios, no tiene su sistema operativo actualizado, o desconocen la importancia de contar con un antivirus en los equipos utilizados en casa, lo que podría ocasionar ataque de virus a los equipos de cómputo.
- Seguridad física y del entorno. Se detectó que no existen áreas seguras, así como seguridad para los equipos informáticos, para esto se sugiere mejor control de los mismos.

- Seguridad de las operaciones, se observó que no se cuenta con un área encargada de hacer las copias de seguridad, control de software ya que los equipos solo cuentan con un usuario con perfil de administrador, lo que permite que los colaboradores de la institución puedan instalar desmedidamente algún programa no autorizado.
- Seguridad de las comunicaciones, se notó que las redes tienen una precaria estabilidad, así como los radio enlace que existen solo son controlados por la empresa proveedora, se sugirió tener un mayor control de estos puntos.

Tabla 6.- ***Procedimiento - Fase Implementación***

FASE IMPLEMENTACIÓN			
TAREA	**INTERESADOS**	**Actividades a Desarrollar**	**Resultados**
Elaboración de las políticas de gestión	Gestor del proyecto, jefe de informática y de la oficina de seguridad, funcionarios, y colaboradores	Elaboración de documentos y formatos para las actualizaciones de los diversos aplicativos. Mantenimiento preventivo de los bienes informáticos.	El área de informática cuenta con formatos para regular las actualizaciones de lo diversos aplicativos
		Revisión de contratos de terceros, que brindan servicios a la institución	Se revisó un total de 8 contratos vigentes de terceros, observando que en todos hay vacíos legales en lo que refiere a seguridad informática, y una vez realizada las observaciones, se mejoró considerablemente este punto.
		Plan de mantenimiento del parque informático de la Corte Superior de Justicia de Lima	Se estableció un calendario de mantenimiento preventivo, así de como un inventario actualizado de los bienes informáticos, para determinar su

			cambio y/o renovación de equipos.
		Se propuso y elaboro un documento de sanciones administrativas por faltas cometidas por el personal que incumpla las normas y políticas de seguridad informática y de la información.	Estos documentos ya existían, pero sin función, se impulsó su cumplimiento, distribuyéndose a todos los trabajadores judiciales.

En la etapa 2 de este plan de implementación de seguridad informática, se elaboró un plan de mantenimiento integral para los equipos informáticos (anexo 2 y 3), así como un plan de copias de seguridad (backup´s) de la información de la institución, para la cual se estableció procedimientos documentados de generación y resguardo de información.

Se implementó, cámaras de video vigilancia en la entrada de los centros de datos, así como en las demás áreas que se encontraban expuestas en el diagnóstico de la etapa 1, pero por razones de estricta confidencialidad de la institución ya que su ubicación es estratégica, no se publicará el anexo correspondiente. Por otro lado, se logró reubicar en un lugar seguro y con puertas con llave, los switchs que se mencionaron en la etapa 1, asimismo, se estableció un control permanente para el ingreso donde se ubican los equipos informáticos, instalando para tal efecto, controles biométricos de acceso a las áreas correspondientes (anexo 4), así como creación de contraseñas para los mismos.

Se capacitó al personal en el correcto uso de la información de la institución, en el riesgo que representa correos dudosos, en la confidencialidad de la información, etc.

Posterior a los puntos observados, se logó implementar en esta segunda etapa lo siguiente:

- Emisión de documentos, cartillas informativas y correos electrónicos, poniendo en conocimiento el uso adecuado de la norma ISO 27002, y su estricto cumplimiento, esta labor fue realizada con el apoyo de las autoridades de la Corte Superior de Justicia de Lima.
- Se organizó al equipo de informática para desarrollar estrategias y medidas preventivas para la correcta seguridad informática donde se del alcance también en los operadores remotos.
- Se capacitó a personal nuevo en lo que respecta a la seguridad de la información, para el uso correcto y confidencial de la información que encierra la institución. (Anexo 5).
- Se procedió con el inventario físico de los bienes informáticos de la institución, con la cual, se obtuvo la realidad del estado de los bienes, así como el tiempo que vienen operando, esto, con la finalidad de solicitar su reemplazo, en el caso se amerite dicho acto.
- Al comprobar que los bienes informáticos no cuentan con protección en lo que respecta al control de acceso, se procedió a establecer contraseñas de inicio de sesión, así como se envió a través de los sistemas que utilizan, la obligatoriedad de cambio de contraseña, buscado con esto mayor protección a la información que almacenan los programas utilizados.
- Por otro lado, se constató que muchos equipos de la institución, así como las computadoras que utilizan en casa los servidores remotos, no cuentan con un antivirus actualizado, lo cual representaba un riesgo latente en la red, razón por la

cual, se procedió al siguiente, y suspensión temporal de dichas conexiones, hasta que subsanar los puntos indicados. Se designó un personal encargado de realizar el control y seguimiento de analizar las vulnerabilidades de algún agujero en los sistemas institucionales.

- Se reubicó los terminales de red, colocación de precintos de seguridad, candados, y chapas en buen funcionamiento, así como mejor control para el libre tránsito de parte de los servidores judiciales, así como terceros.
- Por otro lado, se reparó los equipos de aire acondicionado ubicados en los centros de datos, los cuales venían siendo reemplazados por ventiladores eléctricos y estos no cumplían con el objetivo de mantener a cierto nivel de temperatura el ambiente mencionado.

Recordemos que parte importante en la seguridad de las comunicaciones está conformada por los seres humanos, los procesos y la tecnología. Utilizamos con mayor frecuencia los dispositivos con salida a internet, el internet off Things, cada vez es más popular en nuestro día a día, sin embargo, esta conexión permanente implica una serie de riesgos y vulnerabilidades a la institución, ya que le da a los hackers o personas maliciosas, mayores oportunidades de poder invadir nuestras comunicaciones. Para esto se realizó campañas informativas, lo cual se reflejó como mejora en la segunda etapa.

Se realizó una entrevista a los encargados de las áreas descritas con la finalidad de obtener información veraz de sobre el desempeño diario y las formas de laborar de cada integrante de dichas áreas; asimismo se les detallo la finalidad de dicha reunión y entrevista

planteándoles el objetivo de implementar la norma ISO 27002:2013 y los controles que esta encierra; lo cual quedó plasmado en el cuaderno de ocurrencias.

Asimismo, se hizo un mapeo de la estructura funcional que se desarrolla en las áreas en mención y se pudo constatar los siguientes puntos.

- Algunos operadores logísticos cuentan con salida directa a la internet, es decir, no pasan a través del servidor filtro de la institución, y en otros casos, tienen IPs Nateadas sin restricciones de navegación.
- El correo electrónico institucional asignado a los colaboradores, en muchas ocasiones es atacado de phishing y otras modalidades invasivas.
- Las computadoras de los trabajadores no cuentan con claves o contraseñas de inicio de sesión, ni protectores de pantalla.
- Los expedientes físicos pueden ser visualizados por cualquier trabajador del área y en algunos casos por personal ajeno.
- No todas las computadoras cuentan con antivirus y algunas sí lo tienen, pero desactualizado.
- No se realizan pruebas en la red con la finalidad de buscar intrusiones.
- Por su clasificación de algún tipo de información de la empresa, no tiene el tránsito por la red como cifrada.

Estas deficiencias se repiten en las oficinas administrativas de Logística y Contabilidad y con esto se pudo evidenciar que no manejan políticas de seguridad informáticas, razón por la cual se propone un conjunto de medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información.

Tabla 7.- ***Procedimiento - Fase Evaluación***

FASE EVALUACIÓN			
TAREA	**INTERESADOS**	**Actividades a Desarrollar**	**Resultados**
Puesta en marcha las políticas de seguridad informática.	Gestor del proyecto, jefe de informática y de la oficina de seguridad	La Presidencia y Gerencia de Administración dispusieron el cumplimiento obligatorio de las políticas de seguridad informática y de la información.	Se dio cumplimiento a las políticas establecidas en la norma ISO 27002.
Evaluación de los controles sugeridos en la norma ISO 27002	Gestor del proyecto, jefe de informática y de la oficina de seguridad	Cuestionarios para el marcado a través del check list, invocando la norma ISO 27002, verificando el nivel de su cumplimiento.	Cuestionario muestra resultados positivos luego de implementar mejoras.

Luego del diagnóstico en la primera etapa donde se encontró deficiencias ya mencionadas, donde se vulneraba, la seguridad informática, así como la seguridad de la información, viene el paso de la evaluación luego de haber implementado en la segunda etapa, algunos puntos del uso de la norma ISO 27002:2013.

- Implementación de 14 controles de un total de 144 que sugiere la norma ISO 27002:2013, a desplegarse en la Corte Superior de Justicia de Lima, utilizando para esto, recursos tecnológicos, humanos, materiales y logísticos.
- Evaluación sobre capacitación y orientación de los trabajadores judiciales.
- Ejecución de las políticas de seguridad de la información de acuerdo a la norma ISO invocada.
- Permanente difusión sobre la seguridad informática, así como seguridad de la información.

- Capacitación a todo el personal involucrado en la manipulación de la información de la institución judicial.

CAPÍTULO IV.

4.1. Resultados

La Corte Superior de Justicia de Lima, por ser la Corte más grande del Perú, también posee la mayor cantidad de Salas y Juzgados en las diferentes especialidades y para poder abastecer de materiales logísticos a toda esta población judicial, realiza grandes movimientos económicos a través de las áreas de Logística y Contabilidad, oficinas que se tomaran como muestra en la implementación de la Seguridad Informática y el propósito de un buen Sistema de Gestión de Seguridad de la Información (SGSI)

A continuación, se muestran los resultados donde se reflejan las dos etapas descritas en el presente trabajo de investigación.

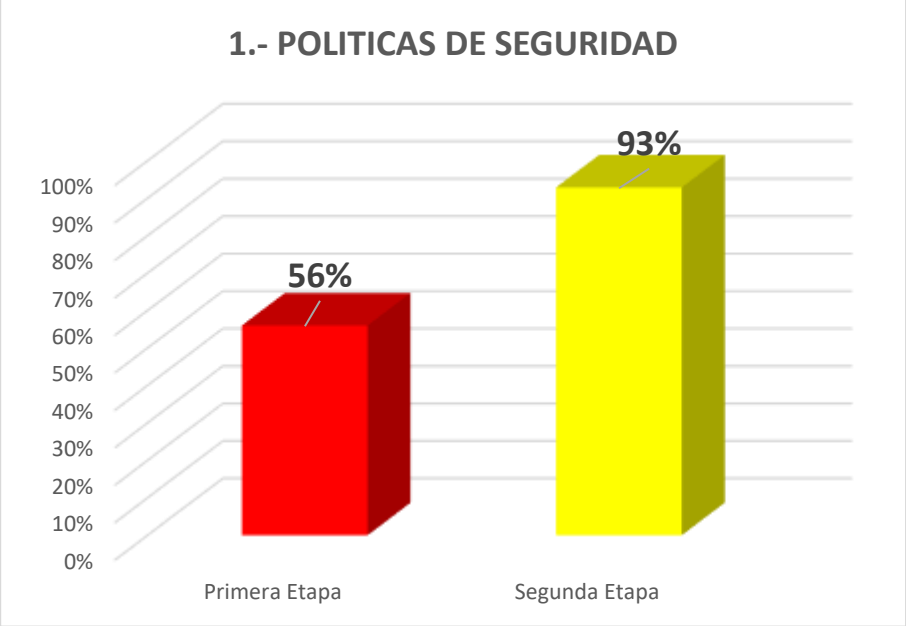


Figura 9.- Políticas de Seguridad – Comparativo 1era y 2da Etapa
Fuente: Elaboración propia

Según el dominio 1, Políticas de seguridad. Se tuvo un incremento significativo en la segunda etapa, por la emisión de directrices emitidas por la Gerencia de Administración

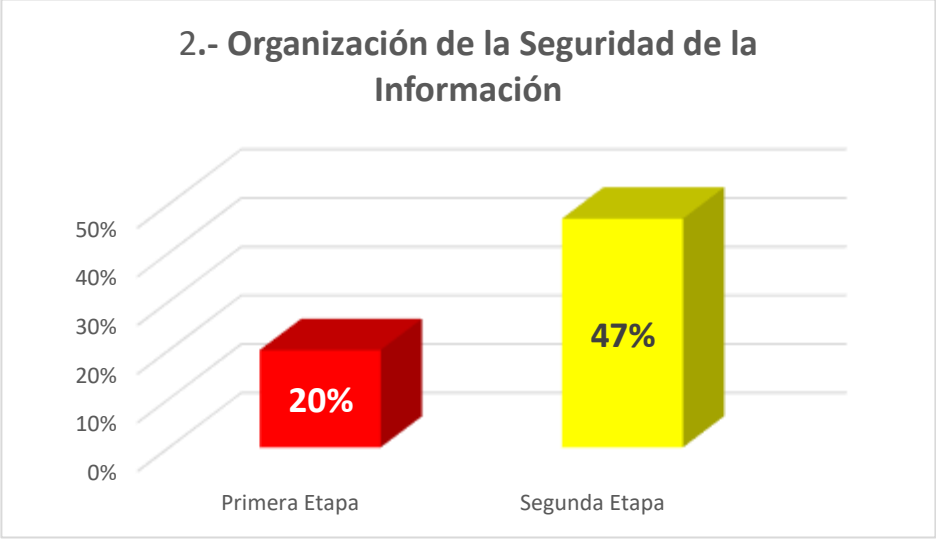


Figura 10.- Organización de la Seguridad de la Información - Comparativo 1era y 2da Etapa.

Fuente: Elaboración propia.

Según el dominio 2. Organización de la Seguridad de la Información, actualmente ya se cuenta con el apoyo de la Presidencia de Corte, así como la Gerencia de Administración, quienes apoyan con la iniciativa de implementar un Plan de Seguridad Informática.

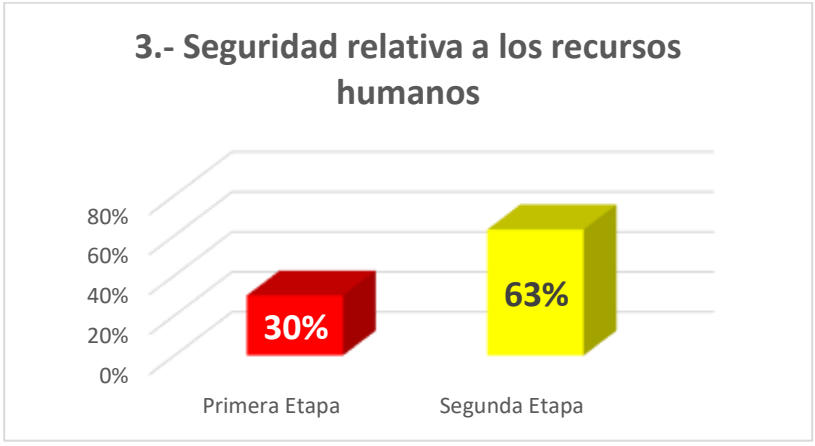


Figura 11.- Seguridad relativa a los recursos humanos - Comparativo 1era y 2da Etapa

Fuente: Elaboración propia

Según el dominio 3. Seguridad relativa a los recursos humanos, tuvo un incremento en la segunda etapa por medidas que se tomaron antes, durante y finalizar o cambiar del puesto de trabajo, los servidores judiciales.

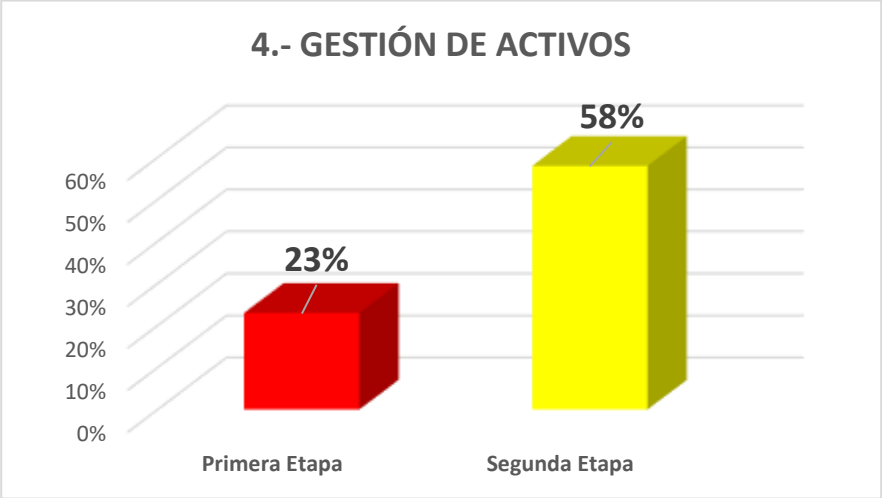


Figura 12.- Gestión de activos - Comparativo 1era y 2da Etapa
Fuente: Elaboración Propia

Según el dominio 4. Gestión de activos, tuvo un incremento en la segunda etapa ya que se efectuó campañas informativas de información.

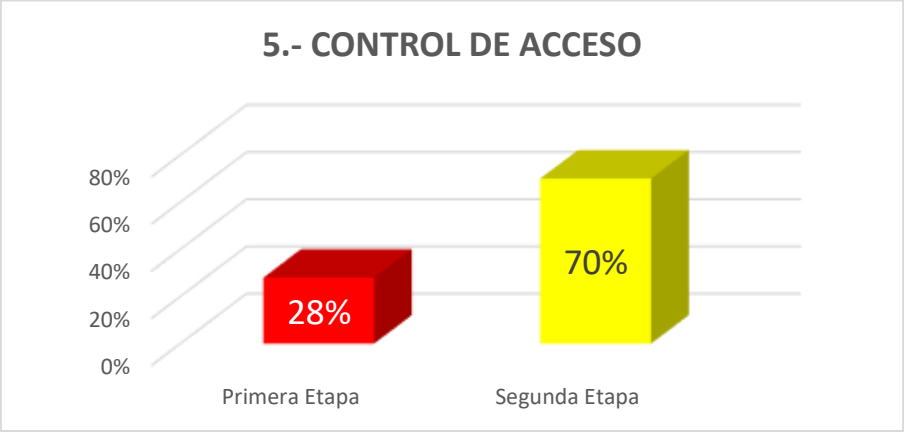


Figura 13.- Control de acceso - Comparativo 1era y 2da Etapa
Fuente: Elaboración propia.

Según el dominio 5. Control de acceso. – Aumento significativo a un 70%, ya que se incrementaron controles de accesos biométricos en muchas áreas.

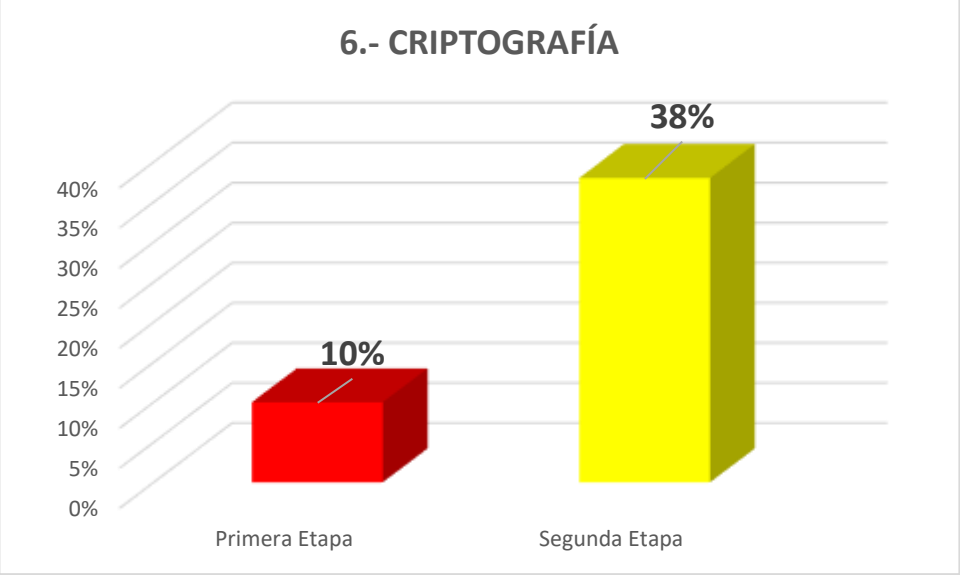


Figura 14.- Criptografía - Comparativo 1era y 2da Etapa
Fuente: Elaboración propia

Según el dominio 6.- Criptografía. – también tuvo un incremento en la segunda etapa debido al uso de información cifrada a través del software de VPN Forticlient.

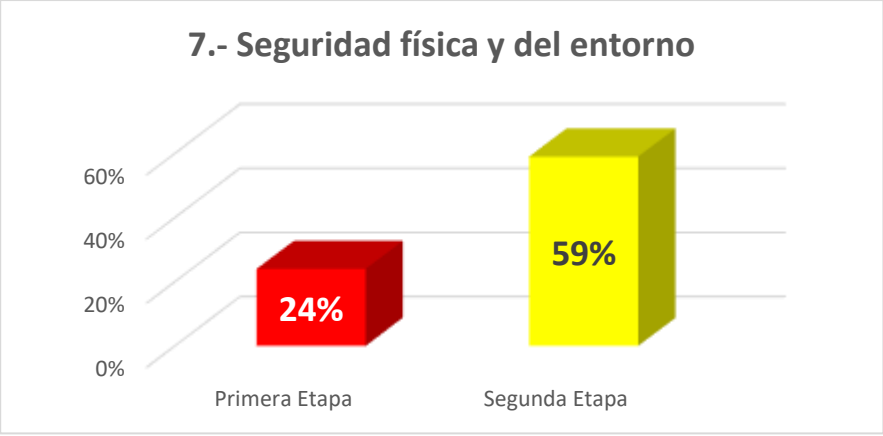


Figura 15.- Seguridad física y del entorno - Comparativo 1era y 2da Etapa
Fuente: Elaboración propia

Según el dominio 7.- Seguridad física y del entorno. – Mejora visible en la segunda etapa por los controles establecidos a través de cámaras de videovigilancia y otros.

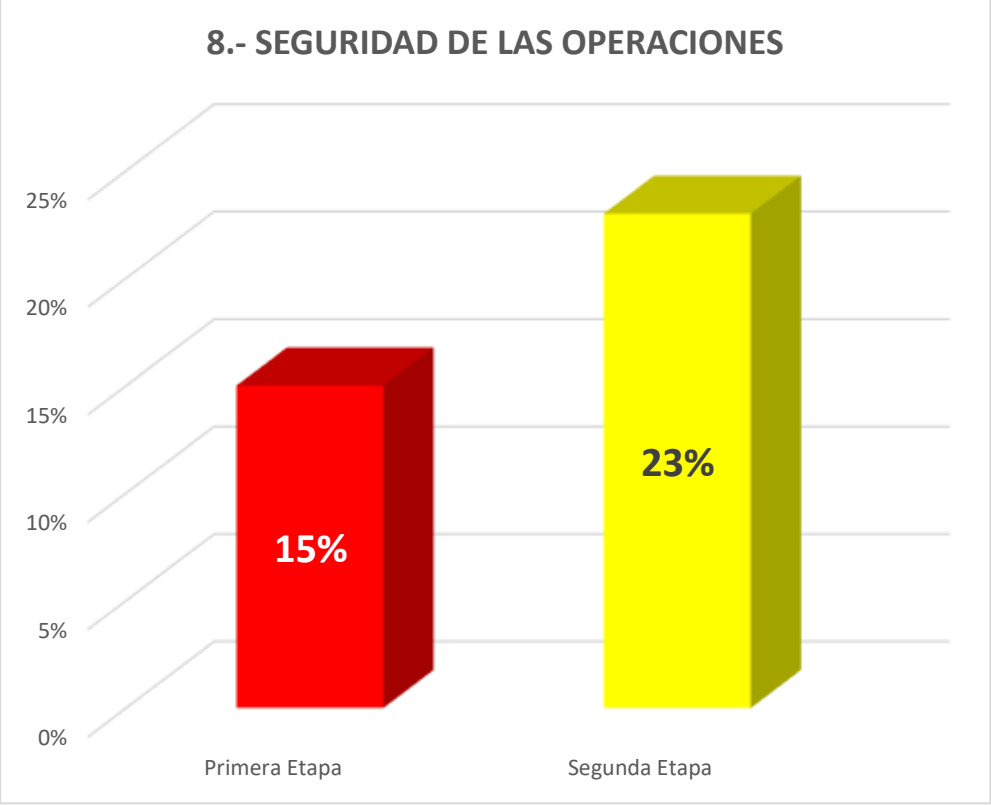


Figura 16.- Seguridad de las operaciones - Comparativo 1era y 2da Etapa
Fuente: Elaboración propia

Según el dominio 8. Seguridad de las operaciones. – Tuvo un ligero incremento favorable, debido a que solo se ejecutó la revisión de software malicioso y aún está en proceso de desarrollo, razón por la cual no se refleja cambios marcados en esta segunda etapa.

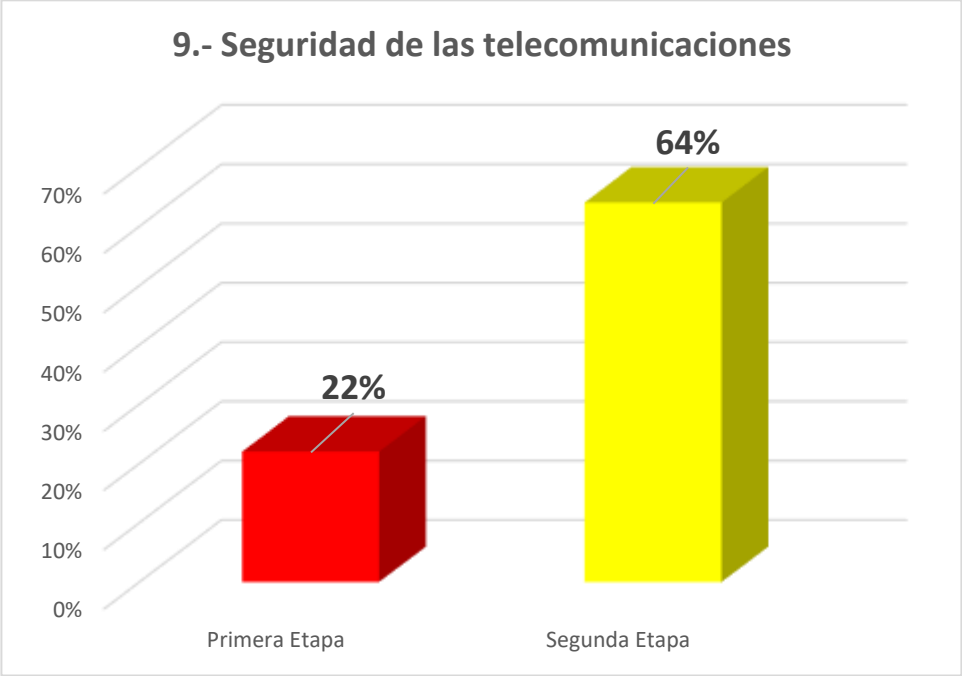


Figura 17.- Seguridad de las telecomunicaciones - Comparativo 1era y 2da Etapa
Fuente: Elaboración propia

Según el dominio 9.- Seguridad de las comunicaciones. – Se incrementó favorablemente por mejoras y controles en los servicios de la red judicial.

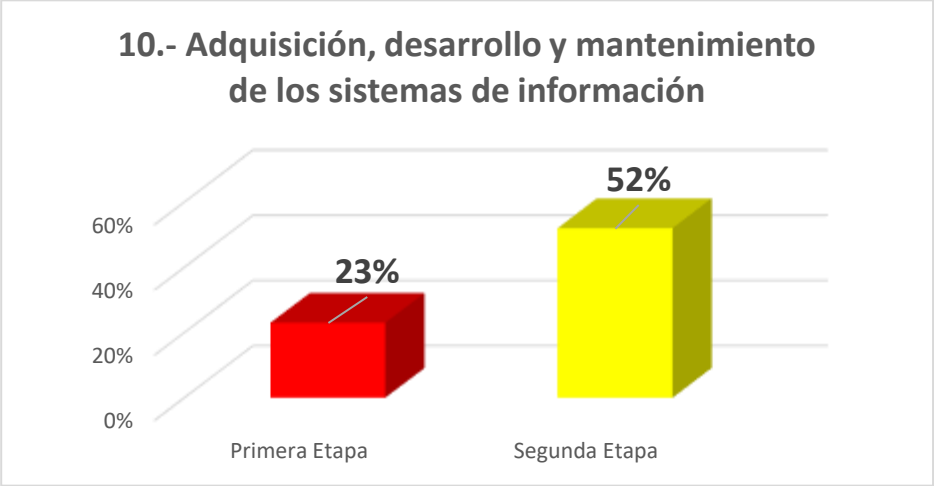


Figura 18.- Adquisición, desarrollo y mantenimiento de los sistemas de información - Comparativo 1era y 2da Etapa Fuente: Elaboración propia

Según el dominio 10. Adquisición, desarrollo y mantenimiento de los sistemas de información. – En la primera etapa de la investigación, este punto venía siendo muy precario entre gestiones que realiza personal de sistemas con logística, encontrándose expuestos a alguna intrusión mal intencionada de parte de terceros; esto tuvo sus mejoras significativas luego de la segunda etapa.

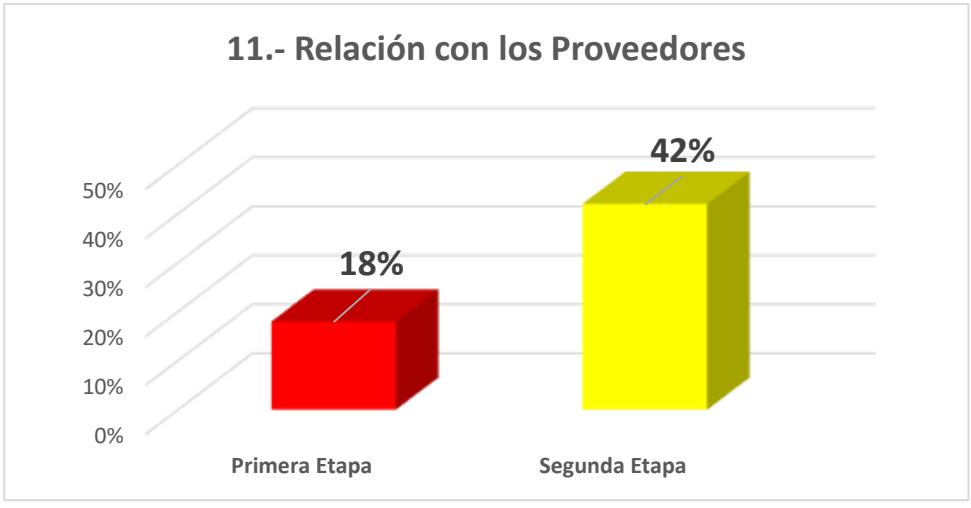


Figura 19.- Relación con los proveedores - Comparativo 1era y 2da Etapa
Fuente: Elaboración propia

Según el dominio 11. Relación de Proveedores. – Se mejoró en la segunda etapa favorablemente por las distintas áreas que tienen comunicación con los proveedores o terceros que se involucran con la información de la institución donde son supervisadas constantemente por personal asignado para esta labor, asimismo la documentación cuando es de carácter físico, está debidamente lacrado y etiquetado por parte del proveedor.

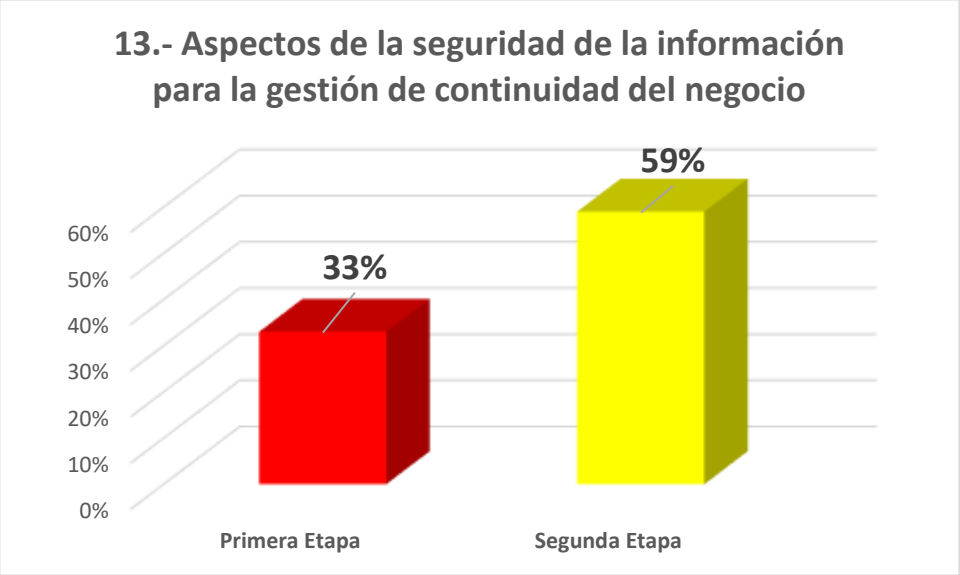


Figura 20.- Aspectos de la seguridad de la información para la gestión de continuidad del negocio - Comparativo 1era y 2da Etapa Fuente: Elaboración propia

Según el dominio 13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio. – Mejora significativa debido a que la seguridad de la información fue integrada en el proceso de gestión.

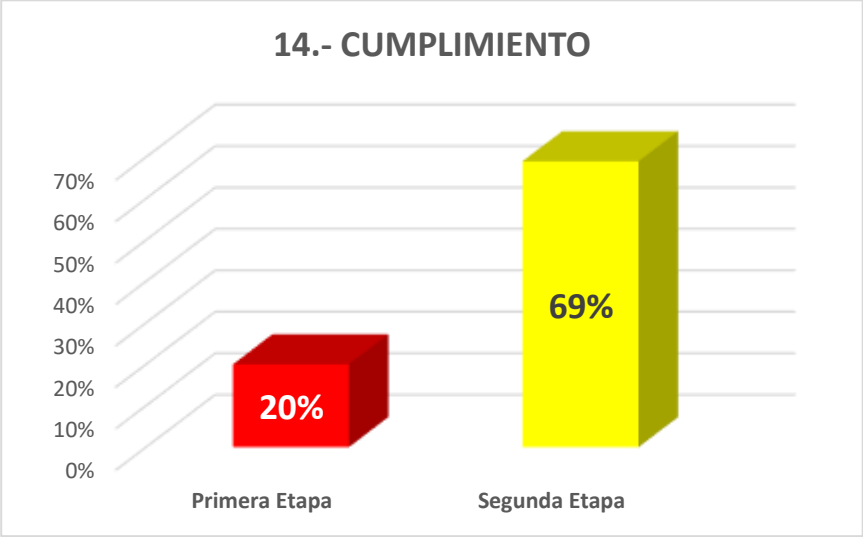


Figura 21.- Cumplimiento - Comparativo 1era y 2da Etapa
Fuente: Elaboración propia

Según el dominio 14. Cumplimiento. – Incremento favorable ya que se alineo a la legislación y disposiciones vigentes.

Discusión de los resultados

A partir de los hallazgos encontrados y luego de la revisión de diferentes investigaciones sobre seguridad informática implementando la norma ISO 27002:2013, coincido con la teoría de muchos investigadores, donde se establece que la mejor forma de prevenir y mejorar la seguridad informática, es utilizando métodos, software, configuraciones, accesorios, y normas que cautelen ataques mal intencionados de personas que buscan dañar, manipular, robar o eliminar lo más valioso de toda institución, la información.

El objetivo es crear o desarrollar formas de prevención que beneficien y protejan la bases tecnológicas y humanas dentro de toda institución, así como cautelar la seguridad de la información. **Tasinchana, C., & Maribel, S. (2017).**

Gómez y Andrés (2012) afirman que la norma ISO/IEC 27002 establece las directrices y principios generales para el inicio, implementación, mantenimiento y mejora de la gestión de la seguridad de la información en una organización. En ese sentido, los controles escogidos para esta investigación fueron los que más se ajustan a la institución judicial, buscando mejorar la seguridad informática, en beneficio de los trabajadores y del público en general.

El punto que diferimos todos los investigadores, son las tecnologías y metodologías utilizadas como apoyo en la investigación, tal como el COBIT, PAM, PPDIOO, PMBOK, etc., pero todos enfocados a un mismo norte, la seguridad de la información.

CAPÍTULO V.

5.1. Conclusiones y recomendaciones

5.1.1. Conclusiones

Se concluye que, en un alto nivel porcentual, la implementación de un Plan de seguridad informática, basado en la norma ISO 27002:2013, permite elevar la seguridad de la información en la Corte Superior de Justicia de Lima, y para esto se tomó 14 de 144 controles que son los que más se ajustan a las necesidades de la institución judicial.

La implementación de un Plan de Seguridad Informática basado en la norma y controles de la ISO 27002:2013, mejoró el nivel de la seguridad de la información que venía atravesando las áreas de Gerencia de Administración, contabilidad y logística de la Corte Superior de Lima. Los análisis previos y las entrevistas realizadas a los coordinadores de las áreas, proporcionó vital información para el uso correspondiente en la implementación de los controles de dicha norma de acuerdo a los puntos descritos en la sección resultados de este trabajo de investigación.

Con estos datos se identificó los puntos críticos que carecían de seguridad de la información, y se trabajó en eso volcando la norma acotada.

Se observa que muchos de los controles utilizados, son utilizados por otras organizaciones públicas y privadas en materias de seguridad y en otros casos, se piensa que dicha implementación puede ocasionar gastos elevados, sin tener en cuenta, que la protección de la información de la institución podría tener un costo invalorable.

Por último, el hecho de establecer el uso de algunos puntos de la norma ISO 27002:2013, no da a entender que la institución judicial, se encontrará blindada ante cualquier ataque malicioso,

pero sí podrá afrontar y quizá minimizar las probabilidades de atravesar momentos adversos por la falta de la seguridad informática y de la información.

Las competencias profesionales adquiridas durante mi desempeño en el tiempo con que cuento en la institución ya que realicé funciones en las áreas administrativas y ahora en el área de informática, me hicieron comprender mejor los procesos que se utilizan en los sistemas utilizados en la Corte de Lima, las vulnerabilidades y precariedad con que se venían desarrollado las labores diarias de los colaboradores de la institución, me hicieron aplicar paulatinamente, mejoras en el parque informático, tales como, mantenimiento preventivo a los equipos y explicar a los usuarios, la importancia de la seguridad de la información, y ya luego con el fin de mis estudios profesionales, impulsar a través del desarrollo de mi trabajo de investigación, la implementación de 14 controles de la norma ISO 27002, con la finalidad de mejorar la seguridad informática, de esta institución judicial.

5.1.2. Recomendaciones

Debido a la emergencia sanitaria que atraviesa el mundo entero, lo cual no es ajeno el Perú y sus poderes del estado, en este caso, el Poder Judicial, entidad que encierra a la Corte Superior de Justicia de Lima, donde se realizó el proyecto de la implementación de un Plan de seguridad buscando optimizar la gestión en dicha entidad, y aun teniendo a los trabajadores en proporción distribuida entre trabajo presencial, mixto y remoto, queda pendiente poner en conocimiento y en práctica lo que sugiere el uso de la norma ISO 27002, razón por la cual, se recomienda, que se efectúen sesiones de capacitación remota al personal que aún no toma conocimiento de lo efectuado, buscando así, poder abarcar la totalidad de usuarios con que cuenta la entidad.

Realizar el monitoreo permanente de la seguridad informática, para lo cual, las jefaturas de cada área, deban crear comités de información, difusión y ejecución de la citada norma, buscando llegar a la totalidad del personal.

Luego de este estudio y análisis real de los riegos y vulnerabilidades que puedan afectar el normal funcionamiento de la institución pública que se viene investigando, se sugiere la continuidad del plan de implementación de seguridad informática, el uso de la norma ISO 27002:2013, para así poder afrontar alguna amenaza o vulnerabilidad y con esto:

- Lograr los objetivos integrales que se plantean en esta investigación.
- Establecer un plan que continuidad en la institución ante cualquier amenaza, vulnerabilidad o incidente provocado por la naturaleza o por terceros.
- Las jefaturas deberán continuar con las capacitaciones a los colaboradores nuevos de la oficina de informática para el manejo de la norma ISO 27007:2013, para un buen uso de la base de datos y sus demás sistemas.
- Continuar con el plan del mantenimiento preventivo, así como el monitoreo de los bienes de la Corte Superior de Justicia de Lima.
- Continuar con el proyecto de renovación de equipos informáticos para estar a la vanguardia de la tecnología.
- Realizar copia de seguridad periódicas de las bases de datos de los sistemas que utiliza la entidad judicial.
- Se realizó el convenio entre la gerencia de informática del Poder Judicial y la Presidencia del Consejo de ministros, para el dictado de cursos diversos, incluyendo cursos de seguridad de la información, para nutrir los conocimientos de los trabajadores judiciales (Anexo 6).

Los resultados de este estudio, deben ser evaluados y analizados periódicamente y se debe actualizar ya que esto permitirá un alto compromiso de la seguridad en favor de la Corte Superior de Justicia de Lima.

LECCIONES APRENDIDAS

Como trabajador de esta institución judicial ya hace más de 25 años, noté muchas deficiencias en lo que concierne no solo a la seguridad informática, si no, a la seguridad integral de la entidad, puntos que se fueron corrigiendo con el paso de los años, y lo que me motivó, durante el desarrollo de mi carrera profesional, aportar mejoras en lo que me compete, esto es, el campo de la informática, razón por la cual, me incliné a desarrollar una tesis, donde se implemente la seguridad informática buscando mejorar la gestión, en este caso, de las oficinas administrativas para luego abarcar a toda la Corte Superior de Justicia de Lima, y quien sabe, quizá a todo el Poder Judicial.

Con la lectura de material bibliográfico ubicados en los buscadores científicos como Alicia Concytec, Scielo y Redalyc, se pudo determinar que el uso de las normas ISO 27001 la cual nos da posibilidad de conocer el Sistema de Gestión de la Seguridad de la Información, y enfocados en la norma 27002, se realizó la presente investigación, tomando como referencia 14 controles de esta última norma ISO. Asimismo, se determinó en esta investigación que el activo más importante de toda institución, es la información, y el uso de esta norma, nos permitió tener un mayor alcance para el cuidado y beneficio de los activos de la institución judicial.

A continuación, un breve detalle de las lecciones aprendidas:

1. Esta pandemia, trajo para muchas instituciones estatales, el inicio del trabajo remoto o teletrabajo, lo cual trajo consigo, una serie de vulnerabilidades que podría afectar la seguridad informática de la institución judicial.
2. La importancia de la difusión en las medidas de seguridad, a través de los correos institucionales.
3. La importancia de saber la cantidad de bienes de la institución para así tomar medidas de seguridad informática, tales como contar con antivirus actualizado en todos los equipos.
4. La importancia de los mantenimientos preventivos y medidas de control.

REFERENCIAS

Alexander, a. G. (2007). Diseño de un sistema de gestión de seguridad de información: Óptica ISO 27001:2005. Bogotá: Alfaomega Colombiana.

Talavera Álvarez, V. R. (2015). Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de Acuerdo a la Iso/Iec 27001: 2013.

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica-ESPOL, 28(5).

(2018 - Jaime Vásquez Escalante – Implementación del sistema de gestión ISO – UNMSM).

Bertolín, J. A. (2008). Seguridad de la información. Redes, informática y sistemas de información. Editorial Paraninfo.

Luis Castro (2019) Análisis y diseño de un sistema de gestión de seguridad informática para la empresa star audio.

Muñoz, j. (2018). Diseño de un plan estratégico para la seguridad de la información de cias & profesionales sas.

Michel Miranda Cairo ; Osmany Valdés Puga ; Iván Pérez Mallea ; RenierPortelles Cobas ; Raúl Sánchez Zequeira ; Revista Cubana de Ciencias Informáticas 2016, 10 (2)

Vallejo, M. R. L. (2017). Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. Revista Publicando, 4(10 (1)), 31-51.

Alexander, Alberto.: Diseño de un Sistema de Gestión de Seguridad de la Información – óptica ISO 27001:2005. Alfaomega. Bogotá - Colombia (2007)

Metodología de la Investigación - Roberto Hernández Sampieri – 6ta edición

Knapp, K. J., Franklin Morris Jr., R., Marshall, T. E., & Byrd, T. A. (2009). Informationsecuritypolicy: Anorganizational-levelprocessmodel. Computers Security, 28(7), 493-508. Elsevier Ltd.

Escalante Terán, O. M. (2018). Conflictos entre la gobernabilidad y la soberanía en organizaciones multilaterales: Estudio de la implementación de políticas de seguridad informática entre los años 2004 - 2016 en la Unión Europea.

Celis Figueroa, L. A. (2018). Plan de seguridad de la información aplicado a la central hidroeléctrica Carhuaquero.

Aguilera, P. (2011). Redes seguras (Seguridad informática). Madrid, España: Editex.

Huanca Suaquita, J. R. (2018). La falsa percepción en la seguridad de los sistemas informáticos.

Guevara Pérez, O., & Miranda Zelada, A. A. (2014). Diseño de una red de datos para el policlínico Señor de los Milagros S.R.L., usando metodología Top Down Network Design y aplicando estándares ISO/IEC 27002.

Acevedo Gutiérrez, A. (2017). Propuesta de implementación de tecnología Sandbox en una entidad financiera para la prevención de presencia de Ransomware en la red interna y mitigación de incidentes.

García Paredes, A. (2016). Implementación de un sistema de gestión de Seguridad de la información, aplicado a los Riesgos asociados a los activos de información En la empresa Net – Consultores S.A.C.

Gil Izurraga, J. E., & Maihuiri Vargas, L. A. (2018). Implementación de un Data Center Virtual en Cloud Computing para mejorar los servicios del departamento de TI en la Empresa Venus peruana S.A.C.

Cortéz Rodríguez, A. I., & Santiago Cueva, W. J. (2018). Plan de seguridad informática basado en la norma Iso 27002 para mejorar la gestión tecnológica del colegio carmelitas – Trujillo.

Gavidia Mamani, S., & Torres Torres, L. D. (2018). Implementación de los controles de la ISO/IEC 27002: 2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte.

Angulo Castillo, A. M. (2014). Plan de seguridad informático para mejorar la calidad en el servicio del call center de la empresa telsat perú sac.

López Sovero, C. E. (2015). Sistema de Control basado en COBIT para la certificación SOX. Caso: AFP en Perú.

Martínez Borja, J. J. (2014). Controles de seguridad para reducir la cantidad de incidencias de seguridad de la información del año 2012 en el servicio de administración tributaria de Huancayo.

Franco, D. C., & Guerrero, C. D. (2013). Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002. In 11th Latin American and Caribbean Conference for Engineering and Technology (pp. 1-10).

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (22), 73-88.

Ramos, Y., Urrutia, O., Bravo, A., & Ordoñez, D. (2017, July). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002: 2013 para la Cooperativa Codelcauca. In Memorias de Congresos UTP (pp. 88-95).

Aliaga Flores, L. C. (2013). Diseño de un sistema de gestión de seguridad de información para un instituto educativo.

Camelo, L., de Negocios, A. D. I., del Negocio, C., de Aplicabilidad, D., Informáticos, D., & Externos, D. (2010). Seguridad de la Información en Colombia. Obtenido de http://seguridadinformacioncolombia. blogspot. com. co/2010/02/marco-legal-deseguridad-de-la. html.

Tasinchana, C., & Maribel, S. (2017). Análisis e Implantación de la norma ISO/IEC 27002: 2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos).

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia et technica, 22(2).

Infante Moro, A., Infante Moro, J. C., Martínez López, F. J., & García Ordaz, M. (2016). Percepción de la importancia de la seguridad informática en la industria hotelera española. El turismo y la experiencia del cliente: IX jornadas de investigación en turismo (2016), p 77-89.

Pinto, M. G. H., & Sánchez, B. A. N. (2016). Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial. Obtenido de Escuela Superior Politécnica del Litoral: https://www. dspace. espol. edu. ec/retrieve/94448/D-71165. pdf.

Haro, C. A. R. (2015). La Seguridad Informática. Ciencia Unemi, 4(5), 26-33.

https://www.calameo.com/books/0040572544de9b12d95ed

Antúnez Pajuelo, J. M. (2012). Plan de contingencia para casos de emergencia tienda Cassinelli - Surquillo.

Ortiz (2013) Controles de seguridad según la norma ISO/IEC 27002:2013 para el mejoramiento de la gestión de Seguridad de la información en la universidad Nacional agraria de la selva.

Leiva Peña, R. (2017). Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015.

Sandoval Fernández, L. R. (2019). Modelo de buenas prácticas aplicando ISO 27002 para gestión de incidencias de la red Wncor.

Palomino Palomino, K. (2017). Buenas Prácticas en Seguridad de la Información Basada en Iso 27002 en la Asociación Para el Desarrollo Empresarial en Apurímac – ADEA.

García Rivera, J. E., & Del Águila Salas, C. A. R. (2017). Análisis e implementación de la seguridad de la información del centro de datos de la Universidad Nacional de la Amazonía Peruana bajo la norma ISO 27002.

Rodríguez Barbarán, L. V. (2019). Implementación de un sistema de gestión de la calidad basado en la norma ISO 9001 en el proyecto: “Construcción de Viviendas Masivas”.

Calderón Juárez, F. A. (2018). Desarrollo e implementación de un sistema de información online usando dispositivos móviles para optimizar la gestión de recaudación de efectivo en el área de cobranza diaria de la cooperativa de ahorro y crédito san francisco, Huánuco, 2015.

Ingunza Lastra, K. Y., & Valdivia Jaimes, J. A. (2018). Implementación del modelo "Arsi" para optimizar la seguridad de la información en la cooperativa de ahorro y crédito san francisco Ltda. 289.

González, M. A., & Vásquez, L. M. (2013). Impacto del uso de Genexus para la optimización del servicio en la empresa Compañía Monterrico de Movilidad y Mensajería SAC (Tesis de licenciatura). Repositorio de la Universidad Privada del Norte. Recuperado de http://hdl.handle.net/11537/193

Veites, A. G. (2001). Enciclopedia de la seguridad Informática 2da Edición. Alfaomega.

https://alicia.concytec.gob.pe/vufind/Record/UDHR_6ec9e24a13451e416a8d557e5604e18f

Sánchez Sánchez, R. M. (2007). Análisis de riesgos en seguridad informática caso UNMSM

ANEXOS

ANEXO N° 01

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS VARIABLE INDEPENDIENTE: IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA

Nº	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. Implementación de un plan	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Cree Ud. que cuenta la Entidad cuenta con un plan de seguridad informática?	X		X		X		
2	¿Considera Ud. que los sistemas operativos instalados en la Entidad cuentan con los parches actualizados?	X		X		X		
3	¿Cree Ud. que existe un plan de mantenimiento preventivo del parque informático?	X		X		X		
4	¿Cree Ud. que la Entidad cuentan con inventario actualizado de los activos informáticos?	X		X		X		
5	¿Cree Ud. que los colaboradores de la Entidad, está capacitado para su correcto uso de los equipos informáticos?	X		X		X		
6	¿Cree Ud. que la Entidad ejecuta el uso de la norma ISO 27002?	X		X		X		
7	¿Cree Ud. que el correo institucional, tiene filtros contra códigos maliciosos, phishing u otro tipo de vulnerabilidad?	X		X		X		
8	¿Cree Ud. que existe controles para reducir los riesgos de la seguridad de la información?	X		X		X		
9	¿Considera Ud. las realiza reuniones periódicas entre los responsables de las áreas son productivas?	X		X		X		

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS VARIABLE INDEPENDIENTE: IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA

Nº	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. Mejora de gestión	Si	No	Si	No	Si	No	
1	¿Considera Ud. que existe la necesidad de estandarizar la documentación generada en las áreas administrativas?	X		X		X		
2	¿Considera Ud. que la carga laboral es equitativa en las diferentes áreas administrativas?	X		X		X		
3	¿Cuenta la entidad con procedimientos y funciones, definidos por cada área administrativa?	X		X		X		
4	¿Considera Ud. que la Entidad cuenta con sistema de medición de productividad de manera periódica?	X		X		X		
5	¿Considera Ud. que la Entidad cuenta con herramientas informáticas estandarizadas?	X		X		X		
6	¿Cree Ud. que el ambiente laboral en la Entidad es el adecuado?	X		X		X		
7	¿Considera Ud. que los colaboradores de la Entidad reciben constantemente capacitaciones para desarrollar mejor sus labores?	X		X		X		
8	¿Cree Ud. que la Entidad realiza las acciones necesarias para la mejora los procesos administrativos?	X		X		X		
9	¿Cree Ud. que los colaboradores tienen conocimiento en temas de seguridad de la información?	X		X		X		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable (X) Aplicable después de corregir ( )
No Aplicable ( )

Apellidos y Nombres del Validador: Javier Ángel Ingaroca Salas
Nº DNI: 09426429 **CIP:** 190076
Especialidad del Validador: Gestión de Tecnologías de la Información y Comunicaciones (TICs)
Grado Académico: Magister (X) Doctor ( )

Lima, 24 de setiembre de 2021

……..
Firma del Validador

ANEXO N° 01

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS VARIABLE INDEPENDIENTE: IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA

Nº	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. Implementación de un plan	Si	No	Si	No	Si	No	
1	¿Cree Ud. que cuenta la Entidad cuenta con un plan de seguridad informática?	X		X		X		
2	¿Considera Ud. que los sistemas operativos instalados en la Entidad cuentan con los parches actualizados?	X		X		X		
3	¿Cree Ud. que existe un plan de mantenimiento preventivo del parque informático?	X		X		X		
4	¿Cree Ud. que la Entidad cuentan con inventario actualizado de los activos informáticos?	X		X		X		
5	¿Cree Ud. que los colaboradores de la Entidad, está capacitado para su correcto uso de los equipos informáticos?	X		X		X		
6	¿Cree Ud. que la Entidad ejecuta el uso de la norma ISO 27002?	X		X		X		
7	¿Cree Ud. que el correo institucional, tiene filtros contra códigos maliciosos, phishing u otro tipo de vulnerabilidad?	X		X		X		
8	¿Cree Ud. que existe controles para reducir los riesgos de la seguridad de la información?	X		X		X		
9	¿Considera Ud. las realiza reuniones periódicas entre los responsables de las áreas son productivas?	X		X		X		

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS
VARIABLE DEPENDIENTE: OPTIMIZACIÓN DE GESTIÓN

Nº	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. Mejora de gestión	Si	No	Si	No	Si	No	
1	¿Considera Ud. que existe la necesidad de estandarizar la documentación generada en las áreas administrativas?	X		X		X		
2	¿Considera Ud. que la carga laboral es equitativa en las diferentes áreas administrativas?	X		X		X		
3	¿Cuenta la entidad con procedimientos y funciones, definidos por cada área administrativa?	X		X		X		
4	¿Considera Ud. que la Entidad cuenta con sistema de medición de productividad de manera periódica?	X		X		X		
5	¿Considera Ud. que la Entidad cuenta con herramientas informáticas estandarizadas?	X		X		X		
6	¿Cree Ud. que el ambiente laboral en la Entidad es el adecuado?	X		X		X		
7	¿Considera Ud. que los colaboradores de la Entidad reciben constantemente capacitaciones para desarrollar mejor sus labores?	X		X		X		
8	¿Cree Ud. que la Entidad realiza las acciones necesarias para la mejora los procesos administrativos?	X		X		X		
9	¿Cree Ud. que los colaboradores tienen conocimiento en temas de seguridad de la información?	X		X		X		

Observaciones (precisar si hay suficiencia): Existe Suficiencia.

Opinión de aplicabilidad: Aplicable (X) Aplicable después de corregir ( ) No Aplicable ( )

Apellidos y Nombres del Validador: Haydeé Ingrid Castillo Cáceres
Nº DNI: 40852436 **CIP:** 145805
Especialidad del Validador: Ingeniería de Sistemas con Mención en Tecnologías de la Información
Grado Académico: Magister (X) Doctor ( )

Lima, 24 de setiembre de 2021

.....
Firma del Validador

ANEXO Nº 01

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS VARIABLE INDEPENDIENTE: IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA

Nº	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. Implementación de un plan	Si	No	Si	No	Si	No	
1	¿Cree Ud. que cuenta la Entidad cuenta con un plan de seguridad informática?	X		X		X		
2	¿Considera Ud. que los sistemas operativos instalados en la Entidad cuentan con los parches actualizados?	X		X		X		
3	¿Cree Ud. que existe un plan de mantenimiento preventivo del parque informático?	X		X		X		
4	¿Cree Ud. que la Entidad cuentan con inventario actualizado de los activos informáticos?	X		X		X		
5	¿Cree Ud. que los colaboradores de la Entidad, está capacitado para su correcto uso de los equipos informáticos?	X		X		X		
6	¿Cree Ud. que la Entidad ejecuta el uso de la norma ISO 27002?	X		X		X		
7	¿Cree Ud. que el correo institucional, tiene filtros contra códigos maliciosos, phishing u otro tipo de vulnerabilidad?	X		X		X		
8	¿Cree Ud. que existe controles para reducir los riesgos de la seguridad de la información?	X		X		X		
9	¿Considera Ud. las realiza reuniones periódicas entre los responsables de las áreas son productivas?	X		X		X		

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS
VARIABLE DEPENDIENTE: OPTIMIZACIÓN DE GESTIÓN

Nº	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. Mejora de gestión	Si	No	Si	No	Si	No	
1	¿Considera Ud. que existe la necesidad de estandarizar la documentación generada en las áreas administrativas?	X		X		X		
2	¿Considera Ud. que la carga laboral es equitativa en las diferentes áreas administrativas?	X		X		X		
3	¿Cuenta la entidad con procedimientos y funciones, definidos por cada área administrativa?	X		X		X		
4	¿Considera Ud. que la Entidad cuenta con sistema de medición de productividad de manera periódica?	X		X		X		
5	¿Considera Ud. que la Entidad cuenta con herramientas informáticas estandarizadas?	X		X		X		
6	¿Cree Ud. que el ambiente laboral en la Entidad es el adecuado?	X		X		X		
7	¿Considera Ud. que los colaboradores de la Entidad reciben constantemente capacitaciones para desarrollar mejor sus labores?	X		X		X		
8	¿Cree Ud. que la Entidad realiza las acciones necesarias para la mejora los procesos administrativos?	X		X		X		
9	¿Cree Ud. que los colaboradores tienen conocimiento en temas de seguridad de la información?	X		X		X		

Observaciones (precisar si hay suficiencia): Existe Suficiencia.

Opinión de aplicabilidad: Aplicable (X) Aplicable después de corregir ( ) No Aplicable ( )

Apellidos y Nombres del Validador: Verónica Asunción Bravo Mendoza
Nº DNI: 09750797 **CIP:** 87032
Especialidad del Validador: Gestión de Tecnologías de la Información y Comunicaciones (TICs)
Grado Académico: Magister (X) Doctor ( )

Lima, 24 de setiembre de 2021

.....
Firma del Validador

ANEXO N° 2

PLAN DE MANTENIMIENTO PREVENTIVO DE EQUIPOS DE COMPUTO DE LA CORTE SUPEIOR DE JUSTICIA DE LIMA

Este documento tiene como finalidad, elaborar un plan de trabajo propuesto por la oficina de Informática de la Unidad de Planeamiento y Desarrollo, de la Corte Superior de Justicia de Lima, donde se propone la ejecución de un Plan preventivo del parque informático en toda la institución.

La Unidad en mención, tiene la iniciativa de establecer los planes del mantenimiento preventivo, para evitar fallas en los equipos de cómputo de la institución, así como corregir errores de funcionamiento buscando con esto, un estado optimo en todo el parque informático de la institución judicial.

Dicha labor será ejecutada por el personal de soporte técnico de la coordinación de informática, previa coordinación con los administradores de piso y sede, los cuales deberán transmitir dicha orden al personal a su cargo, buscando con esto, el beneficio para todos los trabajadores judiciales.

Actividades a realizar:

1. **Realizar inventario**
   Es muy importante antes de realizar el mantenimiento preventivo, contar con un inventario actualizado de todo el parque informático de la institución para tener un mejor control de los mencionados bienes.
   Estas actividades se programaron para el mes de junio del año en curso.
2. **Mantenimiento preventivo del parque informático.**
   Esta labor se desarrollará en 2 etapas.
   - Equipos muy antiguos que hayan perdido garantía, deberá realizarse por personal de soporte técnico.
   - Los equipos que se encuentren en garantía o bajo alguna modalidad de mantenimiento vigente, deberán ser evaluados por la empresa que corresponda.

Periodo de ejecución

Estos mantenimientos deberán realizarse 2 veces al año, teniendo en cuenta la disponibilidad del personal que ejecutará dicha labor.

PODER JUDICIAL
Coordinación de Informática
Corte Superior de Justicia de Lima

Ing. JUAN W. FELICIANO BARRERA
Coordinador de Informática
Unidad de Planeamiento y Desarrollo
CORTE SUPERIOR DE JUSTICIA DE LIMA

ANEXO N° 3

CALENDARIO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS INFORMÁTICOS DE LA CSJLIMA PARA EL AÑO 2021

Mantenimiento	Taller					
Meses	Julio			Agosto		
Días	01 al 10	11 al 20	21 al 30	01 al 10	11 al 20	21 al 30
Cant. De PC's	500	500	1000	500	500	1000
Mantenimiento de Hardware						
Mantenimiento de Software						

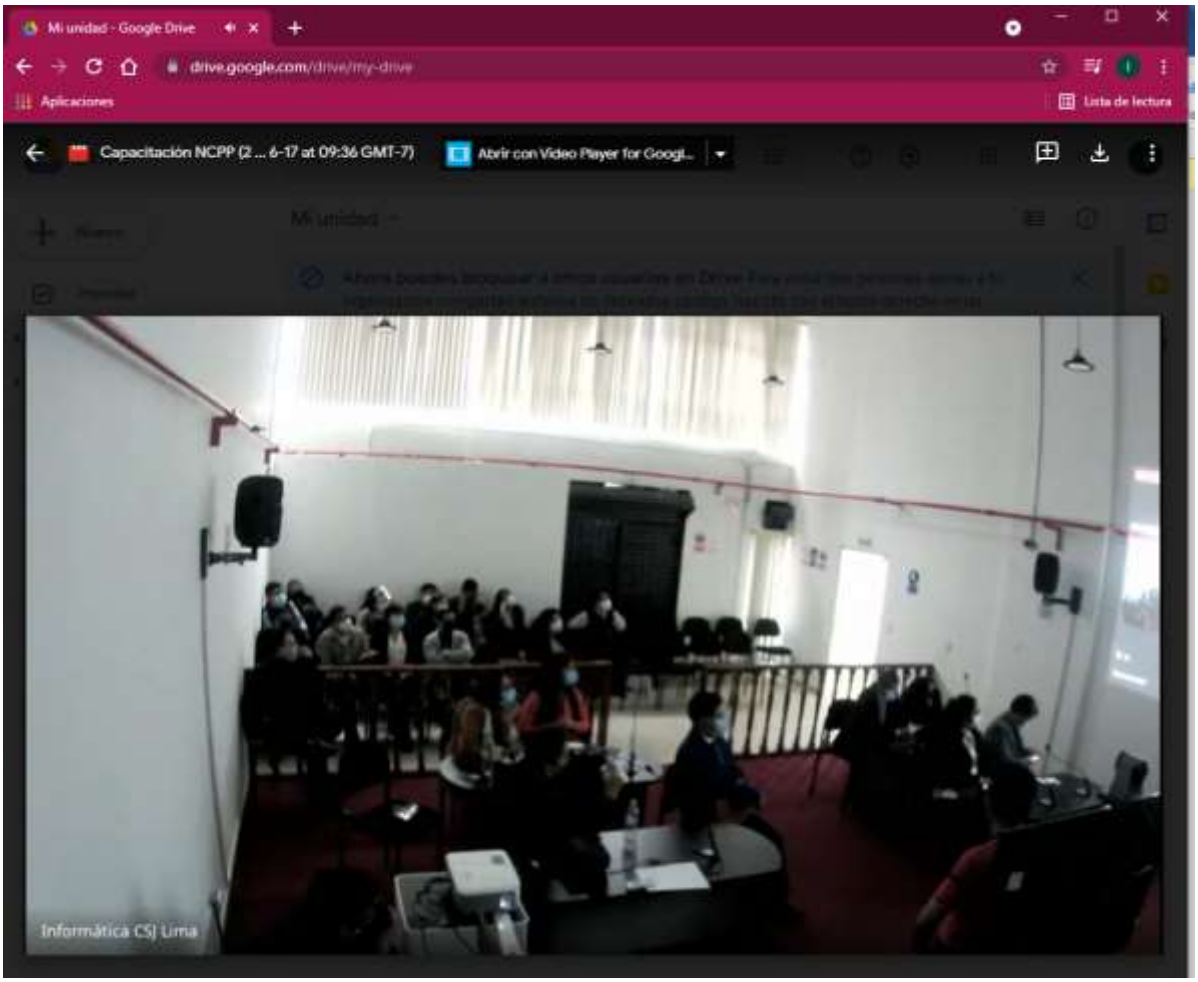
PODER JUDICIAL
Ing. JUAN W. FELIGIANO BARRERA
Coordinador de Informática
Unidad de Planeamiento y Desarrollo
CORTE SUPERIOR DE JUSTICIA DE LIMA

ANEXO 4

INSTALACIÓN DE CONTROLES BIOMETRICOS

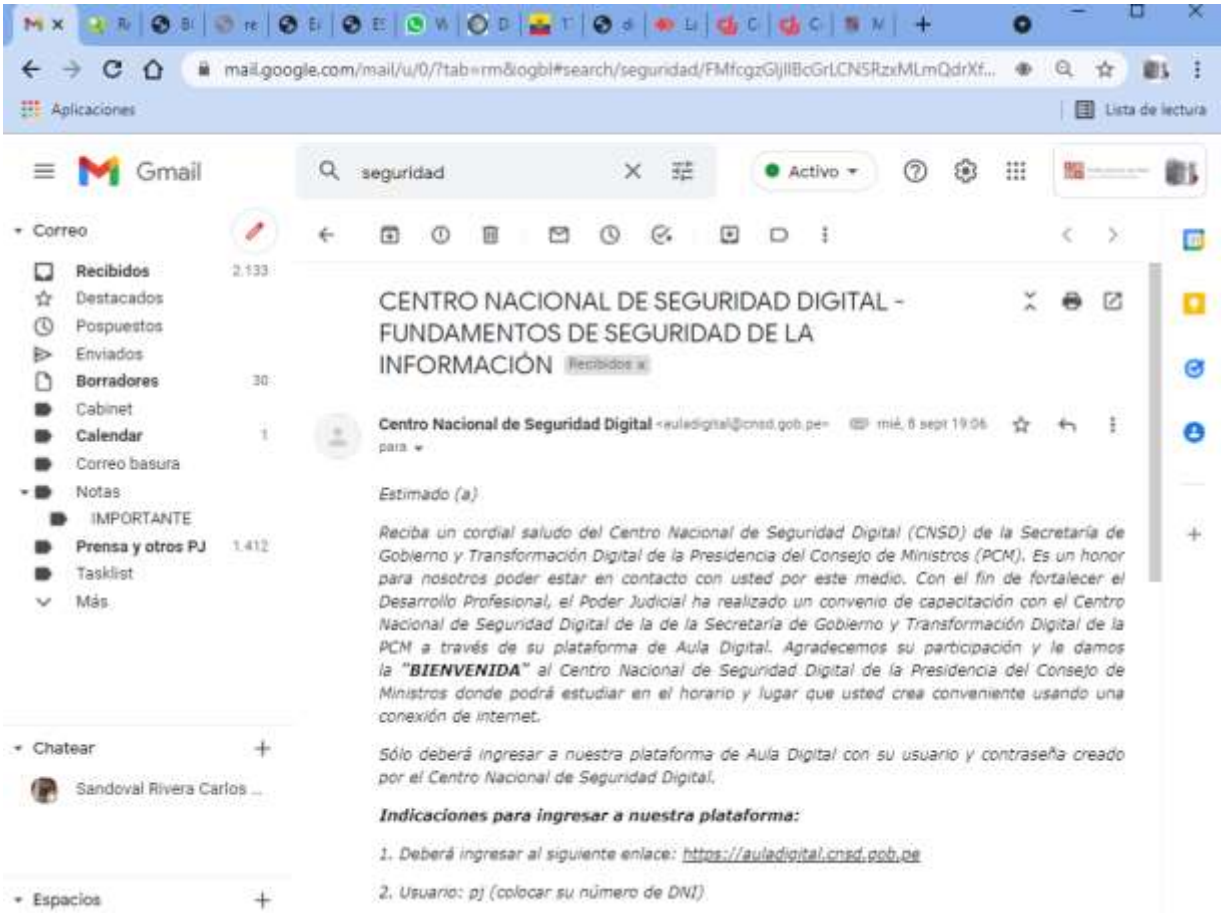
ANEXO 5

Capacitación al personal nuevo, sobre seguridad informática realizado en las instalaciones de la Sala de audiencias de la sede de las Salas y Juzgados Penales



ANEXO 6

Continuidad con cursos de seguridad de la información, difundida por el correo institucional




Instructivo Fund ... der Judicial.pdf
Abrir con Documentos de Google
CENTRO NACIONAL DE SEGURIDAD DIGITAL
CURSO FUNDAMENTOS DE CIBERSEGURIDAD PARA EMPRESAS
Fundamentos de Ciberseguridad para empresas
Presentación del reglamento de la Ley de Gobierno ...
CURSO LINUX ESSENTIALS
Linux Essentials
CURSO FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN
Fundamentos de Seguridad de la Información
CURSO ANÁLISIS DE VULNERABILIDADES DIGITALES
Análisis de Vulnerabilidades Digitales
CURSO AUDITOR INTERNO ISO 27001
Auditor Interno ISO 27001
CYBERWOMEN
PERÚ 2021
Taller Cyberwomen Perú 2021
CURSO IMPLEMENTACIÓN DEL EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DIGITAL
CURSO GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL MARCO DE LA CONFIANZA DIGITAL
Página 2 de 3