UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

HUGO DANIEL OLAZA ALIANO

ASESOR:

DR. FREY ELMER CHAVEZ PINILLOS

LÍNEA DE INVESTIGACIÓN:

AUDITORIA DE SISTEMAS Y SEGURIDAD DE LA INFROMACIÓN

LIMA – PERU

2017

ING. IVAN CRISPIN SANCHEZ

Presidente

MG. FERNANDO MENDOZA APAZA

Secretario

ING. RUDY CHAPOÑAN CAMARENA

Vocal

Dedicatoria

Dedico el presente trabajo:

A mis padres por su sacrificio constante, compañeros de labores, amigos y a todos aquellos que me animaron a siempre continuar a pesar de las adversidades.

Agradecimiento

A los docentes y a la Universidad César Vallejo por mi formación académica, en especial al Doctor Frey Chávez Pinillos, asesor de la presente investigación, por compartir su sabiduría, conocimiento y sobre todo por brindarme su apoyo en todo momento. A mis compañeros de trabajo gracias por el apoyo y amistad brindada y a todas aquellas personas que, de una u otra forma, colaboraron o participaron en la realización de esta investigación, hago extensivo mi más sincero agradecimiento.

DECLARACIÓN DE AUTENTICIDAD

Yo Hugo Daniel Olaza Aliano Con DNI N° 42238844, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad César Vallejo, Facultad de Ingeniería, Escuela de Ingeniería de Sistemas, declaro bajo juramento que toda la documentación que acompaño es veraz y auténtica.

Así mismo, declaro también bajo juramento que todos los datos e información que se presentan en la presente tesis son auténticos y veraces.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada por lo cual me someto a lo dispuesto en las normas académicas de la Universidad César Vallejo.

Lima, julio del 2017

Presentación

Señores miembros del jurado:

En cumplimiento de las normas establecidas en el Reglamento de Grados y Títulos de la Universidad César Vallejo presento ante ustedes la tesis titulada "IMPLEMENTACIÓN DE NTP ISO/IEC 27001 PARA LA SEGURIDAD DE INFORMACIÓN EN EL ÁREA DE CONFIGURACIÓN Y ACTIVOS DEL MINISTERIO DE EDUCACIÓN – SEDE CENTROMIN" la misma que someto a vuestra consideración y espero que cumpla con todos los requisitos de aprobación para obtener el título profesional de Ingeniero de Sistemas.

La presente investigación tiene la finalidad de determinar el efecto de la implementación de la Norma Técnica Peruana ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación Sede Centromin, la cual consta de siete capítulos; el capítulo I plantea una introducción describiendo la realidad problemática, trabajos previos, teorías relacionadas al tema, formulación del problema, justificación del estudio, hipótesis y los objetivos que lo guían, el capítulo II describe y explica el diseño de investigación, las variables de estudio y su operacionalización. Adicionalmente se explica la población, la muestra y se detalla las técnicas e instrumentos para el recojo y procesamiento de la información, la validación y confiabilidad del instrumento, los métodos de análisis de los datos y aspectos éticos de la investigación, el capítulo III se refiere a los resultados de la investigación así como a la comprobación de las hipótesis, en el capítulo IV se presenta y se discuten los resultados de la investigación, en el capítulo V se presentan las conclusiones, en el capítulo VI se presentan las recomendaciones, en el capítulo VII se detallan las referencias bibliográficas utilizadas y finalmente se completa con los anexos.

Se espera señores miembros del jurado que la presente investigación se ajuste a los requerimientos establecidos y que este trabajo de origen a posteriores estudios.

El autor

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE ANEXOS

RESUMEN

La presente investigación tuvo como objetivo determinar el efecto de la implementación de la NTP ISO/IEC 27001 para la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación Sede Centromin.

La investigación realizada fue de tipo aplicada, con un diseño experimental de tipo pre experimental. La población estuvo formada por 4783 registros de la base de datos de activos informáticos, con una muestra de 136, dicho muestreo fue probabilístico y del subtipo aleatorio simple. Se usó como técnica de recopilación de datos la observación. Así mismo, se usó el instrumento ficha de observación. El instrumento de recolección de datos fue validado por medio del juicio de expertos con un resultado de opinión de aplicabilidad y la confiabilidad se realizó mediante la prueba de Wilcoxon, cuyo resultado de las pruebas indican que el Sig. de las muestras es menor que 0.05 (nivel de significancia alfa).

Los resultados de esta investigación confirman que la implementación de la Norma Técnica Peruana ISO/IEC 27001 tuvo un efecto positivo para la Seguridad de Información; en cuanto al número de información confidencial divulgada antes se registraban 182 casos, después de la implementación se registró 50 casos, para el número o porcentaje de accesos y/o cambios no autorizados a los datos de producción antes se registró 322 casos, después de la implementación disminuyó a 47 casos, para el porcentaje de tiempo durante el cual un sistema está disponible para el usuario se registró un porcentaje de 70.36%, después de la implementación aumentó a 98.22% respectivamente.

Palabras clave: Seguridad de Información, ISO/IEC 27001, Disponibilidad, Confidencialidad, Integridad.

ABSTRACT

The present investigation aimed to determine the effect of the implementation of the NTP ISO / IEC 27001 for Information Security in the Configuration and Assets area of the Ministry of Education Centromin.

The research was applied type, with an experimental design of pre-experimental type. The population consisted of 4783 records of the database of computer assets, with a sample of 136, this sampling was probabilistic and of the simple random subtype. Observation was used as data collection technique. Likewise, the instrument of observation was used. The data collection instrument was validated by expert judgment with an applicability opinion result and reliability was performed using the Wilcoxon test, whose test result indicates that the Sig of the samples is less than 0.05 (level of alpha significance).

The results of this investigation confirm that the implementation of the Peruvian Technical Standard ISO / IEC 27001 had a positive effect for Information Security; In terms of the number of confidential information previously disclosed, 182 cases were recorded, 50 cases were recorded after the implementation, for the number or percentage of unauthorized access and / or changes to the production data before 322 cases were recorded, after Implementation decreased to 47 cases, for the percentage of time during which a system is available to the user was recorded a percentage of 70.36%, after implementation increased to 98.22% respectively.

Keywords: Information Security, ISO / IEC 27001, Availability, Confidentiality, Integrity.

1. INTRODUCCIÓN

1.1. Realidad Problemática

En la actualidad, a nivel mundial, uno de los temas que va tomando cada vez más protagonismo en las empresas es de establecer metodologías o estándares relacionadas con la seguridad de información; se conoce que muchas instituciones, tanto públicas o privadas, tienen la errónea idea de invertir dinero y recursos en infraestructura para sanear las necesidades que la empresa requiere en su momento sin realizar estrategias, provocando grandes pérdidas económicas. Por otro lado, se han desarrollado diferentes metodologías para atender esta necesidad, entre ellas, la más aplicada en las empresas es la norma ISO 27001 que hace referencia al Sistema de Gestión de Seguridad de la Información SGSI, cuyo objetivo es la preservación de la Confidencialidad, Integridad y Disponibilidad de la información.

Para Gómez y Suárez:

> En las propias empresas, la creciente complejidad de las relaciones con el entorno y el elevado número de transacciones realizadas como parte de su actividad han propiciado el soporte automatizado e informatizado de muchos de sus procesos, situación que se ha acelerado con la implantación de los ERP, o paquetes software de gestión integral.
>
> Por todo ello, en la actualidad las actividades cotidianas de las empresas y de las distintas Administraciones Públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad.
>
> De ahí la gran importancia que se deberá conceder a todos los aspectos relacionados con la seguridad informática en una organización. La proliferación de los virus y códigos malignos y su rápida distribución a través de redes como Internet, así como los miles de ataques e incidentes de seguridad que se producen todos los años

> han contribuido a despertar un mayor interés por esta cuestión (2011, p. 226).

En el Perú, esto no ha pasado desapercibido, muchas instituciones están encaminándose a la certificación ISO 27001 con el fin de implementar las buenas prácticas para la Seguridad de Información.

El Ministerio de Educación (MINEDU) ubicada en la ciudad de Lima y fundada en el año 1837, cuenta actualmente con más de 200 colaboradores en la Oficina de Tecnologías de la Información y Comunicación (OTIC), con áreas de trabajo basado bajo el enfoque de ITIL, una de ellas es Configuración y Activos, en dicha área será donde se centra esta investigación, la función de dicha área es la de velar por la correcta administración de los activos TI del MINEDU, así como ver los mantenimientos (preventivos y correctivos), altas y bajas, garantías y movimientos de equipos informáticos. En esta oficina se pudo identificar diversas deficiencias como: las “bases de datos” donde se almacenan estos registros están volcadas en una hoja de Excel, donde cualquier usuario con accesos mínimos de red puede acceder a dicha información, poniendo en riesgo la confidencialidad de los datos. Asimismo, no cuenta con servidores de bases de datos para la migración de dichos archivos en Excel. Esta ineficiencia tiene un gran impacto en la OTIC ya que dificulta la toma de decisiones de adquisición de activos informáticos que fueron reportados como “obsoletos” por no tener la disponibilidad de la información. Por otro lado, los colaboradores del área de Configuración y Activos desconocen si la totalidad de la información se encuentra en los archivos, que asumen el papel, de base de datos propia del área, esto conlleva a la pérdida de tiempo ya que el colaborador realiza una búsqueda manual entre los diferentes comprobantes de pago hasta llegar al activo requerido, afectando la integridad de la información, ya que al no estar completa no se tiene un registro exacto de los activos de TI del MINEDU. De continuar con esta realidad la oficina de Configuración y Activos podría colapsar ante una incidencia grave que puedan presentar los equipos informáticos,

condenándolo a una restructura del personal que labora en dicha oficina. Por esta razón se pretende ayudar a la oficina de Configuración y Activos, a implementar las buenas practicas que la ISO 27001 dispone para la Seguridad de Información basado en la NTP ISO/IEC 27001, mejorando la calidad de servicio, así como la gestión de los diferentes activos informáticos y en consecuencia mejorar el prestigio del área y de la OTIC.

1.2. Trabajos Previos

En la tesis de Carlos Barrantes y Javier Hugo del 2012, con el título "**Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos**" con motivo de optar el título profesional de ingeniero de computación y Sistemas de la ciudad de Lima – Perú, la cual busca reducir los riesgos de los activos de información de los procesos que se encuentran bajo la gerencia de tecnologías de Card Perú que ponen en peligro los recursos servicios y continuidad de los procesos tecnológicos. Llegando a la conclusión que la implementación permitió un gran aumento en la seguridad de los activos de información de la empresa Card Perú, que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y tecnologías.

En la tesis de Diana Tola Franco del 2015, con el título "**Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de Consultoría y Auditoría aplicando la norma ISO /IEC 27001**"; buscó la implementación de un sistema de gestión de seguridad de la información basado en la ISO 27001:2005 para preservar la confidencialidad, integridad y disponibilidad de la información que maneja empresa A&CGroup S.A para lo cual se aplicó la metodología de PDCA, y la aplicación correcta de la gestión de riesgo para así identificar y focalizar aquellos elementos que se encuentran más expuestos, dando como resultado implementar controles o salvaguardas con la finalidad de lograr

minimizar la probabilidad de que materialice los riesgos o el impacto que pueda tener sobre la organización.

En la tesis de Vasco Rodrigo Talavera Álvarez del 2015, con el título "**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**", con motivo de optar el título profesional de ingeniero informático de la ciudad de Lima – Perú busca realizar el análisis y Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad pública del sector Salud – el Instituto Nacional Materno Perinatal – sujeta al cumplimiento de la normativa vigente relativa a Seguridad de la Información

En la tesis de Carlos Alberto Guzman Silva en el año 2015, con el título "**Diseño de un Sistema de Gestión de Seguridad de la información para una entidad Financiera de Segundo Piso**"; con motivo de optar el título profesional de Ingeniero de Sistemas y Computación de la ciudad de Chiclayo –Perú donde realizo el diseño de un Sistema de Seguridad de la Información para la empresa IGM S.A., teniendo como referencia la NTC-ISO-IEC: 27001:2013, para ello realizó un análisis y desarrolló de una propuesta para el diseño de un Sistema de Seguridad de la Información; tomando en cuenta el método de investigación de campo que permitirá el analizar sistemáticamente a la realidad del problema, con la finalidad de describir, interpretar, entender su naturaleza y explicar causas y efectos. Llegando como resultado a la conclusión que el nivel de cumplimiento frente al requerimiento del anexo A de la norma ISO/IEC 27001:2013 es del 46% lo que implica que la implementación de Sistema de Seguridad de la Información, aplicará a la entidad un refuerzo considerable debido a la ausencia de controles o al bajo cumplimiento.

Finalmente la tesis de Julio Cesar Alcantara Flores del año 2015, con título "**Guía de Implementación de la Seguridad basado en ISO/ IEC 27001, para apoyar la seguridad en los Sistemas de Información de la Comisaria norte P.N.P. en la ciudad de Chiclayo**", contribuye a mejorar el

nivel de seguridad de la información basado en la norma ISO/IEC 27001, para lo cual realiza una investigación aplicada y realizar un estudio bajo la información de gestión y guías de implementación para seguridad de sistemas de información; además manejará el diseño cuasi-experimental, ya que debido a que analizará el efecto producido por las acciones o la manipulación de una variable independiente sobre una dependiente; para finalmente proponer una guía de implementación que apoye a la seguridad de los Sistemas de Información con la finalidad de medir los riesgos y evaluar los controles en el uso de las Tecnologías de Información. La metodología y el marco teórico empleado en esta investigación sirvieron como base para el desarrollo de esta investigación.

1.3. Teorías relacionadas al tema

1.3.1. Información:

Se sostiene que la información "Es un conjunto de datos transformados (véase figura 1) de forma que constituye a reducir la incertidumbre del futuro y, por tanto, ayuda a la toma de decisiones" (Lapiedra, Devece y Guiral, 2001, p.5).

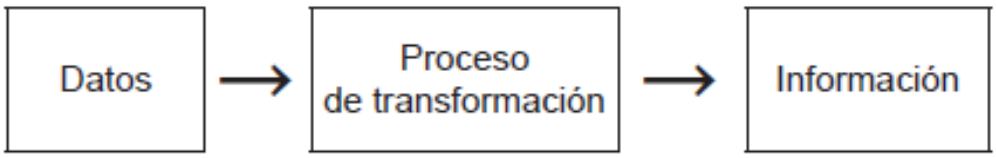


Figura 1. Proceso de trasformación de datos en información.

Así mismo, se indica que la información "Se obtiene una vez que los hechos se procesan, agregan y presentan de la manera adecuada para que puedan ser útiles a alguien dentro de la organización y procesados presentan un mayor valor que en su estado original" (Gómez y Suarez, 2009, p.34)

1.3.2. Características de la información:

Para definir las características de la información Gomes y Suarez explican qué:

> Para que la información sea útil para la organización este deberá tener los siguientes requisitos:
>
> - **Exactitud:** la información ha de ser precisa y libre de errores.
> - **Completitud:** la información debe contener todos aquellos hechos que pudieran ser importantes para la persona que la va utilizar.
> - **Economicidad,** el coste en que se debe incurrir para obtener la información debería ser menor que el beneficio proporcionado por esta a la organización.
> - **Confianza,** para dar crédito a la información obtenida, se ha de garantizar tanto la calidad de los datos utilizados, como la de las fuentes información.
> - **Relevancia,** la información ha de ser útil para la toma de decisiones. En este sentido, conviene evitar todos aquellos hechos que sean superfluos o que no aporten ningún valor.
> - **Nivel de detalle:** la información debería presentar el nivel de detalle indicado a la decisión que se destina se debe proporcionar con la presentación y el formato adecuados, para que resulte sencilla y fácil de manejar.
> - **Oportunidad**, se de entregar la información a la persona que corresponde y en el momento en esta la necesidad para poder tomar una decisión.
> - **Verificabilidad,** la información ha de poder ser contratada y comprobada en todo momento. (2011, p. 35).

1.3.3. Sistemas de información

Para Purificación Aguilera Lopez:

> Un sistema de información (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos, (tal como se aprecia en la figura 2)
>
> Estos elementos son:
>
> - **Recursos**. Pueden ser físicos, como ordenadores, componentes, periféricos y conexiones, recursos no informáticos; y lógicos, como sistemas operativos y aplicaciones informáticas.
> - **Equipo humano**. Compuesto por las personas que trabajan para la organización.
> - **Información**. Conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.
> - **Actividades**. que se realizan en la organización, relacionadas o no con la informática (2010, p. 8).

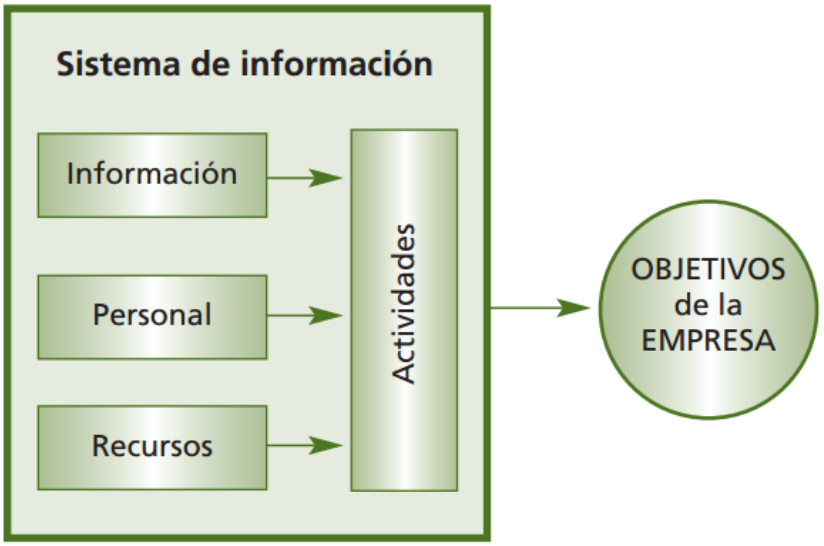


Figura 2. Relación entre los Sistemas de Información y Objetivos de la Empresa

Así mismo, para Gomes y Suarez afirma que:

> Los Sistemas de Información han adquirido una dimensión estratégica en las empresas del nuevo milenio y han dejado de ser considerados una simple herramienta para automatizar procesos operativos para convertirse en una pieza clave a tener en cuenta a la hora de formular la estrategia empresarial, para llevar a cabo su implantación y para realizar el control de la gestión.
>
> Los Sistemas de Información no sólo llegan a condicionar la estrategia de la moderna empresa, sino que, además, constituyen el elemento fundamental para poder llevar a cabo una gestión horizontal de la empresa, orientada a procesos y no a funciones, que permita poner el énfasis en la mejora continua de los resultados, con una clara orientación total hacia el cliente.
>
> Éste es un aspecto que hoy en día se considera clave, no ya para alcanzar el éxito, sino para garantizar la supervivencia de la organización en un entorno tan competitivo y exigente como el actual. De ahí que el estudio de los Sistemas de Información, en relativamente poco tiempo, se haya consolidado como una disciplina por sí misma, constituida por una serie de conceptos, herramientas y técnicas utilizadas para llevar a cabo su planificación, análisis, diseño e implantación.
>
> Hay que tener en cuenta que tradicionalmente se ha puesto el énfasis en los aspectos puramente técnicos, enfocando el estudio hacia la descripción de los componentes tecnológicos del Sistema de Información (las TICs), en detrimento de los aspectos humanos y organizativos, y ello ha provocado una visión sesgada y limitada de toda la problemática asociada al estudio de los Sistemas de Información.

Nuestra experiencia en los campos profesional y académico nos lleva a creer que la planificación y el diseño de los Sistemas de Información en las empresas y organizaciones requieren una perspectiva multidisciplinar que tenga en cuenta los tres aspectos referidos, tal y como se pone de manifiesto en la figura.

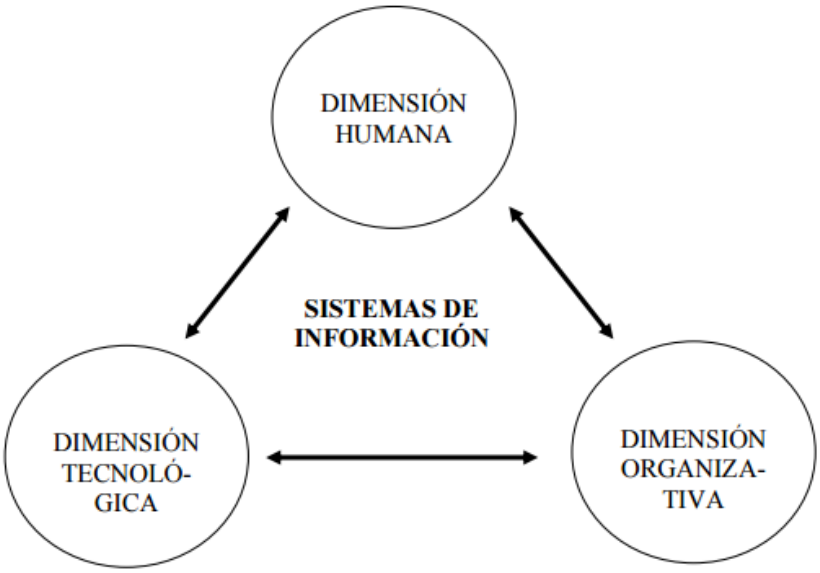


Figura 3. La triple dimensión Humana, Organizativa y Tecnológica de los Sistemas de Información.

CARACTERÍSTICAS DE UN SISTEMA DE INFORMACIÓN:

Si tuviéramos que resumir con una sola frase el principal cometido de un sistema de Información dentro de una organización, podríamos afirmar que éste se encarga de entregar la información oportuna y precisa, con la presentación y el formato adecuados, a la persona que la necesita dentro de la organización para tomar una decisión o realizar alguna operación y justo en el momento en que esta persona necesita disponer de dicha información.

Hoy en día, la información debería ser considerada como uno de los más valiosos recursos de una organización y el Sistema

de Información es el encargado de que ésta sea gestionada siguiendo criterios de eficacia y eficiencia (2011, p. 35).

1.3.4. Procesos del sistema de información

Para entender mejor el concepto de Sistema de Información, Gomes y Suarez nos menciona que:

> Un Sistema de Información se puede definir como un conjunto de elementos interrelacionados (entre los que podemos considerar los distintos medios técnicos, las personas y los procedimientos) cuyo cometido es capturar datos, almacenarlos y transformarlos de manera adecuada y distribuir la información obtenida mediante todo este proceso.
>
> Su propósito es apoyar y mejorar las operaciones cotidianas de la empresa, así como satisfacer las necesidades de información para la resolución de problemas y la toma de decisiones por parte de los directivos de la empresa.
>
> Por lo tanto, se trata de un sistema que tiene unos inputs (datos) y unos outputs (información), unos procesos de transformación de los inputs en outputs y unos mecanismos de retroalimentación, como se puede apreciar en la siguiente figura: (2011, p. 42)

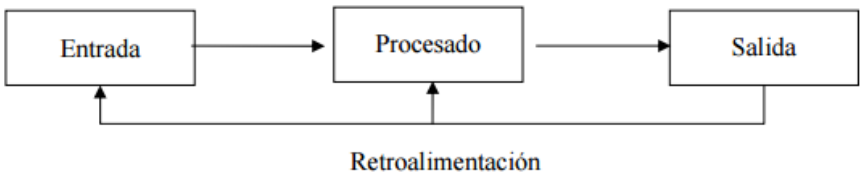


Figura 4. Los procesos del Sistema de Información.

1.3.5. Clasificación de los sistemas de información

Según Gomes y Suarez considera que existen dos funciones básicas (véase figura 5) para los sistemas:

- **Soporte a las actividades operativas**, que da lugar a sistemas de información para actividades más estructuradas (aplicaciones de contabilidad, nómina, pedidos y, en general, lo que se denomina "gestión empresarial") o también sistemas que permiten el manejo de información menos estructurada: aplicaciones ofimáticas, programas técnicos para funciones de ingeniería, etc.

- **Soporte a las decisiones y el control de gestión**, que puede proporcionarse desde las propias aplicaciones de gestión empresarial (mediante salidas de información existentes) o a través de aplicaciones específicas, como se presentará en este apartado. (2011, p. 46)

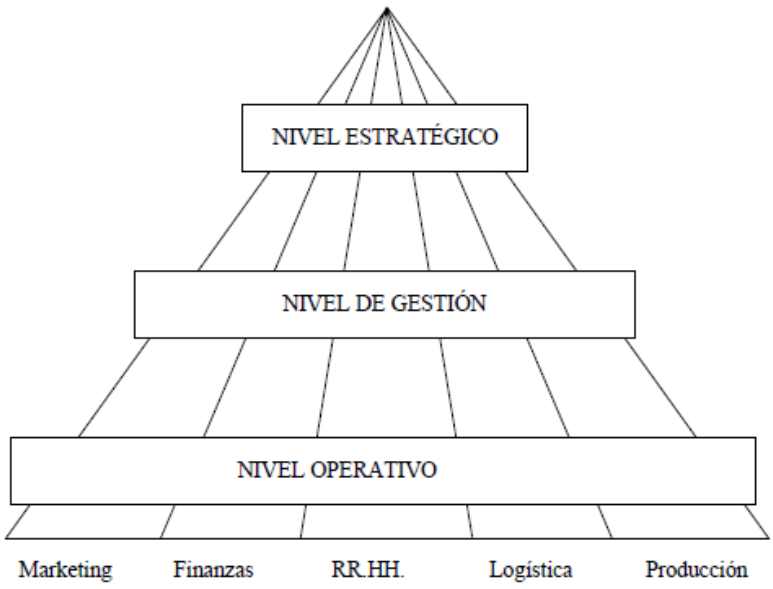


Figura 5. Clasificación de los sistemas por nivel y función.

1.3.6. Seguridad de información

Para Purificación Aguilera López afirma que:

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Un sistema de información, no obstante, las medidas de seguridad que se le apliquen, no deja de tener siempre un margen de riesgo.

Para afrontar el establecimiento de un sistema de seguridad en necesario conocer:

- Cuáles son los elementos que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización para la que se hace el estudio de riesgos y mediante apreciación directa.
- Cuáles son los peligros que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreos sobre el mismo.
- Cuáles son las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decidir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible (2010, p. 9).

1.3.7. Tipos de seguridad

Según Purificación Aguilera López existen dos tipos de seguridad:

Activa

Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.

Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes.

Pasiva

Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos (2010, p. 10).

1.3.8. Propiedades de un sistema de información seguro

Diferentes autores mencionan diferentes posturas con respecto a las propiedades de un Sistema de Información Seguro, según Costas Santos, Jesús manifiesta que:

> Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información. Por tanto, actualmente se considera generalmente aceptado que la seguridad de los datos y la información comprende tres aspectos fundamentales:
>
> - **Confidencialidad**, es decir, no desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
> - **Integridad**, permite asegurar que los datos no se han falseado.

- **Disponibilidad**, esto es, que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.

Hay que tener en cuenta que tanto las amenazas como los mecanismos para contrarrestarlas, suelen afectar a estas tres características de forma conjunta. Así, por ejemplo, fallos del sistema que hacen que la información no sea accesible pueden llevar consigo una pérdida de integridad.

Generalmente **tienen que existir los tres aspectos descritos para que haya seguridad** (2010, p. 21, 22).

Así mismo, para que un sistema se considere seguro debe cumplir ciertas propiedades que Purificación Aguilera López (2010, p,10). Menciona: "**integridad, confidencialidad y disponibilidad** de la información. Cada una de estas propiedades conlleva la implantación de determinados servicios y mecanismos de seguridad".

1.3.9. Dimensiones

1.3.9.1. Confidencialidad

Según Costas Santos, Jesús:

> Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.
>
> De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y sólo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada (véase figura 6). En el caso de un mensaje esto evita que exista una intercepción de éste y que pueda ser leído por una persona no autorizada (2010 p, 23).

Figura 6. Ejemplo de Confidencialidad.

Así mismo, para Purificación Aguilera Lopez:

> La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus Directrices para la Seguridad de los Sistemas de Información define la confidencialidad como «el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada».
>
> Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema: quién puede acceder, a qué parte del sistema, en qué m omento y para realizar qué tipo de operaciones (2010, p. 10).

1.3.9.2. Integridad

Para Costas Santos, Jesús:

> La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original (véase figura 7). Aplicado a las

bases de datos sería la correspondencia entre los datos y los hechos que refleja (2010, p.25).

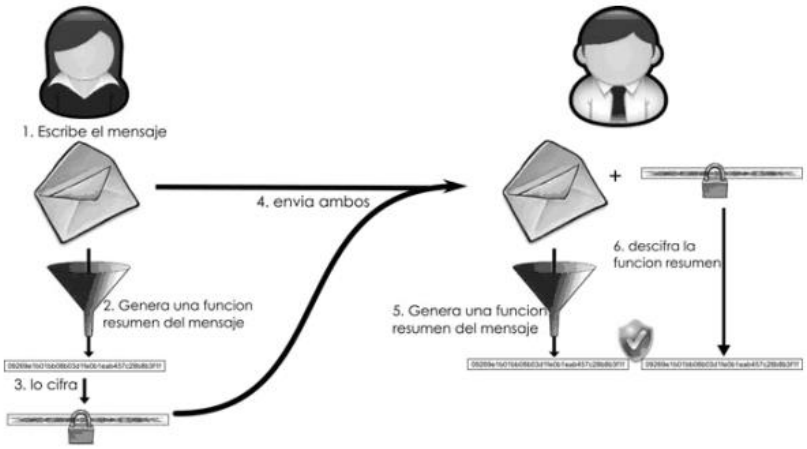


Figura 7. Ejemplo de Integridad.

Así mismo, para Purificación Aguilera Lopez:

> Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que esta se solicita, o, dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado.
>
> Para evitar este tipo de riesgos se debe dotar al sistema de mecanismos que prevengan y detecten cuándo se produce un fallo de integridad y que puedan tratar y resolver los errores que se han descubierto (2010, p.10).

1.3.9.3. Disponibilidad

Según Costas Santos, Jesús:

> Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando éstos lo requieran.
>
> También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite,

esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor (2010, p 26).

A su vez, Purificación Aguilera López:

> La información ha de estar disponible para los usuarios autorizados cuando la necesiten.
>
> El programa MAGERIT define la disponibilidad como «grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información».

Se deben aplicar medidas que protejan la información, así como crear copias de seguridad y mecanismos para restaurar los datos que accidental o intencionadamente se hubiesen dañado o destruido (2010, p.11).

1.3.10. ISO

Según la Organización Internacional para Normalización – ISO, es una red mundial que identifica cuáles normas internacionales son requeridas por el comercio, los gobiernos y la sociedad; las desarrolla conjuntamente con los sectores que las van a utilizar; las adopta por medio de procedimientos transparentes basados en contribuciones nacionales proveniente de múltiples partes interesadas; y las ofrece para ser utilizadas a nivel mundial.

Las normas ISO están basadas en un consenso internacional conseguido de la base más amplia de grupos de partes interesadas. La contribución de expertos proviene de aquellos más cercanos a las

necesidades en materia de normas y de los resultados de su implementación.

De esta manera, aunque voluntarias, las normas ISO son muy respetadas y aceptadas a nivel internacional por sectores públicos y privados.

ISO, una organización no gubernamental, es una federación de organismos de normalización nacional provenientes de todas las regiones del mundo; uno por país, incluyendo países desarrollados y en vías de desarrollo, así como países con economías en proceso de transición. Cada miembro de la ISO es el principal organismo de normalización de su país. Los miembros proponen las nuevas normas, participan en su desarrollo y ofrecen el apoyo, conjuntamente con la Secretaría General de la ISO, a los 3000 grupos técnicos que actualmente desarrollan las normas (iso.org/iso).

1.3.11. Estándar

Para la Organización Internacional para Normalización – ISO:

> Una norma es un documento que proporciona los requisitos, especificaciones, directrices o características que se pueden utilizar constantemente para asegurar que los materiales, productos, procesos y servicios son adecuados para su propósito (iso.org/iso/home/standars.htm).

Así mismo, para el Project Management Institute – PMI, nos dice que: “Un estándar es un documento establecido por consenso, aprobado por un cuerpo reconocido, y que ofrece reglas, guías o características para que se use repetidamente” (http://pmi.org.py/index.php/pmi/estándares).

1.3.12. Norma ISO/IEC 27001

Para la Organización Internacional para Normalización – ISO esta norma:

> Pertenece a la familia de normas de ISO 2700 de normas que ayuda a las organizaciones mantener los activos de información segura.
>
> El uso de esta familia de normas ayudará a su organización a administrar la seguridad de los activos, tales como información financiera, la propiedad intelectual, detalles de los empleados o la información confiada a usted por terceros.
>
> El origen de la Norma ISO 27001 está en el estándar británico BSI (British Standards Institution) BS7799- Parte 2, estándar que fue publicado en 1998, y era certificable desde entonces (véase la historia de ISO 27001 en la figura 8). Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de octubre de 2005 (iso27000.es).

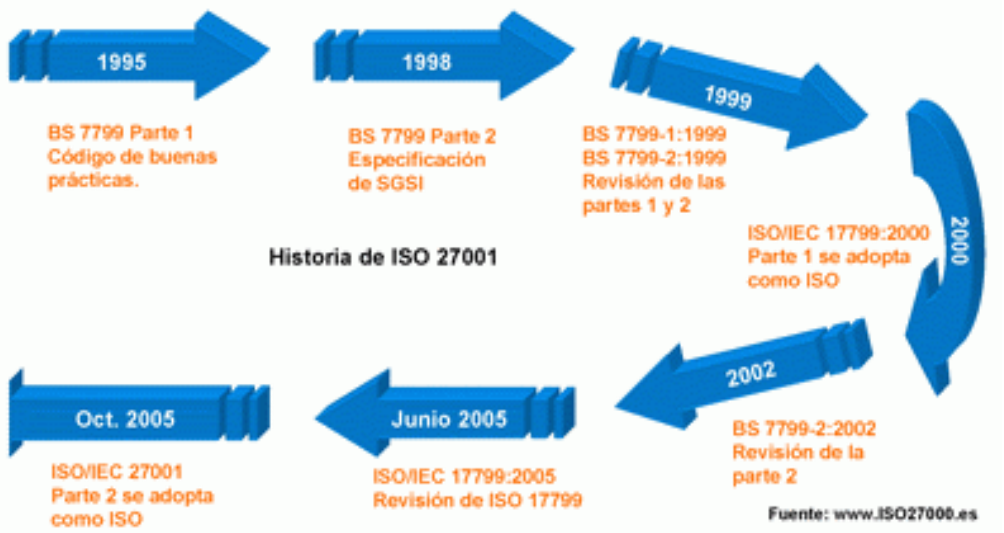


Figura 8. Historia de ISO 27001.

Así mismo, la ISO 27001 hace mención que:

El enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño del SGSI
- Realizar mejoramiento continuo en base a la medición del objetivo (2005, p. 6)

1.3.13. ¿Cómo se implementa un SGSI en base a la norma ISO/IEC 27001?

Según la ISO 27001:

> Este estándar internacional adopta el modelo del proceso Planear – Hacer – Chequear – Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI (véase figura 9). Donde un SGSI, toma como insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas.
>
> Asimismo, es un estándar internacional que proporciona un modelo sólido para implementar los principios aquellos lineamientos que gobiernan la evaluación del riesgo, diseño e implementación de seguridad, gestión y re-evaluación de la seguridad. (2005, p. 05)

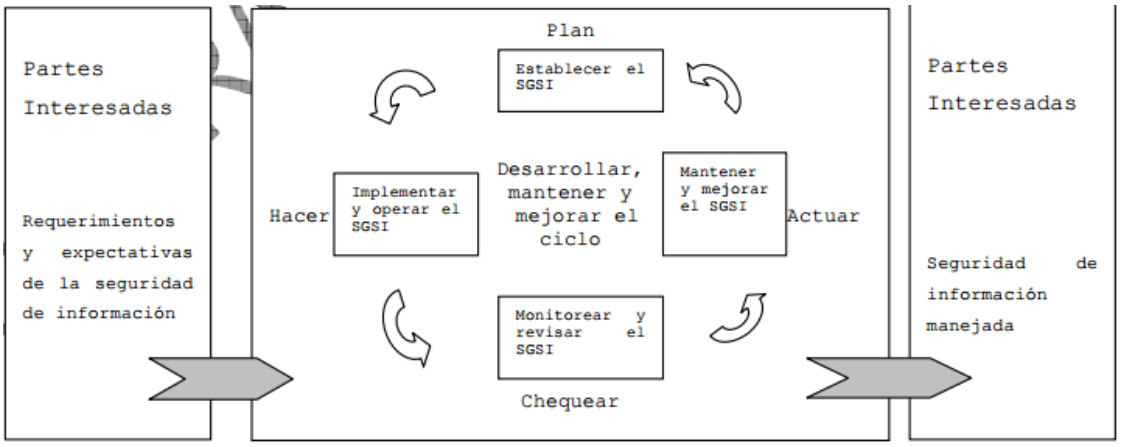


Figura 9. Modelo PDCA aplicado a los procesos SGSI.

1.3.14. Modelo PDCA

Según la ISO 27001, indica que:

> Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.
>
> - **Plan (planificar):** establecer el SGSI.
> - **Do (hacer):** implementar y utilizar el SGSI.
> - **Check (verificar):** monitorizar y revisar el SGSI.
> - **Act (Actuar):** mantener y mejorar el SGSI.
>
> (www.iso2700.es/sgsi.html)

1.3.14.1. Plan – Planificación

> Según la ISO 27001, indica que: “se encarga de establecer políticas, objetivos, procesos y procedimientos SGSI relevantes para mejorar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.” (2005, p. 07)
>
> Asimismo, en el ISO 27000 en español indica que:

En esta fase se realiza lo siguiente:

- Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, los límites del SGSI. El SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado.
- Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad.
- Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable.
- Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
- Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
- Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo

resultante y determinar si el riesgo es aceptable o requiere tratamiento.

- Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido, eliminado, aceptado o transferido.

- Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior.

- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento.

- Confeccionar una Declaración de Aplicabilidad: Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo (www.iso2700.es/sgsi.html).

1.3.14.2. Hacer – Implementación

Según la ISO 27001, indica que: “Se encarga de implementar y operar la política, controles, procesos y procedimientos SGSI” (2005, p.07).

Asimismo, en el ISO 27000 en español indica que:

En esta fase se realiza lo siguiente (véase figura 10):

- Definir plan de tratamiento de riesgos: que identifique las acciones, recursos,

responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los que se seleccionaron en la fase anterior.
- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad (www.iso2700.es/sgsi.html).

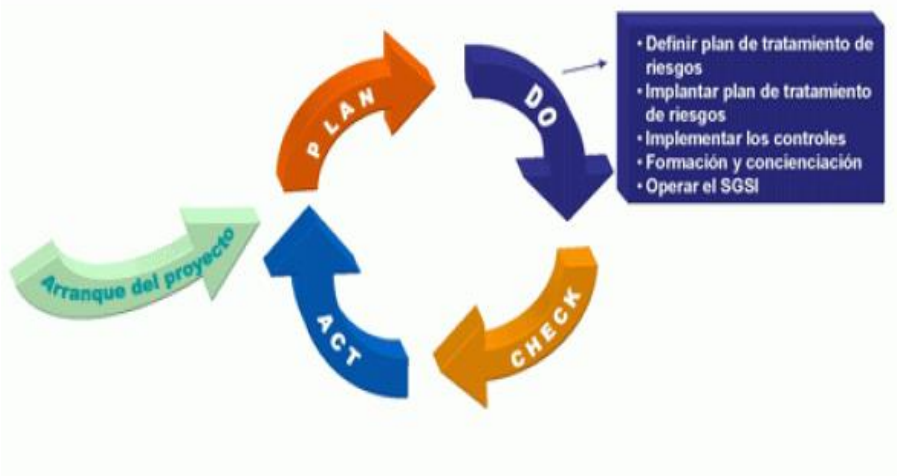


Figura 10. Fase Hacer – Implementación.

1.3.14.3. Chequear – Seguimiento

Según la ISO 27001, indica que: “Se encarga de evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencia prácticas SGSI y reportar los resultados a la gerencia para revisión” (2005, p. 07).

Asimismo, en el ISO 27000 en español indica que:

> En esta fase (véase figura 11) se realiza lo siguiente:
>
> - Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
> - Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad.
> - Medir la eficacia de los controles.
> - Revisar regularmente la evaluación de riesgos: influencian los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno.
> - Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001.
> - Revisar regularmente el SGSI por parte de la Dirección.
> - Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.

- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI (www.iso2700.es/sgsi.html).

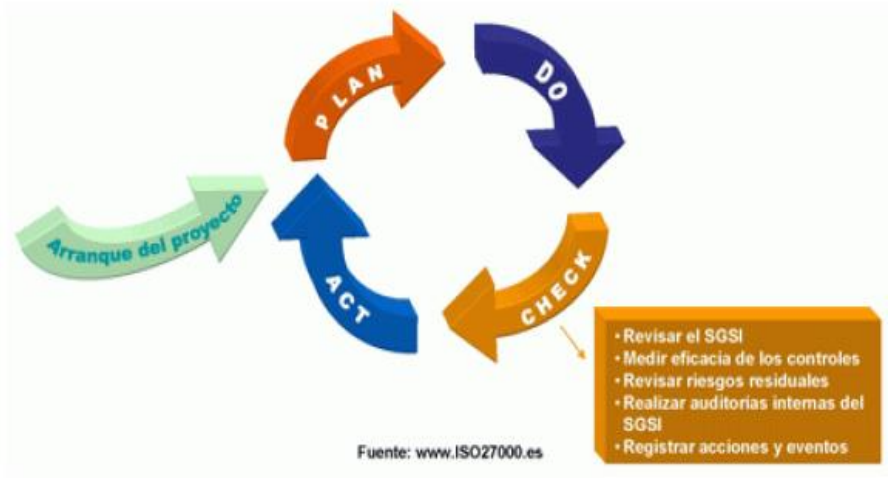


Figura 11. Fase Chequear – Seguimiento.

1.3.14.4. Actuar – Mejora continua

Según la ISO 27001, indica que: "se encarga de tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para logar el mejoramiento continuo del SGSI" (2005, p. 07).

Asimismo, en el ISO 27000 en español indica que:

> En esta fase (véase figura 12) se realiza lo siguiente:
>
> - Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
> - Acciones correctivas: para solucionar no conformidades detectadas.
> - Acciones preventivas: para prevenir potenciales no conformidades.

- Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre (www.iso2700.es/sgsi.html).

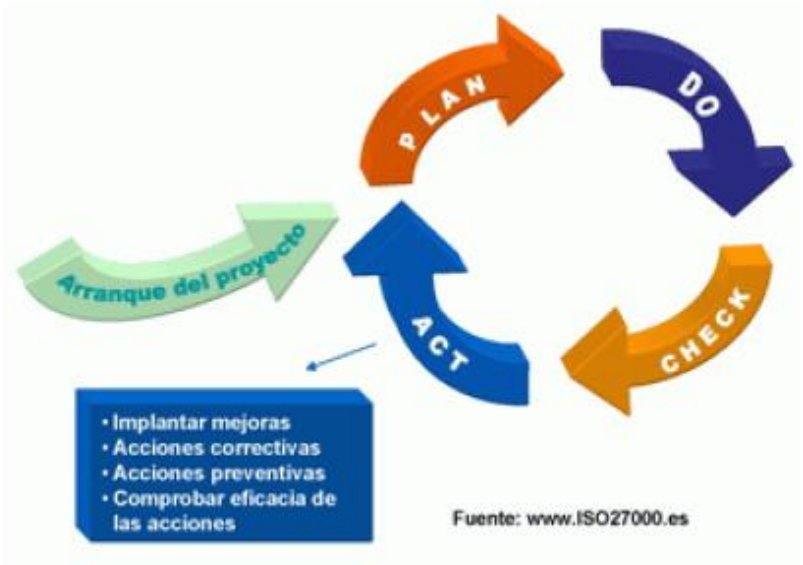


Figura 12. Fase Actuar – Mejora Continua.

1.3.15. Modelo MAGERIT

Según Amutio:

> Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (2012, p. 07).

1.4. Formulación del problema

1.4.1. Problema general

PG: ¿Cuál será el efecto de la implementación de la NTP ISO/IEC 27001 para la seguridad de información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin?

1.4.2. Problemas específicos

PE1: ¿Cuál será el efecto de la implementación de la NTP ISO/IEC 27001 en la confidencialidad de la seguridad de información en el área de Configuración y Activos del MINEDU?

PE2: ¿Cuál será el efecto de la implementación de la NTP ISO/IEC 27001 en la integridad de la seguridad de información en el Área de Configuración y Activos del MINEDU?

PE3: ¿Cuál será el efecto de la implementación de la NTP ISO/IEC 27001 en la disponibilidad de la seguridad de información en el Área de Configuración y Activos del MINEDU?

1.5. Justificación del estudio

1.5.1. Justificación Económica:

A través del desarrollo del tema de esta tesis, se pretende brindar apoyo en cierto modo al área de Configuración y Activos del MINEDU, ya que no poseen alguna seguridad de información para el registro de los activos de TI, el cual permitirá reducir los costos en caso de incidentes de seguridad de información; ya que mediante una implementación de la norma ISO 27001, nos permitirá tener procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, amenazas y vulnerabilidades que pueda presentar los activos de información.

1.5.2. Justificación Tecnológica:

La tecnología se ha convertido en los últimos días como una herramienta de uso fundamental para toda organización ya que los proceso e información que se manejaba en medio físico han pasado a un medio electrónico, esto ha instaurado la necesidad de contar lineamientos para la seguridad de la información, basados en la norma ISO 27001, que brindará medidas para gestionar los riesgos y lograr un nivel de seguridad óptimo, esto con la finalidad de minimizar considerablemente los riesgos de pérdida o daños en los activos de información.

1.5.3. Justificación Institucional:

La seguridad de Información, basados en la norma ISO 27001, permitirá mejorar la imagen del área de Configuración y Activos dentro de la Oficina de Tecnologías de la Información y Comunicación del MINEDU, ya que habrá un respeto de confidencialidad y transparencia en el manejo de sus activos de información y la responsabilidad del equipo de trabajo en mantener la integridad de los mismos.

Según la norma ISO 27001:2005 (1.1 – P.8), “Está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas”.

1.5.4. Justificación Operativa:

El desarrollo de este tema de tesis permitirá implementar las buenas prácticas para la Seguridad de Información basados en la norma ISO 27001, para el manejo de un control de seguridad y el tratamiento rápido de incidentes en los registros de activos de TI en el área de Configuración y Activos del MINEDU. Así mismo, permitirá mejorar la imagen del área dentro de la Oficina de Tecnologías de la Información y Comunicación del MINEDU.

1.6. Hipótesis

1.6.1. Hipótesis General

HG: La implementación de la NTP ISO/IEC 27001 mejora significativamente la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

1.6.2. Hipótesis Específico

HE1: La implementación de la NTP ISO/IEC 27001 mejora significativamente la confidencialidad de la Seguridad de Información en el área de configuración y Activos del Ministerio de Educación – Sede Centromin.

HE2: La implementación de la NTP ISO/IEC 27001 mejora significativamente la integridad de la Seguridad de Información en el área de configuración y Activos del Ministerio de Educación – Sede Centromin.

HE3: La implementación de la NTP ISO/IEC 27001 mejora significativamente la disponibilidad de la Seguridad de Información en el área de configuración y Activos del Ministerio de Educación – Sede Centromin.

1.7. Objetivos

1.7.1. Objetivo General

OG: Determinar el efecto de la implementación de la NTP ISO/IEC 27001 para la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

1.7.2. Objetivos Específicos:

OE1: Determinar el efecto de la implementación de la NTP ISO/IEC 27001 en la confidencialidad de la Seguridad de Información en

el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

OE2: Determinar el efecto de la implementación de la NTP ISO/IEC 27001 en la integridad de la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

OE3: Determinar el efecto de la implementación de la NTP ISO/IEC 27001 en la disponibilidad de la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

2. METODO

2.1. Diseño de investigación

Para Bernal, Cesar manifiesta que los diseños pre-experimentales:

> Presentan el más bajo control de variables y no efectúan asignación aleatoria de los sujetos al experimento, y son aquellos en los que el investigador no ejerce ningún control sobre las variables extrañas o intervinientes, no hay asignación aleatoria de los sujetos participantes de la investigación ni hay grupo control (2010, p.146.)

Para el desarrollo de esta tesis se utilizará el diseño experimental del tipo pre-experimental, ya que se manipulará ambas variables. Además, se aplicará la causa efecto entre ambas variables, mediante un estudio de dos etapas: pre test y post test.

En el pre-test, se llevó a cabo una medición previa a la implementación de la NTP ISO/IEC 27001, una vez implementada la NTP ISO/IEC 27001 se realizó y una medición post-test, la cual permitirá comparar ambos resultados y demostrar las hipótesis que se viene planteando.

2.2. Variables, operacionalización

2.2.1. Definición conceptual

Variable Independiente (VI): NTP ISO/IEC 27001

Según la NTP ISO/IEC 27001, indica que:

> Esta Norma Técnica Peruana es una adopción de la Norma ISO/IEC 17799:2005. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995. (2007, p .iv).

Variable dependiente (VD): Seguridad de Información

Según la Norma Técnica Peruana NTP-ISO/IEC 17799 - 2007, indica que:

> La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades.
>
> La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene. La Seguridad de la Información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios (2007, p.01).

2.2.2. Definición operacional

Esta sección se detallarán las variables independientes y dependientes, (véase tabla N° 1)

Variable Independiente (VI): NTP ISO/IEC 27001

Es un estándar o norma que ha sido creado con el propósito de asegurar la información para las empresas o instituciones públicas, tomando en cuenta un ciclo de cuatro fases como son establecer un sistema, implementarlo y operarlo, mantenerlo y mejorarlo y por ultimo monitorearlo; todo esto permitirá minimizar a los riesgos y amenazas externas o internas a la información que maneja cada empresa; asimismo, permitirá a estar preparados ante cualquier evento relacionado a la divulgación de información.

Variable dependiente (VD): Seguridad de Información

Es un conjunto de medidas establecidas que permitirá asegurar la confidencialidad, integridad y disponibilidad de la información dentro de una organización.

Asimismo, luego de su aplicación en la organización pueda estar preparado ante una amenaza y o riesgos de la información.

Tabla 1. *Matriz de Operacionalización de Variables.*

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	ITEM / INDICADOR	ESCALA
Seguridad de la Información	Según la Norma Técnica Peruana NTP-ISO/IEC 17799 - 2007, indica que: La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Por otro lado, la seguridad de información es considerada como un conjunto de medidas técnicas y legales que permiten a la institución asegurar la confidencialidad, integridad y disponibilidad de un sistema de información.	Es un conjunto de medidas establecidas que permitirá asegurar la confidencialidad, integridad y disponibilidad de la información dentro de una organización. Asimismo, luego de su aplicación en la organización pueda estar preparado ante una amenaza y o riesgos de la información	Confidencialidad	Número de información confidencial divulgada	Ordinal
			Integridad	Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción	Ordinal
			Disponibilidad	Porcentaje de tiempo durante el cual un sistema está disponible para el usuario	Razón
				D = (tiempo total transcurrido – suma de tiempo de inactividad) / tiempo total transcurrido	

2.3. Población y muestra

2.3.1. Población

Según Quezada (2010), la población “Constituye el conjunto de elementos más grande del cual se puede tomar una muestra representativa para el experimento científico” (p. 95). En esta investigación, la población estuvo constituida por la base de datos de activos del área de Configuración y Activos de la OTIC, que está conformada por 4783 registros de elementos de configuración.

2.3.2. Muestra

Según Quezada (2010), indica que la muestra “constituye una selección al azar de una población, es decir un subconjunto que se selecciona de la población” (p. 95). En tanto para esta investigación, dado que se conoce el tamaño de la población (N=4783), el cálculo de la muestra se realizará mediante la siguiente formula según el mismo autor (2010, p. 98):

$$n = \frac{n_0}{1 + \frac{n_0}{N}} \qquad y \qquad n_0 = \frac{{Z_\propto}^2 \, \sigma^2}{E^2}$$

Donde:

n: muestra.

n_0: tamaño de muestra aproximado.

N: Tamaño de la población que se está estudiando. (N=4783)

Z_α: Valores correspondiente al nivel de significancia. (Z_α=1.96 que corresponde al 95% de confianza según la tabla de distribución normal).

E: Error de tolerancia de la estimación. (E=0.5)

$\sigma^{2:}$ varianza de la variable (según esta investigación realizado se encontró una varianza de 8.997)

$$n_0 = \frac{1.96^2\ 8.997}{0.5^2} = 139 \qquad la\ muestra\ es: \quad n = \frac{139}{1 + \frac{139}{4783}} = 136$$

Luego de reemplazar los valores en la fórmula se encuentra que la muestra es 136 registros de elementos de configuración del área de Configuración y Activos. Para obtener dicha información se emplearon 60 días de evaluación, 30 días antes de la implementación y 30 días después.

2.3.3. Muestreo

Según Quezada (2010) Indica:

> El muestreo aleatorio todos los elementos tienen la misma probabilidad de ser elegidos. Los individuos que formaran parte de la muestra se elegirían al azar mediante números aleatorios. Existen varios métodos para obtener números aleatorios, los más frecuentes son la utilización de tablas de números aleatorios o generarlos por un ordenador. (p.103)

El muestreo para este proyecto de investigación será del tipo probabilístico y del subtipo aleatorio simple, puesto que el registro de los elementos de configuración permite extraer cierta cantidad de individuos al azar.

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

Según Quezada (2010), indica:

> Que para obtener información se realizara un procedimiento sistemático que implica tres actividades estrechamente vinculadas entre sí:
>
> - Instrumento de medición (encuesta, entrevista, observación, experimento, prueba, etc.).

- Equipos de medición.
- Codificación de datos (p, 115).

Para el logro de cada uno de los objetivos específicos se procederá a emplear las siguientes técnicas y herramientas.

2.4.1. Técnicas

Observación

Para Bernal (2010), afirma que esta técnica “cada día cobra mayor credibilidad y su uso tiende generalizarse, debido a que permite obtener información directa y confiable, siempre y cuando se haga mediante un procedimiento sistematizado y muy controlado” (p, 194). En este proyecto de investigación se utilizó para realizar las observaciones referentes a los indicadores propuestos**.**

2.4.2. Instrumentos

Ficha de Observación

Según Quezada (2010), consiste en:

> Un registro sistemático, valido, y confiable de comportamiento o conducta manifiesta. Es un método más utilizado por quienes están orientados conductualmente.
>
> Pasos para construir un sistema de observación son:
>
> - Definir con precisión el universo de aspectos, eventos o conductas a observar.
> - Extraer una muestra representativa de los aspectos, eventos o conductas a observar.
> - Un repertorio suficiente de conductas a observar.
> - Establecer y definir las unidades de observación
> - Establecer y definir las categorías y subcategorías de observación (p.130).

En la presente investigación se usará para registrar el porcentaje de tiempo durante el cual un sistema está disponible para el usuario mediante una ficha de observación: Ficha de Observación del registro del tiempo de disponibilidad del sistema del área de Configuración y Activos.

2.4.3. Validez de los instrumentos

Según Hernández et. (2006), la validez de instrumentos, “se refiere al grado en que un instrumento realmente mide la variable que pretende medir” (p. 277).

Para este proyecto de investigación se tomará la validez por contenido puesto que se tomará en cuenta el contenido específico que medirán los instrumentos, la cual será consultada a investigadores familiarizados con la variable (juicio de expertos).

2.4.4. Confiabilidad de los instrumentos

Según Hernández et. (2006), la confidencialidad de un instrumento de medición “se refiere al grado en que su aplicación repetida al mismo sujeto u objeto produce resultados iguales” (p. 277).

2.5. Métodos de análisis de datos

Para este proyecto de investigación se consideró el análisis descriptivo, que procederá el cálculo de la media, varianza, tablas y gráficos de barras o circulares estadísticos según la naturaleza de los resultados y a su vez permitirá contrastar cada una de las variables utilizadas.

Para la comprobación de hipótesis de las dimensiones: Confidencialidad, Integridad y Disponibilidad se realizó la prueba de normalidad de datos por medio del método de kolmogorov-Smirnov, Asimismo, para las mismas hipótesis se realizó la prueba no paramétrica de 2 muestras relacionadas a través de Wilcoxon.

2.6. Aspectos éticos

El Investigador se compromete a respetar la propiedad intelectual y los derechos de autor, también se guarda la confidencialidad de la información proporcionada por el área de Configuración y Activos del Ministerio de Educación a fines de estudio. Asimismo, se mantendrá la confidencialidad de la identidad de los individuos que participan en el proyecto.

3. RESULTADOS

3.1. Análisis Descriptivo

En la presente investigación se implementó la NTP ISO/IEC 27001 para determinar su efecto en la mejora significativa de la Confidencialidad, Integridad y Disponibilidad de la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin; para tal efecto, evaluó el comportamiento de 136 registros que corresponde a la muestra de esta investigación durante un periodo de 30 días hábiles (como se aprecia en la tabla 2, 3 y 4), para ello se aplicó la evaluación del pre test para conocer el estado inicial de los tres indicadores; posteriormente se implementó la NTP ISO/IEC 27001 y nuevamente se procedió a evaluar la condiciones de los indicadores en el área de Configuración de Activos del Ministerio de Educación – Sede Centromin (posTest). Los resultados descriptivos de estas medidas se observan en las tablas 02, 03 y 04.

1° Indicador: Número de información confidencial divulgada

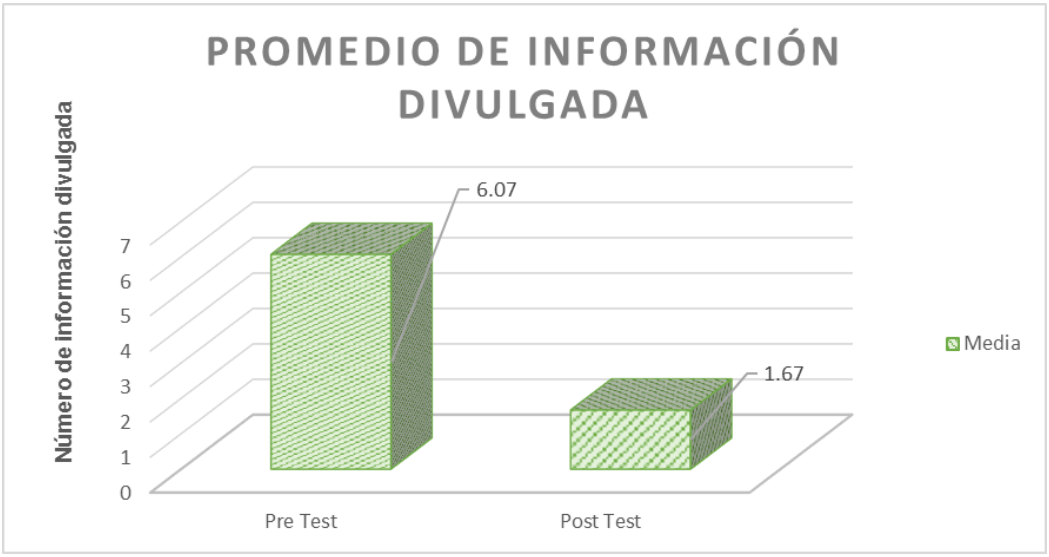
Tabla 2. *Medidas descriptivas del número de información confidencial divulgada antes y después de la implementación de la NTP ISO/IEC 27001.*

	Media	Mínimo	Máximo	Mediana	Desviación Típica	Coeficiente de Variación
Número de información confidencial divulgada antes	6.07	3	9	6	1.886	31.10%
Número de información confidencial divulgada después	1.67	0	4	1.5	1.1929	71.47%

Fuente: Elaboración propia

Se obtuvo como media del número de información confidencial divulgada en el pre test de la muestra el valor de 6,07, mientras que para el post test el número fue de 1,67 de información confidencial divulgada (como se aprecia en la figura 13), esto muestra que existe una gran diferencia entre antes y después de la implementación de la NTP ISO/IEC 27001. Asimismo, el número mínimo de información confidencial divulgada del pre test fueron 3 y el del post test fue 0.

La dispersión en el número de información confidencial divulgada, en el pre test fue de 31.01% y el post test de 71,47%, se valida que la variabilidad con respecto a los datos no difiere en gran medida, por lo tanto, la comparación de medias se considera adecuada.



© Elaboración propia

Figura 13. Promedio de Número de información confidencial divulgada antes y después de implementado la NTP ISO/IEC 2017.

2° Indicador: Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción.

Tabla 3. *Medidas descriptivas del número o porcentaje de accesos y/o cambios no autorizados a los datos de producción antes y después de la implementación de la NTP ISO/IEC 27001.*

	Media	Mínimo	Máximo	Mediana	Desviación Típica	Coeficiente de Variación
Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción antes	10.76	8	14	10.00	1.812	16.84%
Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción después	1.55	0	4	1.00	1.173	75.58%

Fuente: Elaboración propia

Se obtuvo como media del número o porcentaje de accesos y/o cambios no autorizados a los datos de producción, en el pre test de la muestra, el valor de 10.76, mientras que para el post test el número fue de 1,55 (como se aprecia en la figura 14), esto muestra que existe una diferencia entre antes y después de la implementación de la NTP ISO/IEC 27001. Asimismo, el número o porcentaje mínimo de accesos y/o cambios no autorizados a los datos de producción del pre test fueron 8 y en el post test fue de 0.

La dispersión en el número o porcentaje de accesos y/o cambios no autorizados a los datos de producción, en el pre test fue de 16.84% y el post test de 75,58%, se observa que la variabilidad es mayor en el post test, sin embargo, esto no impide la comparación de medias en ambos momentos.

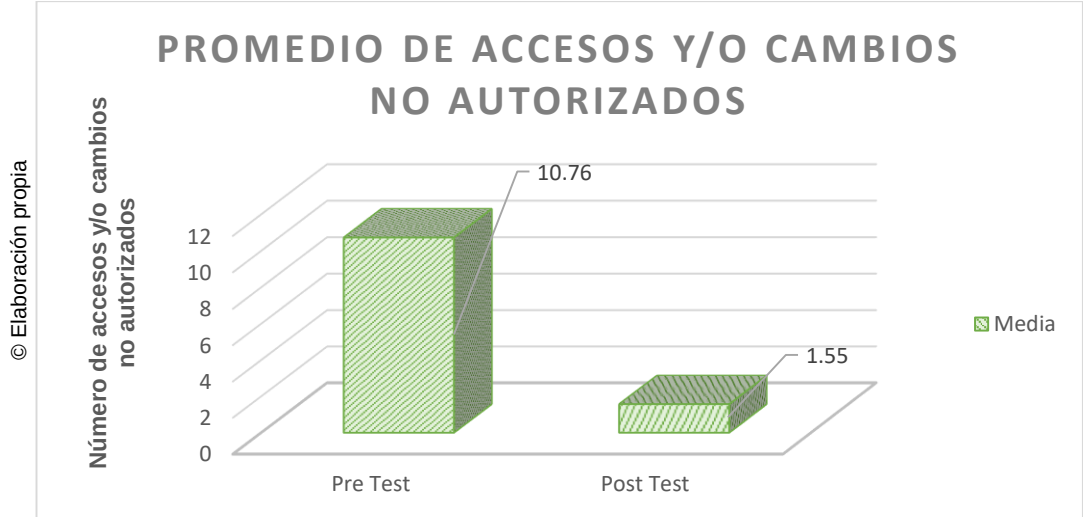


Figura 14. Promedio del número de accesos y/o cambios no autorizados a los datos de producción antes y después de la implementación de la NTP ISO/IEC 27001.

3° Indicador: Porcentaje de tiempo que se encuentra activo el sistema.

Tabla 4. *Medidas descriptivas del porcentaje de tiempo que se encuentra activo el sistema antes y después de la implementación de la NTP ISO/IEC 27001.*

	Media	Mínimo	Máximo	Mediana	Desviación Típica	Coeficiente de Variación
Porcentaje de tiempo que se encuentra activo el sistema antes	0.703	0.631	0.739	0.708	0.026	3.69%
Porcentaje de tiempo que se encuentra activo el sistema después	0.982	0.973	0.995	0.982	0.007	0.68%

Fuente: Elaboración propia

Se obtuvo como media del porcentaje del tiempo que se encuentra activo el sistema en el pre test de la muestra el valor de 0.703 porcentaje de tiempo, mientras que para el post test el valor fue de 0.982 (como se aprecia en la figura 15), esto muestra que existe una diferencia entre antes y después de la implementación de la NTP ISO/IEC 27001. Asimismo, el porcentaje mínimo de tiempo que se encuentra activo el sistema del pre test fue 0.631 y en el post test fue de 0.973.

La dispersión en el porcentaje de tiempo que se encuentra activo el sistema, en el pre test fue de 3.69% y el post test de 0.68%, se valida que la variabilidad con respecto a los datos no difiere en gran medida, por lo tanto, la comparación de medias se considera adecuada.

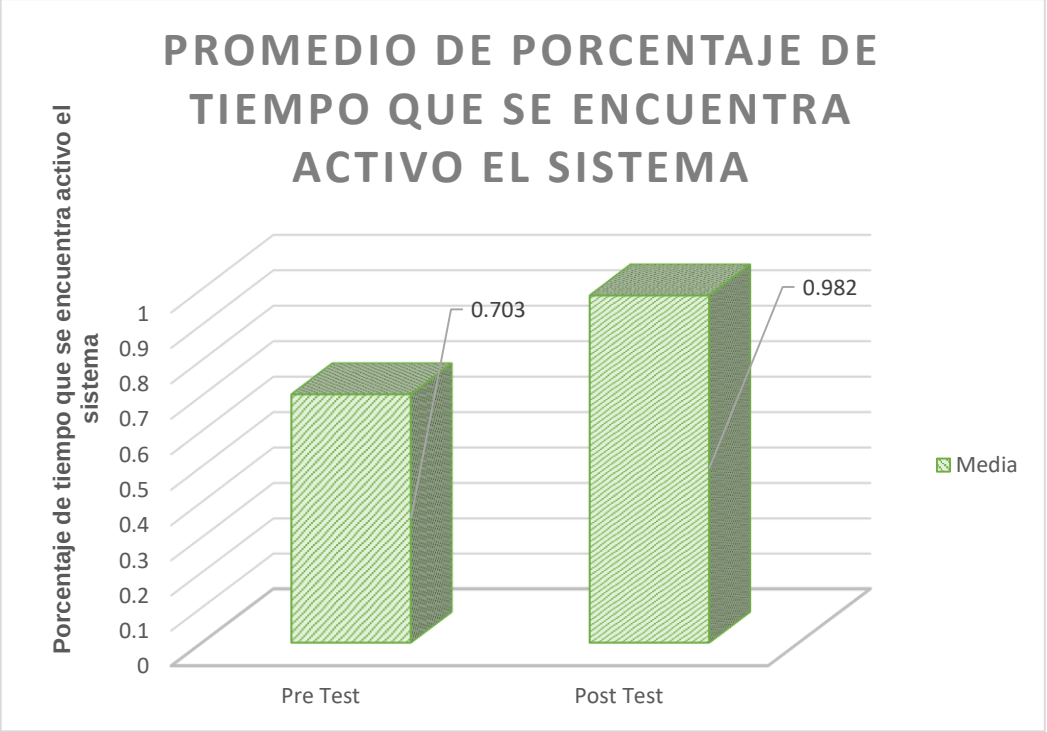


Figura 15. Porcentaje promedio de tiempo que se encuentra activo el sistema antes y después de la implementación de la NTP ISO/IEC 27001.

3.2. Análisis Inferencial

3.2.1. Prueba de Normalidad

Con la finalidad de seleccionar la prueba de hipótesis para la presente investigación, los datos se sometieron a una prueba de normalidad para validar su distribución, para lo cual se realizó la prueba de Kolmogorov-Smirnov para cada uno de los 03 indicadores, esta prueba es necesaria para probar normalidad y se aplica cuando las muestras son grandes en este trabajo de investigación la muestra es de tamaño 136 registros (como se aprecia en la tabla 5, 6 y 7).

1° Indicador: Número de información confidencial divulgada

Para poder determinar la distribución de los datos se planteó la hipótesis nula (H_o) y la hipótesis alterna (H_a), para luego comprobar si los datos del número de información confidencial divulgada cuentan con una distribución normal. A continuación, se detalla las hipótesis planteadas:

H_o : Los datos tiene distribución normal.
H_a : Los datos no tienen distribución normal.

Tabla 5. *Prueba de normalidad del número de información confidencial divulgada antes y después de implementada la NTP ISO/IEC 27001.*

	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
Número de información confidencial divulgada - Antes	0.177	136	0.000
Número de información confidencial divulgada - Después	0.213	136	0.000

Fuente: Elaboración propia

Los resultados de la prueba indican que el Sig. de la muestra del número de información confidencial divulgada antes fue de 0.00, cuyo valor es menor que 0.05 (nivel de significancia alfa), entonces se rechaza la hipótesis nula, por lo que se puede afirmar que el número de información no cumple el requisito de normalidad que es necesario para aplicar las pruebas paramétricas.

Asimismo, los resultados de la prueba indican que el Sig. de la muestra del número de información confidencial divulgada después fue de 0.000 cuyo valor es menor que 0.05 (nivel de significancia alfa), por lo que se puede afirmar que el número de información no cumple el requisito de normalidad que es necesario para aplicar las pruebas paramétricas.

Las siguientes figuras muestran la distribución de los datos, lo cual confirma que la distribución de los datos de la muestra no cumple el requisito de normalidad:

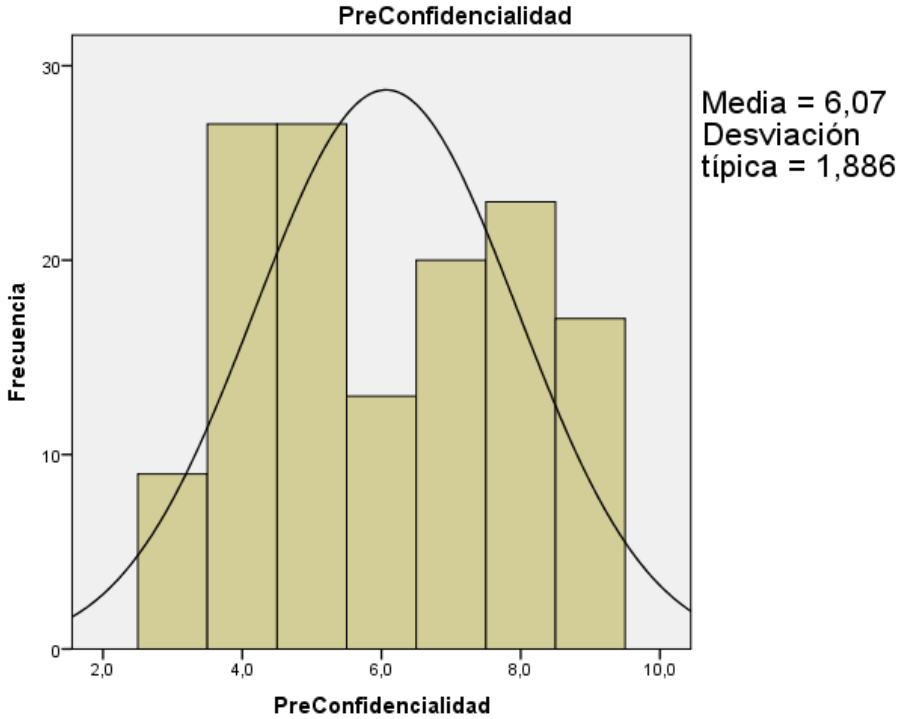
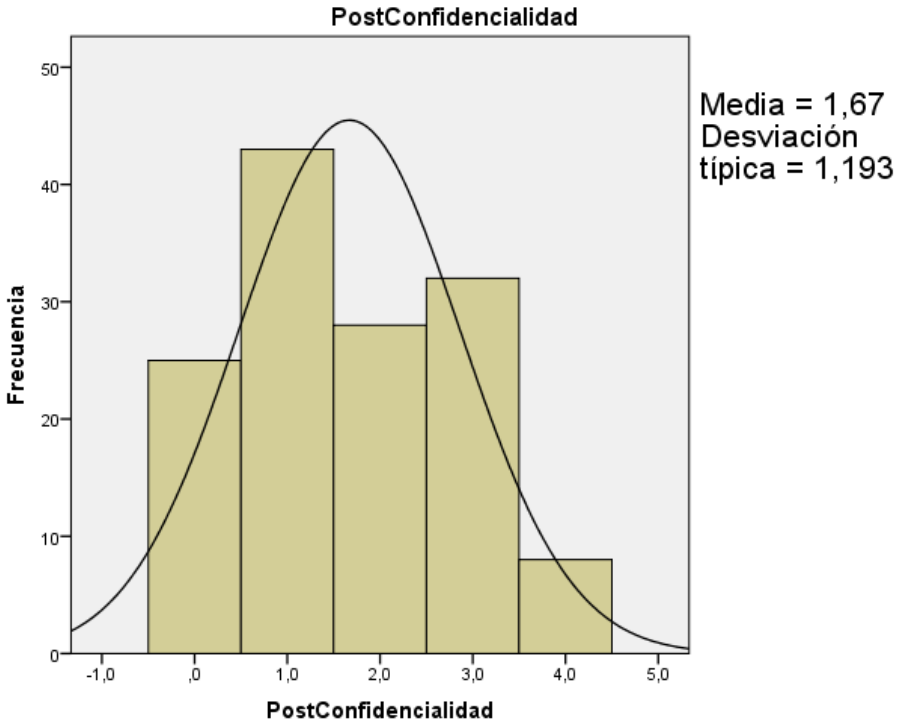


Figura 16. Histograma de prueba de normalidad del promedio de número de información confidencial divulgada antes de la implementación de la NTP ISO/IEC 27001.



2° Indicador: Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción.

Para poder determinar la distribución de los datos se planteó la hipótesis nula (H_o) y la hipótesis alterna (H_a), para luego comprobar si los datos del número accesos y/o cambios no autorizados cuenta con una distribución normal. A continuación, se detalla las hipótesis planteadas:

H_o: Los datos tiene distribución normal.

H_a: Los datos no tienen distribución normal.

Tabla 6. *Prueba de normalidad del número o porcentaje de accesos y/o cambios no autorizados a los datos de producción antes y después de implementada la NTP ISO/IEC 27001.*

	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
número o porcentaje de accesos y/o cambios no autorizados a los datos de producción- antes	0.177	136	0.000
número o porcentaje de accesos y/o cambios no autorizados a los datos de producción - después	0.188	136	0.000

Fuente: Elaboración propia

Los resultados de la prueba indican que el Sig. de la muestra del número o porcentaje de accesos y/o cambios no autorizados a los datos de producción antes fue antes de 0.0, cuyo valor es menor que 0.05 (nivel de significancia alfa), entonces se rechaza la hipótesis nula, por lo que indica que el número de accesos y/o cambios no autorizados no cumplen el requisito de normalidad.

Asimismo, los resultados de la prueba indican que el Sig. de la muestra del número o porcentaje de accesos y/o cambios no autorizados a los datos de producción después fue de 0.0 cuyo valor es menor que 0.05 (nivel de significancia alfa), por lo que indica que el número de accesos y/o cambios no autorizados no cumple el requisito de normalidad.

Las siguientes figuras muestran la distribución de los datos, lo cual confirma que la distribución de los datos de la muestra no cumple el requisito de normalidad:

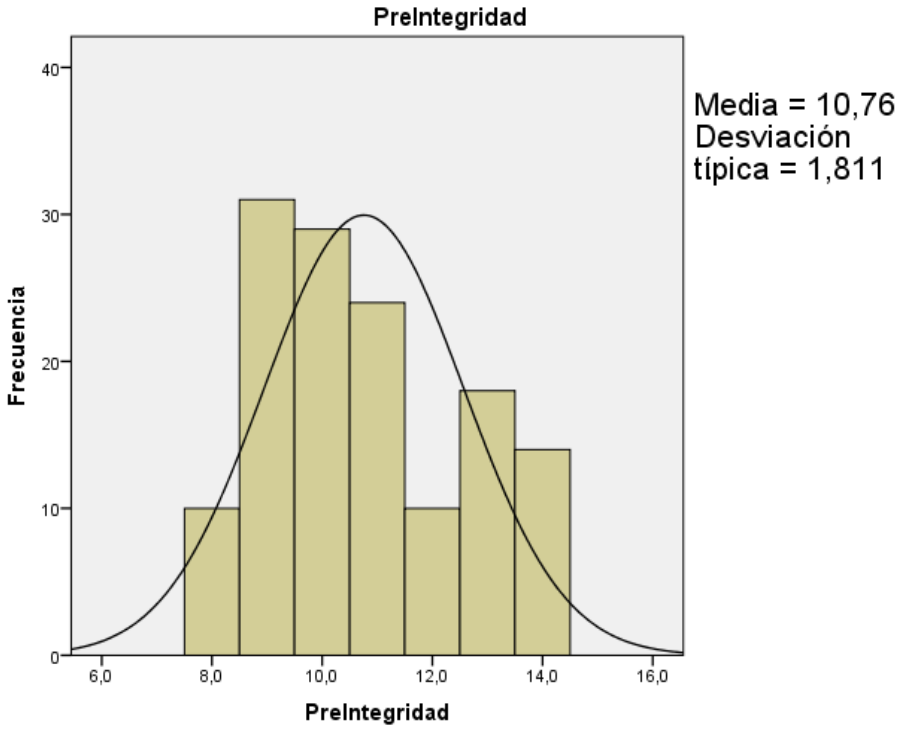


Figura 17. Histograma de prueba de normalidad del promedio del número o porcentaje de accesos y/o cambios no autorizados a los datos de producción antes de la implementación de la NTP ISO/IEC 27001.

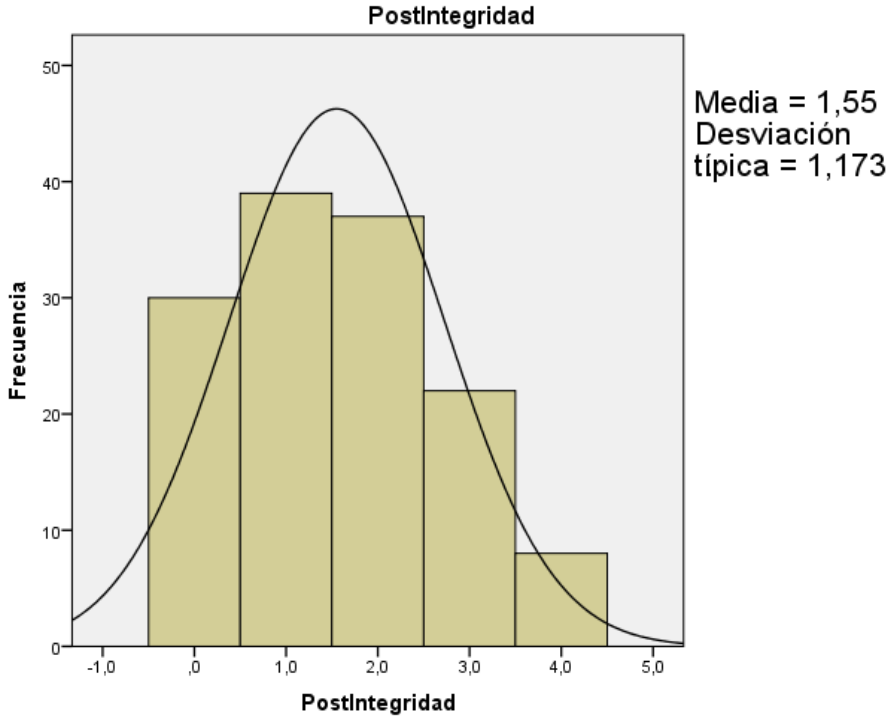


Figura 18. Histograma de prueba de normalidad del promedio del número o porcentaje de accesos y/o cambios no autorizados a los datos de producción después de la implementación de la NTP ISO/IEC 27001.

3° Indicador: Porcentaje de tiempo que se encuentra activo el sistema.

Para poder determinar la distribución de los datos se planteó la hipótesis nula (H_o) y la hipótesis alterna (H_a), para luego comprobar si los datos del porcentaje de tiempo que se encuentra activo el sistema cuentan con una distribución normal. A continuación, se detalla las hipótesis planteadas:

H_o: Los datos tiene distribución normal.
H_a: Los datos no tienen distribución normal.

Tabla 7. *Prueba de normalidad del porcentaje de tiempo que se encuentra activo el sistema antes y después de la implementación de la NTP ISO/IEC 27001.*

	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
Porcentaje de tiempo que se encuentra activo el sistema-antes	0.116	136	0.00
Porcentaje de tiempo que se encuentra activo el sistema-después	0.166	136	0.00

Fuente: Elaboración propia

Los resultados de la prueba indican que el Sig. de la muestra del porcentaje de tiempo que se encuentra activo el sistema antes fue de 0.00, cuyo valor es menor que 0.05 (nivel de significancia alfa), entonces se rechaza la hipótesis nula, por lo que los datos no cumplen el requisito de normalidad.

Asimismo, los resultados de la prueba indican que el Sig. de la muestra del porcentaje de tiempo que se encuentra activo el sistema después fue de 0.00 cuyo valor es menor que 0.05 (nivel de significancia alfa), por lo que indica que los datos no cumplen el requisito de normalidad.

Las siguientes figuras muestran la distribución de los datos, lo cual confirma que la distribución de los datos de la muestra no cumple el requisito de normalidad:

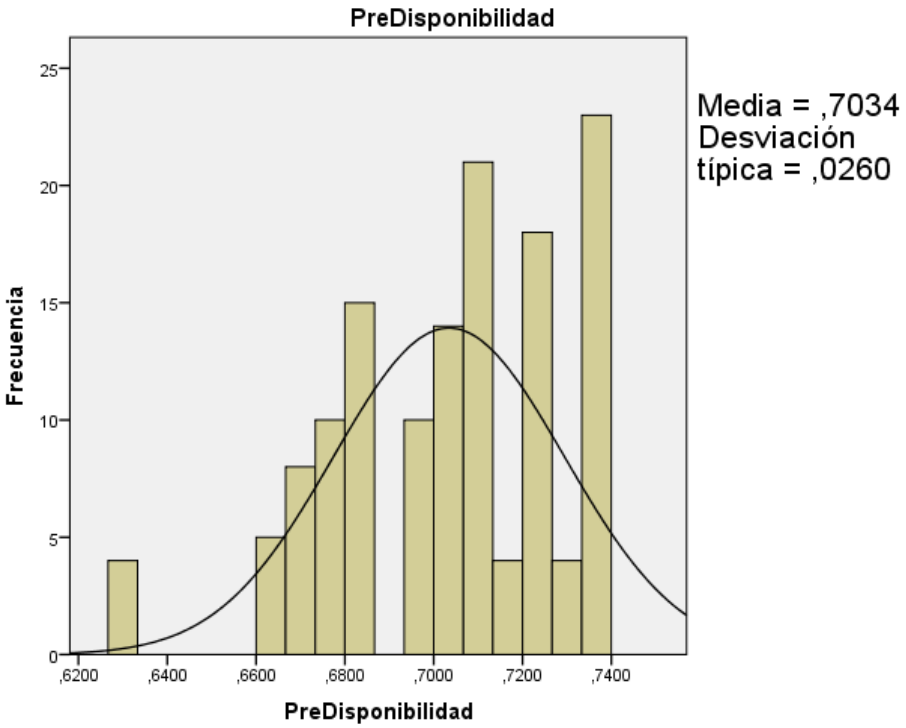


Figura 19. Histograma de prueba de normalidad en el porcentaje de tiempo que se encuentra activo el sistema antes de la implementación de la NTP ISO/IEC 27001.

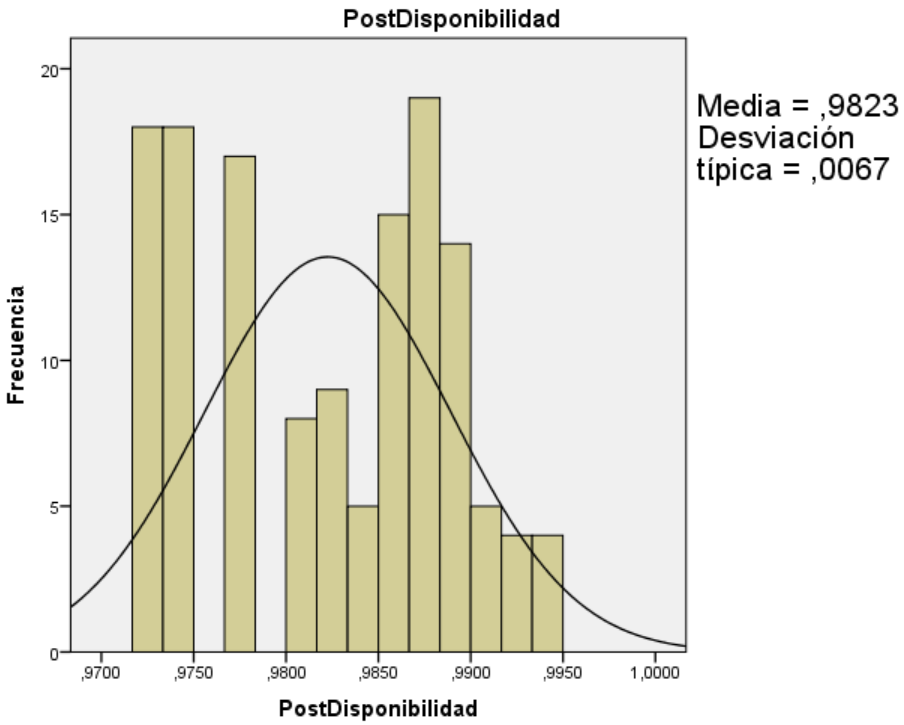


Figura 20. Histograma de prueba de normalidad en el porcentaje de tiempo que se encuentra activo el sistema después de la implementación de la NTP ISO/IEC 27001.

3.2.2. Prueba de la Hipótesis

Como el resultado de la prueba de normalidad mostro que ninguno de los indicadores cumple este requisito, los valores del pre test y post test fueron comprados por la prueba de rangos con signos de Wilcoxon con una significancia del 5% (como se aprecia en la tabla 8, 9 y 10).

A. Hipótesis de Investigación N° 01

H1: La implementación de la NTP ISO/IEC 27001 mejora significativamente la confidencialidad de la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

I1: Número de información confidencial divulgada

Hipótesis Estadísticas

Definición de Variables:

- **$NICD_a$:** Número de información confidencial divulgada sin la implementación de la NTP ISO/IEC 27001.

- **$NICD_d$:** Número de información confidencial divulgada con la implementación de la NTP ISO/IEC 27001.

  - **$H1_0$** : La implementación de la NTP ISO/IEC 27001 no mejora significativamente la confidencialidad de la Seguridad de Información.

    $H1_0 : NICD_d \geq NICD_a$

    El indicador de la implementación propuesta es mayor o igual que el indicador actual.

  - **H1a:** La implementación de la NTP ISO/IEC 27001 mejora significativamente la confidencialidad de la Seguridad de Información.

    $H1_a : NICD_d < NICD_a$

    El indicador de la implementación de la NTP ISO/IEC 27001 propuesta es menor que el indicador antes de la implementación propuesta.

Tabla 8. *Prueba de Rangos de Wilcoxon para el número de información confidencial divulgada antes y después de implementado la NTP ISO/IEC 27001.*

Test	Media	Prueba de Rangos de Wilcoxon	
		Z	Sig. (p)
Número de información confidencial divulgada - Antes	6.07	-9.963	0.000
Número de información confidencial divulgada - Después	1.67		

Fuente: Elaboración propia

Los resultados de la prueba de rangos de Wilcoxon muestra una probabilidad de 0.000, menor a la probabilidad asumida de 0.05, con ello se rechaza la hipótesis nula, por lo que el número de información confidencial divulgada antes de la implementación de la NTP ISO/IEC 27001 es significativamente mayor al observado después de la implementación de la NTP ISO/IEC 27001.

La figura N° 22, muestra que el número de la información confidencial divulgada es menor en el post test (media = 1.67) en comparación al pre test (media = 6.07); por lo tanto, la implementación de la NTP ISO/IEC 27001 mejora significativamente el número de la información confidencial divulgada.

Lo cual, se confirma en los resultados de la muestra.

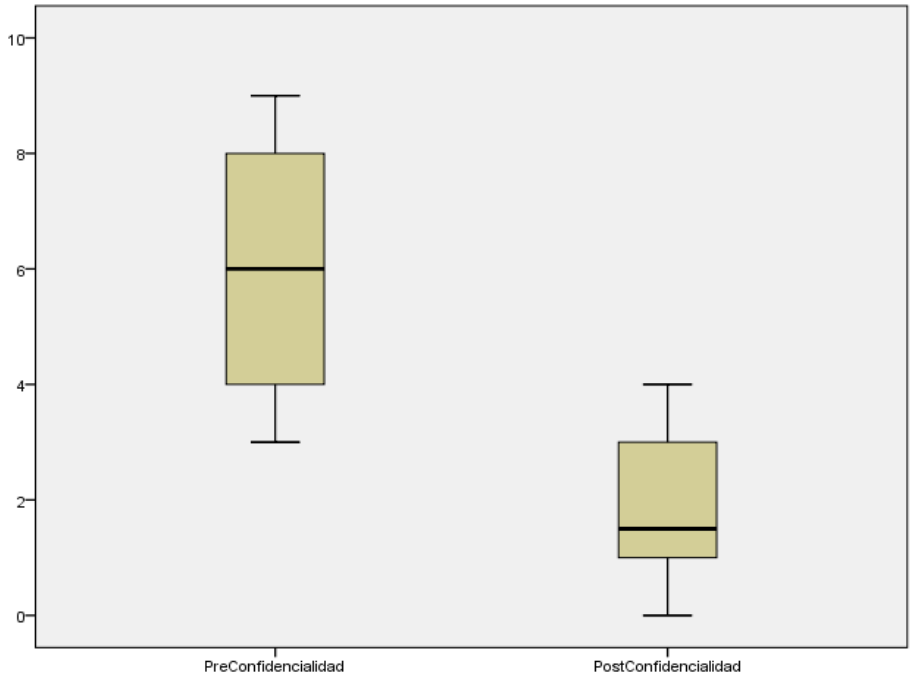


Figura 21. Comparación del número de información confidencial divulgada antes y después de la implementación de la NTP ISO/IEC 27001.

B. Hipótesis de Investigación N° 02

H2: La implementación de la NTP ISO/IEC 27001 mejora significativamente la integridad de la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

I2: Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción

Hipótesis Estadísticas

Definición de Variables:

- **$NACNA_a$:** Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción sin la implementación de la NTP ISO/IEC 27001.
- **$NACNA_d$:** Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción con la implementación de la NTP ISO/IEC 27001.

- **$H2_0$**: La implementación de la NTP ISO/IEC 27001 no mejora significativamente la integridad de la Seguridad de Información.

  $H2_0$: $NACNA_d \geq NACNA_a$

  El indicador de la implementación propuesta es mayor o igual que el indicador actual.

- **H2a:** La implementación de la NTP ISO/IEC 27001 mejora significativamente la integridad de la Seguridad de Información.

  $H2_a$: $NACNA_d < NACNA_a$

  El indicador de la implementación de la NTP ISO/IEC 27001 propuesta es menor que el indicador antes de la implementación propuesta.

Tabla 9. *Prueba de Rangos de Wilcoxon para el número o porcentaje de accesos y/o cambios no autorizados a los datos de producción antes y después de implementado la NTP ISO/IEC 27001.*

Test	Media	Prueba de Rangos de Wilcoxon	
		Z	Sig. (p)
Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción - Antes	10.76	-10.1464	0.000
Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción - Después	1.55		

Fuente: Elaboración propia

Los resultados de la prueba de rangos de Wilcoxon muestra una probabilidad de 0.000, menor a la probabilidad asumida de 0.05, con ello se rechaza la hipótesis nula, se concluye que el número o porcentaje de accesos y/o cambios no autorizados antes de la

implementación de la NTP ISO/IEC 27001 es mayor al observado después de la implementación de la NTP ISO/IEC 27001.

La figura N° 23, muestra que el número o porcentaje de accesos y/o cambios no autorizados es menor en el post test (media=1.55) en comparación al pre test (media = 10.76); por lo tanto, la implementación de la NTP ISO/IEC 27001 mejora significativamente el número o porcentaje de accesos y/o cambios no autorizados a los datos de la producción.

Lo cual se confirma en los resultados de la muestra.

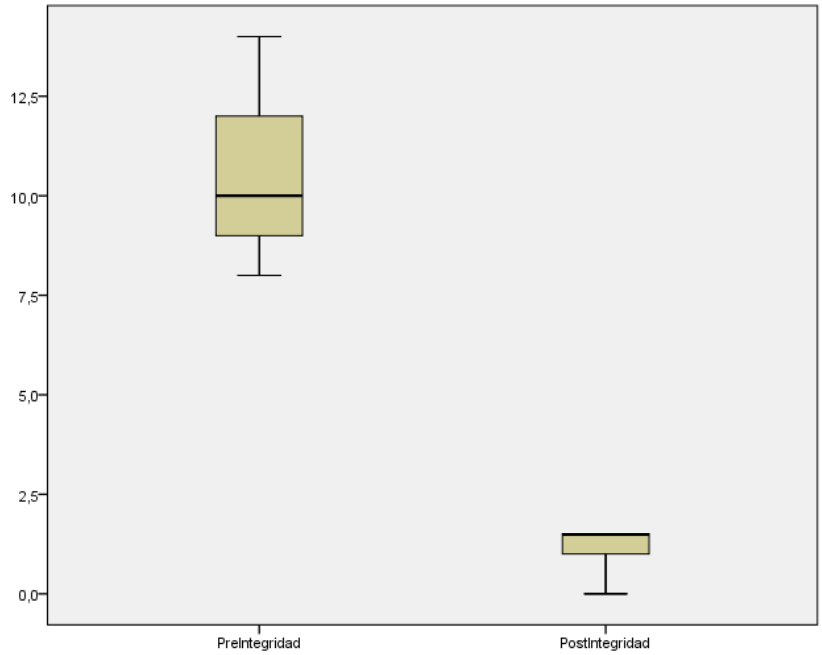


Figura 22. Comparación del número o porcentaje de accesos y/o cambios no autorizados antes y después de la implementación de la NTP ISO/IEC 27001.

C. Hipótesis de Investigación N° 03

H3: La implementación de la NTP ISO/IEC 27001 mejora significativamente la disponibilidad de la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

I3: Porcentaje de tiempo que se encuentra activo el sistema

Hipótesis Estadísticas

Definición de Variables:

- **$PTEAS_a$:** Porcentaje de tiempo que se encuentra activo el sistema sin la implementación de la NTP ISO/IEC 27001.

- **$PTEAS_d$:** Porcentaje de tiempo que se encuentra activo el sistema con la implementación de la NTP ISO/IEC 27001.

  - **$H3_0$**: La implementación de la NTP ISO/IEC 27001 no mejora significativamente la disponibilidad de la Seguridad de Información.

    $H3_0$: $PTEAS_a \leq PTEAS_d$

    El indicador actual es menor o igual que el indicador de la implementación propuesta.

  - **H3a:** La implementación de la NTP ISO/IEC 27001 mejora significativamente la disponibilidad de la Seguridad de Información.

    $H3_a$: $PTEAS_d > PTEAS_a$

    El indicador de la implementación de la NTP ISO/IEC 27001 propuesta es mayor que el indicador antes de la implementación propuesta.

Tabla 10. *Prueba de Wilcoxon para el porcentaje de tiempo que se encuentra activo el sistema antes y después de implementado la NTP ISO/IEC 27001.*

Test	Media	Prueba de Rangos de Wilcoxon	
		Z	Sig. (p)
Porcentaje de tiempo que se encuentra activo el sistema - Antes	0.703	-10.119	0.000
Porcentaje de tiempo que se encuentra activo el sistema - Después	0.982		

Fuente: Elaboración propia

Los resultados de la prueba de rangos de Wilcoxon muestra una probabilidad de 0.000, menor a la probabilidad asumida de 0.05, se rechaza la hipótesis nula, por lo que el porcentaje de tiempo que se encuentra activo el sistema antes de la implementación de la NTP ISO/IEC 27001 es menor al porcentaje de tiempo que se encuentra activo el sistema después de la implementación de la NTP ISO/IEC 27001.

En la figura N° 24, muestra que el porcentaje de tiempo que se encuentra activo el sistema es mayor en el post test (media = 0.982) en comparación al pre test (media = 0.703); por lo tanto, la implementación de la NTP ISO/IEC 27001 mejora significativamente el porcentaje de tiempo que se encuentra activo el sistema.

Lo cual se confirma en los resultados de las siguientes figuras

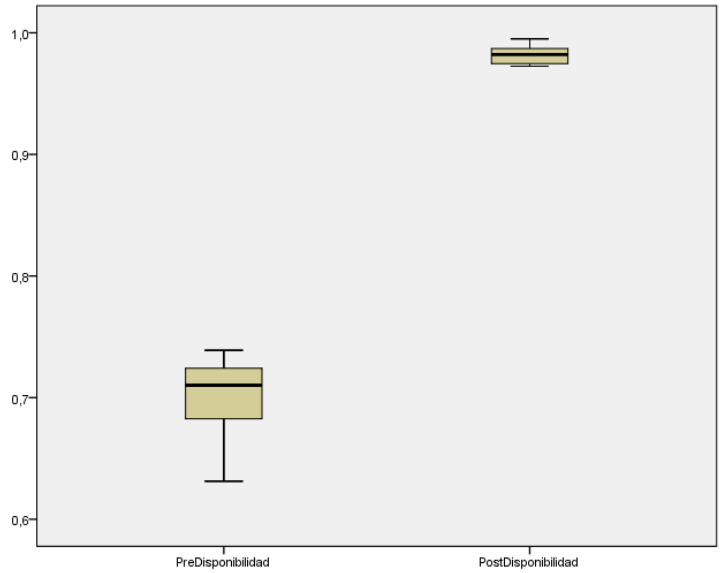


Figura 23. Comparación del porcentaje de tiempo que se encuentra activo el sistema antes y después de la implementación de la NTP ISO/IEC 27001.

Sobre la base del análisis realizado y dado que se ha demostrado la efectividad de la implementación de la NTP ISO/IEC 27001 en cada una de las dimensiones de Confidencialidad, Integridad y Disponibilidad de la Seguridad de la Información analizada en el área de Configuración y Activos de la OTIC, luego se puede concluir

que la hipótesis general ha sido demostrada y se concluye que la implementación de la NTP ISO/IEC 27001 mejora significativamente la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin .

4. DISCUSIÓN

De acuerdo a los resultados obtenidos en la presente investigación se analizó y se comparó el número de información confidencial divulgada, número o porcentaje de acceso y/o cambios no autorización a los datos de la producción y porcentaje de tiempo que se encuentra activo el sistema antes y después de la implementación de la NTP ISO/IEC 27001 para la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación Sede Centromin.

- El número de información confidencial divulgada, en la medición pre-test, alcanzó hasta un promedio de 6.07 de información confidencial divulgada y con la implementación de la NTP ISO/IEC 27001 se redujo a 1.67. Los resultados obtenidos muestran que existe una reducción de 4.4 en la información confidencial divulgada, con lo que se puede afirmar que con la implementación de la NTP se ha logrado una reducción del 72.5% en el número de información confidencial divulgada del Área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

  Según la investigación realizada por Barrantes, C. (2012), demostró que el diseño e implementación de un sistema de gestión de seguridad de información, se observa una mejoría de 78.5% al implementar políticas de seguridad, relacionada a la confidencialidad, desplegada a los colaboradores de la gerencia de tecnologías; en relación a los datos obtenidos en el número de información confidencial divulgada se redujo en 72.5% en esta presente investigación.

- El número de accesos y/o cambios no autorizados a los datos de producción, en la medición del pre-test, alcanzó hasta un promedio de 10.76 accesos y/o cambios no autorizados y con la implementación de la NTP ISO/IEC 27001 se redujo a 1.55. Los resultados obtenidos muestran que existe una reducción del 9.21 accesos y/o cambios no autorizados con lo que se puede afirmar que con la implementación de la NTP se ha logrado una reducción del 85.4% en el número de accesos y/o cambios no autorizados a los datos de producción del Área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

  Según la investigación realizada por Alcantara, J. (2015), demostró que la Implementación de la Seguridad basado en ISO/ IEC 27001, disminuyo los niveles de riesgo, respecto a los activos de información considerados amenazas y vulnerabilidades en un 10%; en relación a los datos obtenidos en el número de accesos y/o cambios no autorizados a los datos de producción se redujo en 85% en esta presente investigación.

- El porcentaje de tiempo durante el cual un sistema está disponible para el usuario, en la medición del pre-test, alcanzó hasta un promedio de 0.703 de tiempo donde el sistema se encuentra disponible y con la implementación de la NTP ISO/IEC 27001 se aumentó al 0.982. Los resultados obtenidos muestran que existe un aumento de 0.279 en el tiempo disponible del sistema con lo que se puede afirmar que con la implementación de la NTP se ha logrado una incrementar al 39.7 % al tiempo durante el cual un sistema está disponible del Área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

  Según la investigación realizada por Alcantara, J. (2015), demostró que la Implementación de la Seguridad basado en ISO/ IEC 27001, mejoró el proceso utilizado para detectar anomalías en la seguridad de la información al incrementar en un 4%, el cual colabora con el beneficio al momento de requerirse la información en el momento adecuado y exacto para la institución; en relación a los datos obtenidos en el porcentaje de tiempo

durante el cual el sistema está disponible para el usuario que se incrementó en 39.7% en esta presente investigación.

5. CONCLUSIÓN

Primera: Se ha determinado que la implementación de la NTP ISO/IEC 27001, mejoró la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, logrando demostrar las hipótesis planteadas con una confidencialidad del 95%, y esto se vio reflejado al incrementar el nivel de seguridad en la misma.

Segunda: Se ha determinado que el número de información confidencial divulgada implementando la NTP ISO/IEC 27001 en la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, sin la NTP fue un promedio de 6.07 de información confidencial y con la implementación de la NTP fue de 1.67 información confidencial, logrando una reducción 4.4 información confidencial, que representa el 72.5% en el número de información confidencial divulgada.

Tercera: Se ha determinado que el número de accesos y/o cambios no autorizados a los datos de producción implementando la NTP ISO/IEC 27001 en la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, sin la NTP fue un promedio de 10.76 de accesos y/o cambios no autorizados y con la implementación de la NTP fue de 1.55 de accesos y/o cambios no autorizados, logrando una reducción 9.21 de accesos y/o cambios no autorizados, que representa el 85.4% en el número de accesos y/o cambios no autorizados a los datos de producción.

Cuarta: Se ha determinado que el porcentaje de tiempo durante el cual un sistema está disponible para el usuario, implementando la NTP

ISO/IEC 27001 en la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, sin la NTP fue un promedio de 0.703 de tiempo y con la implementación de la NTP fue de 0.982, logrando un incremento de 0.279 de tiempo, que representa el 39.7% en el tiempo durante el cual un sistema está disponible.

6. RECOMENDACIONES

Primera: Se recomienda realizar un análisis del estado situacional de los recursos informáticos de las demás áreas de Gestión Tecnologías de la Información GTI de la Oficina de Tecnologías de la Información – OTIC, para encontrar debilidades en la Seguridad de la Información, como ya se visto evidenciado en esta tesis realizado en el área de Configuración y Activos.

Segunda: Se recomienda la implementación de la Norma Técnica Peruana ISO/IEC 27001 para optimizar los procesos y recursos informáticos de la OTIC y salvaguardar los activos de TI y evitar la pérdida de información como ha venido ocurriendo hasta la implementación de la norma mencionada en el área de Configuración y Activos.

Tercera: Se recomienda a la OTIC la capacitación al personal encargado de administración de datos y a especialistas informáticos de la Norma Técnica Peruana ISO/IEC 27001, Así como la concientización sobre la Seguridad de Información. Lo que permita analizar el estado de la Integridad, Disponibilidad y Confidencialidad de sus respectivas áreas y la interrelación segura entre las otras oficinas de la OTIC.

Cuarta: Se recomienda a la OTIC establecer como prioridad la certificación internacional de la norma ISO 27001 Foundation, a los especialistas informáticos encargados con la implementación de la misma en sus

respectivas áreas, con el fin de priorizar la Seguridad de la Información en las dependencias del MINEDU.

7. REFERENCIAS

- Aguilera, Purificación. 2008. Seguridad Informática. MADRID: Editex, 2010.240pp.
  ISBN: 978-84-9771-657-4

- Alcántara, Julio. 2015. Guía de Implementación de la Seguridad basado en ISO/IEC 27001, para apoyar la seguridad en los Sistemas de Información de la Comisaría norte P.N.P. en la ciudad de Chiclayo. PERÚ: Universidad Católica Santo Toribio de Mogrovejo, 2015. 157pp

- Amutio, Miguel y Candau, Javier. 2012. MAGERIT. Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I. Método. MADRID: Ministerio de Hacienda y Administraciones Pública. España, 2012. 127pp

- Areito, Javier. 2008. Seguridad de la Información, Redes, informática y sistemas de información. MADRID: Paraninfo, 2008.592pp.
  ISBN-13: 978-8497325028

- Barrantes, Carlos y Javier Hugo. 2012. Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos. PERÚ: Universidad de San Martín de Porres, 2012. 330pp.

- Bernal, César. 2010. Metodología de la investigación, administración economía, humanidades y ciencias sociales (3ª. ed.) COLOMBIA: PEARSON, 2010. 320pp.
  ISBN: 978-958-699-128-5

- Costas, Jesús. 2010. Seguridad Informática. ESPAÑA: RA-MA Editorial, 2010. 308pp.
  ISBN: 978-84-7897-979-0

- Gomés, Álvaro y SUÁREZ, Carlos. 2011. Sistemas de Información. Herramientas prácticas para la gestión (3ª. ed.) MEXICO: Alfa y Omega Grupo Editor, 2011. 360pp.
  ISBN: 978-607-7854-45-6

- Guzmán, Carlos. 2015. Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad Financiera de Segundo Piso. COLOMBIA: Institución Universitaria Politécnico Grancolombiano, 2015. 173pp

- Hernández, Roberto, Fernández, Carlos y Baptista, Pilar. 2010. Metodología de la investigación (4ª. ed.) MEXICO: McGRAW-HILL/Interamericana editores S.A. de C.V., 2006. 850pp.
  ISBN: 970-10-5753-8

- ISACA – Information Systems Audit and Control Association -en español - La integridad de los datos: el aspecto más relegado de la seguridad de la información [en línea] [Fecha de consulta: 26.08.2016] consultado en: http://www.isaca.org/JOURNAL/ARCHIVES/2011/VOLUME-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

- ISO 27001. Information Security Management. 2013 ISO.ORG. 2013. 23pp

- ISO Management system standards [en línea] ISO/IEC 27001 - Information security management [Fecha de consulta: 15.08.2016] consultado en http://www.iso.org/iso/iso27001

ISO en español – Portal de ISO 27001 en español [en línea] [Fecha de consulta: 20.08.2016] consultado en http://www.iso27000.es/

- Lapiedra, Rafael, Devece, Carlos y Guiral Joaquin. 2011. Introducción a la gestión de sistemas de información en la empresa. Colección Sapientia. 72pp
  ISBN: 978-84-693-9894-4

- NORMA TECNICA PERUANA. 2014. NTP-ISO/IEC 17799 – 2007. LIMA. 2007. 173pp.

- NORMA TECNICA PERUANA. 2014. NTP-ISO/IEC 27001– 2014 – 2da Edición. LIMA. 2014. 45pp.

- PMI – Project Management Institute [en línea] [Fecha de consulta: 21.08.2016] consultado en http://pmi.org.py/index.php/pmi/ estándares

- Quezada, Nel. 2010. Metodología de la investigación, estadística aplicada en la investigación. PERÚ: EMPRESA EDITORIAL MACRO, 2010. 320pp.
  ISBN: 978-612-4034-50-3

- Talavera, Vasco. 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. PERÚ: Pontificia Universidad Católica del Perú, 2015. 90pp.

- Tola, Diana. 2015. Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de Consultoría y Auditoría aplicando la norma ISO/IEC. ECUADOR: Escuela Superior Politécnica del Litoral, 2015. 135pp.

8. ANEXOS

8.1 ANEXO 01: Instrumento ficha de observación

A continuación se muestra la ficha de observación empleada en este trabajo de investigación incluyendo las tres dimensiones empleadas con sus respectivas métricas.

Registro	DIMENSIONES					
	Confidencialidad		Integridad		Disponibilidad	
	Número de información confidencial divulgada		Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción		Porcentaje de tiempo que se encuentra activo el sistema	
	PRE TEST	POS TEST	PRE TEST	POS TEST	PRE TEST	POS TEST
1	8	3	13	4	63.12%	99.50%
2	9	3	9	4	73.15%	99.30%
3	5	2	9	3	71.59%	98.20%
4	4	1	10	3	72.41%	97.40%
5	9	4	13	3	71.23%	97.25%
6	9	3	9	2	70.52%	98.10%
7	8	3	14	2	72.11%	97.80%
8	3	3	10	2	72.25%	97.46%
9	6	4	13	2	70.25%	98.23%
10	3	1	13	2	69.36%	99.14%
11	4	2	12	3	69.45%	98.78%
12	7	3	11	2	68.49%	97.25%
13	7	3	11	3	67.54%	98.61%
14	4	2	10	1	68.26%	98.71%
15	5	2	9	1	73.41%	98.89%
16	6	1	8	1	71.23%	98.49%
17	9	2	8	2	70.52%	97.25%
18	4	1	9	1	72.48%	98.61%
19	7	1	11	1	73.65%	98.71%
20	5	1	12	1	73.89%	98.89%
21	5	2	9	2	67.85%	97.80%
22	5	0	14	1	66.23%	97.46%
23	8	1	14	0	68.21%	98.61%
24	4	1	11	0	66.67%	98.71%
25	8	0	11	0	73.54%	98.89%
26	4	0	10	0	71.22%	97.80%
27	5	1	10	1	70.83%	97.46%
28	8	0	9	0	66.67%	97.25%

29	7	0	10	0	73.54%	98.10%
30	6	0	10	0	71.21%	97.80%
31	6	4	9	4	73.15%	99.30%
32	9	3	13	4	63.12%	99.50%
33	5	2	9	3	71.59%	98.20%
34	5	2	10	3	72.41%	97.40%
35	9	4	13	3	71.23%	97.25%
36	9	3	9	2	70.52%	98.10%
37	8	3	14	2	72.11%	97.80%
38	3	3	10	2	72.25%	97.46%
39	8	3	13	2	70.25%	98.23%
40	3	1	13	2	69.36%	99.14%
41	4	2	12	3	69.45%	98.78%
42	7	3	11	2	68.49%	97.25%
43	7	3	11	3	67.54%	98.61%
44	4	2	10	1	68.26%	98.71%
45	4	1	9	1	73.41%	98.89%
46	6	1	8	1	71.23%	98.49%
47	9	2	8	2	70.52%	97.25%
48	4	1	9	1	72.48%	98.61%
49	7	1	11	1	73.65%	98.71%
50	5	1	12	1	73.89%	98.89%
51	5	2	9	2	67.85%	97.80%
52	5	0	14	1	66.23%	97.46%
53	8	1	14	0	68.21%	98.61%
54	4	1	11	0	66.67%	98.71%
55	8	0	11	0	73.54%	98.89%
56	4	0	10	0	71.22%	97.80%
57	5	1	10	1	70.83%	97.46%
58	8	0	9	0	66.67%	97.25%
59	7	0	10	0	73.54%	98.10%
60	6	0	10	0	71.21%	97.80%
61	6	4	9	4	73.15%	99.30%
62	9	3	13	4	63.12%	99.50%
63	5	2	9	3	71.59%	98.20%
64	5	2	10	3	72.41%	97.40%
65	9	4	13	3	71.23%	97.25%
66	9	3	9	2	70.52%	98.10%
67	8	3	14	2	72.11%	97.80%
68	3	3	10	2	72.25%	97.46%

69	8	3	13	2	70.25%	98.23%
70	3	1	13	2	69.36%	99.14%
71	4	2	12	3	69.45%	98.78%
72	7	3	11	2	68.49%	97.25%
73	7	3	11	3	67.54%	98.61%
74	4	2	10	1	68.26%	98.71%
75	4	1	9	1	73.41%	98.89%
76	6	1	8	1	71.23%	98.49%
77	9	2	8	2	70.52%	97.25%
78	4	1	9	1	72.48%	98.61%
79	7	1	11	1	73.65%	98.71%
80	5	1	12	1	73.89%	98.89%
81	5	2	9	2	67.85%	97.80%
82	5	0	14	1	66.23%	97.46%
83	8	1	14	0	68.21%	98.61%
84	4	1	11	0	66.67%	98.71%
85	8	0	11	0	73.54%	98.89%
86	4	0	10	0	71.22%	97.80%
87	5	1	10	1	70.83%	97.46%
88	8	0	9	0	66.67%	97.25%
89	7	0	10	0	73.54%	98.10%
90	6	0	10	0	71.21%	97.80%
91	6	4	9	4	73.15%	99.30%
92	9	3	13	4	63.12%	99.50%
93	5	2	9	3	71.59%	98.20%
94	5	2	10	3	72.41%	97.40%
95	9	4	13	3	71.23%	97.25%
96	9	3	9	2	70.52%	98.10%
97	8	3	14	2	72.11%	97.80%
98	3	3	10	2	72.25%	97.46%
99	8	3	13	2	70.25%	98.23%
100	3	1	13	2	69.36%	99.14%
101	4	2	12	3	69.45%	98.78%
102	7	3	11	2	68.49%	97.25%
103	7	3	11	3	67.54%	98.61%
104	4	2	10	1	68.26%	98.71%
105	5	1	9	1	73.41%	98.89%
106	6	1	8	1	71.23%	98.49%
107	9	2	8	2	70.52%	97.25%
108	4	1	9	1	72.48%	98.61%

109	7	1	11	1	73.65%	98.71%
110	5	1	12	1	73.89%	98.89%
111	5	2	9	2	67.85%	97.80%
112	5	0	14	1	66.23%	97.46%
113	8	1	14	0	68.21%	98.61%
114	4	1	11	0	66.67%	98.71%
115	8	0	11	0	73.54%	98.89%
116	4	0	10	0	71.22%	97.80%
117	6	1	10	1	70.83%	97.46%
118	8	0	9	0	66.67%	97.25%
119	7	0	10	0	73.54%	98.10%
120	8	0	10	0	71.21%	97.80%
121	3	3	13	2	72.25%	97.46%
122	8	3	13	2	70.25%	98.23%
123	5	1	12	3	69.36%	99.14%
124	4	2	11	2	69.45%	98.78%
125	7	3	11	3	68.49%	97.25%
126	7	3	10	1	67.54%	98.61%
127	4	2	9	1	68.26%	98.71%
128	5	1	8	1	73.41%	98.89%
129	6	1	8	2	71.23%	98.49%
130	9	2	9	1	70.52%	97.25%
131	4	1	11	1	72.48%	98.61%
132	7	1	12	1	73.65%	98.71%
133	5	1	9	2	73.89%	98.89%
134	7	2	14	1	67.85%	97.80%
135	4	0	14	0	66.23%	97.46%
136	8	1	11	0	68.21%	98.61%
Total	**825**	**227**	**1463**	**211**	**70.342%**	**98.225%**

ANEXO 02: Validación de los instrumentos

INFORME DE VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS

I. **Datos Generales**

1.1 Apellidos y nombres del validador: Frey Elmer Chavez Pinillos - Juan Carlos Sánchez Torres – Rudy Chapoñan Camarena

1.2 Institución donde labora/cargo: Docente Tiempo Completo.

1.3 Especialidad del validador: Ingeniero de Sistemas

1.4 Nombre del instrumento y finalidad de su aplicación: Ficha de Observación usando Indicadores para la medición de la Seguridad de la Información.

1.6 Título de la investigación: "NTP-ISO/IEC 27001 PARA LA SEGURIDAD DE INFORMACIÓN EN EL ÁREA DE CONFIGURACIÓN Y ACTIVOS DEL MINISTERIO DE EDUCACIÓN – SEDE CENTROMIN"

1.8 Autor del Instrumento: Hugo Daniel Olaza Allano

II. **Definición conceptual de las variables y sus dimensiones**

Variable: Seguridad de Información

Según la Norma Técnica Peruana NTP-ISO/IEC 17799- 2007, indica: La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios (2007, p.8)

1

Dimensiones de las variables:

Dimensión 1
Confidencialidad Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado. (Costas Santos J 2010 p, 23).

Dimensión 2
Integridad La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicado a las bases de datos sería la correspondencia entre los datos y los hechos que refleja (Costas Santos J 2010, p.25).

Dimensión 3
Disponibilidad Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando éstos lo requieran. (Costas Santos J 2010, p 26).

III. **Matriz de operacionalización de las variables**

Variable: Seguridad de la Información.

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	ITEM / INDICADOR	INSTRUMENTO	ESCALA
Seguridad de la Información	Según la Norma Técnica Peruana NTP-ISO/IEC 17799 - 2007, indica que: La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Por otro lado, la seguridad de información es considerada como un conjunto de medidas técnicas y legales que permiten a la institución asegurar la confidencialidad, integridad y disponibilidad de un sistema de información.	Es un conjunto de medidas establecidas que permitirá asegurar la confidencialidad, integridad y disponibilidad de la información dentro de una organización. Asimismo, luego de su aplicación en la organización pueda estar preparado ante una amenaza y o riesgos de la información	**Confidencialidad**	Número de información confidencial divulgada	**Ficha de Observación**	**Ordinal**
			Integridad	Número o porcentaje de accesos y/o cambios no autorizados a los datos de la producción	**Ficha de Observación**	**Ordinal**
			Disponibilidad	Porcentaje de tiempo durante el cual un sistema está disponible para el usuario D = (tiempo total transcurrido – suma de tiempo de inactividad) / tiempo total transcurrido	**Ficha de Observación**	**Razón**

IV. Certificado de validez de contenido del instrumento

N°	DIMENSIONES / Indicadores	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1	Si	No	Si	No	Si	No	
1								
2								
3								
	DIMENSION 2	Si	No	Si	No	Si	No	
1								
2								
3								
	DIMENSION 3	Si	No	Si	No	Si	No	
1								
2								

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: **Aplicable [ ]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: ..... **DNI:**.....

Especialidad del validador:.....

.....**de**.....**del 20**.....

[1]**Pertinencia:** El indicador corresponde al concepto teórico formulado.
[2]**Relevancia:** El indicador es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los indicadores planteados son suficientes para medir la dimensión

---

Firma del Experto Informante.

ANEXO 03: Matriz de consistencia

TÍTULO GENERAL	PROBLEMA GENERAL	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLE INDEPENDIENTE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADOR	FORMULA
Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin	¿Cuál será el efecto de la implementación de la NTP ISO/IEC 27001 para la seguridad de información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin?	Determinar el efecto de la implementación de la NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin.	La implementación de la NTP ISO/IEC 27001 mejora significativamente la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin.	**Norma Técnica Peruana ISO/IEC 27001**	Esta Norma Técnica Peruana es una adopción de la Norma ISO/IEC 17799:2005. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995. (2007, p .iv).	Es un estándar o norma que ha sido creado con el propósito de asegurar la información para las empresas o instituciones públicas, tomando en cuenta un ciclo de cuatro fases como son establecer un sistema, implementarlo y operarlo, mantenerlo y mejorarlo y por ultimo monitorearlo; todo esto permitirá minimizar a los riesgos y amenazas externas o internas a la información que maneja cada empresa; asimismo, permitirá a estar preparados ante cualquier evento relacionado a la divulgación de información.			
	PROBLEMAS ESPECIFICOS	**OBJETIVOS ESPECIFICOS**	**HIPOTESIS ESPECIFICOS**	**DEPENDIENTE**	**DEFINICIÓN CONCEPTUAL**	**DEFINICIÓN OPERACIONAL**	**DIMENSIONES**	**INDICADOR**	**FORMULA**
	¿Cuál será el efecto de la implementación de la NTP ISO/IEC 27001 en la confidencialidad de la seguridad de información en el Área de Configuración y Activos del MINEDU?	Determinar el efecto de la implementación de la NTP ISO/IEC 27001 en la confidencialidad de la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.	La implementación de la NTP ISO/IEC 27001 mejora significativamente la confidencialidad de la Seguridad de Información en el área de configuración y Activos del Ministerio de Educación – Sede Centromin.	**Seguridad de la Información**	Según la Norma Técnica Peruana NTP-ISO/IEC 17799 - 2007, indica que: La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades.	Es un conjunto de medidas establecidas que permitirá asegurar la confidencialidad, integridad y disponibilidad de la información dentro de una organización. Asimismo, luego de su aplicación en la organización pueda estar preparado ante una amenaza y o riesgos de la información.	CONFIDENCIALIDAD	Número de información confidencial divulgada	
	¿Cuál será el efecto de la implementación de la NTP ISO/IEC 27001 en la integridad de la seguridad de información en el Área de Configuración y Activos del MINEDU?	Determinar el efecto de la implementación de la NTP ISO/IEC 27001 en la integridad de la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación – Sede Centromin.	La implementación de la NTP ISO/IEC 27001 mejora significativamente la integridad de la Seguridad de Información en el área de configuración y Activos del Ministerio de Educación – Sede Centromin.				INTEGRIDAD	Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción	
	¿Cuál será el efecto de la implementación de la NTP ISO/IEC 27001 en la disponibilidad de la seguridad de información en el Área de Configuración y Activos del MINEDU?	Determinar el efecto de la implementación de la NTP ISO/IEC 27001 en la disponibilidad de la Seguridad de Información en el área de Configuración y Activos del Ministerio	La implementación de la NTP ISO/IEC 27001 mejora significativamente la disponibilidad de la Seguridad de Información en el área de configuración y Activos del Ministerio				DISPONIBILIDAD	Porcentaje de tiempo durante el cual un sistema está disponible para el usuario	D = (tiempo total transcurrido – suma de tiempo de inactividad) / tiempo total transcurrido

		de Educación – Sede Centromin.	de Educación – Sede Centromin.						

Elaborado por: Hugo Daniel Olaza Aliano

ANEXO 04: Implementación de la NTP ISO/IEC 27001 - Análisis de Riesgos en el área de Configuración y Activos

ANÁLISIS DE RIESGOS EN EL ÁREA DE CONFIGURACIÓN Y ACTIVOS

1. Introducción

El presente documento muestra las actividades relacionados a la mejora continua relacionado al Análisis de Riesgos basado en la metodología de MAGERIT, como parte del plan de la implementación de la Norma Técnica Peruana ISO/IEC 27001 en al área de Configuración y Activos. Para ello, identifica a las partes involucradas, define la interrelación entre actividades, especifica la información de entrada y resultados de salida. Asimismo, se declaran los criterios de control, que conducirán la oportuna acción de los recursos y herramientas en el análisis.

1.1. Objetivo

Suministrar la documentación de la evaluación de riesgos elaborada al área de Configuración y Activos de la OTIC. Este orientará el alcance, las actividades y los tiempos, que facilitaran el detalle necesario para comprender el funcionamiento del análisis.

2. Alcance

El presente procedimiento se aplicará para las actividades del área de Configuración y Activos de la OTIC del MINEDU.

3. Marco Normativo

- R.S.M. N° 246-2007-PCM Aprueban uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición" en todas las entidades integrantes del Sistema Nacional de la Informática.

- R.S.G. N° 710-2015 - Directiva 003–2015–MINEDU/SPE-OTIC "Directiva para el Acceso y Uso Adecuado de los Recursos Informáticos en el Ministerio de Educación" y "Directiva para la Administración de los Recursos Informáticos del Ministerio de Educación".
- R.S.G. N°908-2015-MINEDU Directiva N°006-2015-MINEDU/SPE-OPEP-UNOME denominada “Metodología para la gestión por procesos en el Ministerio de Educación”
- R.S.G. N°908-2015-MINEDU Directiva N°007-2015-MINEDU/SPE-OPEP-UNOME denominada “Elaboración, Aprobación y Actualización de los Manuales de Procedimientos (MAPRO) del Ministerio de Educación”
- D.S. N° 109-2012-PCM, aprueba la “Estrategia de Modernización de la Gestión Pública”.
- D.S. N° 004-2013-PCM, “Política Nacional de Modernización de la Gestión Pública”.

4. Definiciones, siglas y abreviaturas

Se definen los términos empleados en el documento para comprensión del mismo.

- **MINEDU:** Ministerio de Educación
- **TI:** Tecnologías de la Información
- **OTIC:** Oficina de Tecnologías de la Información y Comunicación
- **GTI:** Gestión de Tecnologías de Información
- **NTP:** Norma Técnica Peruana
- **MAGERIT:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

5. Organización

Para la realización del presente análisis se requiere establecer el organigrama e identificar las partes involucradas que actuaran en la realización de las actividades y tratamiento de la información.

5.1. Organigrama

Para la realización del presente análisis se establece el siguiente organigrama funcional.

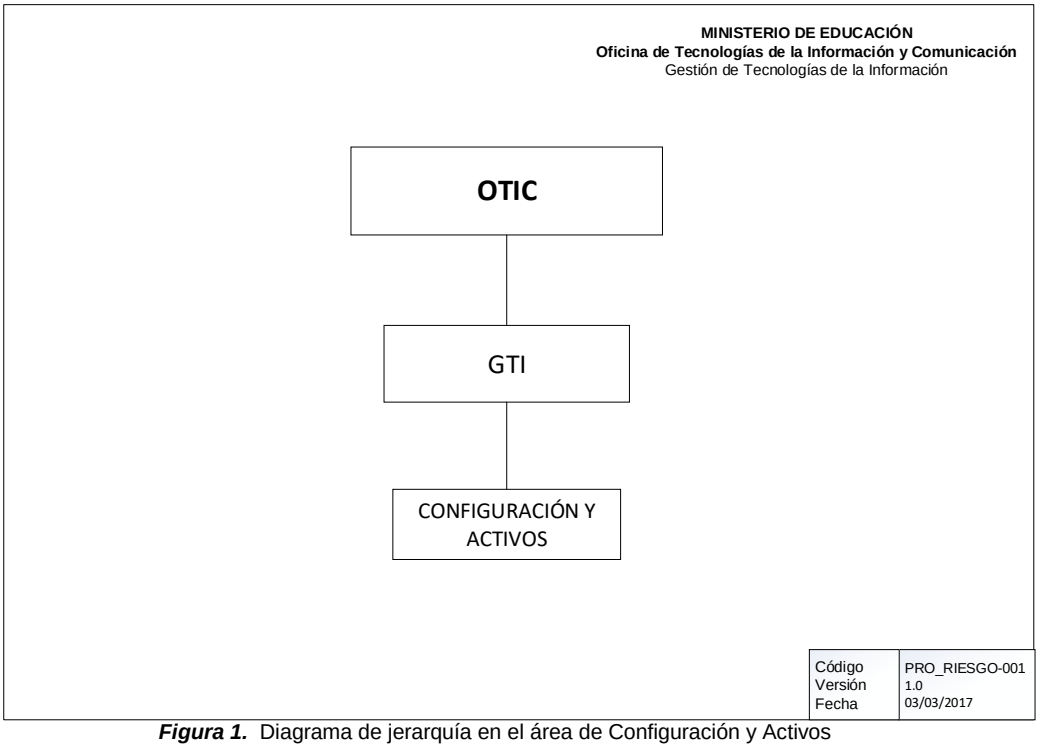


Figura 1. Diagrama de jerarquía en el área de Configuración y Activos

6. Partes involucradas

Para la realización del presente análisis se establecen los siguientes roles.

Tabla 1.

Estructura de los roles y responsabilidades

ROL	FUNCIÓN	EQUIPO DE TRABAJO	UNIDAD
Coordinador de Análisis	Responsable de velar por la correcta realización del análisis, medir el rendimiento funcional, y aportar las mejoras al mismo.	Configuración y Activos	GTI
Responsable de Configuración de Activos	Responsable de velar por la disponibilidad de información requerida sobre Elementos de Configuración (CI's) y de brindar información técnica, bajo un modelo lógico que contiene los componentes de la infraestructura de TI y sus respectiva correlación.	Configuración y Activos	GTI

ROL	FUNCIÓN	EQUIPO DE TRABAJO	UNIDAD
Coordinador de Análisis	Responsable de velar por la correcta realización del análisis, medir el rendimiento funcional, y aportar las mejoras al mismo.	Configuración y Activos	GTI
Analista de Configuración y Activos	Responsable de registrar y clasificar las peticiones e incidencias y llevar a cabo los esfuerzos inmediatos para su respectiva restauración o atención de los equipos informáticos del MINEDU.	Configuración y Activos	GTI
Operador de Configuración de Activos	Responsable de ejecutar la actualización de los correlativos de configuración de los equipos informáticos del MINEDU.	Configuración y Activos	GTI

6.1. Diagrama de actores

Para la realización del presente procedimiento se establecen los siguientes actores.

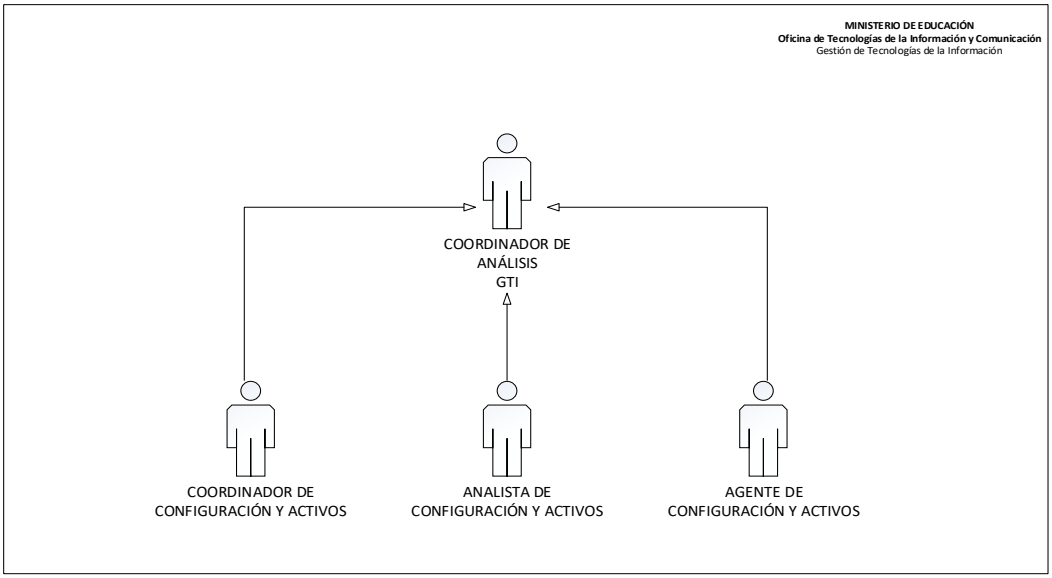


Figura 2. Estructura orgánica de las partes involucradas

7. Factores de control para la realización del procedimiento

DESCRIPCIÓN	FUENTE
• Documento y/o guía de información necesaria para el análisis de riesgo	Coordinador de Análisis

8. Flujos de entrada

- Documentos de atención

- Fichas de Observación

9. Flujos de salida

- Resultado de Análisis

10. Desarrollo de Análisis

Para la realización del presente análisis se requiere establecer los factores necesarios para implementaciónón de la NTP ISO/IEC 27001 e identificar las partes involucradas que actuarán en la realización de dicha implementación.

11. Metodología de evaluación de riesgo.

Se manejó la metodología de MAGERIT para el análisis y gestión de los riesgos, ya que permite determinar los riesgos paso a paso. A continuación de indican los pasos a seguir:

- Paso 1: Inventario de Activos
- Paso 2: Amenazas
- Paso 3: Salvaguardas

12. Paso 1: Inventario de Activos.

Cada empresa y/o compañía se encargan de proteger la confidencialidad, integridad y disponibilidad de la información para velar la continuidad de sus servicios y mantener su actividad. Con la finalidad de proteger la información de los riesgos y amenazas el área de Configuración y Activos de la Oficina de Tecnologías de la Información – OTIC del Ministerio de Educación –MINEDU, realizó un inventario de sus activos teniendo en cuenta la Metodología de Magerit los cuales se clasifican en los siguientes grupos:

- Activos esenciales
- Datos o información
- Inventario de servicios
- Las aplicaciones de software.

- Equipos informáticos
- Redes de Comunicación
- Soportes de Información
- Equipamiento Auxiliar
- Instalaciones
- Personal

12.1. Activos esenciales.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área
[vr]	Datos vitales	[I_Activos_TI]	Información de Activos de TI (base de datos y registro de altas y bajas)
		[I_Licencias]	Información de Licencias
[classified]	Datos clasificados	[E_S_Licenciado]	Ejecutable software Licenciado
		[D_Historicos]	Información Histórica de activos de TI

12.1.1. Datos / Información.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área
[Files]	Ficheros	[I_Activos_TI]	Archivo de Activos de TI
		[A_Informes y Licencias]	Archivos de Informes y Licencias adquiridas
[backup]	Copia de Respaldo	[A_copias de Seguridad]	Archivos de copias de seguridad de la información
[conf]	Datos de configuración	[D_configuración_comp]	Datos de configuración de computadoras personales
[int]	Datos de gestión interna	[D_GestiónActivos]	Datos de Gestión de Activos
[password]	Credenciales	[D_credenciales]	Credenciales por usuario

12.1.2. Inventario Servicios.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área
[ext]	A usuarios externos (sedes descentralizadas)	[S_U_Externo]	Servicios prestados a usuarios externos de sede descentralizadas (DRE y UGEL)

[int]	Interno (a usuarios propios del MINEDU)	[S_U_Interno]	Servicios prestados a los trabajadores propios del MINEDU
[int]	Interno (a usuarios propios del MINEDU)	[S_Telefonia_Movil]	Servicios de telefonía móvil prestado a los trabajadores propios del MINUEDU
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la institución y el lugar de donde esté ingresando, considerando el desempeño.

12.1.3. Software – Aplicaciones informáticas.

En vista que el área de configuración de activos de la OTIC, se dedica a emitir los estados de los activos de TI que mantiene en ejecución los servicios de TI del MINEDU, este cuenta con registros conformado de hojas de cálculo donde se registra, actualiza y almacena las altas, baja de los activos de TI

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área
[Office]	Ofimática	[Office]	Office 2013
[os]	Sistema Operativo	[OS_Win8.1]	Sistema Operativo Windows 8, en su versión profesional con actualizaciones automáticas activadas
[av]	Antivirus	[Antivirus]	Sophos original con actualizaciones automáticas.

12.1.4. Equipos informáticos.

Se consideran todos los equipos informáticos del Área de Configuración y Activos.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[host]	Grandes Equipos (Servidor de base de datos)	[S_Database]	Servidor de Base de Datos
		[S_DML]	Servidor de Biblioteca de Medios Definidos
[mid]	Equipos Medios (Equipos de trabajo conectados a través de red física)	[PC_funcionarios]	Computadora personal de Escritorio

[pc]	Equipos que son fáciles de transportar	[PC_portatiles]	Computadora personal portátil
[print]	Equipos de Impresión	[E_impresoras]	Impresoras

12.1.5. Redes de comunicaciones.

Se considera todas las redes de comunicación que es usado por el Área de configuración y Activos.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[pstn]	Red Telefónica	[R_telefónica]	Red telefónica
[wifi]	Red inalámbrica	[R_wifi]	Red inalámbrica
[mobile]	Telefonía móvil	[T_móvil]	Telefonía móvil
[LAN]	Red local	[R_Local]	Red local
[Internet]	Internet	[Internet]	Internet

12.1.6. Soporte de Información _ almacenamiento electrónico.

Se considera dispositivos físicos de almacenamiento electrónico.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[san]	Almacenamiento en Red	[A_UR]	Almacenamiento en Red
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro Externo

12.1.7. Soporte de Información _ almacenamiento no electrónico.

Se considera dispositivos físicos de almacenamiento electrónico.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[printed]	Material impreso	C_ Documentación_Activos_TI	Carpetas con la documentación de cada alta y baja (ctm, orden, propuestas de postor, orden compra guía de remisión evaluación técnica)
		C_Reporteseinformes	Carpetas de reporte e informes impresos de atenciones por garantía.
		C_fichasdemovimientos	Carpetas con ficha de movimientos de los activo informáticos

12.1.8. Equipamiento Auxiliar.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[printed]	Sistema de alimentación interrumpida	U_Computadores	UPS computadora personal de escritorio
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales(papel, sobres, carpetas, etc)
[Fumiture]	Mobiliario	M_Mobiliario	Mobiliario(Módulos, escritorios, archivadores, armariós, etc)

12.1.9. Instalaciones.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[building]	Edificio	E_empresa	Instalación de la Sede Centromin

12.1.10. Personal.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[ui]	Usuarios internos	C_CYA	Coordinador de Configuración y activos
		A_CYA	Analista de Configuración y Activos
		Ag_CYA	Agente de configuración y Activos

12.2. Valoración cualitativa de los activos.

Sabiendo que todos los activos no tienen la misma importancia para una empresa y en el caso de que sean atacados o presente una incidencia generará un impacto diferente en la institución, por tal se realiza una valorización cualitativa para cada uno de los activos teniendo en cuenta las dimensiones de seguridad como es la confidencialidad, integridad y disponibilidad según a la siguiente tabla.

Tabla 2.

Criterios de Valoración

Valor		***Criterio***
10	Extremo	Daño extremadamente grande
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	despreciable	Irrelevante a efectos prácticos

Fuente: Tomado del MAGERIT v3 libro 2 Catalogo de elementos

12.2.1. Valoración Cualitativa de Activos esenciales.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Dimensión de Seguridad	Criterio
[vr]	Datos vitales	[I_Activos_TI]	Información de Activos de TI (base de datos y registro de altas y bajas)	Confidencialidad	7
				Integridad	7
				Disponibilidad	7
		[I_Licencias]	Información de Licencias	Confidencialidad	7
				Integridad	7
				Disponibilidad	6
[classified]	Datos clasificados	[E_S_Licenciado]	Ejecutable software Licenciado	Confidencialidad	
				Integridad	6
				Disponibilidad	4
		[D_Historicos]	Información Histórica de activos de TI	Confidencialidad	3
				Integridad	3
				Disponibilidad	3

12.2.2. Valoración Cualitativa Datos / Información.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Dimensión de Seguridad	Criterio
[Files]	Ficheros	[I_Activos_TI]	Archivo de Activos de TI	Confidencialidad	6
				Integridad	6
				Disponibilidad	
		[A_Informes y Licencias]	Archivos de Informes y Licencias adquiridas	Confidencialidad	5
				Integridad	4
				Disponibilidad	5
[backup]	Copia de Respaldo	[A_copias de Seguridad]	Archivos de copias de seguridad de la información	Confidencialidad	7
				Integridad	7
				Disponibilidad	4
[conf]	Datos de configuración	[D_configuración_comp]	Datos de configuración de computadoras personales	Confidencialidad	
				Integridad	6
				Disponibilidad	
[int]	Datos de gestión interna	[D_GestiónActivos]	Datos de Gestión de Activos	Confidencialidad	6
				Integridad	5

				Disponibilidad	7
[password]	Credenciales	[D_credenciales]	Credenciales por usuario	Confidencialidad	
				Integridad	7
				Disponibilidad	

12.2.3. Valoración Cualitativa Servicios.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Dimensión de Seguridad	Criterio
[ext]	A usuarios externos (sedes descentralizadas)	[S_U_Externo]	Servicios prestados a usuarios externos de sede descentralizadas (DRE y UGEL)	Confidencialidad	6
				Integridad	6
				Disponibilidad	
[int]	Interno (a usuarios propios del MINEDU)	[S_U_Interno]	Servicios prestados a los trabajadores propios del MINEDU	Confidencialidad	7
				Integridad	7
				Disponibilidad	7
[int]	Interno (a usuarios propios del MINEDU)	[S_Telefonia_Movil]	Servicios de telefonía móvil prestado a los trabajadores propios del MINUEDU	Confidencialidad	6
				Integridad	6
				Disponibilidad	7
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la institución y el lugar de donde esté ingresando, considerando el desempeño.	Confidencialidad	7
				Integridad	7
				Disponibilidad	

12.2.4. Valoración Cualitativa Software – Aplicaciones informáticas.

En vista que el área de configuración de activos de la OTIC, se dedica a emitir los estados de los activos de ti que mantiene en ejecución los servicios de TI del MINEDU, este cuenta con registros conformado de hojas de cálculo donde se registra, actualiza y almacena las altas, baja de los activos de TI.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Dimensión de Seguridad	Criterio

[Office]	Ofimática	[Office]	Office 2013	Confidencialidad	
				Integridad	7
				Disponibilidad	7
[os]	Sistema Operativo	[OS_Win8.1]	Sistema Operativo Windows 8, en su versión profesional con actualizaciones automáticas activadas	Confidencialidad	
				Integridad	7
				Disponibilidad	7
[av]	Antivirus	[Antivirus]	Sophos original con actualizaciones automáticas.	Confidencialidad	7
				Integridad	
				Disponibilidad	7

12.2.5. Valoración Cualitativa de Equipos informáticos.

Se consideran todos los equipos informáticos del Área de Configuración y Activos.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo al Área	Dimensión de Seguridad	Criterio
[host]	Grandes Equipos (Servidor de base de datos)	[S_Database]	Servidor de Base de Datos	Confidencialidad	7
				Integridad	7
				Disponibilidad	7
		[S_DML]	Servidor de Biblioteca de Medios Definidos	Confidencialidad	6
				Integridad	7
				Disponibilidad	7
[mid]	Equipos Medios (Equipos de trabajo conectados a través de red física)	[PC_funcionarios]	Computadora personal de Escritorio	Confidencialidad	6
				Integridad	6
				Disponibilidad	
[pc]	Equipos que son fáciles de transportar	[PC_portatiles]	Computadora personal portátil	Confidencialidad	6
				Integridad	6
				Disponibilidad	
[print]	Equipos de Impresión	[E_impresoras]	Impresoras	Confidencialidad	
				Integridad	
				Disponibilidad	6

12.2.6. Valoración Cualitativa de Redes de comunicaciones.

Se considera todas las redes de comunicación que es usado por el Área de configuración y Activos:

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo al area	Dimensión de Seguridad	Criterio
[pstn]	Red Telefónica	[R_telefónica]	Red telefónica	Confidencialidad	7
				Integridad	7
				Disponibilidad	7
[wifi]	Red inalámbrica	[R_wifi]	Red inalámbrica	Confidencialidad	7
				Integridad	7
				Disponibilidad	7
[mobile]	Telefonía móvil	[T_móvil]	Telefonía móvil	Confidencialidad	7
				Integridad	7
				Disponibilidad	7
[LAN]	Red local	[R_Local]	Red local	Confidencialidad	7
				Integridad	7
				Disponibilidad	7
[Internet]	Internet	[Internet]	Internet	Confidencialidad	
				Integridad	
				Disponibilidad	7

12.2.7. Valoración Cualitativas de Soporte de Información _ almacenamiento electrónico.

Se considera dispositivos físicos de almacenamiento electrónico:

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[san]	Almacenamiento en Red	[A_UR]	Almacenamiento en Red	Confidencialidad	6
				Integridad	7
				Disponibilidad	7
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro	Confidencialidad	
				Integridad	5
				Disponibilidad	5

12.2.8. Valoración Cualitativa de Soporte de Información _ almacenamiento no electrónico.

Se considera dispositivos físicos de almacenamiento no electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[printed]	Material impreso	C_ Documentación_Activos_TI	Carpetas con la documentación de cada alta y baja (ctm, orden, propuestas de postor, orden compra guía de remisión evaluación técnica)	Confidencialidad	
				Integridad	7
				Disponibilidad	5
		C_Reporteseinformes	Carpetas de reporte e informes impresos de atenciones por garantía.	Confidencialidad	
				Integridad	7
				Disponibilidad	6
		C_fichasdemovimientos	Carpetas con ficha de movimientos de los activo informáticos	Confidencialidad	
				Integridad	7
				Disponibilidad	5

12.2.9. Valoración Cualitativa de Soporte de Información _ almacenamiento no electrónico.

Se considera dispositivos físicos de almacenamiento no electrónico.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[printed]	Material impreso	C_ Documentación_Activos_TI	Carpetas con la documentación de cada alta y baja (ctm, orden, propuestas de postor, orden compra guía de remisión evaluación técnica)	Confidencialidad	
				Integridad	7
				Disponibilidad	5
		C_Reporteseinformes	Carpetas de reporte e informes impresos de atenciones por garantía.	Confidencialidad	
				Integridad	7
				Disponibilidad	6
		C_fichasdemovimientos	Carpetas con ficha de movimientos de los activo informáticos	Confidencialidad	
				Integridad	7
				Disponibilidad	5

12.2.10. Valoración Cualitativa de Equipamiento Auxiliar.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[printed]	Sistema de alimentación interrumpida	U_Computadores	UPS computadora personal de escritorio	Confidencialidad	
				Integridad	
				Disponibilidad	**4**
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales(papel,	Confidencialidad	
				Integridad	

			sobres, carpetas, etc)	Disponibilidad	**6**
[Fumiture]	Mobiliario	M_Mobiliario	Mobiliario(Módulos, escritorios, archivadores, armariós, etc)	Confidencialidad	
				Integridad	
				Disponibilidad	**6**

12.2.11. Valoración Cualitativa de Instalaciones.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[building]	Edificio	E_empresa	Instalación de la Sede Centromin	Confidencialidad	
				Integridad	
				Disponibilidad	**6**

12.2.12. Valoración Cualitativa de Personal.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[ui]	Usuarios internos	C_CYA	Coordinador de Configuración y activos	Confidencialidad	
				Integridad	
				Disponibilidad	**7**
		A_CYA	Analista de Configuración y Activos	Confidencialidad	
				Integridad	
				Disponibilidad	**7**
		Ag_CYA	Agente de configuración y Activos	Confidencialidad	
				Integridad	
				Disponibilidad	**7**

13. Paso 2: Identificación de Amenazas.

La probabilidad de las amenazas se realiza teniendo en cuenta la frecuencia con la que pueda ocurrir, además para las dimensiones de seguridad se toma de acuerdo a esta investigación a su se tomara la escala de rango porcentual de impactos en los activos.

13.1. Escala de rango de Probabilidad de amenaza.

En la siguiente tabla se determina los rangos y valores de probabilidad de amenaza en el área de Configuración y Activos de la OTIC.

Tabla 3.

Criterio de escala de rango de Probabilidad de amenaza.

Vulnerabilidad	Rango	Valor
Casi Seguro	1 vez al dia	100
Muy probable	1 vez cada semana	70
Probable	1 vez cada 2 meses	50
Poco probable	1 vez al 6 meses	10
Improbable	1 vez al año	5

Fuente*: Modulo de Seguridad de la Información*

13.2. Dimensión de Seguridad MAGERIT.

Dimensiones de Seguridad a valorar	Identificación
Confidencialidad	C
Integridad	I
Disponibilidad	D

Fuente: MAGERIT 3.0

13.3. Escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

En la siguiente tabla se determina la escala porcentual de impacto en los activos en el área de Configuración y Activos de la OTIC

Impacto	Valor cualitativo
Extremo	**100%**
Alto	**75%**
Medio	**50%**
Bajo	**20%**
Mínimo	**5%**

Fuente*: Modulo de Seguridad de la Información*

13.4. Escala del impacto y la probabilidad de las amenazas.

En base a las tablas predecesoras donde se detalla la escala del impacto y la probabilidad de las amenazas, se procede a identificar las amenazas para el inventario de activos realizado.

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión de Seguridad (%)**		
			[C]	**[I]**	**[D]**
[N.1] Fuego [N.2] Daños por agua	Equipos informáticos	5			100 %
	Instalaciones	5			100 %
[I.1] Fuego [I.2] Daños por agua	-Equipos informáticos -Instalaciones	10			100%
N.1] Fuego [N.2] Daños por agua	Soporte de almacenamiento electrónico y no electrónico	5			100 %
[I.1] Fuego [I.2] Daños por agua	Soporte de almacenamiento electrónico y no electrónico	5			100 %
[N.1] Fuego [N.2] Daños por agua	Equipamiento Auxiliar	5			50 %
[I.1] Fuego [I.2] Daños por agua	Equipamiento Auxiliar	5			50 %
[N.*] Desastres industriales	Equipos informáticos	10			100 %
	Soporte de Información	5			75 %
	Equipamiento Auxiliar	5			20 %
	Instalaciones	5			100%
[I.*] Desastres industriales	Equipos informáticos	10			100 %
	Soporte de Información	5			75 %
	Equipamiento Auxiliar	5			20 %
	Instalaciones	5			100%
[I.3] Contaminación mecánica	Equipos informáticos	50			75%
	Soporte de Información	5			50%
	Equipamiento Auxiliar	5			20%
[I.5] Avería de origen físico o lógico	Software - Aplicaciones Informáticas	50			100%
	Equipos informáticos	10			100%
	Soportes de Información	5			20%
	Equipamiento Auxiliar	5			20%
	Equipos Informáticos	50			100%

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión de Seguridad (%)**		
			[C]	**[I]**	**[D]**
[I.6] Corte del suministro eléctrico	Soporte de Información (electrónicos)	5			50%
	Ups computadores	5			5%
[I.7] Condiciones inadecuadas de temperatura o humedad	Equipos Informáticos	50			100%
[I.8] Fallo de servicios de comunicaciones	Redes de comunicaciones (Red inalámbrica, red local e internet)	50			100%
[I.9] Interrupción de otros servicios y suministros esenciales.	Equipamiento Auxiliar	5			5 %
[I.10] Degradación de los soportes de almacenamiento de la información.	Soportes de Información	5			5%
[E.1] Errores de los usuarios **Datos /Información**	Archivos de Altas de Activos de TI	50	100%	100%	75%
	Archivos de Bajas de Activos de TI	50	100%	100%	75%
	Archivos de Informes y Licencias adquiridas	50	100%	100%	75%
	Archivos de Informes y Licencias adquiridas	10	100%	100 %	50 %
	Archivos de copias de seguridad de la información	5	100%	100 %	50 %
	Datos de configuración de computadoras personales	5	100%	100 %	50 %
	Datos de Gestión de Activos	5	100%	100%	100%
	Credenciales por usuario	5	50 %	50 %	50 %
	Datos de validación de credenciales por usuarios	5	50 %	50 %	50 %
[E.1] Errores de los usuarios **Servicios**	Servicios prestados a usuarios externos de sede descentralizadas (DRE y UGEL)	5	50 %	50 %	50 %
	Servicios prestados a los trabajadores propios del MINEDU	5	100%	100%	75%
	Servicios de Telefonía móvil institucional	10	75 %	50 %	50 %
	Manejo de privilegios de acuerdo al rol dentro de la	5	50 %	50 %	75 %

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión de Seguridad (%)**		
			[C]	**[I]**	**[D]**
	institución y el lugar de donde esté ingresando, considerando el desempeño.				
[E.1] Errores de los usuarios **Aplicaciones**	Office 2013	5	75%	50%	75%
	Sistema Operativo Windows 8, en su versión profesional con actualizaciones automáticas activadas	5	75%	20%	75%
	Sophos original con actualizaciones automáticas.	10	75%	20%	75%
[E.1] Errores de los usuarios. **Soporte de información**	Soportes de Información almacenamiento electrónico.	10	50 %	50 %	50 %
	Soportes de Información _almacenamiento no electrónico.	10	50 %	50 %	50 %
[E.2] Errores del administrador	Datos/Información	50	100 %	75%	50%
	Servicios	5	75%	50%	75%
	Aplicaciones	5	100%	75%	75%
	Redes de Comunicación	10	100%	75%	75%
[E.4] Errores de configuración.	Datos de configuración de servidores y equipos	5		100%	
[E.7] Deficiencias en la organización	Coordinador de Configuración y activos	50		75%	
	Analista de Configuración y Activos	50		75%	
	Agente de configuración y Activos	50		75%	
[E.8] Difusión de software dañino	Software –Aplicaciones Informáticas	5	50%	50%	75%
[E.9] Errores de [re-]encaminamiento	Servicios	5		20%	
	Software-aplicaciones Informáticas	5		20%	
	Redes de comunicaciones	5		20%	
[E.14] Escapes de información	Activos esenciales	5		100%	
	Datos / información	5		100%	
[E.15] Alteración accidental de la información	Datos / información	10			100%
[E.18] Destrucción de información	Datos / información	10			
	Aplicaciones	5			50%
	Soporte Información	5			20%
[E19] Fuga de información	Datos / información	10	75%		

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión de Seguridad (%)**		
			[C]	**[I]**	**[D]**
	Servicios	10	75%		
	Aplicaciones	10	50%		
	Personal	10	75%		
[E20] Vulnerabilidades de los programas	Office 2013	10	50%	20%	75%
	Sistema Operativo Windows 8, en su versión profesional con actualizaciones automáticas activadas	10	50%	20%	75%
	Sophos original con actualizaciones automáticas.	5	75%	20%	100%
[E21] Errores de mantenimiento/actualización de programas (software)	Office 2013	5		20%	20%
	Sistema Operativo Windows 8, en su versión profesional con actualizaciones automáticas activadas	10		50%	50%
	Sophos original con actualizaciones automáticas.	10		5%	20%
[E.24] Caída del sistema por agotamiento de recursos	Servicios	5			100%
	Equipos informáticos	10			100%
	Redes de comunicaciones	5			100%
[E.25] Pérdida de equipos - Robo	Equipos informáticos	5	75%		100%
	Soporte informático	5	20%		100%
	Equipamiento auxiliar	5	5%		20%
[E.28]Indisponibilidad del personal	Coordinador de Configuración y activos	10			75%
	Analista de Configuración y Activos	10			75%
	Agente de configuración y Activos	10			75%
[A.5] Suplantación de la identidad del usuario	Datos / información	5	75%		75%
	Servicios	5	75%		50%
	Aplicaciones	5	75%		50%
	Redes de Comunicaciones	5	75%		75%
[A.6] Abuso de privilegios de acceso	Datos / información	5	75%	100%	5%
	Servicios	5	50%	50%	75%
	Equipos informáticos	50	75%	75%	75%
	Redes de Comunicaciones	10	75%	50%	75%
[A.7] Uso no previsto	Servicios	5	75%	75%	75%
	Aplicaciones	10	75%	75%	75%

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión de Seguridad (%)**		
			[C]	**[I]**	**[D]**
	Equipos Informáticos	50	75%	75%	75%
	Redes de comunicaciones	10	75%	75%	75%
	Soporte de información	5	20%	20%	20%
	Equipamiento Auxiliar	5	20%	20%	20%
	Instalaciones	10	75%	50%	20%
[A.8]Difusión de software dañino	Aplicaciones	5	50%	75%	75%
[A.11] Acceso no autorizado	Datos / información	10	100%	75%	50%
	Servicios	5	75%	50%	50%
	Aplicaciones	10	75%	50%	50%
	Equipos informáticos	10	75%	20 %	75%
	Redes de Comunicaciones	10	75%	20%	75%
	Soporte de información	5	20%	20%	20%
	Equipamiento Auxiliar	5	5%	5%	5%
	Instalaciones	5	75%	20%	20%
A.13] Repudio	Servicios	5		50%	
[A.14] Interceptación de información (escucha pasiva)	Redes de comunicaciones	5	75%		
A.15] Modificación deliberada de la información	Datos / información	5		75%	
	Servicios	5		75%	
	Aplicaciones	5		75%	
[A.18] Destrucción de información	Datos / información	5			100%
	Servicios	5			100%
	Aplicaciones	5			100%
	Soporte de la información	5			75%
[A.19] Divulgación de información	Datos / información	10	100%		
	Soporte de la información	5			
[A.22] Manipulación de programas	Aplicaciones	10	100%	100%	100%
[A.23] Manipulación de los equipos	Equipos informáticos	50	75%		100%
	Soporte de la información	5	20%		20%
	Equipamiento Auxiliar	5	5%		5%
[A.24] Denegación de servicio	Equipos informáticos	5			75%
	Servicios	5			75%
	Redes de comunicaciones	5			75%

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión de Seguridad (%)**		
			[C]	**[I]**	**[D]**
[A.25] Robo	Equipos informáticos	5	75%		100%
	Equipamiento Auxiliar	5	75%		20%
[A.26] Ataque destructivo	Soporte de la información	5	75%		20%
	Equipos informáticos	5			100%
	Equipamiento Auxiliar	5			50%
	Instalaciones	5			50%
A.28] Indisponibilidad del Personal	Personal	5			75%
[A.29] Extorsión	Personal	5	75%	75%	75%
[A.30] Ingeniería Social	Personal	5	75%	75%	75%

14. Paso 3: Salvaguardas.

Una vez culminado el inventario de activos y haber identificado las amenazas y vulnerabilidades, se definirán las salvaguardas que son procedimientos tecnológicos que reduce el riesgo, de acuerdo a los activos que se van proteger, para esta investigación se tendrá en cuenta las salvaguardas definidas en MAGERIT.

14.1. Tipos de Salvaguardas

Para clasificar los tipos de salvaguardas, se basó en lo indicado en la metodología MAGERIT, tal como se detalla en la siguiente tabla.

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

14.2. Salvaguardas de Activos esenciales

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
[vr]	Datos vitales	[I_Activos_TI]	Información de Activos de TI (base de datos y registro de altas y bajas)	Preventivas (PR)	Políticas de Altas y Bajas de un Activo Informático
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos
		[I_Licencias]	Información de Licencias	Preventivas (PR)	Políticas de Altas y Bajas de un Activo Informático
				Recuperación (RC)	Respaldo de Seguridad de los archivos de licencias – uno por semana
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos
[classified]	Datos clasificados	[I_S_Licenciado]	Instalador software Licenciado	Preventivas (PR)	Políticas de Altas y Bajas de un Activo Informático
				Recuperación (RC)	Respaldo de Seguridad de los archivos de licencias – uno por semana
				Concienciación (AW)	Charlas informativas para el

					personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos
		[D_Historicos]	Información Histórica de activos de TI	Preventivas (PR)	Políticas de Altas y Bajas de un Activo Informático
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos

14.3. Salvaguardas de Datos / Información.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
[Files]	Ficheros	[I_Activos_TI]	Archivo de Activos de TI	Preventivas (PR)	Políticas de Seguridad Activo Informático
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos

		[A_Informes y Licencias]	Archivos de Informes y Licencias adquiridas	Preventivas (PR)	Políticas de Seguridad Activo Informático
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos
[backup]	Copia de Respaldo	[A_copias de Seguridad]	Archivos de copias de seguridad de la información	Preventivas (PR)	Políticas de Seguridad Activo Informático
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos
[conf]	Datos de configuración	[D_configuración_ PC]	Datos de configuración de computadoras personales	Preventivas (PR)	Políticas de Altas y Bajas de un Activo Informático
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos

[int]	Datos de gestión interna	[D_GestiónActivos]	Datos de Gestión de Activos	Preventivas (PR)	Políticas de Altas y Bajas de un Activo Informático
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos
[password]	Credenciales	[D_credenciales]	Credenciales por usuario	Preventivas (PR)	Políticas de prohibiciones y restricciones de los activos de información
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos

14.4. Salvaguardas de Servicios.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
[ext]	A usuarios externos (sedes descentralizadas)	[S_U_Externo]	Servicios prestados a usuarios externos de sede descentralizadas (DRE y UGEL)	Preventivas (PR)	Políticas del uso de servicio a los sistemas de información interinstitucionales
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI

				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
[int]	Interno (a usuarios propios del MINEDU)	[S_U_Interno]	Servicios prestados a los trabajadores propios del MINEDU	Preventivas (PR)	Políticas del uso de servicio a los sistemas de información interinstitucionales
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
[int]	Interno (a usuarios propios del MINEDU)	[S_Telefonia_Movil]	Servicios de telefonía móvil prestado a los trabajadores propios del MINUEDU	Preventivas (PR)	Políticas del uso de servicio a los sistemas de información interinstitucionales
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la institución y el lugar de donde esté ingresando, considerando el desempeño.	Preventivas (PR)	Políticas de prohibiciones y restricciones de los activos de información
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
				Eliminatorias (EL)	Gestión de accesos

14.5. Salvaguardas de Software – Aplicaciones informáticas.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
[Office]	Ofimática	[Office]	Office 2013	Preventivas (PR)	Políticas de Sistemas de Información y/o Aplicaciones
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Monitorización (Mn)	Registro de instalación y activación
				Eliminatorias (EL)	Gestión de accesos
[os]	Sistema Operativo	[OS_Win8.1]	Sistema Operativo Windows 8, en su versión profesional con actualizaciones automáticas activadas	Preventivas (PR)	Políticas de Sistemas de Información y/o Aplicaciones
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Monitorización (Mn)	Registro de instalación y activación
				Eliminatorias (EL)	Gestión de accesos
[av]	Antivirus	[Antivirus]	Sophos original con actualizaciones automáticas.	Preventivas (PR)	Políticas de Gestión de Privilegios
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Monitorización (Mn)	Registro de instalación y activación
				Eliminatorias (EL)	Gestión de accesos

14.6. Salvaguardas de Equipos informáticos.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
[host]	Grandes Equipos (Servidor de base de datos)	[S_Database]	Servidor de Base de Datos	Preventivas (PR)	Políticas de prohibiciones y restricciones de los activos de información
				Correctivas(CR)	Registro de incidencias
				Minimización (IM)	Suspensión de los servicios DB en caso de ataque
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Monitorización (Mn)	Registro de acceso y descarga de archivos
				Eliminatorias (EL)	Eliminación de cuentas que no cuenten con contraseña
		[S_DML]	Servidor de Biblioteca de Medios Definidos	Preventivas (PR)	Políticas de prohibiciones y restricciones de los activos de información
				Correctivas(CR)	Registro de incidencias
				Minimización (IM)	Suspensión de los servicios DB en caso de ataque
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Monitorización (Mn)	Registro de acceso y descarga de archivos
[mid]	Equipos Medios (Equipos de trabajo conectados a través de red física)	[PC_funcionarios]	Computadora personal de Escritorio	Preventivas (PR)	Lineamientos para el acceso y uso adecuado de los recursos informáticos
				Concienciación (AW)	Charlas informativas para el

					personal sobre la información de los activos de TI
				Detección (DC)	Activación de firewall y antivirus.
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Correctivas(CR)	Registro de incidencias
				Eliminatorias (EL)	Eliminación de cuentas que no cuenten con contraseña
[pc]	Equipos que son fáciles de transportar	[PC_portatiles]	Computadora personal portátil	Preventivas (PR)	Lineamientos para el acceso y uso adecuado de los recursos informáticos
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Detección (DC)	Activación de firewall y antivirus.
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Correctivas(CR)	Registro de incidencias
				Eliminatorias (EL)	Eliminación de cuentas que no cuenten con contraseña
[print]	Equipos de Impresión	[E_impresoras]	Impresoras	Preventivas (PR)	Lineamientos para el acceso y uso adecuado de los recursos informáticos
				Correctivas(CR)	Registro de incidencias

14.7. Salvaguardias de Redes de comunicaciones.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo al área	Tipo de Protección	Des. Salvaguarda
[pstn]	Red Telefónica	[R_telefónica]	Red telefónica	Preventivas (PR)	Políticas de Gestión de Privilegios
				Correctivas(CR)	Registro de incidencias

				Minimización (IM)	Detención del servicio en caso de ataque
[wifi]	Red inalámbrica	[R_wifi]	Red inalámbrica	Preventivas (PR)	Políticas de Gestión de Privilegios
				Correctivas(CR)	Registro de incidencias
				Minimización (IM)	Detención del servicio en caso de ataque
[LAN]	Red local	[R_Local]	Red local	Preventivas (PR)	Políticas de Gestión de Privilegios
				Correctivas(CR)	Registro de incidencias
				Minimización (IM)	Detención del servicio en caso de ataque
[Internet]	Internet	[Internet]	Internet	Preventivas (PR)	Políticas de Gestión de Privilegios
				Correctivas(CR)	Registro de incidencias
				Minimización (IM)	Detención del servicio en caso de ataque

14.8. Salvaguardas de Soporte de Información _ almacenamiento electrónico.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[san]	Almacenamiento en Red	[A_UR]	Almacenamiento en Red	Preventivas (PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro	Preventivas (PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Charlas informativas para el personal sobre

					la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001

14.9. Salvaguardas de Soporte de Información _ almacenamiento no electrónico.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[printed]	Material impreso	C_ Documentación_ Activos_TI	Carpetas con la documentación de cada alta y baja (ctm, orden, propuestas de postor, orden compra guía de remisión evaluación técnica)	Preventivas (PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
		C_Reporteseinformes	Carpetas de reporte e informes impresos de atenciones por garantía.	Preventivas (PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
		C_fichasdemovimientos	Carpetas con ficha de movimientos de los activo informáticos	Preventivas (PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Charlas informativas para el personal sobre la información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001

14.10. Salvaguardas de Equipamiento Auxiliar.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[printed]	Sistema de alimentación interrumpida	U_Computadores	UPS computadora personal de escritorio	Preventivas (PR)	Lineamientos para el acceso y uso adecuado de los recursos informáticos
				Concienciación (AW)	Charlas informativas para el personal sobre el acceso y uso adecuado de los recursos informáticos
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales(papel, sobres, carpetas, etc)	Preventivas (PR)	Lineamientos para el acceso y uso adecuado de los recursos informáticos
				Concienciación (AW)	Charlas informativas para el personal sobre el acceso y uso adecuado de los recursos informáticos
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
[Fumiture]	Mobiliario	M_Mobiliario	Mobiliario(Módulos, escritorios, archivadores, armariós, etc)	Preventivas (PR)	Lineamientos para el acceso y uso adecuado de los recursos informáticos
				Concienciación (AW)	Charlas informativas para el personal sobre el acceso y uso adecuado de los recursos informáticos
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001

14.11. Salvaguardias de Instalaciones.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[building]	Edificio	E_empresa	Instalación de la Sede Centromin	Disuasión (DR)	Personal de Seguridad
				Detección(DC)	Sistema de detección de Incendios

14.12. Salvaguardas Cualitativa de Personal.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[ui]	Usuarios internos	C_CYA	Coordinador de Configuración y activos	Concienciación (AW)	Charlas, Curso, entrenamiento informativas sobre la seguridad de información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
		A_CYA	Analista de Configuración y Activos	Concienciación (AW)	Charlas, Curso, entrenamiento informativas sobre la seguridad de información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001
		Ag_CYA	Agente de configuración y Activos	Concienciación (AW)	Charlas, Curso, entrenamiento informativas sobre la seguridad de información de los activos de TI
				Administrativas (AD)	Puesta en marcha de la NTP-ISO 27001

15. Métricas

- Número de Riesgos a los sistemas de información.
- Número de Salvaguardas para los activos de TI.
- Número de Amenazas a los sistemas de información.
- Número de conformidades de accesos.

ANEXOS:

Anexo 1: Resolución Ministerial del Uso obligatorio de la NTP ISO/IEC 27001 para las instituciones públicas del Estado Peruano

ANEXO 2

RELACIÓN DE REPRESENTANTES DEL GOBIERNO NACIONAL ANTE COMISIÓN INTERGUBERNAMENTAL DEL SECTOR AGRICULTURA Y RIEGO, CONFORMADA EN EL MARCO DEL DECRETO SUPREMO Nº 047-2009-PCM

	CARGO	DEPENDENCIA / INSTITUCIÓN	CARGO
1	Viceministro (a) de Política Agrarias	Despacho Viceministerial	Presidente Comisión Intergubernamental
2	Director (a) de la Oficina General de Planeamiento	Oficina General de Planeamiento y Presupuesto	Miembro
3	Profesional		Miembro Alterno
4	Profesional	Oficina General de Asesoría Jurídica	Miembro
5	Profesional	Oficina General de Administración	Miembro
6	Profesional	Oficina General de Gestión de Recursos Humanos	Miembro
7	Director (a) General de Articulación Intergubernamental	Dirección General de Articulación Intergubernamental	Miembro
8	Director (a) de Gestión Descentralizada		Miembro
9	Director de Seguimiento y Evaluación de Políticas (a)	Dirección General de Seguimiento y Evaluación de Políticas	Miembro
10	Director (a) de Estadística Agraria		Miembro Alterno
11	Director (a) General de Políticas Agrarias	Dirección General de Políticas Agrarias	Miembro
12	Director (a) de Políticas y Normatividad Agraria		Miembro
13	Profesional	Dirección General de Negocios Agrarios	Miembro
14	Profesional		Miembro Alterno
15	Profesional	Dirección General de Asuntos Ambientales Agrarios	Miembro
16	Profesional	Dirección General de Infraestructura Agraria y Riego	Miembro
17	Profesional	Servicio Nacional Forestal y de Fauna Silvestre	Miembro
18	Profesional		Miembro
19	Profesional	Programa de Desarrollo Productivo Agrario Rural - AGRORURAL	Miembro
20	Profesional		Miembro Alterno
21	Jefe (a) del Programa	Programa de Compensaciones para la Competitividad - AGROIDEAS	Miembro
22	Jefe (a) de la Unidad de Planificación, Seguimiento y Evaluación		Miembro
23	Director (a) de Gestión del Riego	Programa Sub Sectorial de Irrigaciones (PSI)	Miembro
24	Profesional		Miembro Alterno
25	Director (a) de la Unidad de Estudios y Cooperación de la Oficina de Planificación y Desarrollo Institucional	Servicio Nacional de Sanidad Agraria (SENASA)	Miembro
26	Profesional		Miembro
27	Director (a) General de la Oficina de Planeamiento y Presupuesto	Instituto Nacional de Innovación Agraria (INIA)	Miembro
28	Profesional		Miembro Alterno
29	Director (a) de Conservación y Planeamiento de Recursos Hídricos	Autoridad Nacional del Agua (ANA)	Miembro

1332846-1

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM

Lima, 8 de enero de 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008;

Que, la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", aprobada mediante Resolución Nº 42-2008/INDECOPI-CNB, por la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.2ª Edición" aprobada por Resolución Nº 129-2014/DNB-INDECOPI;

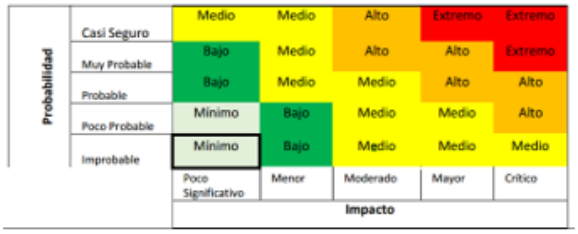
Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo Nº 063-2007-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), siendo ésta la encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo Nº 066-2011-PCM, establece en su Objetivo Nº 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia Nº 4, la implementación de mecanismos para mejorar la seguridad de la información, la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo Nº 081-2013-PCM, prevé determinados Lineamientos Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema

Anexo 2: ficha de revisión de hallazgos de vulnerabilidades

PERÚ | Ministerio de Educación | Secretaría de Planificación Estratégica | Oficina de de Tecnologías de la Información y Comunicación | Unidad de Sistemas de Información

	REPORTE DE HALLAZGOS	
	ESPECIALISTA DE CYA	
	FECHA Y HORA DE REVISIÓN	
	NOMBRE DEL HALLAZGO	
	PLATAFORMA	
	DESCRIPCIÓN DEL HALLAZGO	
SEGURIDAD	**ANALISIS DE RIESGOS**	
	DEPENDENCIAS	
	CONEXIONES A INTERNET	**Acción** / **Proceso** / **Destino** / **Comentario**
	ANALISIS	
	RECOMENDACIÓN	

Formato V. 1 | Elaboración Propia | Página 1

Anexo 3: Resolución Ministerial N° 129-2012-PCM de ONGEI. Implementación Incremental de la Norma Técnica Peruana ISO/IEC 27001:2008

PERÚ | Presidencia del Consejo de Ministros | Oficina Nacional de Gobierno Electrónico e Informática - ONGEI

Implementación incremental de NTP-ISO/IEC 27001:2008

Resolución Ministerial N° 129-2012-PCM

FASE	Nombre	Objetivo	Actividades Principales	Plazo máximo por fase
I	ORGANIZACIÓN	Desarrollar las actividades principales para la dirección e inicio de la implantación del SGSI.	* Obtener el apoyo institucional * Determinar el alcance del Sistema de Gestión de Seguridad de la Información * Determinar la declaración de Política de Seguridad de la Información y objetivos * Desarrollar documentos necesarios para la Fase II * Determinar criterios para la evaluación y aceptación de riesgos	Hasta 3 meses
II	PLANIFICACIÓN	Desarrollar las actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo.	* Realizar evaluación de Riesgos * Conducir un análisis entre los riesgos identificados y las medidas correctivas existentes * Desarrollar un plan de tratamiento de riesgos * Desarrollar documentos necesarios para la Fase III * Desarrolla la declaración de Aplicabilidad	Hasta 4 meses
III	DESPLIEGUE	Desplegar las actividades de implementación del SGSI	* Elaborar el plan de trabajo priorizado * Desarrollar documentos y registros necesarios * Implementar los controles seleccionados	Hasta 12 meses
IV	REVISIÓN	Realizar actividades de revisión del SGSI evidenciando el cumplimiento de los requisitos de la norma	* Monitorear el desempeño del SGSI * Fortalecer la gestión de incidentes * Desarrollar documentos y registros necesarios * Desarrollar las actividades para evidenciar la mejora continua	Hasta 4 meses
V	CONSOLIDACIÓN	Auditar e implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la norma.	* Auditar internamente el SGSI * Implementar las acciones correctivas * Implementar las acciones preventivas pertinentes * Desarrollar, corregir y mejorar documentación nueva o existente	Hasta 4 meses

FASE OPCIONAL:

VI	CERTIFICACIÓN		* Iniciar el proceso de certificación internacional en ISO/IEC 27001:2005 y obtener la certificación	No Aplica

ANEXO 05: Implementación de la NTP ISO/IEC 27001 - Políticas de Control de Accesos

POLÍTICAS PARA EL CONTROL DE ACCESO

1. Introducción

El presente documento muestra las políticas relacionadas al control de acceso relacionado al plan de la implementación de la Norma Técnica Peruana ISO/IEC 27001 en al área de Configuración y Activos. Para ello, identifica a las partes involucradas, define la interrelación entre actividades, especifica la relación de políticas para salvaguardar la Seguridad de Información del área en mención. Asimismo, se declaran los criterios de control, que conducirán la oportuna acción de los recursos y herramientas en el análisis.

1.1. Objetivo

Suministrar la documentación de las políticas de control de accesos elaborada por el área de Configuración y Activos de la OTIC. Este orientará el alcance, las actividades y los tiempos, que facilitarán el detalle necesario para comprender la finalidad del documento.

2. Alcance

El presente procedimiento se aplicará para las actividades del área de Configuración y Activos de la OTIC del MINEDU.

3. Marco Normativo

- R.S.M. N° 246-2007-PCM Aprueban uso de la Norma Técnica Peruana “NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición” en todas las entidades integrantes del Sistema Nacional de la Informática.

- R.S.G. N° 710-2015 - Directiva 003–2015–MINEDU/SPE-OTIC "Directiva para el Acceso y Uso Adecuado de los Recursos Informáticos en el Ministerio de Educación" y "Directiva para la Administración de los Recursos Informáticos del Ministerio de Educación".
- R.S.G. N°908-2015-MINEDU Directiva N°006-2015-MINEDU/SPE-OPEP-UNOME denominada “Metodología para la gestión por procesos en el Ministerio de Educación”
- R.S.G. N°908-2015-MINEDU Directiva N°007-2015-MINEDU/SPE-OPEP-UNOME denominada “Elaboración, Aprobación y Actualización de los Manuales de Procedimientos (MAPRO) del Ministerio de Educación”
- D.S. N° 109-2012-PCM, aprueba la “Estrategia de Modernización de la Gestión Pública”.
- D.S. N° 004-2013-PCM, “Política Nacional de Modernización de la Gestión Pública”.

4. Definiciones, siglas y abreviaturas

Se definen los términos empleados en el documento para comprensión del mismo.

- **MINEDU:** Ministerio de Educación
- **TI:** Tecnologías de la Información
- **OTIC:** Oficina de Tecnologías de la Información y Comunicación
- **GTI:** Gestión de Tecnologías de Información
- **NTP:** Norma Técnica Peruana
- **MAGERIT:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

5. Organización

Para la realización del presente análisis se requiere establecer el organigrama e identificar las partes involucradas que actuaran en la realización de las actividades y tratamiento de la información.

5.1. Organigrama

Para la realización del presente análisis se establece el siguiente organigrama funcional.

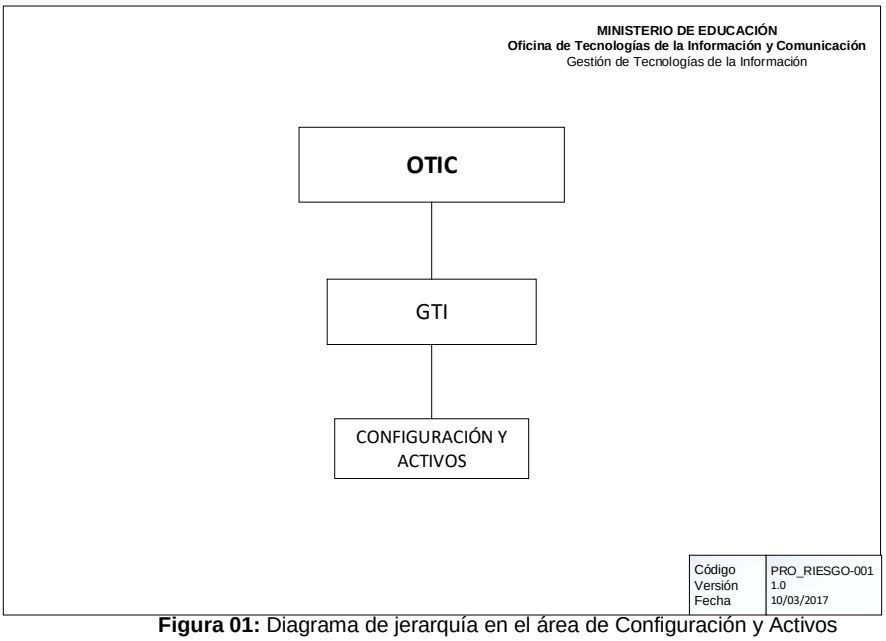


Figura 01: Diagrama de jerarquía en el área de Configuración y Activos

6. Partes involucradas

Para la realización del presente documento se establecen los siguientes roles.

Tabla 1.

Estructura de los roles y responsabilidades

ROL	FUNCIÓN	EQUIPO DE TRABAJO	UNIDAD
Coordinador de Análisis	Responsable de velar por la correcta realización del análisis, medir el rendimiento funcional, y aportar las mejoras al mismo.	Configuración y Activos	GTI
Responsable de Configuración de Activos	Responsable de velar por la disponibilidad de información requerida sobre Elementos de Configuración (CI's) y de brindar información técnica, bajo un modelo lógico que contiene los componentes de la infraestructura de TI y sus respectiva correlación.	Configuración y Activos	GTI
Analista de Configuración y Activos	Responsable de registrar y clasificar las peticiones e incidencias y llevar a cabo los esfuerzos inmediatos para su respectiva restauración o atención de los equipos informáticos del MINEDU.	Configuración y Activos	GTI

ROL	FUNCIÓN	EQUIPO DE TRABAJO	UNIDAD
Coordinador de Análisis	Responsable de velar por la correcta realización del análisis, medir el rendimiento funcional, y aportar las mejoras al mismo.	Configuración y Activos	GTI
Operador de Configuración de Activos	Responsable de ejecutar la actualización de los correlativos de configuración de los equipos informáticos del MINEDU.	Configuración y Activos	GTI

7. Diagrama de actores

Para la realización del presente procedimiento se establecen los siguientes actores.

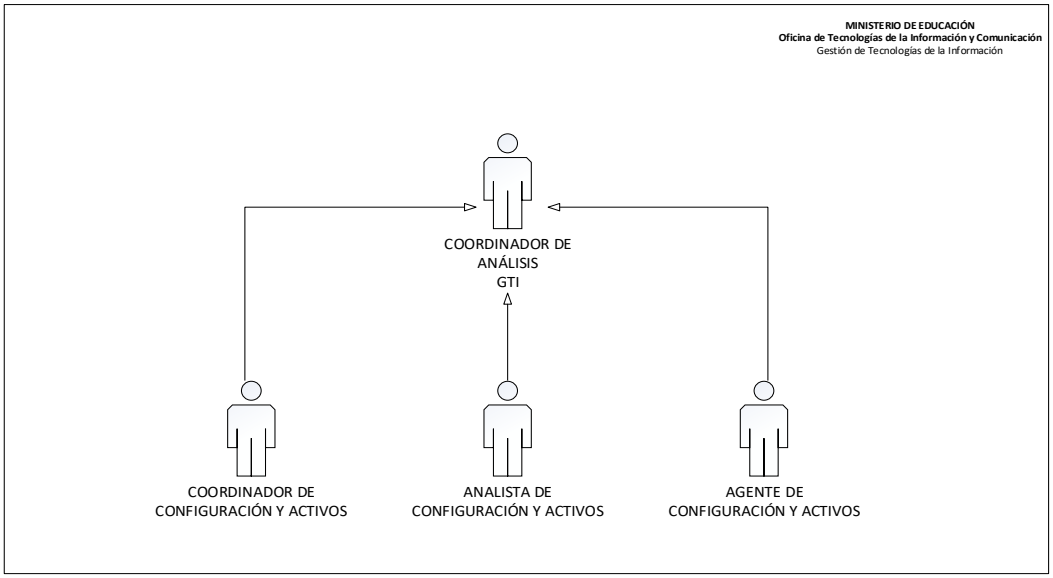


Figura 02: Estructura orgánica de las partes involucradas

8. Factores de control para la realización del procedimiento

DESCRIPCIÓN	FUENTE
• Documento y/o guía de información necesaria para las políticas de control de acceso	BD de políticas propuestas

9. Flujos de entrada

- Formato de Políticas de Control de Acceso

10. Flujos de salida

- Acta de conformidad de políticas firmada

11. Políticas

Las presentes políticas son de uso obligatorio para todo el personal del área de Configuración y Activos y a todo aquel que se le haya asignado un o varios servicios que se encuentran dentro del área mencionada. Así mismo, deberá firmar el acuerdo de confidencialidad y el acta de solicitud de accesos provistos en el anexo 01.

- Políticas del Uso del Servicio de Acceso a la Red de Datos.
- Políticas del Uso del Servicio de la Base de Datos.

11.1. Políticas del Uso del Servicio de Acceso a la Red de Datos

11.1.1. Política de Operatividad

Se describe la forma como operará el servicio de acceso a la red de datos, siendo este el principal medio para el acceso a los demás servicios y recursos de red brindado por área de Configuración y Activos.

- Todos los usuarios deberán contar con un nombre de usuario de red la misma que será única para su identificación correspondiente.
- Los usuarios que tengan derechos para el acceso a la red deberán estar sujetos a la norma de seguridad basado a la Norma Técnica Peruana ISO/IEC 27001 según dispuesto por la R.S.M. N° 246-2007-PCM.
- Los usuarios están obligados a cambiar la contraseña, cuando se le asigne por primera vez una cuenta y contraseña de acceso red.
- El usuario es responsable de la confidencialidad de la contraseña de red y de los cambios hechos por el mismo usuario.
- Cualquier información vertida a la red de datos del área de Configuración y Activos a través de la cuenta de usuario de red, será responsabilidad del usuario.
- El usuario que ingrese a la red de datos del área de Configuración y Activos y no lo usara durante 10 minutos automáticamente se bloqueara, con la finalidad de que este acceso sea usado por otro usuario.
- Se registrará del usuario, por temas de auditoria:

- Accesos exitosos.
- Intentos de conexión fallidos.
- Operaciones críticas.
- Eliminación de archivos

- Se encuentran obligados los jefes o responsables que solicitaron el acceso a la red de datos del área de Configuración y Activos, a determinados usuarios, que también informen y soliciten las bajas de los mismos, cuando este ha dejado de brindar servicios al MINEDU.
- Todas las cuentas que no tienen una actividad por dos (02) meses serán desactivados, posteriormente eliminada.
- La cuenta se bloqueará con tres intentos fallidos.
- Por disposiciones de seguridad de información la clave deberá cambiarse cada 45.

11.1.2. Políticas de Prohibiciones y Restricciones

En este punto se describen las prohibiciones y restricciones del servicio de red la misma que están afectas todas las Dependencias relacionadas con el área de Configuración y Activos.

- Utilizar los servicios de red de datos del área de Configuración y Activos para juegos a través del servicio de Internet o Intranet.
- La suplantación o uso no autorizado de la cuenta de otra persona serán considerados como falta grave.
- No hacer un uso racional, eficiente y considerado de los recursos disponibles de espacio en disco, acumulando material no relacionado con el aspecto institucional, software no autorizado o documentos que no corresponda a las actividades encomendadas.
- Intentar apoderarse de claves de acceso de otros usuarios, acceder y/o modificar archivos de otro usuario, y en especial los

pertenecientes a las bases de datos de los activos de TI del área de Configuración y Activos.

- Decodificar el tráfico de la red o cualquier intento de obtención de información que se transmita a través de la misma.
- Está terminantemente prohibido usar cualquier herramienta o código de red para escanear la red de datos del área de Configuración y Activos.
- Un usuario no debe de compartir su contraseña con ningún otro personal, ya que esta es personal e intransferible
- El usuario no deberá ingresar a otro equipo que no sea el asignado, porque podría ser afectada su información.
- El usuario no deberá insertar cualquier tipo de memoria extraíble a los servidores del área de Configuración y Activos bajo ninguna condición.

11.2. Políticas del Uso del Servicio de la Base de Datos

11.2.1. Política de Operatividad

Se describe la forma como gestionar las solicitudes para Uso del Servicio de la Base de Datos.

- Solo se brindará este servicio a las Dependencias que requieran acceso a la base de datos del área de Configuración y Activos.
- Todas las solicitudes se deben realizar por la mesa de ayuda como un requerimiento.
- Los requerimientos de acceso a la base de datos del área de Configuración y Activos se deben realizar a través de documentos oficiales: oficio o memorándum.
- Todo permiso solicitado va a estar aprobada por el coordinador de Configuración y Activos.
- Toda solicitud de acceso a la base de datos del área de Configuración y Activos va estar firmada por el usuario, indicando su conformidad del servicio.

- Los responsables de Dependencias se encuentran obligados a comunicar de los accesos que no están siendo utilizados para su baja respectiva.
- Es responsabilidad de la asignación y baja de accesos el coordinador de Configuración y Activos.

11.2.2. Políticas de Prohibiciones y Restricciones

En este punto se describen las prohibiciones y restricciones del servicio de acceso a la base de

datos del área de Configuración y Activos.

- No se va a realizar este servicio a Dependencias o instituciones que no tengan relación con el área de Configuración y Activos.
- No se brindará este servicio fuera de las horas laborales establecidas por el MINEDU.
- Está prohibido el ingreso a las instalaciones donde se encuentran los servidores.
- El ingreso permitido y planeado deberá ser registrado con el coordinador del área de Configuración y Activos.

11.3. Política de Alta y Baja de un activo de TI

- Los equipos de cómputo, periféricos y software son considerados activos informáticos o activo de TI.
- Cualquier activo de TI que se adquiera deberá estar debidamente registrada por la Oficina de Tecnologías de la Información OTIC.
- Todos los activos informáticos que ingresan a los recursos informáticos del área de Configuración y Activos, deberán ser registrados como altas antes de su distribución.
- Los equipos de cómputo que ingresarán a los recursos de Configuración y Activos, deberán contar con el sistema operativo original para evitar intromisiones de terceros.

- Para los equipos alquilados que vengan con software, estas deberán tener licencias autorizadas, las mismas que se deberán estar registradas por la OTIC como alta en calidad de alquiler.
- La OTIC es el responsable de emitir el informe técnico de obsolescencia tecnológica sobre un activo Informático.
- Todo activo informático una vez considerado obsoleto, el área usuaria a quien corresponda dicho activo, deberá tramitar el traslado a la Unidad de Abastecimiento, para que se proceda con la baja respectiva.
- Ninguna dependencia del Ministerio de Educación podrá mantener guardados activos informáticos, si fuera el caso, la dependencia usuaria deberá comunicar a la OTIC para las actividades correspondientes.

12. Responsables

- Es responsabilidad de la OTIC de comunicar y hacer cumplir las políticas antes señaladas.
- Es responsabilidad del personal del MINEDU en el cumplimiento de todas las políticas descritas.
- Es responsabilidad de los Jefes de las dependencias de comunicar e informar sobre las incidencias de activos de TI que incurran en el incumplimiento de las políticas.
- El incumplimiento de las políticas descritas estará afecto a sanciones administrativas y legales dependiendo de la grave de la falta.

13. Sanciones

En este punto se indican las sanciones a las que se hará merecedora toda aquella dependencia o usuario que no respete cada punto de la directiva.

- Cualquier acción que contravenga a la presente Directiva, ameritará la aplicación de la sanción correspondiente, de parte del órgano correspondiente.
- Las Dependencias del MINEDU, que por primera y segunda vez se detecte algún tipo de infracción según la directiva correspondiente será amonestado, a través de un documento oficial emitido por la dependencia que corresponda indicando la infracción cometido.

- Las Dependencias del MINEDU, que por tercera vez incurra en falta a la directiva será restringirá el uso del equipo informático, al mismo tiempo comunicando al órgano que corresponda.

14. Métricas

- Número de formatos de solicitud remitidas por el usuario.
- Número de conformidades de accesos.
- Número de quejas, reclamos o sugerencias suscitadas durante la atención de solicitud de acceso.
- Número de accesos a la información brindada por el área de Configuración y Activos.
- Número de accesos no permitidos a la base de datos del área de Configuración y Activos.
- Tiempo de disponibilidad de los recursos brindado por el área de Configuración y Activos.

ANEXOS

Anexo 1: Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD

Mediante la presente, el suscrito declara que yo, [USUARIO] identificado con DNI: [DNI|], declaro que cumplo prestaciones el Ministerio de Educación - MINEDU.

Que, como consecuencia del contrato de locación de servicios suscrito con el MINEDU, me comprometo a lo siguiente:

Primero, Confidencialidad

El USUARIO, está obligado en forma irrevocable ante el MINEDU a no revelar, divulgar o facilitar, bajo cualquier forma, a ninguna persona natural o jurídica y a no utilizar para su propio beneficio de cualquier otra persona, toda la información relacionada con el ejercicio de sus funciones como también las políticas y/o cualquier otra información vinculada con el MINEDU.

El USUARIO se compromete a cumplir con las siguientes pautas y de aceptar lo indicado por las políticas de Control de Accesos suministrada por el área de Configuración y Activos, las mismas que buscan asegurar la confidencialidad de la información y el buen manejo de sus recursos.

1. Se responsabiliza de las acciones que realizan con sus cuentas de acceso
2. Solo podrá utilizarla con fines relacionados al cumplimiento de su prestación según contrato.
3. Debe usar contraseñas seguras y mantenerla en secreto.
4. No puede editar o eliminar archivos, registros o demás recursos solicitados.
5. Difundir información a través de canales no autorizados.
6. No puede compartir su contraseña ya que todo acceso es único e intransferible.

Segundo, Sanción

Queda expresamente convenido que ante todo incumplimiento total o parcial en relación a las obligaciones de confidencialidad asumidas por el presente, el MINEDU podrá actuar contra el suscrito conforme a Ley.

San Borja, [día, mes y año]

_____

El Usuario

Anexo 2: Formato de Solicitud de Acceso

PERÚ | Ministerio de Educación | Secretaría de Planificación Estratégica | Oficina de Tecnologías de la Información y Comunicación

"Año del Buen Servicio al Ciudadano"

FORMATO DE SOLICITUD DE ACCESO A LA RED (S03)

DIA	MES	AÑO

I. SOLICITANTE

Dirección ( ) Oficina ( ) Unidad ( )	

II. RELACION DE USUARIO(S)

N°	Responsable de la Cuenta		DNI	CARGO	ANEXO	Usuario de Red	Tipo de Correo		Regimen Legislativo			Cuenta Genérica	Nombre de Cuenta (Sugerido para Cuentas Genéricas) - Máx 20 caracteres	Crear(C) Actualiza(A) Elimina(E)
	APELLIDOS (Deberá de consignar los 02 Apellidos)	NOMBRES					Correo Interno (*)	Correo Externo (**)	276	728	1057			
1														
2														
3														
4														
5														

(*): Correo Interno: Recibir y enviar correos solo a personas del MINEDU y órganos intermedios.

(**): Correo Externo : Recibir y enviar correos a personas de otras organizaciones externas al MINEDU.

Nota: Para las cuentas genéricas, la firma de los correos electrónicos debe ser el nombre de la misma cuenta y de la oficina que corresponde, lo cual será configurado por personal de OTIC

III. FIRMA Y SELLOS

Firma	Firma
Responsable de la(s) cuenta(s) genérica(s)	Jefe o Director de la Unidad / Oficina /Dirección

ANEXO 06: Articulo Resumen

Implementación de NTP ISO/IEC 27001 para la Seguridad de Información

Implementation of NTP ISO / IEC 27001 for Information Security

Hugo Olaza, Ministerio de Educación

Resumen

La presente investigación tuvo como objetivo determinar el efecto de la implementación de la NTP ISO/IEC 27001 para la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación Sede Centromin.

La investigación realizada fue de tipo aplicada, con un diseño experimental de tipo pre experimental. La población estuvo formada por 4783 registros de la base de datos de activos informáticos, con una muestra de 136, dicho muestreo fue probabilístico y del subtipo aleatorio simple. Se usó como técnica de recopilación de datos la observación. Así mismo, se usó el instrumento ficha de observación. El instrumento de recolección de datos fue validado por medio del juicio de expertos con un resultado de opinión de aplicabilidad y la confiabilidad se realizó mediante la prueba de Wilcoxon, cuyo resultado de las pruebas indican que el Sig. de las muestras es menor que 0.05 (nivel de significancia alfa).

Palabras clave: Seguridad de Información, ISO/IEC 27001, Disponibilidad, Confidencialidad, Integridad.

Abstract

The present investigation aimed to determine the effect of the implementation of the NTP ISO / IEC 27001 for Information Security in the Configuration and Assets area of the Ministry of Education Centromin.

The research was applied type, with an experimental design of pre-experimental type. The population consisted of 4783 records of the database of computer assets, with a sample of 136, this sampling was probabilistic and of the simple random subtype. Observation was used as data collection technique. Likewise, the instrument of observation was used. The data collection instrument was validated by expert judgment with an applicability opinion result and reliability was performed using the Wilcoxon test, whose test result indicates that the Sig of the samples is less than 0.05 (level of alpha significance).

Keywords: Information Security, ISO / IEC 27001, Availability, Confidentiality, Integrity.

Introducción

La presente investigación tiene la finalidad de determinar el efecto de la implementación de la Norma Técnica Peruana ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación Sede Centromin, la cual consta de siete capítulos; el capítulo I plantea una introducción describiendo la realidad problemática, trabajos previos, teorías relacionadas al tema, formulación del problema, justificación del estudio, hipótesis y los objetivos que lo guían, el capítulo II describe y explica el diseño de investigación, las variables de estudio y su operacionalización. Adicionalmente se explica la población, la muestra y se detalla las técnicas e instrumentos para el recojo y procesamiento de la información, la validación y confiabilidad del instrumento, los métodos de análisis de los datos y aspectos éticos de la investigación, el capítulo III se refiere a los resultados de la investigación así como a la comprobación de las hipótesis, en el capítulo IV se presenta y se discuten los resultados de la investigación, en el capítulo V se presentan las conclusiones, en el capítulo VI se presentan las recomendaciones, en el capítulo VII se detallan las referencias bibliográficas utilizadas y finalmente se completa con los anexos.

Antecedentes del problema

Como antecedentes para la presente investigación de tuvo a bien consultar las siguientes tesis:

En la tesis de Carlos Barrantes y Javier Hugo del 2012, con el título “**Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos**” con motivo de optar el título profesional de ingeniero de computación y Sistemas de la ciudad de Lima –Perú, la cual busca reducir los riesgos de los activos de información de los procesos que se encuentran bajo la gerencia de tecnologías de Card Perú que ponen en peligro los recursos servicios y continuidad de los procesos tecnológicos.

En la tesis de Julio Cesar Alcantara Flores del año 2015, con título “**Guía de Implementación de la Seguridad basado en ISO/ IEC 27001, para apoyar la seguridad en los Sistemas de Información de la Comisaria norte P.N.P. en la ciudad de Chiclayo**”, contribuye a mejorar el nivel de seguridad de la información basado en la norma ISO/IEC 27001, para lo cual realiza una investigación aplicada y realizar un estudio bajo la información de gestión y guías de implementación para seguridad de sistemas de información; además manejará el diseño cuasi-experimental.

Estos trabajos de investigación se relacionan con la presente investigación ya que implementan las buenas practicas que la ISO 27001 dispone para la Seguridad de Información basado en la NTP ISO/IEC 27001, lo cual permitirá mejorando la calidad de servicio, así como la gestión de los diferentes activos informáticos y en consecuencia mejorar el prestigio del área.

En la Tabla 11, se aprecia los resultados obtenidos en los indicadores en las tesis antes mencionadas, siendo todos los casos favorables.

Tabla 11. *Resultados obtenidos en los antecedentes consultados.*

Dimensiones	Indicadores	Antecedentes	Signo	Autores
Confidencialidad	Número de información confidencial divulgada	78.50%	+	Barrantes
Integridad	Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción	10.00 %	-	Alcantara
Disponibilidad	Porcentaje de tiempo durante el cual un sistema está disponible para el usuario	4.00 %	+	Alcantara

Revisión de la Literatura

El Ministerio de Educación (MINEDU) ubicada en la ciudad de Lima y fundada en el año 1837, cuenta actualmente con más de 200 colaboradores en la Oficina de Tecnologías de la Información y Comunicación (OTIC), con áreas de trabajo basado bajo el enfoque de ITIL, una de ellas es Configuración y Activos encargada de la correcta administración de los activos TI del MINEDU.

Citando a Gómez y Suárez, se habla que en la actualidad las actividades cotidianas de las empresas y de las distintas Administraciones Públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad.

De ahí la gran importancia que se deberá conceder a todos los aspectos relacionados con la seguridad informática en una organización. (Gómez y Suárez ,2011, p. 226).

El área de Configuración y Activos, busca implementar las buenas practicas que la ISO 27001 dispone para la Seguridad de Información basado en la NTP ISO/IEC 27001, mejorando la calidad de servicio, así como la gestión de los diferentes activos informáticos.

"Según NTP ISO/IEC 27001 (Norma Técnica Peruana) Generalidades. - que ha sido preparada para proporcionar los requisitos para establecer, mantener y mejorar continuidad un sistema de gestión de seguridad de la información." (NTP ISO/IEC 27001, 2007, p.06).

Conociendo el fin con el que fue creado la NTP, se procederá a detallar algunas teorías relacionados al tema

INFORMACIÓN

- Se sostiene que la información "Es un conjunto de datos transformados de forma que constituye a reducir la incertidumbre del futuro y, por tanto, ayuda a la toma de decisiones" (Lapiedra, Devece y Guiral, 2001, p.5).
- Así mismo, se indica que la información "Se obtiene una vez que los hechos se procesan, agregan y presentan de la manera adecuada para que puedan ser útiles a alguien dentro de la organización y procesados presentan un mayor valor que en su estado original" (Gómez y Suarez, 2009, p.34)

CARACTERÍSTICAS DE LA INFORMACIÓN:

Según Gomes y Suarez explican qué:

Para que la información sea útil para la organización este deberá tener los siguientes requisitos:

- Exactitud: la información ha de ser precisa y libre de errores.

- Completitud: la información debe contener todos aquellos hechos que pudieran ser importantes para la persona que la va utilizar.
- Economicidad, el coste en que se debe incurrir para obtener la información debería ser menor que el beneficio proporcionado por esta a la organización.
- Confianza, para dar crédito a la información obtenida, se ha de garantizar tanto la calidad de los datos utilizados, como la de las fuentes información.
- Relevancia, la información ha de ser útil para la toma de decisiones. En este sentido, conviene evitar todos aquellos hechos que sean superfluos o que no aporten ningún valor.
- Nivel de detalle: la información debería presentar el nivel de detalle indicado a la decisión que se destina se debe proporcionar con la presentación y el formato adecuados, para que resulte sencilla y fácil de manejar.
- Oportunidad, se de entregar la información a la persona que corresponde y en el momento en esta la necesidad para poder tomar una decisión.
- Verificabilidad, la información ha de poder ser contratada y comprobada en todo momento. (2011, p. 35).

SISTEMAS DE INFORMACIÓN

Según Purificación Aguilera Lopez:

> Un sistema de información (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos.
>
> Estos elementos son:
>
> - Recursos. Pueden ser físicos, como ordenadores, componentes, periféricos y conexiones, recursos no informáticos; y lógicos, como sistemas operativos y aplicaciones informáticas.
> - Equipo humano. Compuesto por las personas que trabajan para la organización.
> - Información. Conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.
> - Actividades. que se realizan en la organización, relacionadas o no con la informática (2010, p. 8).

Así mismo, para Gomes y Suarez afirma que:

> Los Sistemas de Información han adquirido una dimensión estratégica en las empresas del nuevo milenio y han dejado de ser considerados una simple herramienta para automatizar procesos operativos para convertirse en una pieza clave a tener en cuenta a la hora de formular la estrategia empresarial, para llevar a cabo su implantación y para realizar el control de la gestión.
>
> Los Sistemas de Información no sólo llegan a condicionar la estrategia de la moderna empresa, sino que, además, constituyen el elemento fundamental para poder llevar a cabo una gestión horizontal de la empresa, orientada a procesos y no a funciones, que permita poner el énfasis en la mejora continua de los resultados, con una clara orientación total hacia el cliente.
>
> Éste es un aspecto que hoy en día se considera clave, no ya para alcanzar el éxito, sino para garantizar la supervivencia de la organización en un entorno tan competitivo y exigente como el actual. De ahí que el estudio de los Sistemas de Información, en relativamente poco tiempo, se haya consolidado como una disciplina por sí misma, constituida por una serie de conceptos, herramientas y técnicas utilizadas para llevar a cabo su planificación, análisis, diseño e implantación.
>
> Hay que tener en cuenta que tradicionalmente se ha puesto el énfasis en los aspectos puramente técnicos, enfocando el estudio hacia la descripción de los componentes

tecnológicos del Sistema de Información (las TICs), en detrimento de los aspectos humanos y organizativos, y ello ha provocado una visión sesgada y limitada de toda la problemática asociada al estudio de los Sistemas de Información.

Nuestra experiencia en los campos profesional y académico nos lleva a creer que la planificación y el diseño de los Sistemas de Información en las empresas y organizaciones requieren una perspectiva multidisciplinar que tenga en cuenta los tres aspectos referidos, tal y como se pone de manifiesto en la figura.

Características de un sistema de información:

Si tuviéramos que resumir con una sola frase el principal cometido de un sistema de Información dentro de una organización, podríamos afirmar que éste se encarga de entregar la información oportuna y precisa, con la presentación y el formato adecuados, a la persona que la necesita dentro de la organización para tomar una decisión o realizar alguna operación y justo en el momento en que esta persona necesita disponer de dicha información.

Hoy en día, la información debería ser considerada como uno de los más valiosos recursos de una organización y el Sistema de Información es el encargado de que ésta sea gestionada siguiendo criterios de eficacia y eficiencia (2011, p. 35).

PROCESOS DEL SISTEMA DE INFORMACIÓN

Según Gomes y Suarez nos menciona que:

Un Sistema de Información se puede definir como un conjunto de elementos interrelacionados (entre los que podemos considerar los distintos medios técnicos, las personas y los procedimientos) cuyo cometido es capturar datos, almacenarlos y transformarlos de manera adecuada y distribuir la información obtenida mediante todo este proceso.

Su propósito es apoyar y mejorar las operaciones cotidianas de la empresa, así como satisfacer las necesidades de información para la resolución de problemas y la toma de decisiones por parte de los directivos de la empresa.

Por lo tanto, se trata de un sistema que tiene unos inputs (datos) y unos outputs (información), unos procesos de transformación de los inputs en outputs y unos mecanismos de retroalimentación, como se puede apreciar en la siguiente figura: (2011, p. 42)

CLASIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN

Según Gomes y Suarez considera que existen dos funciones básicas para los sistemas:

- Soporte a las actividades operativas, que da lugar a sistemas de información para actividades más estructuradas (aplicaciones de contabilidad, nómina, pedidos y, en general, lo que se denomina "gestión empresarial") o también sistemas que permiten el manejo de información menos estructurada: aplicaciones ofimáticas, programas técnicos para funciones de ingeniería, etc.
- Soporte a las decisiones y el control de gestión, que puede proporcionarse desde las propias aplicaciones de gestión empresarial (mediante salidas de información existentes) o a través de aplicaciones específicas, como se presentará en este apartado. (2011, p. 46)

SEGURIDAD DE INFORMACIÓN

Para Purificación Aguilera López afirma que:

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Un sistema de información, no obstante, las medidas de seguridad que se le apliquen, no deja de tener siempre un margen de riesgo.

Para afrontar el establecimiento de un sistema de seguridad en necesario conocer:

- Cuáles son los elementos que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización para la que se hace el estudio de riesgos y mediante apreciación directa.
- Cuáles son los peligros que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreos sobre el mismo.
- Cuáles son las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decidir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible (2010, p. 9).

TIPOS DE SEGURIDAD

Según Purificación Aguilera López existen dos tipos de seguridad:

- Activa: Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.
  Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes.
- Pasiva: Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos (2010, p. 10).

PROPIEDADES DE UN SISTEMA DE INFORMACIÓN SEGURO

Según Costas Santos, Jesús manifiesta que:

> Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información. Por tanto, actualmente se considera generalmente aceptado que la seguridad de los datos y la información comprende tres aspectos fundamentales:
>
> - Confidencialidad, es decir, no desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
> - Integridad, permite asegurar que los datos no se han falseado.
> - Disponibilidad, esto es, que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.
>
> Hay que tener en cuenta que tanto las amenazas como los mecanismos para contrarrestarlas, suelen afectar a estas tres características de forma conjunta. Así, por ejemplo, fallos del sistema que hacen que la información no sea accesible pueden llevar consigo una pérdida de integridad.
>
> Generalmente tienen que existir los tres aspectos descritos para que haya seguridad (2010, p. 21, 22).

Así mismo, para Purificación Aguilera López (2010, p,10). Menciona:

> “integridad, confidencialidad y disponibilidad de la información. Cada una de estas propiedades conlleva la implantación de determinados servicios y mecanismos de seguridad”.

Problema

En la actualidad, a nivel mundial, uno de los temas que va tomando cada vez más protagonismo en las empresas es de establecer metodologías o estándares relacionadas con la seguridad de información; se conoce que muchas instituciones, tanto públicas o privadas, tienen la errónea idea de invertir dinero y recursos en infraestructura para sanear las necesidades que la empresa requiere en su momento sin realizar estrategias, provocando grandes pérdidas económicas. Por otro lado, se han desarrollado diferentes metodologías para atender esta necesidad, entre ellas, la más aplicada en las empresas es la norma ISO 27001 que hace referencia al Sistema de Gestión de Seguridad de la Información SGSI, cuyo objetivo es la preservación de la Confidencialidad, Integridad y Disponibilidad de la información.

Para poder evaluar un sistema de información de una empresa pública y/o privada se maneja métodos que permiten gestionar los riesgos dentro de su marco de trabajo, lo cual facilitará mejores tomas de decisiones ya que tendrán en cuenta los riesgos presentados en el uso de las Tecnologías de la Información. Además, esta gestión de riesgo dentro de una empresa, permite implementar las buenas prácticas para la Seguridad de Información diseñando normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable; dando como resultado mejoras en la calidad de los servicios, así como la gestión de los diferentes activos informáticos de la empresa.

Objetivo

Para la seguridad de información de una empresa es necesario analizar y evaluar el tipo de información que maneja, la transferencia de datos que se realiza día a día, determinar los usuarios que tienen alcance al mismo y sobre todo analizar los riesgos a los que están sujetos y así poder diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema seguro confiable; lo cual podremos observar como resultado mejoras en la calidad de los servicios.

Para Costas Santos, Jesús manifiesta que:

> Actualmente se considera generalmente aceptado que la seguridad de los datos y la información comprende tres aspectos fundamentales:
>
> - **Confidencialidad**, es decir, no desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
> - **Integridad**, permite asegurar que los datos no se han falseado.
> - **Disponibilidad**, esto es, que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.
>
> Generalmente **tienen que existir los tres aspectos descritos para que haya seguridad** (2010, p. 21, 22).

Método

La población para esta investigación está constituida por la base de datos de activos del área de Configuración y Activos de la OTIC. La muestra está conformada por 4783 registros de elementos de configuración. El muestreo es del tipo probabilístico y del subtipo aleatorio simple, puesto que el registro de los elementos de configuración permite extraer cierta cantidad de individuos al azar. El diseño de investigación utilizado es Experimental; del tipo pre-experimental.

Resultados

La técnica de recolección de datos es la observación, el instrumento de recolección de datos utilizado fue la ficha de observación; la validez de los instrumentos utilizada fue validez de contenido en base a juicio de expertos. Para este caso se utilizará un análisis descriptivo para lo cual se mostraron los valores hallados como la media aritmética, desviación estándar, mediana, mínimo, máximo y coeficiente de variación.Para realizar el análisis inferencial se utilizó la prueba de normalidad de Kolmogrov-Smirnov y para la demostración de la hipótesis se utilizó la prueba no paramétrica de Wilcoxon.
Al tratarse de un diseño pre-experimental, se buscará comparar los resultados tomados en el Pre-Test y compararlos con los resultados obtenidos, después de la implantación del NTP ISO/IEC 27001 Post-Test.
Se utilizó la Aplicación Computarizada, Software Estadístico SPSS, donde se realizó el análisis estadístico.

Tabla 12. *Resultados de la investigación.*

Dimensiones	Indicadores	Presente Tesis	Signo
Confidencialidad	Número de información confidencial divulgada	72.50%	+
Integridad	Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción	85.00 %	-
Disponibilidad	Porcentaje de tiempo durante el cual un sistema está disponible para el usuario	39.70 %	+

Discusión

Con los resultados obtenidos en la presente investigación se analizó y se comparó el número de información confidencial divulgada, número o porcentaje de acceso y/o cambios no autorización a los datos de la producción y porcentaje de tiempo que se encuentra activo el sistema antes y después de la implementación de la NTP ISO/IEC 27001 para la Seguridad de Información en el área de Configuración y Activos del Ministerio de Educación Sede Centromin.
El número de información confidencial divulgada, en la medición pre-test, alcanzó hasta un promedio de 6.07 de información confidencial divulgada y con la implementación de la NTP ISO/IEC 27001 se redujo a 1.67. Los resultados obtenidos muestran que existe una reducción de 4.4 en la información confidencial divulgada, con lo que se puede afirmar que con la implementación de la NTP se ha logrado una reducción del 72.5% en el número de información confidencial divulgada del Área de Configuración y Activos del Ministerio de Educación – Sede Centromin.
Según la investigación realizada por Barrantes, C. (2012), demostró que el diseño e implementación de un sistema de gestión de seguridad de información, se observa una mejoría de 78.5% al implementar políticas de seguridad, relacionada a la confidencialidad, desplegada a los colaboradores de la gerencia de tecnologías; en relación a los datos obtenidos en el número de información confidencial divulgada se redujo en 72.5% en esta presente investigación.

El número de accesos y/o cambios no autorizados a los datos de producción, en la medición del pre-test, alcanzó hasta un promedio de 10.76 accesos y/o cambios no autorizados y con la implementación de la NTP ISO/IEC 27001 se redujo a 1.55. Los resultados obtenidos muestran que existe una reducción del 9.21 accesos y/o cambios no autorizados con lo que se puede afirmar que con la implementación de la NTP se ha logrado una reducción del 85.4% en el número de accesos y/o cambios no autorizados a los datos de producción del Área de Configuración y Activos del Ministerio de Educación – Sede Centromin.
Según la investigación realizada por Alcantara, J. (2015), demostró que la Implementación de la Seguridad basado en ISO/ IEC 27001, disminuyo los niveles de riesgo, respecto a los activos de información considerados amenazas y vulnerabilidades en un 10%; en relación a los datos obtenidos en el número de accesos y/o cambios no autorizados a los datos de producción se redujo en 85% en esta presente investigación.
El porcentaje de tiempo durante el cual un sistema está disponible para el usuario, en la medición del pre-test, alcanzó hasta un promedio de 0.703 de tiempo donde el sistema se encuentra disponible y con la implementación de la NTP ISO/IEC 27001 se aumentó al 0.982. Los resultados obtenidos muestran que existe un aumento de 0.279 en el tiempo disponible del sistema con lo que se puede afirmar que con la implementación de la NTP se ha logrado una incrementar al 39.7 % al tiempo durante el cual un sistema está disponible del Área de Configuración y Activos del Ministerio de Educación – Sede Centromin.
Según la investigación realizada por Alcantara, J. (2015), demostró que la Implementación de la Seguridad basado en ISO/ IEC 27001, mejoró el proceso utilizado para detectar anomalías en la seguridad de la información al incrementar en un 4%, el cual colabora con el beneficio al momento de requerirse la información en el momento adecuado y exacto para la institución; en relación a los datos obtenidos en el porcentaje de tiempo durante el cual el sistema está disponible para el usuario que se incrementó en 39.7% en esta presente investigación.

Conclusiones

Después de analizar las tres dimensiones como son: número de información confidencial divulgada, número de accesos y/o cambios no autorizados a los datos de producción y porcentaje de tiempo durante el cual un sistema está disponible para el usuario, podemos concluir

1. Se ha determinado que la implementación de la NTP ISO/IEC 27001, mejoró la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, logrando demostrar las hipótesis planteadas con una confidencialidad del 95%, y esto se vio reflejado al incrementar el nivel de seguridad en la misma.

2. Se ha determinado que el número de información confidencial divulgada implementando la NTP ISO/IEC 27001 en la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, sin la NTP fue un promedio de 6.07 de información confidencial y con la implementación de la NTP fue de 1.67 información confidencial, logrando una reducción 4.4 información confidencial, que representa el 72.5% en el número de información confidencial divulgada.

3. Se ha determinado que el número de accesos y/o cambios no autorizados a los datos de producción implementando la NTP ISO/IEC 27001 en la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, sin la NTP fue un promedio de 10.76 de accesos y/o cambios no autorizados y con la implementación de la NTP fue de 1.55 de accesos y/o cambios no autorizados, logrando una reducción 9.21 de accesos y/o cambios no autorizados, que representa el 85.4% en el número de accesos y/o cambios no autorizados a los datos de producción.

4. Se ha determinado que el porcentaje de tiempo durante el cual un sistema está disponible para el usuario, implementando la NTP ISO/IEC 27001 en la seguridad de información en el área de Configuración y Activos del Ministerio de Educación - Sede Centromin, sin la NTP fue un promedio de 0.703 de tiempo y con la implementación de la NTP fue de 0.982, logrando un incremento de 0.279 de tiempo, que representa el 39.7% en el tiempo durante el cual un sistema está disponible.

Recomendaciones

1. Se recomienda realizar un análisis del estado situacional de los recursos informáticos de las demás áreas de Gestión Tecnologías de la Información GTI de la Oficina de Tecnologías de la Información – OTIC, para encontrar debilidades en la Seguridad de la Información, como ya se visto evidenciado en esta tesis realizado en el área de Configuración y Activos.

2. Asimismo, la implementación de la Norma Técnica Peruana ISO/IEC 27001 para optimizar los procesos y recursos informáticos de la OTIC y salvaguardar los activos de TI y evitar la pérdida de información como ha venido ocurriendo hasta la implementación de la norma mencionada en el área de Configuración y Activos.

3. También, se recomienda a la OTIC la capacitación al personal encargado de administración de datos y a especialistas informáticos de la Norma Técnica Peruana ISO/IEC 27001, Así como la concientización sobre la Seguridad de Información. Lo que permita analizar el estado de la Integridad, Disponibilidad y Confidencialidad de sus respectivas áreas y la interrelación segura entre las otras oficinas de la OTIC.

4. Por último, se recomienda a la OTIC establecer como prioridad la certificación internacional de la norma ISO 27001 Foundation, a los especialistas informáticos encargados con la implementación de la misma en sus respectivas áreas, con el fin de priorizar la Seguridad de la Información en las dependencias del MINEDU.Realizar un análisis del estado situacional de los recursos informáticos, para encontrar debilidades en la Seguridad de la Información.

Referencia

- Aguilera, Purificación. 2008. Seguridad Informática. MADRID: Editex, 2010.240pp. ISBN: 978-84-9771-657-4

- Alcántara, Julio. 2015. Guía de Implementación de la Seguridad basado en ISO/IEC 27001, para apoyar la seguridad en los Sistemas de Información de la Comisaría norte P.N.P. en la ciudad de Chiclayo. PERÚ: Universidad Católica Santo Toribio de Mogrovejo, 2015. 157pp

- Barrantes, Carlos y Javier Hugo. 2012. Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos. PERÚ: Universidad de San Martín de Porres, 2012. 330pp.

- Costas, Jesús. 2010. Seguridad Informática. ESPAÑA: RA-MA Editorial, 2010. 308pp. ISBN: 978-84-7897-979-0

- Gomés, Álvaro y Suárez, Carlos. 2011. Sistemas de Información. Herramientas prácticas para la gestión (3ª. ed.) MEXICO: Alfa y Omega Grupo Editor, 2011. 360pp. ISBN: 978-607-7854-45-6

- Lapiedra, Rafael, Devece, Carlos y GUIRAL Joaquin. 2011. Introducción a la gestión de sistemas de información en la empresa. Colección Sapientia. 72pp
  ISBN: 978-84-693-9894-4

- NORMA TECNICA PERUANA. 2014. NTP-ISO/IEC 27001– 2014 – 2da Edición. LIMA. 2014. 45pp.