Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de
Ingeniería de Sistemas e Informática

Trabajo de Investigación

Análisis de los factores de éxito y limitantes para la implementación de la norma técnica peruana Iso NTP/IEC 27001;2014 2A. Edición en la Municipalidad provincial de Huancayo- I trimestre 2018

Isabel Corina Pino Malpica

Huancayo, 2019

Para optar el Grado Académico de Bachiller
en Ingeniería de Sistemas e Informática

AGRADECIMIENTOS

En primer lugar, a Dios, por regalarme el don preciado de la vida, por ser mi fortaleza y protegerme en cada instante.

A mi madre, por ser una madre amorosa, por alentarme y exigirme a dar lo mejor de mí en cada momento.

A mis familiares por sus consejos, palabras de aliento y estar pendientes de que cumpla con mis objetivos.

A la Universidad Continental por creer en sus alumnos y brindar a los mejores docentes y administrativos con calidad profesional y humana.

A mi perro Marlon Toro V por acompañarme en mis largas horas de estudio e inclusive en las amanecidas.

A mis amigos y compañeros de trabajo presentes y pasados, quienes compartieron sus experiencia laborales a modo de enseñanza.

Isabel Corina Pino Malpica

DEDICATORIA

Este proyecto de investigación la dedico a mi adorada madre María Isabel Malpica Solórzano por su sacrificio, esfuerzo, amor y por ser ejemplo de líder en lo profesional y en lo personal.

Isabel Corina Pino Malpica

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La Presidencia de Consejo de Ministros (PCM) emitió un conjunto de normas entre ellas algunas relacionadas a la seguridad de la información, con la cual se dispuso la obligatoriedad de uso de la NTP ISO/IEC 27001:2008 (aprobada con RM Nº 129-2012-PCM del 4 de junio de 2012), posteriormente la Norma Técnica Peruana NTP-ISO /IEC 27001:2014 2da Edición (aprobada con RM N° 004-2016-PCM del 8 de enero de 2016).

Sin embargo, han pasado 6 años desde entonces, y pocas entidades han logrado la implementación total de la norma, es por ello que este trabajo de investigación tiene como objetivo identificar estos factores de éxito o limitantes para la implementación de la norma.

La investigación se desarrolló en la Municipalidad Provincial de Huancayo, para lo cual elabore un check list en base a lo que solicita la norma y verifique la existencia en la Municipalidad durante I trimestre del año 2018, cualquiera fuese el resultado se solicitó información de los factores que permitieron el nivel alcanzado.

Al finalizar la investigación se identificó que la entidad implemento 32% de lo solicitado por la norma, que algunos de los factores de éxito fue el conocimiento, experiencia e interés por parte del funcionario público responsable, y entre los limitantes la falta de procesos, cultura organizacional, presupuesto y capacitaciones.

ABSTRACT

The Presidency of the Council of Ministers (PCM) issued a set of rules, among them some related to information security, with which the compulsory nature of the use of the NTP ISO / IEC 27001: 2008 (approved with RM Nº 129-2012-PCM of June 4, 2012), subsequently the Peruvian Technical Standard NTP-ISO / IEC 27001: 2014 2nd Edition (approved with RM º. 004-2016-PCM of January 8, 2016).

However, 6 years have passed since then, and few entities have achieved full implementation of the standard, which is why this research work aims to identify these success factors or limitations for the implementation of the standard.

The investigation was developed in the Provincial Municipality of Huancayo, for which elaborate a check list based on what the standard requests and verify the existence in the Municipality during I quarter of the year 2018, whatever the result was requested information of the factors that allowed the level reached.

At the end of the investigation it was identified that the entity implemented 32% of what was requested by the norm, that some of the success factors was the knowledge, experience and interest on the part of the responsible public official, and among the constraints the lack of processes, culture organizational, budget and training.

INTRODUCCIÓN

La revolución tecnológica no es ajena para las entidades públicas, por ello en el Perú desde el año 2000 existen intenciones de implementar reformas en el estado para estar a la altura de esta revolución, la primera etapa consistió en asegurar la economía presupuestal y la segunda en establecer un marco normativo. (1 pág. 30 y 31)

Durante esta segunda etapa la Presidencia de Consejo de Ministros (PCM) emitió un conjunto de normas entre ellas algunas relacionadas a la seguridad de la información, con la cual se dispuso la obligatoriedad de uso de la NTP ISO/IEC 27001:2008 (aprobada con RM Nº 129-2012-PCM del 4 de junio de 2012), posteriormente la Norma Técnica Peruana NTP-ISO /IEC 27001:2014 2da Edición (aprobada con RM N° 004-2016-PCM del 8 de enero de 2016).

Si bien esta norma fue publicada por primera vez a mediados del 2012, muy pocas entidades le dieron importancia a la implementación, para el 2016, el escenario fue similar, es por ello que en este proyecto de investigación se identifica y analizar aquellos factores de éxito o limitantes para la implementación de la norma en la Municipalidad Provincial de Huancayo, I trimestre 2018.

La identificación y análisis de estos factores de éxito o limitantes podría permitir a la PCM y entidades públicas a adoptar acciones para imitar los factores de éxito e implementar acciones correctivas para los factores limitantes.

Respecto al contenido del presente trabajo de investigación está sea dividido en cinco capítulos: Capitulo I – Planteamiento del estudio, Capitulo II – Marco Teórico, Capitulo III – Metodología, Capitulo IV – Análisis y diseño de la solución y capitulo IV – Construcción, de igual manera se ha incluido las conclusiones y recomendaciones.

CAPITULO I
PLANTEAMIENTO DEL ESTUDIO

1.1 PLANTEAMIENTO DEL PROBLEMA

Desde el año 2000 el estado peruano consecuente con la revolución tecnológica, viene ejecutando un conjunto de reformas en el estado para implementar el gobierno electrónico, como parte de estas reformas el 27 de julio de 2011 aprobó el Plan de Desarrollo de la Sociedad de la Información - La Agenda Digital 2.0. (1 pág. 43)

Esta agenda contiene objetivos y estrategias, dentro del objetivo de desarrollo del Gobierno Electrónico (objetivo 7), se estableció como 4ta estrategia Implementar mecanismos para mejorar la Seguridad de la Información. (1 pág. 45)

Cabe mencionar que esta reforma se ejecutó por etapas, la primera consistía en asegurar que estas reformas cuenten con la economía necesaria, y la segunda de establecer el marco normativo que permita la implementación y control (1 pág. 30 y 31).

Consecuentemente con la Estrategia señalada y como parte de esta segunda etapa la Oficina Nacional de Gobierno Electrónico (ONGEI) a través de la Presidencia del Consejo de Ministros (PCM) aprobaron la siguiente normativa: (1 pág. 50)

- Mediante Resolución Ministerial Nº 224-2004-PCM del 23 de Julio de 2004 se "Aprobó del uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas

para la gestión de la Seguridad de la Información. 1ª Edición.” la misma que es un compendio de controles que toda entidad debería adoptar, sin embargo, no especifico el tiempo, quizá ese sea el motivo, pero muy pocas entidades de las entidades llegaron a implementarlo, pero si despertó algo de interés en ellas.

- Posteriormente emiten la Resolución Ministerial Nº 246-2007-PCM de 25 de agosto de 2007 con la que resuelven aprobar 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 Informática, y se aprecia los primeros resultados con la Contraloría General de la República la cual implementó su política de seguridad de la información la cual fue aprobada con Resolución de Contraloría Nº 352-2008-CG de 10/09/2008.

- El 21 de julio de 2011 mediante RESOLUCION MINISTERIAL Nº 197-2011-PCM resuelven Establecer fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en 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" en esta indican que tiene plazo hasta el 31 de diciembre de 2012 exigiendo a varias entidades del poder judicial y ejecutivo el cumplimiento en la fecha establecida.

- Con Resolución Ministerial N° 129-2012-PCM de 25 de mayo de 2012 resuelven Aprobar el uso obligatorio de 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" en todas las entidades integrantes del Sistema Nacional de Informática, con esta resolución se indica a las entidades que deberán comenzar con la implementación con esta norma y complementar con los controles de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007, pero no indico plazo.

- Finalmente, con Resolución Ministerial N° 004-2016-PCM de 8 de enero de 2016 resuelven la Aprobación del uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad.

Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", para lo cual le otorgan 2 años a partir de la publicación de esta Resolución.

Sin bien este conjunto de normas son descriptivas y de una manera práctica indican como las entidades públicas (ver tabla 1) pueden implementar las políticas de seguridad de la información, no se evidencia informes del estado peruano en la que señale el nivel de cumplimiento, al realizar las búsquedas en el portal web de diversas entidades públicas, tampoco figuran los avances de implementación.

Tabla 1. Entidades del Estado Peruano

ENTIDADES DEL ESTADO	CANTIDAD
GOBIERNOS REGIONALES	333
MUNICIPALIDADES	1938
ORGANISMOS AUTÓNOMOS	76
PODER EJECUTIVO	560
PODER JUDICIAL	32
PODER LEGISLATIVO	1
Total	**2940**

Entonces, debe existir factores de éxito o limitantes para la implementación, por ello en este trabajo de investigación se ha procedido a analizar estos factores para el cumplimiento de la Norma técnica peruana ISO NTP/IEC 27001:2014 en una entidad del estado, pero desde la entidad pública ejecutora u obligada a implementarla, porque podría factores desde la misma Presidencia Del Consejo De Ministros PCM o de la Oficina Nacional de Gobierno electrónico e Informática (ONGEI) pero estas no se tomaran en cuenta en esta oportunidad.

1.2 FORMULACIÓN DEL PROBLEMA

1.2.1 Problema general

¿Cuáles son los factores relacionados a la implementación de la Norma técnica peruana ISO NTP/IEC 27001:2014 en la Municipalidad Provincial de Huancayo, I trimestre 2018?

Problemas específicos

- ¿Cuál es el nivel de implementación de la Norma técnica peruana ISO NTP/IEC 27001:2014 en la municipalidad provincial de Huancayo, I trimestre 2018?
- ¿Cuáles son los factores positivos que permitieron la implementación de la Norma técnica peruana ISO NTP/IEC 27001:2014 en la municipalidad provincial de Huancayo, I trimestre 2018?
- ¿Cuáles son los factores limitantes para la implementación de la Norma técnica peruana ISO NTP/IEC 27001:2014 en la municipalidad provincial de Huancayo, I trimestre 2018?

1.3 OBJETIVOS

1.3.1 Objetivo general

Analizar los factores relacionados a la implementación de la Norma Técnica Peruana ISO NTP/IEC 27001:2014 en la Municipalidad Provincial de Huancayo, I trimestre 2018

1.3.2 Objetivos específicos

- Identificar el nivel de implementación de la Norma Técnica Peruana ISO NTP/IEC 27001:2014 en la Municipalidad Provincial de Huancayo, , I trimestre 2018
- Identificar los factores que permitieron la implementación de la Norma Técnica Peruana ISO NTP/IEC 27001:2014 en la Municipalidad de Provincial de Huancayo, , I trimestre 2018
- Identificar los factores que limitaron la implementación de la Norma Técnica Peruana ISO NTP/IEC 27001:2014 en la Municipalidad de Provincial de Huancayo, I trimestre 2018

1.4 JUSTIFICACIÓN E IMPORTANCIA

Si el Estado Peruano desea ejecutar las reformas de modernización del estado, debe asegurar la implementación y cumplimiento de las Políticas de Seguridad de la Información, pues como señala Escriba y otros en su libro

“Seguridad Informática” “Uno de los activos más valiosos para cualquier empresa es la información que maneja” (2 pág. 7)

Es preciso entender que la información que maneja una entidad pública es información de todos los ciudadanos, pero en muchos de los casos es confidencial y datos personales sensibles, pues según sea la entidad, manejan información de nuestro estado de salud, estado patrimonial, estado económico, estado jurídico, entre otros, entonces debe limitarse y asegurarse de que las amenazas estén controladas y mitigadas durante su procesamiento.

Algunas amenazas en el Perú según la ONGEI se acrecentado debido a: “Crecimiento exponencial de las redes y usuarios interconectados, Profusión de la BD on-line, Inmadurez de las nuevas tecnologías, Alta disponibilidad de herramientas automatizadas de ataque, Nuevas técnicas de ataques distribuidos y Técnicas de ingeniería social” (3)

Es por ello que la PCM y la ONGEI basándose en el estándar ISO/IEC 27001 emitió la Norma Técnica Peruana ISO/IEC 27001:2014, la cual es conjunto de buenas prácticas, el cual señala actividades para la implementación, control y monitoreo, que permiten cumplir con los principios de la seguridad de la información.

Sin embargo, como se ha mencionado anteriormente muchas entidades no han logrado el objetivo esperado, y al parecer muchas presentan las mismas limitaciones, es por ello que es necesario identificar los factores de éxito o limitantes para la implementación de la Norma Técnica Peruana ISO NTP/IEC 27001:2014 en las entidades públicas.

La identificación de estos factores permitirá a las entidades públicas hacer una réplica de las acciones para cumplir con el objetivo, o pueden adoptar acciones para revertir el problema y lograr el objetivo esperado.

En todo caso, si uno de estos factores no estaría al alcance de la entidad pública, es posible que la Presidencia de Consejos de Ministros, a través de la Oficina de Gobierno Electrónico e Informática pueda evaluar estos factores y

promover los factores de éxito, y en el caso de los factores limitantes, puede evaluar y verificar si se debe cambiar el procedimiento o adoptar otros mecanismos para que las entidades logren sus objetivos.

La culminación de este proyecto de investigación, brindaría un aporte aplicado pues la finalidad es que todas las entidades públicas, logren el objetivo de implementar el sistema de seguridad de la información de forma real, y de esa forma garantizar que la información de todos los ciudadanos peruanos y extranjeros que procesan nuestras entidades públicas, estén a salvo de amenazas y al mismo tiempo aseguren la confidencialidad, disponibilidad e integridad de la información.

1.5 HIPÓTESIS Y DESCRIPCIÓN DE LA VARIABLE

El presente estudio no presenta hipótesis por ser descriptivo y no se intenta pronosticar un hecho un dato. (4)

1.6 VARIABLES

1.6.1 Definición conceptual de la variable

- Nivel de implementación de la Norma técnica peruana ISO NTP/IEC 27001:2014

1.6.2 Definición operacional de la variable

- Factores de éxito
- Factores limitantes

1.7 DELIMITACIONES DE LA INVESTIGACIÓN

Se realizará el análisis de los factores relacionados a la implementación de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la

Información. Requisitos 2a. Edición" en la Municipalidad Provincial de Huancayo, I trimestre del 2018.

Para tal fin se realizará un análisis del cumplimiento normativo, y se identificara los factores de éxito o limitantes según sea el caso que permitieron el logro del objetivo.

1.8 LIMITACIONES DE LA INVESTIGACIÓN

Las principales limitaciones son:

- Es posible que durante o después del desarrollo de esta investigación la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 podría ser modificado o actualizado por la Presidencia de Consejos de Ministros.

- De igual manera es posible que en el transcurso del desarrollo de esta investigación, el Municipio realice cambios en sus controles de seguridad de la información, procedimientos o normativa interna, y al finalizar el presente trabajo el escenario sea otro.

- Es posible que algunos escenarios o procedimientos de la Municipalidad de la Información cambien.

CAPITULO II
MARCO TEÓRICO

2.1 ANTECEDENTES DEL PROBLEMA

2.1.2 Antecedentes Nacionales

Desde el 2000 el estado peruano tiene intenciones de implementar el Gobierno Electrónico de una forma estandarizada y adecuada, por ello ha organizado diferentes reformas por etapas siendo la primera asegurar la economía en las entidades públicas y como segunda etapa establecer un marco normativo que permita el objetivo. (1 pág. 30 y 31)

Estrategia de estado para implementar el Gobierno Electrónico:

Figura 1. Principios de la Seguridad de la Información (5)

La implementación del Gobierno electrónico en las entidades exige que el gobierno implemente también adecuados niveles de seguridad de la información:

Figura 2. Plan de Desarrollo de Gobierno Electrónico (5)

Las estrategias para la implementación de niveles de seguridad en la información garantizan la confidencialidad, disponibilidad e integridad de la información.

INSTITUCIONES	OE1	OE2	OE3	OE4	OE5
Ministerio de Educación	40%	40%	20%	-	-
Ministerio de Salud	22.2%	22.2%	33.4%	22.2%	-
Ministerio de Desarrollo e Inclusión Social	100%	-	-	-	-
Ministerio de Agricultura	33.3%	16.7%	33.3%	16.7%	-
Región Cusco	27%	28%	20%	20.3%	4.7%

Fuente: Elaboración propia

Figura 3. Iniciativas y proyectos que aseguran los principios de la Seguridad de la Información (5)

La ONGEI es el órgano encargado de impulsar y fomenta el uso de las TIC's para la modernización y desarrollo del estado.

Por ello la ONGEI a través de la Presidencia de Consejo de Ministros (PCM) emitieron un conjunto de normas entre ellas algunas relacionadas a la seguridad de la información, con la cual se dispuso la obligatoriedad de uso de la NTP ISO/IEC 27001:2008 (aprobada con RM Nº 129-2012-PCM del 4 de junio de 2012), posteriormente la Norma Técnica Peruana NTP-ISO /IEC 27001:2014 2da Edición (aprobada con RM N° 004-2016-PCM del 8 de enero de 2016), entre que otros no relacionados directamente a la seguridad de la Información.

2.1.3 Antecedentes Internacionales

Respecto a la referencia internacional, no se encontró fuentes que señalen como esta implementado la seguridad de la Información en los países de América, Europa, Asia y Oriente, por ello solo se citara lo que indica el estado peruano respecto a los avances en la implementación del gobierno electrónico:

> *"Respecto a los datos del Perú, se observa claro retroceso, principalmente porque pasamos del puesto 63 de la encuesta del 2010 al puesto 82 en esta última encuesta. Es decir, descendimos 19 puestos. Pero esta tendencia no es distinta a las encuestas pasadas, puesto que, de haber estado en el puesto 53, en los años 2003 y 2004, pasamos al puesto 56, retrocediendo 3 puestos en el 2005 y avanzando un puesto en el 2008. Lo más lamentable es que no hemos avanzado significativamente desde el 2008, donde empieza nuestra tendencia a la baja, donde retrocedemos del puesto 55 al 63 en el 2010."* (5)

2.2 BASES TEÓRICAS

2.2.1. Composición de las Entidades Públicas

Entidad Pública

Es necesario que se entienda el contexto y composición de la entidad pública en el cual se ejecuta la investigación, es por ello que voy a citar lo que indica la PCM con la RM N° 374-2010-PCM de 14 de diciembre de 2001, respecto a Entidad Pública:

> *"Se considera Entidad Pública a toda organización del Estado Peruano, con Personería jurídica de Derecho Público, creada por norma expresa en el que se le confiere mandato a través del cual ejerce funciones dentro del marco de sus competencias y atribuciones, mediante la administración de recursos públicos, para contribuir a la satisfacción de las necesidades y expectativas de la sociedad, y como tal está sujeta al control, fiscalización y rendición de cuentas."* (5)

De acuerdo a la PCM la composición del estado es la siguiente:

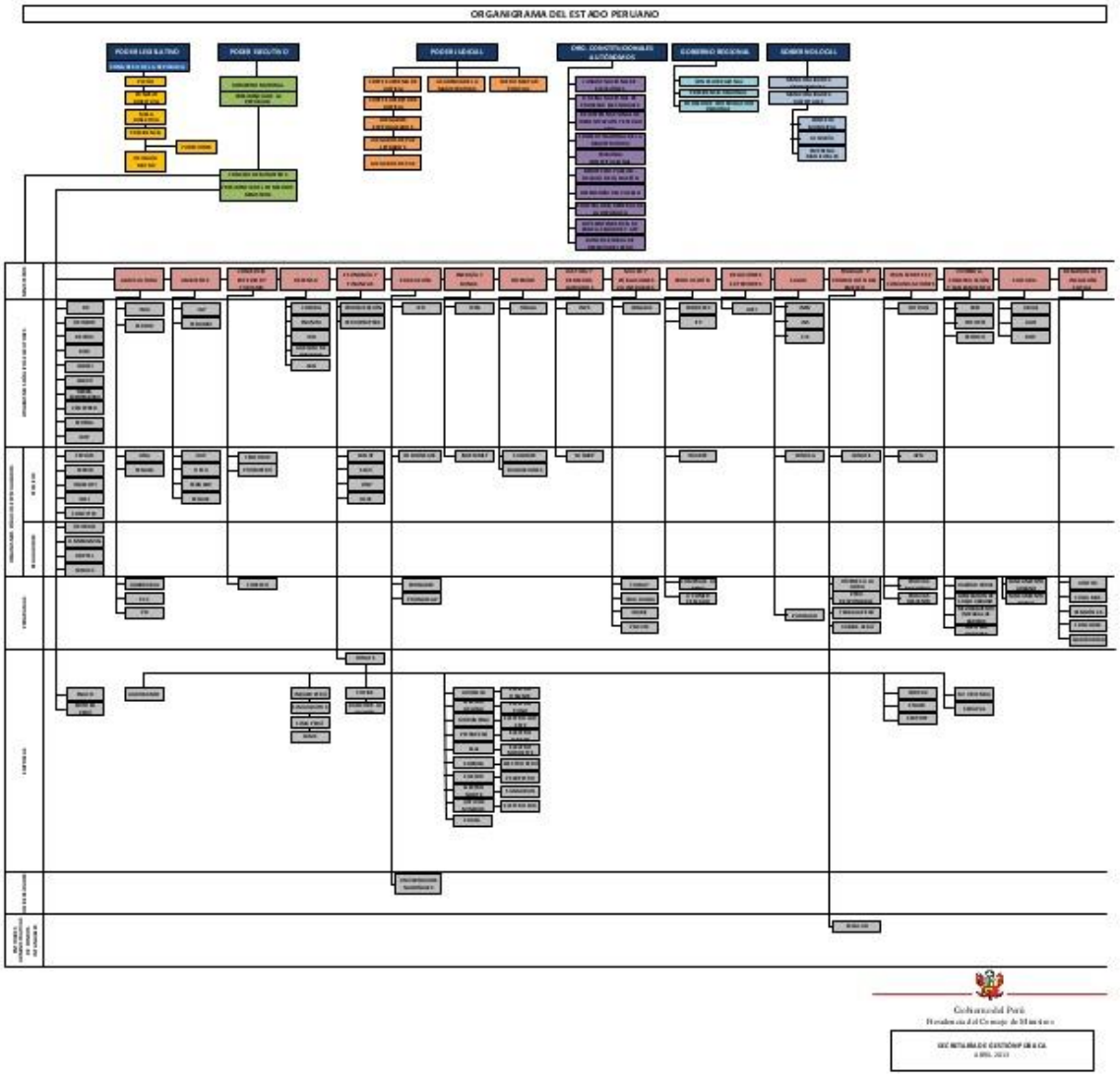


Figura 4. Composición Orgánica del estado peruano

Según la RM N° 374-2010-PCM, reconoce a la Municipalidad Provincial de Huancayo como una entidad pública del estado peruano (5)

La Municipalidad Provincial de Huancayo

La Municipalidad Provincial de Huancayo es un gobierno local, supeditado por la Ley Orgánica de Municipalidades Nº 27972, el cual señala en el artículo 1 lo siguiente:

"ARTÍCULO I.- GOBIERNOS LOCALES Los gobiernos locales son entidades, básicas de la organización territorial del Estado y

canales inmediatos de participación vecinal en los asuntos públicos, que institucionalizan y gestionan con autonomía los intereses propios de las correspondientes colectividades; siendo elementos esenciales del gobierno local, el territorio, la población y la organización. Las municipalidades provinciales y distritales son los órganos de gobierno promotores del desarrollo local, con personería jurídica de derecho público y plena capacidad para el cumplimiento de sus fines." (6)

De conformidad con el artículo 6 de esta ley, el alcalde es la máxima autoridad administrativa, y en el artículo 8 señala que la administración municipal está conformada por funcionarios, servidores, empleados y obreros, por ende, en conjunto son responsables de los servicios que brindan al ciudadano.

La Municipalidad Provincial de Huancayo de conformidad con el Reglamento de Organización y Funciones (ROF) de la Municipalidad Provincial de Huancayo, vigente para el I trimestre 2018, aprobado con ordenanza Municipal Nº 522-MPH/CM del 11 de Julio de 2015, tiene la siguiente composición:

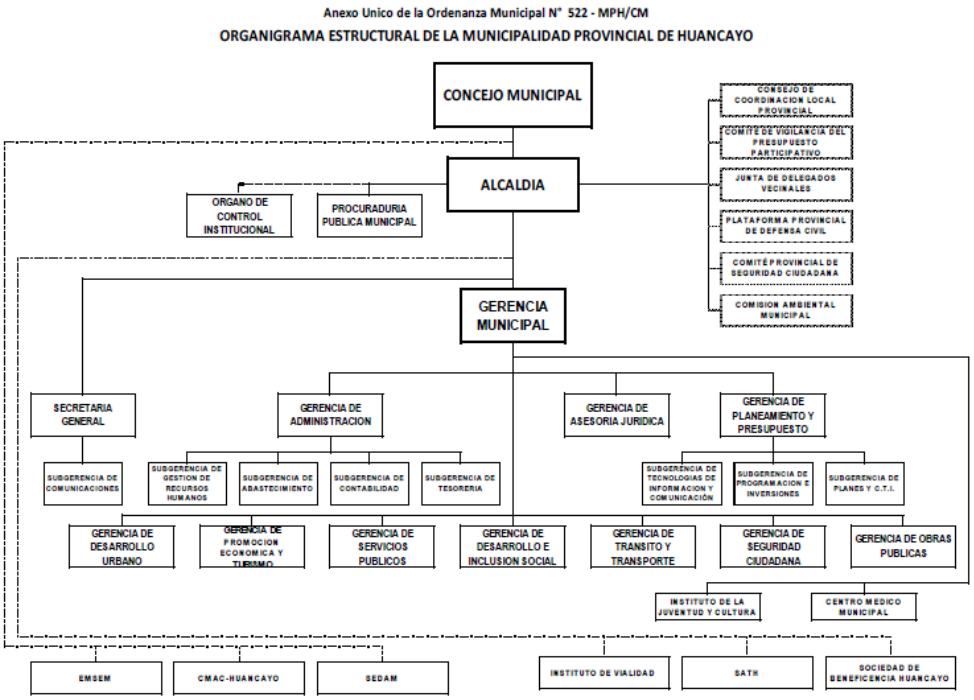


Figura 5. Organigrama de la Municipalidad Provincial de Huancayo

Es preciso señalar diferencias entre los cargos públicos, por ello citaremos lo que indica el Articulo 4 de la Ley 28175 – Ley Marco del Empleo Público respecto a los cargos en las entidades públicas:

"…

1. Funcionario público.- El que desarrolla funciones de preeminencia política, reconocida por norma expresa, que representan al Estado o a un sector de la población, desarrollan políticas del Estado y/o dirigen organismos o entidades públicas. El Funcionario Público puede ser:

a) De elección popular directa y universal o confianza política originaria. (Presidente, Congresistas, alcaldes, etc.)

b) De nombramiento y remoción regulados. (Jefes de reguladores por ejemplo)

c) De libre nombramiento y remoción. (típico caso de ministros de Estado)

2. Empleado de confianza.- El que desempeña cargo de confianza técnico o político, distinto al del funcionario público. Se encuentra en el entorno de quien lo designa o remueve libremente y en ningún

caso será mayor al 5% de los servidores públicos existentes en cada entidad. El Consejo Superior del Empleo Público podrá establecer límites inferiores para cada entidad. En el caso del Congreso de la República esta disposición se aplicará de acuerdo a su Reglamento. Ejemplo: el asesor o personal que trabaja directamente con los Funcionarios.

2. Servidor público.- Se clasifica en

a) Directivo superior.- El que desarrolla funciones administrativas relativas a la dirección de un órgano programa o proyecto, la supervisión de empleados públicos, la elaboración de políticas de actuación administrativa y la colaboración en la formulación de políticas de gobierno. A este grupo se ingresa por concurso de méritos y capacidades de los servidores ejecutivos y especialistas, su porcentaje no excederá del 10% del total de empleados de la entidad. La ineficiencia en este cargo da lugar al regreso a su grupo ocupacional. Una quinta parte del porcentaje referido en el párrafo anterior puede ser designada o removida libremente por el titular de la entidad. No podrán ser contratados como servidores ejecutivos o especialistas salvo que cumplan las normas de acceso reguladas en la presente Ley.

b) Ejecutivo.- El que desarrolla funciones administrativas, entiéndase por ellas al ejercicio de autoridad, de atribuciones resolutivas, las de fe pública, asesoría legal preceptiva, supervisión, fiscalización, auditoría y, en general, aquellas que requieren la garantía de actuación administrativa objetiva, imparcial e independiente a las personas. Conforman un grupo ocupacional.

c) Especialista.- El que desempeña labores de ejecución de servicios públicos. No ejerce función administrativa. Conforman un grupo ocupacional.

De apoyo.- El que desarrolla labores auxiliares de apoyo y/o complemento. Conforman un grupo ocupacional.

…“

El área especializada de administración de las TIC

De conformidad con esta estructura y el ROF vigente de la entidad, se pudo apreciar la existencia de un área especializada en la administración y gestión de las Tecnología de la Información y Comunicaciones (TIC), denominada Subgerencia de Tecnología de la Información y Comunicación, cuya composición fue la siguiente:

Tabla 2. Organización de la Subgerencia de TIC de la MPH

Cargo	Vínculo Contractual – Profesión
Subgerente de TIC	Funcionario- Ingeniero de Sistemas
Arquitecto de software	CAS - Ingeniero de Sistemas
Técnico en soporte Técnico	CAS -Técnico
Analista Programador	Nombrado - Ingeniero de Sistemas
Programador de Sistemas	Nombrado - Ingeniero de Sistemas
Maquetador, Modelador y Programador web	CAS -Ingeniero de Sistemas
Responsable de Soporte	CAS- Técnico
Técnico en soporte	Nombrado - Técnico

Los responsables de la Seguridad de la Información

De conformidad con la Norma Técnica Peruana ISO/IEC 27001:2014, la alta dirección, en este caso el Alcalde debe liderar la gestión e implementación del sistema de seguridad de la información en la entidad (7 págs. 3, 4 y 5), asimismo debe proveer los medios logísticos, para el adecuado funcionamiento.

El Oficial de Seguridad de la Información, de conformidad la NTP-ISO/TEC 27001:2014, este es un rol que se designa a una persona de la entidad para que se haga cargo de controlar y regular la seguridad de la información, puede hacerse cargo de todas las tareas de seguridad de TIC, la intención es de exista un responsable a quien recurrir en caso se genere algún problema de seguridad y alerte debilidades en el proceso de la información. (8)

Es por ello que el alcalde de la Municipalidad, designo como Oficial de Seguridad de la Información al Subgerencia de Tecnología de la Información y Comunicación y conformo una comisión de se Seguridad de la Información, conformada por 5 funcionarios de su gestión.

En consecuencia de manera directa o indirecta el responsable de aplicar los mecanismos de seguridad de la información de la entidad fue el Subgerencia de Tecnología de la Información y Comunicación.

2.2.2. Información Pública

El fascículo del Estado Peruano respecto a "Acceso a la Información Pública" señala que:

> *"La información pública es aquella que ha sido creada u obtenida por las entidades de la administración pública o que posee o que se encuentre bajo su control. La Ley de Transparencia y Acceso a la Información Pública (art. 10º) ha establecido que también se considera como información pública" (9)*

También señala que la información es de forma física o virtual, y que de conformidad con la Ley de Transparencia y Acceso a la Información Pública, aprobado por el Decreto Supremo N° 043-2003-PCM, y su reglamento de esta ley la información debe entregarse al cuidado cuando esta lo solicita de forma fidedigna, y que las entidades de administración pública obligas a brindar información son:

"…

- *El Poder Ejecutivo: todos sus organismos.*
- *El Poder Legislativo, es decir, el Congreso de la República.*
- *El Poder Judicial.*
- *Los Gobiernos Regionales.*
- *Los Gobiernos Locales.*
- *Los organismos constitucionalmente autónomos como, por ejemplo, la Defensoría del Pueblo, la Contraloría General de la República, el Ministerio Público, entre otros.*
- *Las demás entidades, organismos, proyectos y programas del Estado que ejercen las denominadas potestades administrativas*

o poderes específicos otorgados por la ley y, por ello, están sujetas a las normas de derecho público.

- *Las personas jurídicas bajo el régimen privado que prestan servicios públicos, por ejemplo, empresas que siendo privadas prestan servicios de luz, agua, telefonía, entre otras.*
- *Las personas jurídicas bajo el régimen privado que ejercen funciones administrativas del sector público, bajo cualquier modalidad, por ejemplo, instituciones educativas privadas que prestan un servicio educativo en virtud de una autorización del Estado.*

…" (10)

Según el estado peruano, la solicitud a la información puede ser solicitada por una persona natural como jurídica Sin embargo existen límites de acceso a esta información el cual señala:

> *"Ningún derecho es absoluto, todos tienen sus límites en otros derechos o en otros principios constitucionales. El acceso a la información no es una excepción. La Constitución concluye que este derecho tiene límites en:*
> *• El derecho a la intimidad.*
> *• La seguridad nacional.*
> *• El derecho al secreto bancario.*
> *• La reserva tributaria (Const., art. 2, inc. 5).*
> *• El derecho a la autodeterminación informativa, denominado también como derecho "a la protección de datos personales (Const., art. 2, inc. 6)". "* (9)

Asimismo es preciso mencionar que también en las entidades pública existe información confidencial que solo puede ser manejada por la misma entidad, también existe información sensible que se maneja de los ciudades y que se debe proteger en cumplimiento a los derechos a la intimidad personal, como por ejemplo los datos personales y familiares, salud personal, y las comunicaciones, telecomunicaciones, documentos privados en general, entre otros. (9)

Los datos sensibles para el estado peruano son:

> *"Los datos sensibles son un tipo o especie de dato personal, cuyo tratamiento y difusión solo puede realizarse previo consentimiento, por escrito, del titular de tal información (LPDP, art. 13.6). Dentro de los datos sensibles se encuentra la siguiente información (LPDP, art. 2.5):*
> • *"Datos biométricos"13, que por sí mismos permiten identificar al titular.*
> • *Datos referidos al origen racial y étnico.*
> • *Ingresos económicos.*
> • *Opiniones o convicciones políticas, religiosas, filosóficas o morales.*
> • *Afiliación sindical.*
> • *Información relacionada a la salud.*
> • *Información relacionada a la vida sexual."* (9)

Es preciso mencionar en este punto que parte de esta información sensible es la que se almacena en los diferentes sistemas informáticos de las entidades del estado, por ello deben contar con los mecanismos de seguridad en cumplimiento de nuestros derechos.

A veces es necesario acceder a esta información sensible, pero solo pueden acceder algunas autoridades en ejercicio de sus funciones, previo sustento y autorizaciones como, por ejemplo:

- La Comisión investigadora del congreso de la republica
- El Juez
- La Contraloría General de la Republica
- La Defensoría del pueblo
- La Superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones

Cada entidad cuenta con sus propios procesos para acceder a la información, parte de la información pública se puede visualizar en los portales Web de la entidad.

2.2.3. Seguridad de la Información

Es preciso mencionar que la seguridad de la información difiere de la seguridad de la informática, para Escriva y otros indican que "La seguridad de la Información es el conjunto de medidas y procedimientos, tanto humanos como

técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información" (2) y la Seguridad Informática es una subcategoría de la seguridad de la información, que protege la información que es procesada o utilizada por las TIC's.

La seguridad de la Información como tal tiene 3 principios básicos, la integridad, disponibilidad y confidencialidad, cabe mencionar que algunos autores señalan otros más, pero en base a mi experiencia considero que estos 3 embarcan los demás:

- La confidencialidad hace referencia a aquella que información sensible que debe ser visualiza solo por quienes corresponda
- La integridad hace referencia a que esta información debe ser fidedigna, por ende no puede ni debe ser manipulado por quien no corresponda.
- La Disponibilidad hace referencia a que le usuario autorizado tenga acceso a la información cuando lo requiera y de la forma como lo requiera.

Estos 3 principios deben interactuar entre sí para brindar adecuadamente la información contemplando los niveles de seguridad, como se aprecia en la figura siguiente:

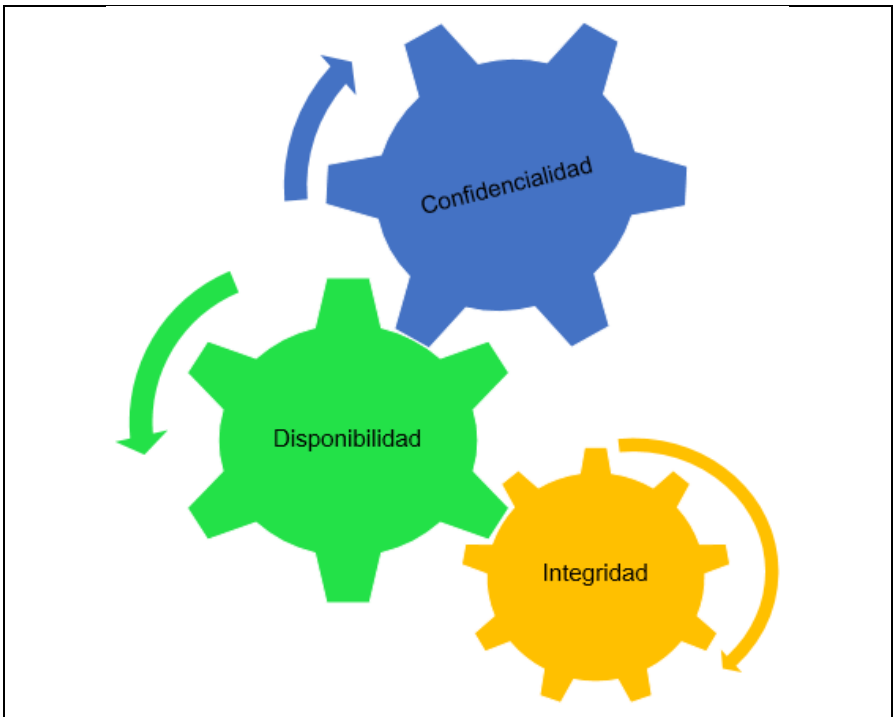


Figura 6. Principios de la Seguridad de la Información

Los Activos de la Información

Los activos de la información es todo aquello que se considere como información, ya sea en físico o virtual.

Estos activos en cualquier entidad están conformados por la Información, hardware, software y usuarios (internos o externos).

Los activos de la información son valiosos para cualquier entidad, por ello existe la necesidad de identificar las vulnerabilidades y controlar las amenazas, para evitar que estas impacten negativamente a la entidad.

AMENAZAS	INTENCIONADO	NO INTENCIONADO
ELECTRONICAS	Robo de Información Manipulación de Datos Virus Otros	Fallas de Red Fallas de servidores Fallas de los aplicativos Otros
FISICAS	Robo de equipos Sabotaje en Línea Vandalismo Otros	Terremoto Inundación Fallo de energía por proveedor Falla de servicios de internet por proveedor Otros

Figura 7. Amenazas a los activos de la información

El flujo, entre amenaza, vulnerabilidad, impacto de activos se visualizan con una adecuada gestión de riesgos, como se puede apreciar en la siguiente imagen:

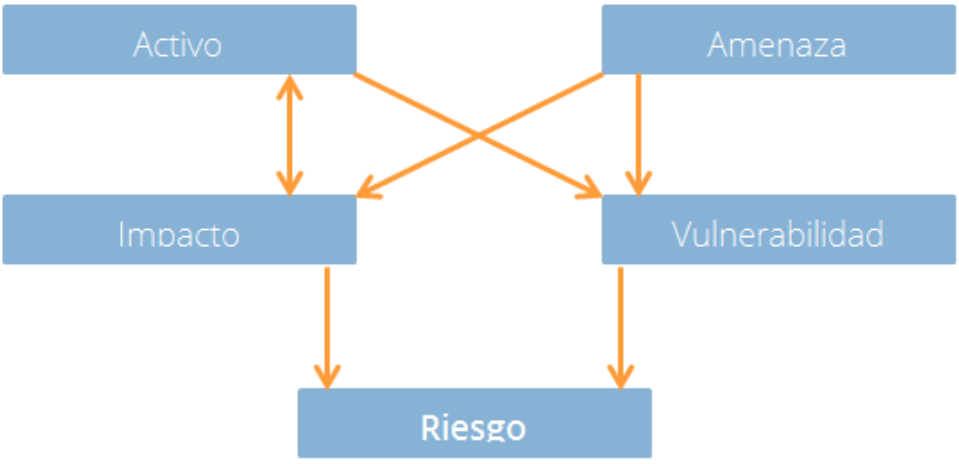


Figura 8. Esquema de Riesgos de la Seguridad de la Información *(11)*

Política de seguridad

La política de seguridad es una norma interna de la entidad que permite definir las bases, listar actividades generales, citar responsables, y sanciones de las acciones a ejecutarse por los usuarios de los sistemas de información.

Esta política debe asegurar que los procesos y actividades de forma genérica aseguren hardware, software, la información y usuarios de las posibles amenazas, asegurar las vulnerabilidades e identificar claramente los riesgos e impacto con la finalidad de implementar y realizar seguimiento a los controles que mitiguen la amenaza y vulnerabilidad.

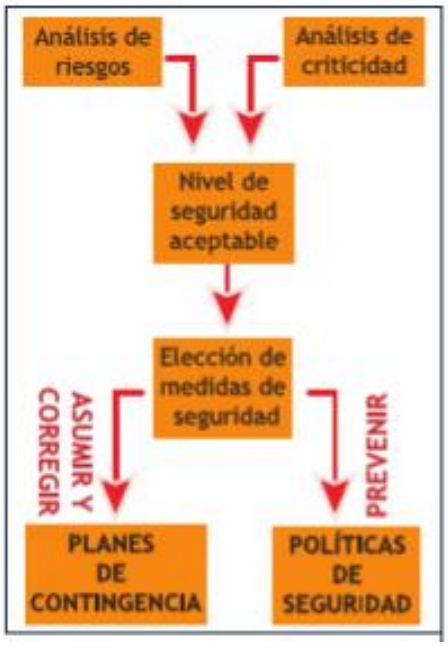


Figura 9. Control de Riesgos *(2)*

Una correcta gestión de riesgos de la seguridad de la información, permitirá identificar los escenarios más críticos, los mismos que deben quedar plasmado en un plan de contingencias.

2.2.1. Estándares y Normas de Seguridad de la Información

- **ISO 27001**

  La ISO 27001 es un estándar de buena calidad y bastante globalizados, consiste en brindar pautas para la “administración de la seguridad de la información, e implica la implementación de toda

una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización". (8)

Basado en este estándar el estado peruano genera la norma técnica peruana sobre la seguridad de la información.

- **COBIT**

Acrónimo de "Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), abarca temas como gobernabilidad, control, aseguramiento y auditorias para TIC.

Si bien no está relacionado directamente a la Seguridad de la Información, si existe una relación indirecta, que que este estándar establecer los controles necesario para administras las TIC, y como parte de ello está la seguridad de la Información.

2.3 DEFINICIÓN DE TÉRMINOS BÁSICOS

2.3.1 Amenaza

"Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización". (12)

"Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización." (13)

2.3.2 Autorización de la información

Mecanismos con sustento de que el emisor tiene permiso para acceder al servicio o información.

2.3.3 Ataque

"Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera". (14)

"Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información". (14)

2.3.4 Control:

“Herramienta de la gestión del riesgo, incluidas políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.”

2.3.5 Comité de Gestión de la seguridad de la información

“Se refiere a un grupo de personas especializadas en temas tecnológicos y de seguridad de la información, y necesariamente se incluye a la máxima autoridad de la empresa.”

2.3.6 Delitos Informáticos

Acciones deliberadas a través de medios informáticos con fines delictivos.

2.3.7 Falsificación de información por terceros

Se refiera a una acción consciente por parte de personas ajenas a la entidad con la finalidad de alterar o modificar información.

2.3.8 Gestión del riesgo

“Actividades coordinadas para dirigir y controlar una organización considerando el riesgo”. (15)

“Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo”. (16)

“Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados”. (17)

2.3.9 Instalaciones de proceso de información:

Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena.

2.3.10 Impacto

“Consecuencia que sobre un activo tiene la materialización de una amenaza. Consecuencia – Resultado de un suceso que afecta a los objetivos”. (16)

“Consecuencia que sobre un activo tiene la materialización de una amenaza”. (17)

2.3.11 Propietario de la Información

Personas responsables del activo.

2.3.12 Virus Informático

Programa malicioso que alteran el funcionamiento de los equipos tecnológicos y/o sistemas de Información.

2.3.13 Vulnerabilidad:

“Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas”. (12)

“Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia”. (16)

CAPITULO III

METODOLOGÍA

3.1 METODOLOGÍA APLICADA PARA EL DESARROLLO DE LA SOLUCIÓN

3.1.1 Método de la Investigación

A) Método general o teórico de la investigación

El método de investigación utilizado es el Método Descriptivo (18), debido a que nuestro interés es identificar los factores relacionados a la implementación de la Norma Técnica Peruana ISO/IEC 27001:2014 en la Municipalidad de Huancayo, para ello se ha tenido que observar, conocer las condiciones de esta Municipalidad a nivel de procesos y personas relacionadas al contexto, sin modificar o manipular la realidad.

Teniendo en cuenta lo descrito, para el presente trabajo de investigación se ha contemplado las siguientes etapas:

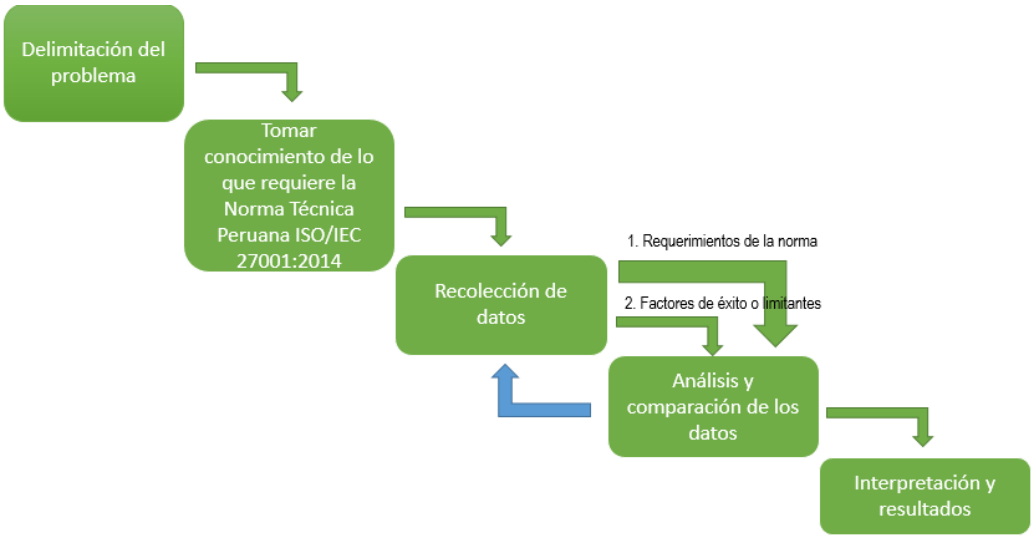


Figura 10. Etapas del Método de Investigación

B) Método específico de la investigación

El nivel o alcance del estudio fue descriptivo (19), debido a que se ha considerado recolectar información de acuerdo a cada requerimiento solicitado por la Norma Técnica Peruana ISO/IEC 27001:2014 dentro de la Municipalidad de Huancayo, por tanto no se está modificando o manipulado las variables

El tipo de estudio descriptivo a utilizarse es el estudio de correlación, debido a que se tiene interés en identificar estos factores que permitieron el cumplimiento o actuaron como limitantes.

En resumen, el método a aplicarse tiene la siguiente característica:

FINALIDAD	ALCANCE TEMPORAL	PROFUNDIDAD	AMPLITUD	FUENTE
Aplicada	Seccional (Con la información actualizada, valida y vigente para el periodo seleccionado)	Descriptiva	Micro sociológica (estudio ejecutado en la Municipalidad Provincial de Huancayo)	Con base en datos primarios

Figura 11. Resumen del Método a aplicarse

3.1.2 Etapas del Método de la investigación

A continuación, se explicará en qué consistirá cada etapa:

1. **Delimitación del problema:** consiste en dar a conocer la problemática, antecedentes, definir el lugar de este estudio, periodo, definir objetivos, es decir establecer el plan de acción el cual nos brindara una dirección en desarrollo de esta investigación.

   El desarrollo de esta etapa se muestra en el Capítulo I del presente trabajo.

2. **Tomar conocimiento de las características de la Norma Técnica peruana ISO/IEC27001:**2014: en esta etapa tomamos conocimiento del marco teórico que engloba esta norma, a quienes aplica, y que es lo que se requiere para su cumplimiento, el detalle se muestra en el Capítulo II del presente trabajo.

3. **Recolección de datos:**

   Esta etapa considera 2 fases:

La primera fase consiste en recopilar información de acuerdo a los requerimientos de la Norma Técnica peruana ISO/IEC27001:2014, para la recolección de datos, se realizará un cuestionario cerrado de acuerdo a los requerimientos de la norma.

Luego utilizando una tabla por cada requerimiento, se listará las acciones o implementaciones realizadas por la municipalidad, de la siguiente forma:

Tabla 3. Recolección de datos I fase

Requerimiento (normativa)	**Acciones por parte de la Municipalidad**
Requerimiento 1	Acción 1 Implementación 1
Requerimiento 2	Acción 2 Implementación 2
Requerimiento 3	Acción 1 Implementación 2

Se debe tener en cuenta que algunas acciones o implementaciones pueden corresponder a más de un requerimiento.

La Segunda fase, una vez concluida el análisis y comparación de la información recabada de la primera fase, se recopilará información sobre los factores que han permitido o logro o limitación por cada requerimiento de la Norma Técnica peruana ISO/IEC27001:2014.

En esta fase se aplicará entrevistas con el o los responsables de la implementación, con la finalidad de obtener información cuales han sido los factores que lo han conllevado a el cumplimiento de la norma o que actuado como obstáculo o limitante.

Para tal fin se implementar una tabla en la que se filtrara solo requerimientos que deberían ser implementados en la Municipalidad (exclusión de los NO APLICA) de la siguiente forma:

Tabla 4. Recolección de datos II fase

Requerimiento (normativa)	**Estado**	**Factor de Éxito**	**Factor Limitante**
Requerimiento 1	Cumple		

Requerimiento 2	Cumple Parcialmente		
Requerimiento 3	No implementado		

4. **Análisis y comparación de los datos**: esta etapa al igual que la anterior, se divide en 2 fases:

Primera fase, se recepciona la información de la primera fase de la anterior etapa, y se procederá a analizar si con la información remitida o las implementaciones realizadas realmente cumple o no cumple lo solicitado por la Norma técnica Peruana ISO/IEC 27001:2014.

Para el análisis de la información recaba se contemplará los estados siguientes:

- **No aplica:** si después del análisis del requerimiento se establece que no debería implementarse en la Municipalidad
- **Cumple:** si las acciones o implementaciones adoptadas por la entidad satisface el requerimiento de forma total.
- **No implementado:** si no se ha adoptado alguna acción o para satisfacer el requerimiento de la norma.
- **Cumple parcialmente:** en caso se haya adoptado algunas acciones, pero no satisface de forma total el requerimiento de la norma

Al finalizar la tabla tendrá el siguiente aspecto:

Tabla 5. Cruce de información I fase

Requerimiento (normativa)	Acciones por parte de la Municipalidad	Estado
Requerimiento 1	Acción 1 Implementación 1	Cumple
Requerimiento 2	Acción 2 Implementación 2	Cumple Parcialmente
Requerimiento 3		No implementado
Requerimiento 4		No aplica

Segunda fase, se recepciona la información de la segunda fase de la anterior etapa, y se procederá a analizar que o cuales son los factores

que han conllevado al cumplimiento o no de cada requerimiento de la Norma técnica Peruana ISO/IEC 27001:2014.

Luego de contar con la tabla de factores rellenada, se **procederá a categorizar estos factores**, debido a que es posible que existan diferentes formas de citar un mismo factor limitante o de logro, las categorías que se listan a continuación no limitan que durante el proceso de análisis se encuentren una nueva categoría:

Factores de éxito (fe):

- Apoyo del titular de la entidad
- Habilitación Presupuestal
- Capacitación del personal
- Experiencia de los responsables
- Cultura Organizacional
- Adecuada gestión del responsable

Factores Limitantes (fl):

- Falta de Presupuesto
- Desconocimiento de la Norma
- Desentendimiento por parte del Titular
- Falta de Cultura Organizacional
- Responsables sin experiencia
- Desidia (o priorización de otras actividades)
- Finalmente, el consolidado tendrá la siguiente forma:

Tabla 6. Cruce de información II fase

Requerimiento (normativa)	**Acciones por parte de la Municipalidad**	**Estado**	**Factor de Éxito**	**Factor Limitante**
Requerimiento 1	Acción 1 Implementación 1	Cumple	fe1 fe2	---
Requerimiento 2	Acción 2 Implementación 2	Cumple Parcialmente	fe3	fl1 fl2 fl3
Requerimiento 3		No implementado	----	fl2 fl4
Requerimiento 4	---	No aplica	----	-----

Si del total de requerimiento al menos más de la mitad se ha cumplido, los factores de éxito se tendrán en cuenta en la etapa siguiente, caso contrario solo se analizará los factores limitantes, y viceversa.

Sean cual sea los factores a analizar o los de éxito o limitante, se listará de acuerdo a su incidencia:

Tabla 7. Tabulación de los factores

Factor	Incidencia
fx5	6
fx2	5
fx1	4
fx3	1
fx4	0

Interpretación y resultados: en esta etapa se procederá la interpretará los resultados obtenidos de la investigación.

Se analizará los 3 factores de mayor incidencia.

3.1 DISEÑO DE LA INVESTIGACIÓN

El diseño de investigación es no experimental (4), ya que no se pretende manipular las variables y tampoco se puede influir sobre ellas, porque es su realidad al igual que sus efectos.

Como ya se mencionó el diseño es transeccional debido a que le tiempo a evaluar corresponde al periodo 2018, y tiene como fin estudiar como las variables se relaciona entre ellas, es decir cómo es que un factor puede ser determinante para el logro o actuar como limitante en el cumplimiento de los requerimientos que cita la Norma técnica Peruana ISO/IEC 27001:2014.

Se aplicara en una primera fase diseños transeccionales descriptivos, ya que como resultado se obtendrá si se logró o no cumplir con cada requerimiento de la norma, posteriormente en una **segunda fase el diseño transeccional es correccional – causal,** en la que se identificara los factores que permitieron el logro o no del requerimiento de la norma, es posible que estos factores tengan incidencia en los resultados de más de 2 requerimientos solicitados por la norma

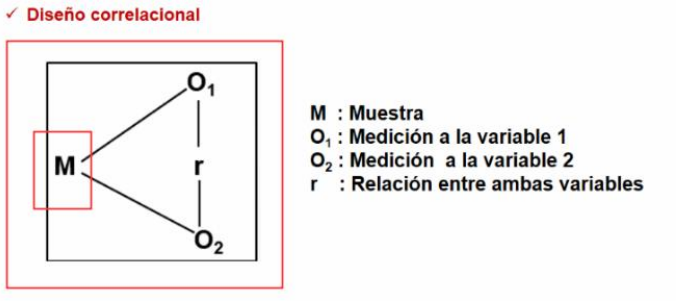


Figura 12. Diseño de la investigación

Fuente: clase virtual de Seminario de Tesis II de la Universidad Continental

3.1.1 Tipo de Investigación

El tipo de investigación para el presente trabajo corresponde a una **investigación de tipo Aplicado** (20), ya que está orientada a resolver problemas de carácter práctico a fin de mejorar la sociedad, que este caso parte de la necesidad asegurar la información privada de los ciudadanos en las entidades de administración del estado, para ello es necesario identificar los factores que no permiten la implementación adecuada de una política de seguridad de la información en las entidades estatales, al final la Presidencia de Consejo de Ministros o la entidad de manera proactiva puede adoptar acciones correctivas y en los factores de éxito hacer replica de ello en otras entidades del estado.

3.1.2 Alcance Temporal

En este caso el alcance temporal es seccional (20), debido a que nos centraremos a un determinado tiempo el cual es el I trimestre del 2018.

3.1.3 Nivel de Investigación

Esta trabajo de investigación tiene un alcance o nivel correlacional (20), se trata de relacionar dos variables de estudio, entre el nivel de implementación y los factores de éxito o limitantes.

3.2 POBLACIÓN Y MUESTRA

3.2.1 Población

En este caso se considera como población todos los controles de seguridad de la información aplicados a la Municipalidad de Huancayo, y que exige la norma técnica peruana ISO NTP/IEC 27001:2014.

3.2.2 Muestra

Para esta investigación se aplicara un Muestreo probabilístico (20), específicamente se aplicara un muestreo aleatorio simple, es decir que cualquier control de seguridad de la información del Municipio Provincial de Huancayo durante el I trimestre del periodo 2018, contemplado dentro de la población tiene la misma probabilidad de ser seleccionados para formar parte de la muestra.

La selección se realizar usando los criterios de quien ejecute la investigación.

3.3 TÉCNICAS DE RECOLECCIÓN Y PROCESAMIENTO DE DATOS

Como ya se mencionó en párrafos anteriores, se aplicara A continuación, presentamos brevemente las técnicas básicas y sus respectivos instrumentos (20):

- **Observación simple**

  La aplicación de esta técnica permitirá obtener los datos cualitativos y cuantitativos que requiere esta investigación. Durante la aplicación de esta técnica no se participará de la actividad.

- **Entrevista**

  Para la aplicación de estas técnicas se realizara un cuestionario cerrado con el fin de obtener respuestas verbales a las interrogantes planteadas sobre los criterios de seguridad de la información.

3.4 TÉCNICAS DE ANÁLISIS DATOS

Se utilizara tablas de comparación, en ellas se vaciara la información recolectada, luego de tener la tabla con los factores, se **procederá a categorizar**

estos factores, debido a que es posible que existan diferentes formas de citar un mismo factor limitante o de logro.

Factores de éxito (fe):

Factores Limitantes (fl):

Finalmente, el consolidado tendrá la siguiente forma:

Tabla 8. Tabla de Consolidación de datos

Requerimiento (normativa)	**Acciones por parte de la Municipalidad**	**Estado**	**Factor de Éxito**	**Factor Limitante**
Requerimiento 1	Acción 1 Implementación 1	Cumple	fe1 fe2	---
Requerimiento 2	Acción 2 Implementación 2	Cumple Parcialmente	fe3	fl1 fl2 fl3
Requerimiento 3		No implementado	----	fl2 fl4
Requerimiento 4	---	No aplica	----	-----

Si del total de requerimiento al menos más de la mitad se ha cumplido, los factores de éxito se tendrán en cuenta en la etapa siguiente, caso contrario solo se analizará los factores limitantes, y viceversa.

Sean cual sea los factores a analizar o los de éxito o limitante, se listará de acuerdo a su incidencia.

CAPITULO IV
RESULTADOS Y DISCUCIÓN

4.1 RESULTADO DEL TRATAMIENTO DE LA INFORMACIÓN

Siguiendo nuestra metodología descrita en el Capítulo III, se ha procedido al levantamiento de la información, cuyo detalle figura en los anexos del presente trabajo de investigación

Nivel de Implementación de la Norma Técnica Peruana **ISO NTP/IEC 27001:2014** en la Municipalidad de Huancayo en el I trimestre del periodo 2018, se basó en la verificación de los siguientes controles que señala la Norma citada.

Tabla 9. Nivel de cumplimiento de los controles de seguridad de la información en la MPH

CRITERIO	CUMPLIMIENTO		
	SI	NO	N/A
EVALUACION Y TRATAMIENTO DEL RIESGO			
Evaluando los riesgos de seguridad		X	
Tratando riesgos de seguridad		X	
POLÍTICA DE SEGURIDAD			
Política de seguridad de la información	X		
ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD			
Organización interna		X	
Seguridad en los accesos de terceras partes		X	
CLASIFICACIÓN Y CONTROL DE ACTIVOS			
Responsabilidad sobre los activos		X	
Clasificación de la información		X	
SEGURIDAD EN RECURSOS HUMANOS			

CRITERIO	CUMPLIMIENTO		
	SI	NO	N/A
Seguridad antes del empleo	X		
Durante el empleo		X	
Finalización o cambio del empleo		X	
SEGURIDAD FÍSICA Y DEL ENTORNO			
Áreas seguras	X		
Seguridad de los equipos	X		
GESTIÓN DE COMUNICACIONES Y OPERACIONES			
Procedimientos y responsabilidades de operación	X		
Gestión de servicios externos			X
Planificación y aceptación del sistema		X	
Protección contra software malicioso	X		
Gestión de respaldo y recuperación	X		
Gestión de seguridad en redes	X		
Utilización de los medios de información		X	
Intercambio de información		X	
Servicios de correo electrónico		X	
Monitoreo		X	
CONTROL DE ACCESOS			
Requisitos de negocio para el control de accesos		X	
Gestión de acceso de usuarios		X	
Responsabilidades de los usuarios		X	
Control de acceso a la red	X		
Control de acceso al sistema operativo	X		
Control de acceso a las aplicaciones y la información	X		
Informática móvil y teletrabajo			X
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
Requisitos de seguridad de los sistemas		X	
Seguridad de las aplicaciones del sistema		X	
Controles criptográficos			X
Seguridad de los archivos del sistema		X	
Seguridad en los procesos de desarrollo y soporte		X	

CRITERIO	CUMPLIMIENTO		
	SI	NO	N/A
Gestión de la vulnerabilidad técnica		X	
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN			
Reportando eventos y debilidades de la seguridad de información		X	
Gestión de las mejoras e incidentes en la seguridad de información		X	
GESTIÓN DE CONTINUIDAD DEL NEGOCIO			
Aspectos de la gestión de continuidad del negocio		X	
CUMPLIMIENTO			
Cumplimiento con los requisitos legales	X		
Revisiones de la política de seguridad y de la conformidad técnica		X	
Consideraciones sobre la auditoria de sistemas	X		

Luego de vaciar la información en nuestra Base de Datos se ha obtenido que el nivel de implementación de la Norma Técnica Peruana ISO NTP/IEC 27001:2014 en la Municipalidad de Huancayo en el I trimestre del periodo 2018, es del 32%, como se aprecia en el siguiente gráfico:

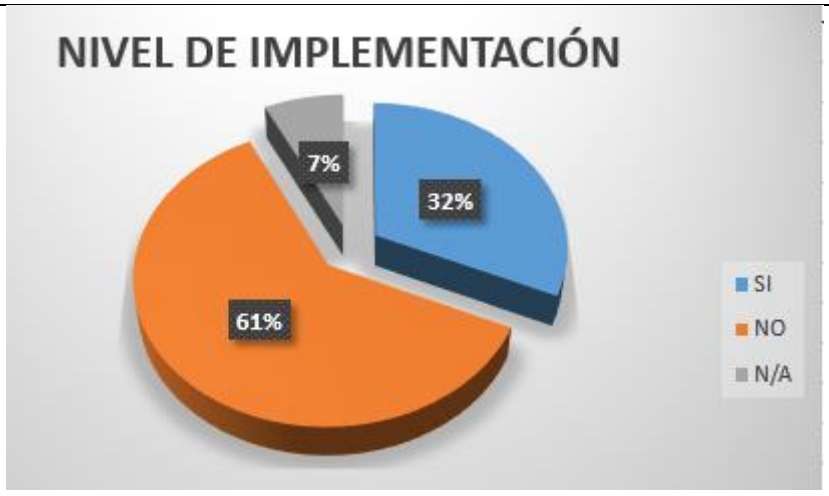


Figura 13. Nivel de implementación de la Norma Técnica Peruana **ISO NTP/IEC 27001:2014** en la Municipalidad de Huancayo en el I trimestre del periodo 2018

Como se puede apreciar la entidad no ha logrado alcanzar óptimo de implementación, pero tampoco se puede decir que no existe ningún control de seguridad de la información.

Respecto a los factores que han influido para el cumplimiento de los criterios de la norma, se tiene que factor importante ha sido la experiencia del responsable de implementar estos controles, como se puede apreciar han contribuido en un 61%, y otro aspecto no muy relevante pero que brinda soporte a todos los controles de la entidad son las políticas generales de la entidad, relacionados con la cultura organizacional y modo de trabajo.

Figura 14. Factores de éxito en la implementación de la Norma Técnica Peruana ISO NTP/IEC 27001:2014 en la Municipalidad de Huancayo en el I trimestre del periodo 2018

En referencia a los factores limitantes, como se puede apreciar en el siguiente gráfico, la Falta de Procesos Internos en la entidad, que de alguna Manera afecta a la Cultura Organizacional, que juntos afectan la implementación en 66%, otro factor no menos importante es la falta de designación de presupuesto esto debido a la falta de importancia que se da este aspecto o mero desconocimiento del titular de la entidad, el cual afecta en 24%, que de alguna manera también está relacionada a la falta de experiencia de los responsables ya que se necesita asignar presupuesto para capacitar al personal, y así mismo genera un cultura para que se replique las capitaciones dentro del equipo responsable.

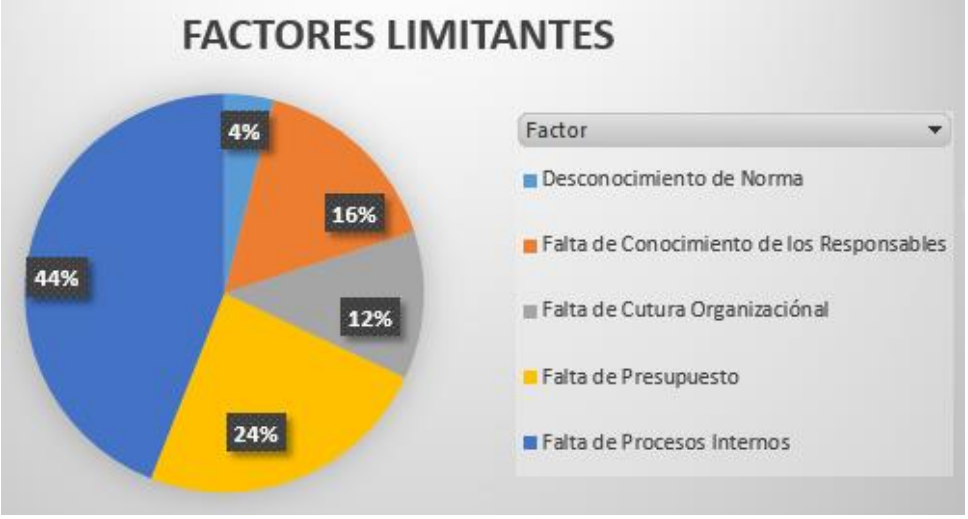


Figura 15. Factores de limitantes en la implementación de la Norma Técnica Peruana **ISO NTP/IEC 27001:2014** en la Municipalidad de Huancayo en el I trimestre del periodo 2018

4.2 PRUEBA DE HIPÓTESIS

El presente estudio no presenta hipótesis por ser descriptivo y no se intenta pronosticar un hecho un dato. (4)

4.3 DISCUSIÓN DE RESULTADOS

El estudio tiene como objetivo identificar los factores de éxito o factores limitantes para la implementación de la norma técnica peruana **ISO NTP/IEC 27001:2014** en la Municipalidad de Huancayo en el I trimestre del periodo 2018, por tanto, corresponde a una investigación de tipo aplicado, con alcance o nivel correlacional.

La investigación es válida ya que se está usando criterios estándar de la ISO 27001 y que la Norma Técnica Peruana ISO NTP/IEC 27001:2014 ha adoptado y ha modificado de acuerdo a la realidad de las entidades de administración pública.

Si bien los aspectos han sido consultados a los responsables durante las entrevistas, también se han va procedido a validar los controles con sus documentos internos y durante las visitas se ha revalidado si realmente estos controles se han implementado, por ende, se indica que los datos son fidedignos a la realidad encontrada en el periodo indicado de la Municipalidad Provincial de Huancayo.

Sobre la metodología utilizada, se puede indicar que fue la apropiada, esta nos permitió establecer las etapas de la investigación de forma clara y seguir con dirección.

Durante el desarrollo del presente trabajo se presentaron algunas limitaciones, respecto a la disponibilidad del Subgerente de Tecnología de Información y Comunicaciones, quien disponía de poco tiempo para las solicitudes de información.

La muestra que se estableció facilito mucho ya que consistió en una selección aleatoria simple para validar la información.

El instrumento también permitió la recolección de datos de manera práctica, ya que, si se utiliza una tabla más consistente y con detalle, la recolección de datos hubiese tomado mayor tiempo, y como se mencionó en párrafos anteriores, la disposición de tiempo de parte del responsable de la subgerencia de tecnología de información y comunicación no era absoluta, ya que debía estar en reuniones o por órdenes de sus superiores debía ejecutar actividades ajenas a las de su puesto.

En realidad, el instrumento planteado inicialmente se ha mantenido, y debido a esta tabla práctica de recolección de datos pese a las limitaciones de tiempo del responsable se ha podido concretar.

CONCLUSIONES

1. La Municipalidad Provincial de Huancayo durante el I trimestre periodo 2018, ha alcanzado un 32% de implementación de controles de seguridad de la información de acuerdo a los criterios establecidos por Norma Técnica Peruana ISO NTP/IEC 27001:2014, si bien en este trabajo de investigación no se ha analizado la calidad del cumplimiento, se puede indicar que el logro es porque cumple estrictamente con los requisitos, parámetros y características que indica la norma.

2. Se ha determinado que los factores de éxito están relacionados con la capacidad de conocimiento, experiencia y gestión del responsable directo de la implementación de estos controles, que en el caso de la Municipalidad Provincial de Huancayo, es del Ing. Roberto Tejada Farfán Subgerente de Tecnología de Información y Comunicaciones.

3. Entre los factores limitantes se encuentran 2 factores que están relacionados y es la falta de procesos y cultura organizacional y que juntos alcanzan un 66%. Una entidad sin procesos claros, es difícil que pueda generar una cultura organizacional adecuada relacionada a la gestión de seguridad de la información. Otro factor importante fue la falta de presupuesto, el cual está relacionado directamente con la falta de importancia o de conocimiento en seguridad de la información por el titular de la entidad, y quizá sea el problema de muchos titulares, quienes se preocupan por vender su gestión con lo que más se hace tangible o reconocido por la ciudadanía.

RECOMENDACIONES

1. Es preciso que la Presidencia de Consejos de Ministros a través de su organismo competente, organice una capacitación para los titulares de las entidades públicas respecto a seguridad de la información, gestión de procesos y cultura organizacional antes de asumir el cargo, ya que es preciso que antes de su gestión tome conocimiento de la importancia y los riesgos no implementar una adecuada gestión de seguridad de la información en las entidades.

2. La Presidencia de Consejos de Ministros a través de su organismo competente debería capacitar a los responsables de las unidades orgánicas relacionadas con la seguridad de la información, sobre la gestión, implementación, procesos y riesgos de seguridad de la información, y exigir que ellos hagan replica en el equipo responsable de su entidad

3. La Presidencia de Consejos de Ministros a través de su organismo competente, debería solicitar un informe que dé cuenta del nivel de implementación de la norma técnica peruana ISO NTP/IEC 27001:2014, y generar reconocimientos y/o incentivos no económicos para estas entidades que cumplan, con la finalidad de motivar el cumplimiento.

4. El estado Peruano a través del órgano competente de La Presidencia de Consejos de Ministros, debería implementar un proyecto de modernización en el estado a nivel de infraestructura tecnológica y estandarizada, con la finalidad de que los datos de todos los peruanos estén en un solo Data Center, así no solo ahorrarían la implementación en cada entidad, si no que se podría implementar todas las medidas de control se seguridad de la información y esto podría conllevar a realizar otro tipo de análisis de la información, para identificar sectores en peligro a nivel

geográfico, por edad, sexo, educación, de igual manera identificar aquellas acciones o personas que vulneran nuestra normativa interna en todos los sectores de educación, salud, e inclusive el poder ejecutivo y Legislativo.

REFERENCIAS BIBLIOGRÁFICAS

1. **Presidencia de Consejo de Ministros y Oficina Nacional de Gobierno Electrónico.** *Una Mirada al Gobierno Electrónico en el Perú.* Primera, Lima, Perú : s.n., Octubre 2013.

2. **ESCRIVA GASCO, Gema, y otros.** *Seguridad Informática.* Madrid : MACMILLAN IBERIA S.A. 28020.

3. **Presidencia del Consejo de Ministros y la Oficina de Gobierno Electrónico e Informática.** http://slideplayer.es/slide/3933475/. *Slider Player.* [En línea] 2016. [Citado el: 10 de Abril de 2018.]

4. **Sampieri, Dr. Roberto Hernández.** *Metodología de la Investigación.* Impreso en México : McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V., 2010. ISBN: 978-607-15-0291-9.

5. **Presidencia de Consejo de Ministros y Oficina Nacional de Gobierno Electrónico.** Plan Nacional de Gobierno Electrónico 2013-2017. *Plan Nacional de Gobierno Electrónico 2013-2017.* Lima, Peru : s.n., 2013.

6. **Presidencia de Consejo de Ministros.** Resolución Ministerial N° 374-2010-PCM. *Aprobar directiva N° 002-2010-PCM/SGP.* Lima : El Peruano, 14 de diciembre de 2010.

7. **Estado Peruano.** LEY Nº 27972. *Ley Orgánica de Municipalidades .* Lima : s.n., 27 de mayo de 2003.

8. **Presidencia de Consejo de Ministros y Oficina Nacional de Gobierno Electrónico.** Norma Técnica Peruana NTP-ISO/IEC 27001:2014. *Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.* Lima : s.n., 20 de noviembre de 2014.

9. **ISO/IEC.** *Information technology — Security techniques — Information security - management systems — Requirements.* 2005.

10. **Presidencia del Consejo de Ministros.** *Acceso a la Información Pública.* Lima, Perú : s.n., 2015.

11. **Estado Peruano.** Ley N° 27444. *Ley de Procedimiento Administrativo General.* Lima : s.n., 10 de abril del 2001.

12. **ISOTools Excellence,.** Blog especializado en Sistemas de Gestión de Seguridad de la Información. [En línea] 2015. [Citado el: 10 de abril de 2018.] https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/.

13. **ISO/IEC.** *ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology Security.* 2004.

14. **UNE.** *Metodología de análisis y gestión de riesgos para los sistemas de información.* 2008.

15. **ISO/IEC.** *Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems.* 2006.

16. **ISO/IEC**. *Risk management -- Vocabulary.* s.l. : ISO/IEC, 2002.

17. **UNE-ISO.** *Gestión del riesgo. Vocabulario.* 2010. UNE-ISO GUIA 73:2010 IN.

18. **Gobierno de España.** *MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid- España : Gobierno de España, 2012. 630-12-171-8.

19. **Hugo Sánchez Carlessi y Carlos Reyes Meza.** *Metodología y diseños en la investigación cientifica.* Lima : Editorial Visión Universitaria, 2009.

20. **Dr. Roberto Hernández.** *METODOLOGÍA DE LA INVESTIGACIÒN.* MEXICO : McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V., 2010. 978-607-15-0291-9.

21. **Zósimo David Anglas Urdánegui.** SEMINARIO DE TESIS II. *SEMINARIO DE TESIS II.* Huancayo : Universidad Continental, 2017. ISBN electrónico N.° 978-612-4196.

22. **ISO/IEC 2013 y INDECOPI 2014.** TECNOLOGÍA DE LA INFORMACIÓN. *Tecnicas de Seguridad. Sistemas de Gestion de Seguridad de la Información. Requisitos.* Lima, perú : Indecopi, 20 de noviembre de 2014. Vol. 2da Edición.

23. **Bird, Katie.** https://www.iso.org/news/ref2228.htm. *ISO.* [En línea] Organización Internacional para la Estandarización, 4 de octubre de 2017. [Citado el: 10 de abril de 2018.] https://www.iso.org/news/ref2228.htm.

24. **ASOCIADOS, SOA CAMACHO &.** *INFORME DE AUDITORIA FINANCIERA EXTERNA 2017.* HUANCAYO : s.n., 2017.

25. **ISO/IEC.** *Information technology -- Security techniques -- Information security incident management.* 2004. ISO/IEC TR 18044:2004.

26. **IT Governance Institute.** *Information Security Governance: Guidance for Boards of Directors and Executive Management.* EE.UU : Gobierno de EEUU, 2006.

27. **M. Farias-Elinos, M. C, Mendoza-Diaz y L. Gómez-Velazco.** *Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática.* s.l. : Information Society book series, 2003.

28. **Presidencia del Consejo de Ministros y Oficina Nacional de Gobierno Electrónico.** http://slideplayer.es/slide/3933475/. *Slider Player.* [En línea] 2016. [Citado el: 10 de Abril de 2018.]

ANEXOS

ANEXO N° 1
ACTA DE VISITA AL DATA CENTER

Lugar: MUNICIPALIDAD PROVINCIAL DE HUANCAYO

Fecha: 15/05/2018

Responsable: Roberto Luis Tejada Farfán

Cargo: Subgerente de Tecnología de Información y Comunicación

CRITERIO	SI	NO	N/A	COMENTARIO
NORMATIVA				
Se cuenta con una normativa interna que les permita regular el acceso al Data Center		X		
Se cuenta con un Plan de Mantenimiento que contenga los equipos críticos del Data Center	X			
Se cuenta con normativa interna que permita la manipulación de los equipos del Data Center		X		
CONTINUIDAD DE NEGOCIO				
Cuentan con el Plan de Recuperación de Servicios de TI actualizada impresa en físico	X			Cuenta con un Plan de Contingencia de Servicios de TI que hace las veces
Cuentan con un mapa de red	X			
Cuentan con un mapa del tendido eléctrico		X		
Implementaron una política de reemplazo de personal	X			Si bien no es una Política, existe un designación formal, en la cual se señala que el responsable directo es el Subgerente de Tecnologías de la Información y Comunicaciones- El Ing. Roberto Luis Tejada Farfán, y reemplazo el Ing. Raúl Surichaqui.
Señaléticas en los lugares específicos	X			
Extintores con fecha de caducidad vigente		X		

CRITERIO	SI	NO	N/A	COMENTARIO
Sensores de humo	X			
Luces de emergencia		X		
Sabe que hacer en caso de incendio	X			
Sabe que hacer en caso de daños al Data Center	X			Se ha verificado la existencia de un Plan de Contingencia, en cual señala 6 escenarios y sus posibles acciones en caso de ocurrencia.
Cuenta con el directorio de sus principales proveedores	X			
Cuenta con equipos de reemplazo en caso de falla	X			Se necesita verificar en su plan de contingencia
Línea de Contingencia			X	No cuenta con servicios críticos.
SEGURIDAD FÍSICA				
El piso falso es a prueba de fuego			X	
Tienen conocimiento de la ductería que va por debajo del piso falso o alrededor		X		
Está en buen estado la ductería que va por debajo del piso falso o alrededor		X		
Cada línea eléctrica, telefónica o lógica está claramente identificada	X			
Se cuenta con detectores de humedad		X		La zona no está expuesta a filtraciones de agua
Funcionan correctamente los detectores de humedad			X	
Funciona correctamente éste sistema de detección de incendios			X	
Cuenta con sistema de extinción de incendios	X			Extintores ubicados en la parte exterior del data center
Funciona correctamente éste sistema de extinción de incendios			X	
Cámaras de seguridad		X		No se ha verificado

CRITERIO	SI	NO	N/A	COMENTARIO
Sensores de movimiento	X			
Se tiene un tablero eléctrico independiente para el Data Center	X			
Desde éste tablero se puede cortar el flujo de potencia	X			
Este tablero eléctrico se encuentra dentro del Data Center	X			
Las líneas de potencia están estabilizadas	X			
La capacidad del estabilizador es la adecuada para la necesidades del Data Center	X			
Se realiza el mantenimiento periódicamente del estabilizador	X			
Las líneas de potencia están conectadas a pozo a tierra		X		No se ha determinado si el pozo a tierra es de la línea comercial o estabilizada.
La capacidad del poza a tierra es la adecuada para las necesidades del Data Center				
Se realiza periódicamente mantenimiento del pozo a tierra			X	Hace un mes se ha implementado
Se cuenta con respaldo de energía eléctrica	X			UPS
El Grupo electrógeno cuenta con la capacidad necesaria para la alimentación de energía a la que esta expuesta		X		En caso de haber fluido eléctrico se esperara hasta el retorno. Sin embargo no se observo la instalación de luces de emergencia o cualquier otro artefacto que les permita visualizar ante la usencia del fluido eléctrico.
Se realiza mantenimiento periódico del grupo electrógeno			X	
Se tiene unidad de potencia ininterrumpida (UPS)	X			
La cantidad y capacidad de UPS abastece las necesidades del Data Center				
Se realiza el mantenimiento periódico de los UPS	X			

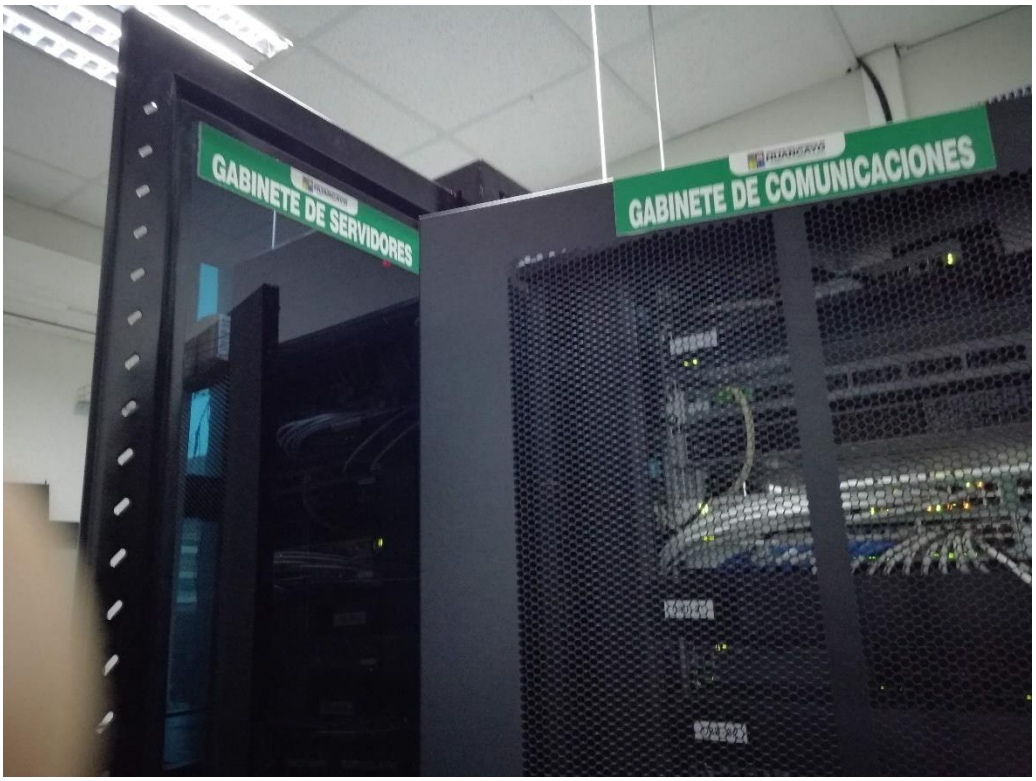
CRITERIO	SI	NO	N/A	COMENTARIO
Se tiene instalado supresor de transientes		X		
Al capacidad del supresor de transientes justifica las necesidades del Data Center			X	
Se realiza el mantenimiento periódico de los supresores de transientes			X	
MEDIO AMBIENTE				
Se cuenta con un sistema central de aire acondicionado	X			
Este sistema es de aireación plena	X			
Se cuenta con equipos de aire acondicionado	X			
El tablero de comando de estos equipos está dentro del Data Center	X			SI pero necesita etiquetar
Se realiza el mantenimiento de los equipos de aire acondicionado	X			
Se cuenta con un dispositivo que mantenga automáticamente un nivel recomendado de temperatura	X			
Funciona correctamente éste dispositivo	X			
Se registra diariamente la temperatura ambiente		X		Tampoco se ha visto necesario, debido a que el panel que informa la temperatura está en la parte externa y emite un señal de alarma, también envía un mensaje al celular del responsable
La temperatura ambiente promedio no supera los 20° C	X			Durante la visita se apreció la temperatura de 17.5°
Es buena la iluminación del área	X			
Se cuida que no exista material inflamable en el Data Center		X		
Hay líquidos inflamables en el Data Center		X		
El material de los muebles y divisiones es ignifugante (resistencia al fuego)	X			
La ubicación de los muebles es buena, tal que ayuda a la protección de los cables de los equipos	X			

CRITERIO	SI	NO	N/A	COMENTARIO
Se tiene instalados extintores manuales de incendio		X		
La ubicación de cada extintor está señalizada de tal forma que permite una fácil localización		X		
Hay un letrero que indique en qué tipo de incendio y cómo usarlo		X		
CONTROL DE ACCESO				
Existe un sistema de control de acceso al Data Center	X			
El sistema de control de acceso al Data Center es manual	X			
Se registran todos los eventos de acceso, concedidos y denegados (control de visitas al Data Center)		X		Necesitan bitácoras de acceso
Dependiendo del Usuario, se define su área y horario de acceso		X		
Se cumplen a cabalidad estas restricciones		X		
Siempre que personas ajenas a la empresa visitan al Data Center, se les acompaña a todo momento durante la misma				Se desconoce
El personal de mantenimiento de equipos ingresa al Data Center	X			
Este personal está totalmente identificado		X		
FACTORES EXTERNOS				
En la vecindad hay fuentes de contaminación ambiental, como polvo, hollín, cenizas, vapores, etc.		X		
Se tienen instalados filtros que protejan al Data Center de esta contaminación ambiental			X	
El aire acondicionado está instalado de tal forma que no succiona aire contaminado	X			
En el área donde se encuentra la empresa se han registrado motines	X			
Se conocen casos de hurto en la vecindad		X		
La entidad cuenta con un aislamiento perimetral	X			Está ubicado en la parte interior en el tercer piso
El Data Center está ubicado en una zona en la que puede ser afectada por incendios forestales, inundaciones, fuertes vientos, lluvias torrenciales		X		

CRITERIO	SI	NO	N/A	COMENTARIO
Se cuenta con las medidas necesarias para disminuir los aniegos de estos eventos externos			X	
Se cuenta con seguros para disminuir el impacto en caso de daños		X		
INSTALACIONES DEPENDIENTES				
Los gabinetes externos se encuentran debidamente identificados	X			Se encuentran debidamente etiquetados y corresponden a su mapa de red.
Los gabinetes externos se encuentran ubicados en áreas adecuadas	X			
Las instalaciones de red y fluido eléctrico a los gabinetes son adecuados		X		En uno de los gabinetes se observó que el tendido eléctrico se mezcla con el tendido de red de datos
La instalación de datos de red en los ambientes de la entidad son los adecuados		X		En la mayoría de las oficinas de la entidad se observó falta de mantenimiento de las instalaciones de la red de datos.

ACCESO AL CENTRO DE DATOS

DISTRBUCIÓN DE GABINTES



SWICTH ELECTRICO

TABLERO ELECTRICO

GABIENTES EXTERNOS

ANEXO N° 2

REVISIÒN DE CODIGO FUENTE

Lugar: MUNICIPALIDAD PROVINCIAL DE HUANCAYO

Fecha: 16/05/2018

Responsable: **Roberto Luis Tejada Farfán**

Cargo: **Subgerente de Tecnología de Información y Comunicación**

Verificación realizada con: Raul Antonio Surichaqui Mari – Analista Programador

-	SI	NO	N/A	COMENTARIO
NORMATIVA				
Cuenta con una metodología formal de aplicación en el desarrollo		X		
Se cuenta con procedimientos de desarrollo		X		
DE LA SEGREGACIÒN DE FUNCIONES				
Se cuenta con un desarrollador por modulo		X		La designación de responsabilidad es pos sistema informático, el personal designado se hace cargo de la atención de incidencias, desarrollo, teste y administración de la BD
Existe un Administrador de la Base de Datos		X		
Existe un Tester de Control de Calidad de los productos desarrollados		X		
DE LA SOLICITUD DE DESARROLLO				
Existe un control de requerimientos		X		Cada requerimiento llega con un informe.
Se cuenta con una metodología de ponderación para priorizar los requerimientos de desarrollo			X	Los requerimientos o cambios solicitados no superan los 5 por año.
Existe un procedimiento definido para aceptar, mejorar o rechazar los requerimientos		X		
Se realiza el análisis de impacto del requerimiento a nivel de procesos y a nivel técnico		X		
Se contrasta que los requerimientos estén relacionados con los objetivos de la entidad, o con las normas del estado.		X		Se sobreentiende que el informe brinda toda la información necesaria
DEL DESARROLLO				

-	SI	NO	N/A	COMENTARIO
Se lleva control de las versiones, y asi asegurar de que se esté usando los objetos del aplicativo o BD de la ultima versión			X	Al tener un solo responsable el control de cambios de objetos del aplicativo y base de datos los realiza el responsable.
Existe un estándar de diseño de formularios		X		
Se establecido un estándar de codificación o identificación de formularios		X		
Se ha definido las formas de usos de variables, objetos, funciones, entre otros.		X		
DE LAS PRUEBAS DE USUARIO				
Se ha definido el procedimiento para la ejecución de pruebas de usuario		X		
Se ha definido la cantidad de veces que puede ser devuelto el producto y al mismo tiempo mejorado o modificado		X		
DE LA PUESTA EN PRODUCCIÒN				
Se cuenta con un control de versionamiento			X	Al tener un solo responsable el control de cambios de objetos del aplicativo y base de datos los realiza el responsable.
Existe sustento de aprobación del usuario del requerimiento		X		
Los manuales de usuario están actualizados		X		
Se actualiza el diccionario de la BD		X		
1. Verificación aleatoria de formularios del Portal de Caja				
Cuenta con la identificación respectiva		X		
Presenta Código duro		X		
Cumple los estándares definidos por la entidad			X	No tienen estándares formalizados
Presenta Código comentado		X		
Cuenta con el identado respectivo	X			