UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN

Escuela de Posgrado

MAESTRÍA EN INGENIERÍA DE SISTEMAS E INFORMÁTICA - ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

MODELO PARA LA VALORACIÓN DE ACTIVOS DE INFORMACIÓN BASADO EN LAS NORMAS ISO 27000

TESIS

PRESENTADA POR:

JAIME FREDDY POLAR FUENTES

Para optar el Grado Académico de:

MAESTRO EN CIENCIAS (*MAGISTER SCIENTIAE*) CON MENCIÓN EN INGENIERÍA DE SISTEMAS E INFORMÁTICA - ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

TACNA - PERÚ

2021

UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN

Escuela de Posgrado

MAESTRÍA EN INGENIERÍA DE SISTEMAS E INFORMÁTICA – ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

MODELO PARA LA VALORACIÓN DE ACTIVOS DE INFORMACIÓN BASADO EN LAS NORMAS ISO 27000

Tesis sustentada y aprobada el 27 de noviembre de 2020; estando el jurado calificador integrado por:

PRESIDENTE : .....
Dra. Karin Yaneth Supo Gavancho

SECRETARIO : .....
M.Sc. Edgar Aurelio Taya Acosta

MIEMBRO : .....
Mgr. Gianfranco Alexey Málaga Tejada

ASESOR : .....
Mgr. Gianfranco Alexey Málaga Tejada

Dedicatoria y agradecimientos

Todo esfuerzo tiene un objetivo,
lograr la felicidad de quienes nos rodean.

Dedicado a mis padres Rodolfo y Teresa;
a mis hijos: María Alejandra, Santiago y Gianella,
y a mi familia, que siempre se mantiene unida.

Los amo.

Mi gratitud a los expertos en seguridad de la información que evaluaron mi trabajo e hicieron importantes aportes, permitiendo que esta investigación se convierta en una herramienta útil, de mayor alcance y aplicabilidad.

Agradezco también el constante apoyo de mis colegas de la Escuela Profesional de Ingeniería en Informática y Sistemas de la UNJBG.

CONTENIDO

Resumen

La norma ISO/IEC 27001:2013 utilizada para la certificación en seguridad de la información, establece que la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de una organización, está influenciado por las necesidades de la organización, sus objetivos, requisitos de seguridad y los procesos organizativos utilizados, cualquiera sea su tipo, tamaño o naturaleza; en Perú, la adopción obligatoria de un SGSI fue propuesto con carácter de Ley, hace 16 años, con 6 Resoluciones Ministeriales, renovando la obligatoriedad de esta normativa y sin éxito alguno. Sin duda la integración de los procesos de la organización y el SGSI, requieren de una planificación que determinen la comprensión de la organización y la valoración de los activos de información a resguardar con una adecuada gestión del riesgo, en el establecimiento de controles compatibles con la dirección estratégica de la organización y cuya inversión esté justificada. La investigación concluye con la propuesta de un modelo para la valoración de activos de información adecuable a toda organización, utilizado con éxito por el investigador y evaluado por expertos en seguridad de la información. El modelo cuenta con herramientas de apoyo descritas en este trabajo.

Palabras clave: Seguridad de la Información, Valoración de Activos de Información y Modelo de Valoración.

Abstract

The ISO / IEC 27001:2013 standard detects the certification in information security, sets up the implementation of the Information Security Management System (ISMS) of an organization, is influenced by the needs of the organization its objectives, security requirements and the organizational processes used, whatever its type, size or nature, in Peru, the mandatory adoption of an ISMS was proposed as a law 16 years ago, with 6 Ministerial Resolutions renewing the obligation of these regulations and without any success. Undoubtedly, the integration of the processes of the organization and ISMS, the organization of a planning that determines the understanding of the organization and the evaluation of the information assets to protect with an adequate risk management, in the establishment of compatible controls with the strategic management of the organization and our investment we are justified. The investigation concludes with the proposal of a model for the evaluation of appropriate information assets to any organization, used successfully by the researcher and evaluated by experts in information security. The model has support tools described in this work.

Keywords: Information Security, Valuation of Information Assets, Valuation Model.

INTRODUCCIÓN

La información se constituye en uno de los activos más importantes para la organización a la que pertenece, su caracterización es variada y de mucha importancia, como la almacenada en documentos o en sistemas de información, las capacidades o conocimiento de los trabajadores o la satisfacción del cliente, y, por esta razón, existen numerosos intentos por valorar y buscar la exactitud de su medida.

La seguridad de la información tiene como fin la protección de la información, del acceso, uso, divulgación, interrupción o destrucción no autorizada, y está basada en la confidencialidad, integridad y disponibilidad de la información, independiente de la forma.

La gestión de la seguridad de información, es un proceso de mejora continua, considerado en la aplicación de este modelo, que busca determinar de forma gradual la valoración de los activos de información de la organización, utilizando una encuesta estructurada para una entrevista guiada, cuyos resultados se consolidarán en una matriz de inventario de activos de información, con valores de riesgo inherente o residual, según cómo se aplique. El modelo propuesto está desarrollado de acuerdo con los criterios normados en seguridad de la información, tomando como base la familia de normas del ISO 27000.

A juicios de expertos, se determina la efectividad del modelo propuesto a través de una guía para la valoración de activos de información y herramientas de apoyo, utilizando hojas de cálculo; además, del método de entrevistas guiadas para el proceso de concientización; como parte del plan de seguridad de la información, este modelo fue también puesto en práctica por el investigador con notable éxito.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DEL PROBLEMA.

El 23 de julio de 2004, se publica en el diario oficial El Peruano, la Resolución Ministerial N°224-2004-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2004, en todas las Entidades integrantes del Sistema Nacional de Informática; estableciéndose un plazo de dieciocho (18) meses para su implantación, es decir, hasta enero de 2006 (Presidencia del Concejo de Ministros, 2004). Con la R. M. N° 395-2005-PCM se modifica los plazos para su implementación, extendiendo su cumplimiento a un plazo que no exceda el 30 de junio de 2006, debiendo considerarse en los respectivos Planes Operativos Informáticos (POI), las actividades necesarias para esta finalidad. (Presidencia del Concejo de Ministros, 2005)

En las siguientes cuatro Resoluciones Ministeriales, publicadas en el diario oficial El Peruano: R. M. N° 246-2007-PCM, R. M. N° 197-2011-PCM, R. M. N° 129-2012-PCM y R. M. N° 004-2016-PCM; se deroga la norma anterior, se actualiza y es nuevamente publicada con carácter de cumplimiento obligatorio y en un plazo definido; que no se logra cumplir (Centro de Desarrollo Industrial, 2018). La última y actual norma publicada el 08 de enero de 2016: Resolución Ministerial Nº 004-2016-PCM, establece a similitud de las anteriores, un plazo máximo de dos (2) años para la implementación y/o adecuación de la norma, es decir, hasta enero de 2018. (Presidencia del Concejo de Ministros, 2016)

Han pasado 16 años desde que se solicitó por primera vez, como ley y con carácter de obligatorio, la implementación de controles en seguridad de la información a todas las entidades integrantes del Sistema Nacional de Informática en el Perú, los resultados hasta ahora (primer trimestre de 2020)

están muy lejos de lo establecido en dichas resoluciones, y el no cumplimiento de estas resoluciones, se debe a la falta de herramientas idóneas que permitan implementar las normativas dispuestas en seguridad de la información. No solo se está incurriendo en una reiterada omisión a la ley, sino que también, como instituciones, se demuestra no tener la madurez que las normas ISO sugieren a todas las organizaciones para el aseguramiento de la información.

1.2. FORMULACIÓN DEL PROBLEMA

La información son los activos más importantes para las organizaciones a la que pertenece (Solarte, Enríquez & Benavides, 2015); hay activos a tener en cuenta en todos los casos de toma de decisiones estratégicas, como las capacidades de los trabajadores, el conocimiento humano o la satisfacción del cliente, y es por esta razón que existen numerosos intentos de valorar y buscar la exactitud de su medida (Álvarez, 2010, p.32).

¿Cómo se identifica, clasifica y valora la información, de acuerdo a las normativas en seguridad de la información?

1.3. JUSTIFICACIÓN E IMPORTANCIA

Se ha tenido la experiencia de trabajar en la implementación de controles para Sistemas de Gestión de Seguridad de la Información (SGSI) y en Gestión del Riesgo de Información, para entidades financieras, desde el 2006, y en marzo de 2017, se asumió el reto de identificar, clasificar y valorar la información de una importante entidad financiera, cumpliendo con requerimientos específicos solicitados por la Superintendencia de Banca, Seguros y AFP (SBS), a través de la Circular N° G-140-2009 Gestión de la seguridad de la información. (SBS Circular N° G-140, 2009).

En la etapa de investigación, revisión de normas, procedimientos, programas de software, tesis, entre otros, se encontró que no existen metodologías que permitan una correcta identificación de los activos de información; la información existente se reduce a encuestas abiertas, inspecciones, observaciones, listas de chequeo, técnicas de auditoría y hasta la utilización de la matriz FODA; nada de lo encontrado cubre las exigencias, tomando como base las Normas de la Organización Internacional para la Estandarización (ISO) en seguridad de la información.

Este trabajo presenta un modelo que facilita la valoración de los activos de información, basado en las normas de la familia ISO 27000; recogiendo nuestra experiencia laboral, investigaciones empleadas, herramientas creadas y estudios complementarios, para proponer un arquetipo útil, escalable y de fácil uso, para quienes estén involucrados en este camino de la seguridad de la información y aplicable a todo tipo de organización, cualquiera sea su tipo, tamaño o naturaleza.

1.4. ALCANCES Y LIMITACIONES

El modelo de valoración de activos de información propuesto, permitirá que su aplicación sea fácil y sencilla, pero no rápida, ya que implica la participación de toda la organización. Su aplicación requiere del conocimiento de las normas de seguridad de la información y concluye con la identificación de los activos de información críticos en una matriz de inventario de activos de información; este modelo no considera, la evaluación de riesgos.

La implementación de políticas de seguridad de la información, está en relación directa al compromiso de la alta dirección de la organización.

El modelo de valoración de activos de información propuesto, contempla su aplicación sin distinciones: geográfica, cultural, temporal o de tamaño organizacional, dado que está basado en las normas ISO en materia de

seguridad de la información. Sin embargo, hay limitaciones de uso que debemos considerar:

- La organización debe tener un grado de madurez acorde a la implementación de un Sistema de Gestión de Seguridad de la Información.

- Es de importancia contar con un inventario de procesos de toda la organización, se recomienda la aplicación de la norma ISO/TR 10013:2001(es) “Directrices para la documentación de sistemas de gestión de calidad”.

- Es recomendable y usual, que el área de Desarrollo Organizacional cuente con un inventario de documentos normativos como: Planes, Políticas, Procedimientos, Guías, Manuales, Perfiles, Reglamentos, etc., los mismos que de estar correctamente identificados, deben ser incluidos en la matriz de inventario de modo directo y no a través de la encuesta, evitando así duplicidad de data, salvo aquellos que sean críticos y que deberán ser reevaluados por sus propietarios para una valoración más acertada.

1.5. OBJETIVOS

1.5.1. Objetivo general

Diseñar un modelo para la valoración de los activos de información, basado en los requerimientos de las normas internacionales ISO de la familia 27000.

1.5.2. Objetivos específicos

Identificar y caracterizar los activos de información críticos de una organización.

Clasificar los activos de información según su tratamiento y el alcance que tiene para la organización.

Valorar los activos de información de acuerdo con los criterios normados en seguridad de la información.

1.6. HIPÓTESIS

Hernández Sampieri, explica que no en todas las investigaciones cuantitativas se plantean hipótesis y de acuerdo al propósito básico de estudio, los planteamientos cuantitativos generalmente se orientan a explorar o describir conceptos, o bien a relacionarlos o compararlos; cuando se vinculan conceptos o variables, el lenguaje usado debe asociarse con una finalidad deductiva para probar teorías o hipótesis, y cuando se orientan a explorar o describir, sin pronosticar un hecho o dato, no se formulan hipótesis (Hernández, Fernández & Baptista, 2014, p.104, p.48).

La presente investigación es de alcance descriptivo y propone un modelo que permita una adecuada valoración de los activos de información en una organización, por tanto, carece de hipótesis.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DEL ESTUDIO

La obligatoriedad de la Norma Técnica Peruana en materia de seguridad de la información, abarca a todas las Entidades integrantes del Sistema Nacional de Informática, solamente están exoneradas de su implementación las entidades públicas que cuenten con la certificación ISO 27001. (Presidencia del Concejo de Ministros, 2016, Art.3)

El Centro de Desarrollo Industrial (CDI) de la Sociedad Nacional de Industrias, registró hasta el 2018 a INDECOPI como la única entidad que había obtenido la acreditación en ISO 27001:2005 en el Perú, con fecha 17 de abril de 2013, certificación actualmente caducada (Centro de Desarrollo Industrial, 2018); luego en diciembre de 2018, el CDI reconoce la Certificación ISO 27001:2014 a la Superintendencia Nacional de Migraciones (MIGRACIONES) para el proceso de Emisión del Pasaporte Electrónico; actualmente, Migraciones es la única entidad del Estado con certificación vigente para el proceso de emisión de pasaporte electrónico. (Superintendencia Nacional de Migraciones, 2018)

2.1.1. Sistema Nacional de Informática

Creado mediante Decreto Legislativo Nº 604 del 30 de abril de 1990, tiene por finalidad planificar, dirigir, normar y organizar las actividades y proyectos que en materia de Informática realizan las entidades de la Administración Pública, todo ello, de manera articulada con otros sistemas y áreas de la Administración Pública. (Secretaría de Gobierno Digital, 2019). Ver también Anexo II.

2.2. BASES TEÓRICAS

- Resolución Ministerial N° 224-2004-PCM del 23 de julio de 2004, establece un plazo de dieciocho (18) meses para la implantación 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. 1º Edición", en todas las Entidades integrantes del Sistema Nacional de Informática. (Presidencia del Concejo de Ministros, 2004).

- Resolución Ministerial N° 395-2005-PCM del 08 de noviembre de 2005, modifica los plazos para la implementación de la Norma Técnica Peruana cuyo uso obligatorio se aprobó mediante la R.M. N° 224-2004-PCM extendiendo su cumplimiento a un plazo que no exceda el 30 de junio de 2006, debiendo considerarse en los respectivos Planes Operativos Informáticos (POI) las actividades necesarias para esta finalidad. (Presidencia del Concejo de Ministros, 2005).

- Resolución Ministerial N° 246-2007-PCM del 22 de agosto de 2007, señala que la norma se aplicará a partir del día siguiente de su publicación, debiendo las Entidades integrantes del Sistema Nacional de Informática, considerar las actividades necesarias en sus respectivos Planes Operativos Informáticos (POI), para la implantación 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". (Presidencia del Concejo de Ministros, 2007).

- Resolución Ministerial Nº 197-2011-PCM del 14 de julio de 2011, establece como fecha límite el 31 de diciembre de 2012, para que las entidades de la Administración Pública, listadas en la misma resolución, 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", aprobada mediante R.M. Nº246-2007-PCM. (Presidencia del Concejo de Ministros, 2011).

- Resolución Ministerial Nº 129-2012-PCM del 23 de mayo de 2012, establece que la implementación de los Sistemas de Seguridad de la Información, en las entidades integrantes del Sistema Nacional de Informática, deberá empezar con la aplicación 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", cuyos controles deberán ser implementados de acuerdo a las recomendaciones 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", dispuesto por la Resolución Ministerial Nº 246-2007-PCM.

Esta resolución detalla, además, las entidades que deben cumplir con implementar dichos sistemas, debiendo iniciar la fase uno en un plazo no mayor a 45 días de publicada la resolución, para las demás entidades de la Administración Pública, el plazo es no mayor a 180 días calendarios. (Presidencia del Concejo de Ministros, 2012).

- Resolución Ministerial Nº 004-2016-PCM del 08 de enero de 2016, actualmente vigente. Aprueba 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" y establece un plazo máximo de dos (2) años para la implementación y/o adecuación de dicha norma. Señala, además, que la responsabilidad de la implementación de la presente norma es del titular de cada entidad. (Presidencia del Concejo de Ministros, 2016).

- Resolución Ministerial Nº 166-2017-PCM del 20 de junio de 2017, modifica el artículo 5 de la R.M. N°004-2016-PCM, sobre el Comité de Gestión de Seguridad de la Información; sobre las funciones del Comité; la priorización del alcance del SGSI; y sobre el Oficial de Seguridad de la Información. (Presidencia del Concejo de Ministros, 2017).

- Resolución Ministerial Nº 087-2019-PCM del 19 de marzo de 2019, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital en cada entidad de la Administración Pública, y que, en su artículo tercero, dispone un plazo no mayor a diez (10) días para transferir al Comité de Gobierno Digital de la entidad, la documentación generada en el marco de la implementación del SGSI, establecida en la R.M. N°004-2016-PCM. (Presidencia del Concejo de Ministros, 2019).

- Circular N° G-140-2009 Gestión de la seguridad de la información. Norma para su cumplimiento con un plazo de adecuación hasta el 31 de marzo de 2010 para todas las Entidades comprendidas en la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros (SBS Circular N° G-140, 2009).

Esta norma en el ítem 5.4 Inventario de activos y clasificación de la información, establece:

a) Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.

b) Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

- NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición, (INDECOPI, 2014).

Esta Norma Técnica Peruana, especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI (Sistema de Gestión de Seguridad de la Información) según las necesidades y tamaño de la organización.

Esta norma destina un dominio completo a la Gestión de Activos, a su identificación, inventario, definición de responsabilidades de protección apropiadas, propiedad de los activos, al uso aceptable y retorno de los mismos, y a la clasificación de la información, asegurando que ésta reciba un nivel apropiado de protección en concordancia con su importancia para la organización.

Entre los controles que esta norma señala, encontramos:

A.8.2.1 La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.

A.8.2.2 Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.

- ISO/IEC 27000:2014 3ra Edición del 15 de enero de 2014. Proporciona una descripción general de los SGSI (sistemas de gestión de seguridad de la información), y los términos y definiciones que se utilizan comúnmente en la familia de normas del SGSI. Su aplicación se recomienda a todos los tipos y tamaños de organizaciones como entidades financieras, entidades gubernamentales, empresas comerciales, organizaciones sin fines de lucro, etc. La norma 27000 define los términos a aplicar en cuanto a la seguridad de la información. (ISO/IEC 27000, 2014)

- ISO/IEC 27001:2013 2da Edición de septiembre de 2013. Contiene un anexo que resume los controles de ISO 27002:2005, fue publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información; esta es la norma que se certifica por auditores externos del SGSI de las organizaciones. En esta investigación buscamos cumplir con lo indicado en las cláusulas A.7.1.1, A.7.1.2, inventario y propiedad de los activos correspondientes a la gestión, y responsabilidad por los activos. (ISO/IEC 27001, 2013)

- ISO/IEC 27002:2013 2da Edición de septiembre de 2013. Con un total de 14 Dominios, 35 Objetivos de Control y 114 Controles, es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información; en este estudio nos enfocamos en la cláusula 8.1.1 Inventario de Activos. (ISO/IEC 27002, 2013)

- ISO/IEC 27005:2011 2da Edición de junio de 2011. Orientada a la gestión del riesgo de la seguridad de la información, como complemento al ISO/IEC 27002 y conceptos especificados en el ISO/IEC 27001. La norma ISO/IEC 27005, basada en un enfoque de gestión de riesgos, determina (ítem 8.2.2) la identificación de activos, a un nivel de detalle adecuado para la posterior evaluación de riesgos. (ISO/IEC 27005, 2011)

Como complemento, esta norma cuenta con el Anexo B que describe la identificación y valoración de los activos, distinguiendo dos importantes grupos de activos: Activos Primarios, que comprende las actividades, procesos del negocio y a la información, y Activos de Soporte, en el que se basan los activos primarios. El ISO 27005 es de suma importancia para la identificación y descripción de los activos de información.

2.3. DEFINICIÓN DE TÉRMINOS

Un activo de información no es aquel elemento que contiene o manipula información, como servidores, bases de datos, correos electrónicos, documentos archivados, computadores, etc. La norma ISO 27005 identifica a los activos organizándolos en activos primarios (procesos e información) y activos de soporte (aquellos que contienen a la información).

Para evitar errores de conceptualización como las encontradas en el proceso de investigación, este trabajo utiliza definiciones basadas principalmente en la norma ISO 27000:2014.

- **Activo,** cualquier cosa que tenga valor para la organización, y por tanto requiere de un nivel de protección adecuado.

- **Activo de Información,** cualquier forma de registro que tenga valor para la organización, susceptible de ser procesada, distribuida y almacenada.

- **Activo de Información Crítico,** aquel activo que tiene valores altos a nivel confidencialidad, integridad y disponibilidad.

- **Autenticación,** garantía de que una característica reivindicada de una entidad es correcta

- **Autenticidad,** propiedad que una entidad es lo que se dice ser.

- **Caracterizar,** presentar o describir una cosa con sus rasgos característicos de manera que resulte inconfundible.

- **Confidencialidad,** propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.

- **Disponibilidad,** propiedad de ser accesible y utilizable a pedido de una entidad autorizada.

- **Datos,** recopilación de valores asignados a medidas de base, medidas derivadas y/o indicadores.

- **Fungible,** que se consume con el uso, que es sustituible.

- **Impacto,** es la consecuencia o consecuencias que podría tener un riesgo, expresado ya sea en términos cualitativos o cuantitativos.

- **Información,** cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible a ser procesada, distribuida y almacenada.

- **Integridad,** propiedad de salvaguardar la exactitud e integridad de los activos.

- **ISO/IEC, ISO,** acrónimo de "*International Organization for Standardization"*, Organización Internacional para la Estandarización, es el organismo que imparte los documentos que especifican requerimientos que pueden ser empleados en organizaciones para garantizar que los productos o servicios ofrecidos por dichas organizaciones cumplen con su objetivo. IEC: acrónimo de *"International Electrotechnical Commission"*, Comisión Electrotécnica Internacional, interviene en los campos: eléctrico, electrónico y tecnologías relacionadas. (http://www.iso.org/).

- **Nivel de Riesgo,** es el grado en que la probabilidad y el impacto de un evento afecta sobre los objetivos de la empresa.

- **Método,** modo de obrar o hacer con orden, procedimiento que se sigue en las ciencias para hallar la verdad o enseñarla. (https://dle.rae.es)

- **Metodología,** ciencia o estudio del método, conjunto de métodos que se siguen en una investigación científica o exposición doctrinal. (https://dle.rae.es)

- **Modelo,** arquetipo o punto de referencia para imitarlo o reproducirlo (https://dle.rae.es)

- **Propietario,** el término propietario de los activos de información define al responsable del activo y cuentan con la aprobación de la alta dirección para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información. El término propietario no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

- **Riesgo Inherente,** es el riesgo identificado y evaluado sin controles establecidos, es la exposición absoluta y pura.

- **Riesgo Residual,** es el riesgo resultante de la aplicación de controles y por tanto es el riesgo para asumir y administrar.

- **Seguridad de la Información,** característica que implica la adecuada combinación de políticas, procedimientos, estructura organizacional y

herramientas informáticas especializadas a efectos de que la información cumpla los criterios de confidencialidad, integridad y disponibilidad, además de involucrar propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

- **Sistema de Gestión de Seguridad de la Información, SGSI,** parte del sistema gerencial general, basada en un enfoque de riesgo, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos.

- **Valoración,** acción y efecto de valorar. (https://dle.rae.es)

- **Valorar,** reconocer, estimar o apreciar el valor de algo. (https://dle.rae.es)

- **Valorizar,** aumentar el valor de algo. (https://dle.rae.es)

CAPÍTULO III

MARCO METODOLÓGICO

La investigación propone un modelo para determinar el valor de los activos de información en cualquier organización, cumpliendo con los requerimientos de las normas internacionales ISO de la familia 27000; el modelo nace de los años de experiencia, trabajos de investigación y estudios complementarios realizados y, es precisamente, en la revisión de las normativas existentes y en las carencias en el cumplimiento de estas normas, el origen a la recolección de información para el desarrollo de este trabajo de investigación.

3.1. TIPO Y DISEÑO DE LA INVESTIGACIÓN

La investigación es no experimental ya que no manipula variables, y de tipo transversal debido a que apunta a un momento y tiempo definido, no estudia la evolución de alguna variable, ni los cambios a través del tiempo. (Hernández, Fernández & Baptista, 2014, p.154).

El estudio es de tipo descriptivo-aplicado; muestra con precisión dimensiones en el contexto de la seguridad de la información y permite definir qué se medirá y sobre qué o quiénes se recolectarán los datos. (Hernández, Fernández & Baptista, 2014, p.92).

La investigación científica aplicada, propone transformar el conocimiento puro en conocimiento útil, la aplicación de los conocimientos y producción de tecnología a través de un modelo al servicio de las organizaciones. (UNJBG, 2017, p.4). El nivel aplicativo nos permite la búsqueda y consolidación del saber y la aplicación del conocimiento en la producción de un modelo dinámico, sencillo

y eficaz, que permita la valoración de los activos de información y facilite la posterior evaluación de riesgos e implantación de controles de seguridad de la información.

3.2. POBLACIÓN Y MUESTRA

La investigación documental se sirve de datos extraídos a partir del análisis, revisión e interpretación de documentos (Ramírez & Zwerg-Villegas, 2012, p.100), como se determinó líneas arriba, esta investigación no estudia la evolución de alguna variable, ni los cambios a través del tiempo; no requiere de muestra ni caso de estudio al no poder revelar los resultados de la valoración de activos de información por criterios de confidencialidad tratados en este mismo documento.

La investigación se basa en los requerimientos de las normas ISO en materia de seguridad de la información, siendo el conjunto de estas normas (familia del ISO 27000) los principales elementos de estudio y análisis.

3.3. OPERACIONALIZACIÓN DE LAS VARIABLES

Como definición conceptual y utilidad metodológica, se considerará como variable de estudio al “modelo para la valoración de activos de información”, propuesto como un nuevo instrumento para recolectar y analizar datos. El principal producto de este modelo es la “guía para la valoración de activos de información”, sobre el que se aplicará el juicio de expertos, que lo validará bajo los criterios de suficiencia, claridad, coherencia y relevancia, en la valoración de los activos de información.

Quecedo y Castaño, haciendo referencia a Taylor S. y Bogdan R. (1986), señalan que "los contextos no son reducidos a variables, sino considerados como un todo" (Quecedo & Castaño, 2003, p.7-8). Entiéndase por variable a las

propiedades de los hechos, cualidades o atributos a estudiarse que puedan modificarse o adquirir diversos valores en la investigación (Martínez, 2012, p.119).

3.4. TÉCNICAS E INSTRUMENTOS PARA LA RECOLECCIÓN DE DATOS

La investigación se basa en la adecuación de las experiencias obtenidas y herramientas creadas para identificar, caracterizar, clasificar y valorar la información de una organización, el producto final de la investigación es la Guía para la valoración de activos de información, que utiliza como herramienta principal, la encuesta de clasificación y valoración de activos de información, a desarrollar en una entrevista-taller a todos los involucrados (dueños de procesos) de la organización, siendo la encuesta el instrumento principal en la recolección de datos.

La encuesta de clasificación y valoración de activos de información, está desarrollada en una hoja de cálculo y se recomienda utilizar una laptop para facilitar los cálculos automáticos de criticidad y cuadro resumen; su aplicación es detallada en el capítulo V del presente documento.

3.5. PROCESAMIENTO Y ANÁLISIS DE DATOS

El modelo contempla la identificación, caracterización, clasificación y valoración de los activos de información, a través de una guía y herramientas complementarias, para lo cual se requerirá:

- Computadora portátil con respaldo para la información digital.
- Guía para la valoración y formatos digitales del modelo propuesto.
- Impresora y papel, para la documentación correspondiente al soporte impreso y evidencias.

- Útiles de oficina como: archivadores, files diseñados para la entrega de encuestas llenas y actas de propiedad, y otros propios al trabajo de oficina.

El tratamiento de datos no corresponde a la investigación, sino a la aplicación del modelo de valoración de activos de información y correspondiente inventario de activos de información, facilitando los consolidados estadísticos para la toma de decisiones y una adecuada gestión del riesgo, en el establecimiento de controles de seguridad de la información a los activos de mayor criticidad.

CAPÍTULO IV

MARCO FILOSÓFICO

La investigación busca compartir mi experiencia laboral y estudios complementarios, hacia la propuesta de un modelo para la valoración de los activos de información, que permita cumplir las exigencias de las normas nacionales e internacionales en seguridad de la información con transparencia, idoneidad, claridad y credibilidad, documentando las evidencias respectivas para la consolidación de información veraz, exacta y sustantiva.

Las normas ISO indican qué lograr, pero no cómo hacerlo y ahí se encuentra uno de los primeros obstáculos en la aplicación de los controles de seguridad, no se puede asegurar lo que no se conoce, ni determinar la magnitud de la inversión si no se cuenta con el valor que determinada información tiene para la organización.

Existen muchas propuestas para el desarrollo de un manual de gestión de seguridad de la información, y la correspondiente implementación de un sistema de gestión de seguridad de la información que proponen el uso de diversas herramientas como encuestas abiertas, observaciones con listas de cotejo, inspecciones, matriz FODA, aplicación de técnicas de auditoría y hasta software especializados en ISO 27001, genéricos y costosos, y que difieren a las normativas dadas en seguridad de la información y de las realidades de las organizaciones; además de no ser escalables.

El modelo propuesto permitirá una rápida definición de los activos de información con estructura, detalle y valoración aceptables, para cada área de la organización. El sustento a la data será a través de las encuestas de clasificación y valoración de activos de información, desarrolladas, impresas y firmadas por los propietarios de la información, y que irán acompañados del acta de

aceptación de propiedad, como evidencia del proceso de capacitación y concientización que las normas solicitan.

Toda esta información será plasmada en la matriz de inventario de los activos de información, que a su vez será la base para la determinación de controles de seguridad y la gestión del riesgo. Es importante mencionar que los controles nos ayudan a mitigar los riesgos, no se deben implementar controles solo por implementar, según se observa en las cláusulas 6 y 8 del ISO/IEC 27001:2013, y se debe contemplar la relación costo de implementación del control y valor del riesgo, donde la identificación y valoración del activo juega un papel importante.

CAPÍTULO V

RESULTADOS

Como resultado de la investigación se presenta la “Guía para la valoración de activos de información”, esta guía se complementa con tres herramientas básicas**:** la encuesta de clasificación y valoración de activos de información, el acta de aceptación de propiedad de activos de información y la matriz de inventario de activos de información. El primero y último desarrollados en hoja de cálculo, mientras el acta es un documento de texto a utilizar como evidencia del proceso de capacitación y concientización, contemplados en este trabajo y que las normas en seguridad de la información exigen.

Un aspecto importante a considerar antes de aplicar la guía para la valoración de activos de información, es la identificación de procesos. Es muy importante que la organización cumpla con la madurez necesaria para la implementación de los controles de seguridad y en ello se encuentra la identificación de los procesos de la organización, de los cuales extraeremos los activos de información de forma ordenada, minimizando duplicidad u omisiones.

La correcta aplicación de la guía para la valoración de activos de información, nos permitirá alcanzar: transparencia, credibilidad, idoneidad y claridad, con información veraz, exacta y sustantiva.

5.1. CONSIDERACIONES PREVIAS

Un activo de información no es aquel que contiene o manipula información, como servidores, bases de datos, correos electrónicos, documentos archivados, computadores, etc. La norma ISO 27005 identifica a los activos

organizándolos en activos primarios (procesos e información) y activos de soporte (aquellos que contienen a la información). Por esta razón partimos del inventario de procesos, para una ordenada identificación de los activos de información.

De acuerdo con la madurez de la organización, esta guía puede aplicarse para la valoración del riesgo inherente o residual; inicialmente se recomienda levantar la información de valoración de activos con riesgo inherente, para tener un inventario con el valor real de cada activo. Luego se podrá volver a aplicar a los procesos críticos o activos de mayor valor, considerando los controles ya existentes para estimar el riesgo residual.

La guía, en la aplicación de la encuesta y posterior entrega del acta de aceptación de propiedad de los activos de información, es un complemento efectivo para el proceso de concientización en seguridad de la información. La matriz de inventario de activos de información, nos permitirá identificar los activos de información más críticos para una adecuada gestión del riesgo, facilitando la selección de controles a implementar en un plan de seguridad que considere costo beneficio.

La frecuencia y la forma de uso de esta guía estará determinada por la organización y los responsables de la seguridad de la información, pudiendo por ejemplo desdoblar los procesos en macroprocesos, procesos y subprocesos, de acuerdo al tamaño o estructura de la organización.

5.2. GUÍA PARA LA VALORACIÓN DE ACTIVOS DE INFORMACIÓN

A continuación, se describen los pasos a seguir para la identificación, caracterización, clasificación y valoración de activos de información, utilizando las siguientes herramientas**:**

Formato 1. Encuesta de clasificación y valoración de activos de información

La encuesta está desarrollada en una hoja de cálculo y se recomienda sea llenada con la asistencia de un especialista del área de seguridad de la información, aunque el desarrollo de la encuesta es simple y deductivo, pudiendo ser llenada fácilmente por los propietarios de los activos de información, la asistencia del especialista en seguridad de la información, facilitará la aclaración a las preguntas relacionadas a los criterios de confidencialidad, integridad y disponibilidad, y de toda consulta relacionada al tema, pero su función principal es la capacitación y concientización en seguridad de la información que las normas solicitan.

Para facilitar los cálculos automáticos de criticidad y cuadro resumen del formato 1, se sugiere al especialista en seguridad de la información que guiará la entrevista-taller para el llenado de la encuesta, el uso de una laptop. Al finalizar el proceso las encuestas utilizadas deben ser impresas en copia doble para las firmas respectivas de conformidad y evidencia correspondiente.

Formato 2. Acta de aceptación de propiedad de los activos de información

Documento de texto que servirá como evidencia de la concientización y responsabilidades de los propietarios, sobre los activos de información.

Formato 3. Matriz de inventario de activos de información

Esta tercera herramienta consolida la información recogida en las encuestas de clasificación y valoración de activos de información, facilitando el análisis de los activos por proceso, clasificación, tipo, ubicación física y/o electrónica, valoración, propietario, custodios o usuarios, y con esta base evaluar la aplicación de los controles de seguridad que las norman nos facilitan.

5.3. CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Este punto contempla la identificación y caracterización de los activos de información, pero antes de ir a las entrevistas pactadas con los dueños de los procesos, es recomendable que se tenga el formato 1, preparado con los datos del propietario (dueño de proceso) y el cargo que éste tiene en la organización, que generalmente corresponde a gerencias o jefaturas, además del nombre del primer proceso a trabajar, así solamente se preguntará por ¿qué información está asociada a este proceso?, ¿esta información nace aquí?, ¿cómo llamaría a esta información? (nombre del activo de información), y ¿en qué se diferencia de otra información similar? (descripción de la información).

El uso de la encuesta requiere entonces, una rápida preparación del instrumento, a medida que se vayan identificando los activos de información, se irá pasando al siguiente proceso, según corresponda al cargo. En un mismo proceso se pueden identificar varios activos de información independientes.

La preparación del formato 1 requiere también que en la parte baja de la hoja de cálculo, se registre del nombre del especialista en seguridad de la información que guiará el desarrollo y llenado de la encuesta, y su respectiva identificación, así como el lugar y fecha, esta última se cargará de forma automática.

El propietario de los activos de información es el dueño del proceso, y es quien los identifica y puede agruparlos según su tratamiento, pudiendo apoyarse en todo momento en sus asistentes o custodios. El propietario de los activos de información, es el responsable del activo de información descrito y cuenta con la aprobación de la Alta Dirección para el control de la producción, desarrollo, mantenimiento, uso y seguridad, de los activos; el término propietario no significa que la persona tenga en realidad derechos de propiedad sobre el activo. (ISO/IEC 27001, 2005, p.25).

5.3.1. Identificación de activos de información

Definidos los procesos de cada cargo organizacional, uno a uno se va identificando los activos de información asociados a cada proceso. Una vez escrito el primer proceso, se empieza por identificar y describir cada activo de información asociado, pudiendo obtenerse diferentes activos para un mismo proceso; en el formato de encuesta preparado se pueden registrar hasta cinco activos diferentes; deben utilizarse tantos formatos cuantos sean necesarios.

A) Nombre del Activo de Información: Identifica al activo de información asociado al proceso indicado. Se recomienda considerar los activos de mayor criticidad, importancia y sensibilidad, identificados por el propietario o dueño del proceso.

B) Descripción: Brinda una explicación corta sobre el activo de información para su mejor entendimiento.

C) Tipo: Se refiere al tipo de activo de información, pudiendo elegir de la lista desplegable una de las siguientes opciones: Físico, Digital, Mixto o Persona.

c.1) Físico: Comprende a todos los documentos impresos, manuales, fotos, impresiones, files, folletos, banners, etc.

c.2) Digital: Corresponde a toda información contenida en equipos de cómputo, dispositivos de memoria, medios magnéticos, archivos de datos, copias de respaldo, correos electrónicos, servidores, smartphones, etc.

c.3) Mixto: Corresponde a aquella información que se encuentra en los dos formatos anteriores, **físico y digital**; su resguardo y ubicación, debe contemplar a ambos tipos de información.

c.4) Persona: Algunas actividades cognitivas o habilidades personales para el tratamiento de la información no están en un procedimiento determinado, el conocimiento único de personas “imprescindibles”, las convierten en un tipo de activo de soporte de información y procesos, ya que la ausencia de estas

personas puede representar un riesgo potencial para la continuidad del negocio. Este rubro comprende el conocimiento de las personas.

Nota. - Los tipos de activos de soporte contemplados en la norma ISO 27005, deben ser considerados en los campos de ubicación física y/o electrónica, ya que por sus vulnerabilidades son aprovechables por las amenazas que apuntan a deteriorar a los activos de información contemplados.

D) Ubicación: Contiene dos casilleros, uno para el registro de la ubicación física y el otro para la ubicación electrónica, según corresponda a la selección del tipo de activo de información definido. En estos campos se contempla las características de los activos de soporte, es decir, el lugar donde se encuentran los activos de información.

E) Clasificación de la información: Se refiere a la clasificación dada por la organización a la información, pudiendo elegir de la lista desplegable una de las siguientes opciones: Confidencial, De uso interno y Pública.

e.1) Confidencial: Información considerada crítica y que puede influir directamente en el funcionamiento de la organización; de hacerse pública afectaría las operaciones y funciones regulares de la organización, esta información que está restringida a alta dirección, gerencias, jefaturas o personal autorizado bajo criterios de confidencialidad. La copia o eliminación de esta información debe ser comunicada a su propietario, el grado de seguridad y resguardo es alto. Por ejemplo: actas de directorio, actas de comité de gerencia, planes de negocio, información de operaciones, registros contables.

e.2) De uso interno: Información de importancia al ámbito de quien la genera y a quien éste autorice para su conocimiento, revisión o uso. Esta información que no está aprobada para ser circulada fuera del ámbito de la organización, está restringida al propietario de la información y a las instancias superiores según corresponda. El grado de seguridad y resguardo es controlado, su difusión puede generar inconvenientes para la institución o su propia administración, pero sin llegar a ser causa de pérdidas financieras o daño mayor. Por ejemplo:

procedimientos, planes, proyectos, actas de reuniones, diseños, normas, reportes, memorandos internos, agendas de reunión, cronogramas, informes.

e.3) Pública: Todo aquello cuya difusión no impliquen repercusiones negativas para la organización y cuyo contenido sea de uso general. Su distribución es controlada pero irrestricta, se mantiene un nivel mínimo de seguridad. Por ejemplo: reportes o informes públicos, tarifarios, notas de prensa, publicidad, datos para investigaciones.

Nota. - El tipo y clasificación de la información se selecciona a través de una lista desplegable que pueden ser editados en la hoja de cálculo, los datos originales de las listas desplegables se encuentran en las siguientes celdas de la misma hoja de cálculo**:** para tipo en las celdas B32:B35 y para clasificación las celdas A32:A34.

5.3.2. Valoración de los activos de información

La valoración de los activos de información se realiza bajo los tres pilares básicos de la seguridad de la información**:** Confidencialidad, Integridad y Disponibilidad.

4	Muy alto
3	Alto
2	Medio
1	Bajo

Para valorar cada activo se responde a las preguntas utilizando la escala de 1 a 4 según su criticidad, siendo 1 un valor bajo y 4 un valor muy alto o de grave impacto. De no corresponder la pregunta al contexto del activo se deja el casillero correspondiente en blanco (vacío). Solo ha de tenerse cuidado, en que al menos una de las preguntas de cada bloque debe ser respondida.

Cada pregunta está orientada a un escenario, el valor de criticidad de cada pilar de seguridad se calcula por promedio simple, excepto las preguntas de confidencialidad 1 y 3 a las que por su impacto se les asignó un peso doble. Este valor promedio se registra en la primera línea de cada bloque, pintada de un

color más oscuro y que tiene la leyenda de “no llenar”, pues su cálculo es automático.

El valor de tasación final y correspondiente valor de criticidad para cada activo de información, se obtiene por el valor máximo de los tres pilares de seguridad y solamente cuando al menos dos de ellos tienen como valor 4 (de criticidad muy alta), se le asignará automáticamente al activo un valor 4,4 de criticidad “Extremadamente alto”.

A) Preguntas para la valoración de activos de información

Agrupadas en tres bloques, que corresponden a cada pilar de la seguridad de la información, las preguntas contemplan escenarios diferentes y se responden en una escala con valores del 1 al 4, aclarando al propietario que no debe considerar los controles ni medidas de seguridad existentes, pues valoraremos inicialmente el riesgo inherente a cada activo de información, bajo los criterios de**:**

A.1) Confidencialidad. (La información debe ser accesible solo a las personas debidamente autorizadas) ¿Cómo organización, en qué nos afecta si la información se hace pública o cae en manos de terceros?:

C.1. ¿La empresa, organización o nosotros, podríamos tener problemas legales? (Responsabilidad Legal o Regulatorio)

C.2. ¿Habría impacto negativo en nuestra reputación o en las relaciones con socios de negocios, clientes o proveedores? (Confianza del Público)

C.3. ¿Se podría generar algún tipo de estafa, operación fraudulenta o algún otro tipo de apropiación indebida? (Fraude / Robo)

C.4. ¿Podría producir disminución de ingresos, aumento de costos, o pérdida de alguna ventaja competitiva? (Costo / Efecto Colateral)

A.2) Integridad. (La información debe ser completa, exacta y válida. La información no debe estar alterada) ¿Cómo organización, en qué nos afecta si la información es incorrecta o contiene errores?:

I.1. ¿Puede generar inexactitudes en los estados financieros u otros reportes gerenciales que afecten a la empresa? (Decisiones de Negocios)

I.2. ¿Podrían ocasionar multas o incumplimiento de obligaciones legales, regulatorias o contractuales? (Responsabilidad Legal o Regulatorio)

I.3. ¿Es difícil detectar errores a corregir?, ¿puede desencadenar un siguiente error? (Impacto en el negocio / hackers)

I.4. ¿Puede ocasionar demoras en las operaciones o afectar negativamente a relaciones comerciales, de negocio o servicios? (Costo / Imagen / Efecto Colateral)

A.3) Disponibilidad. (La información debe ser fácilmente accesible en forma organizada para las personas autorizadas y cuando sea requerida) ¿Cómo organización, en qué nos afecta si la información demora o no está disponible al ser solicitada?:

D.1. ¿Podría generar multas o responsabilidades legales a la empresa? (Responsabilidad Legal o Regulatorio)

D.2. ¿Podría afectar el correcto funcionamiento de otros sistemas, procesos o servicios? [operaciones tardías] (Relaciones Comerciales / Imagen)

D.3. ¿Podría afectar a alguna función o decisión de negocio crítica u ocasionar algún tipo de estafa? (Decisiones de Negocios / Fraude)

B) Custodios y Usuarios

Finalmente, debemos detectar quiénes son los custodios y usuarios de cada activo de información. El propietario del activo puede designar uno o más

custodios para sus activos de información y debe determinar también quiénes son los usuarios de estos activos.

B.1) Custodios. Son los responsables de administrar, proteger y mantener los activos de información haciéndolos accesibles a los usuarios; asimismo, de monitorear el cumplimiento de los controles de seguridad en los activos que se encuentran bajo su custodia.

B.2) Usuarios. Son quienes tienen acceso a los activos de información, al igual que en custodios no se escribe el nombre de la persona sino el cargo o función que éstos cumplen en la organización, pudiendo incluso registrar el nombre del área organizacional usuaria del activo de información descrito.

C) Revisión

Finalmente, al llegar aquí en el formato 1, desarrollado en hoja de cálculo, se podrá apreciar al final de la encuesta, el cuadro resumen de valoración de cada activo de información, para una rápida revisión final. Cada formato permite el registro de hasta cinco activos diferentes asociados o no a un mismo proceso, se pueden utilizar tantos formatos cuantos sean necesarios, inventariando preferentemente los activos de información críticos o de mayor importancia.

Para efectos de registro y evidencia, cada encuesta desarrollada deberá ser impresa con copia, para el registro de las firmas de conformidad por el propietario de los activos de información descritos y por el especialista en seguridad de la información participante de la entrevista y llenado de la encuesta.

A continuación, se presenta el Formato 1, a utilizar en la encuesta para la clasificación y valoración de activos de información**:**

LOGO	Sistema de Gestión de la Seguridad de la Información	Formato 1
	CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN	Versión: 01
		DE USO INTERNO
		Página 1/1

Documento Base: ISO 27001:2014 (8.1, 8.2) - Como dueño del proceso usted debe completar esta encuesta sobre la información que están a su cargo.

Propietario: | **Cargo :**

	Proceso :		Tipo :		Clasificación de la Información :
A1	Nombre de Activo de Información 1 :		Ubicación :		
			Descripción :		
	Proceso :		Tipo :		Clasificación de la Información :
A2	Nombre de Activo de Información 2 :		Ubicación :		
			Descripción :		
	Proceso :		Tipo :		Clasificación de la Información :
A3	Nombre de Activo de Información 3 :		Ubicación :		
			Descripción :		
	Proceso :		Tipo :		Clasificación de la Información :
A4	Nombre de Activo de Información 4 :		Ubicación :		
			Descripción :		
	Proceso :		Tipo :		Clasificación de la Información :
A5	Nombre de Activo de Información 5 :		Ubicación :		
			Descripción :		

Responda las siguientes preguntas con un valor numérico de 1 a **4** para cada activo, según lo considere usted más adecuado.
Deje en blanco si **no** corresponde **:**

4	Muy alto
3	Alto
2	Medio
1	Bajo

Confidencialidad - La información debe ser accesible solo a las personas debidamente autorizadas. **No llenar -->**

Si la información se hace pública o cae en manos de terceros :

		A1	A2	A3	A4	A5
C.1	¿La empresa, organización o nosotros podríamos tener problemas legales? (Responsabilidad Legal o Regulatorio)					
C.2	¿Habría impacto negativo en nuestra reputación o en las relaciones con socios de negocios, clientes o proveedores? (Confianza del Público)					
C.3	¿Se podría generar algún tipo de estafa, operación fraudulenta o algún otro tipo de apropiación indebida? (Fraude / Robo)					
C.4	¿Podría producir disminución de ingresos, aumento de costos, o pérdida de alguna ventaja competitiva? (Costo / Efecto Colateral)					

Integridad - La información debe ser completa, exacta y válida. La información no debe estar alterada. **No llenar -->**

Si la información es incorrecta o contiene errores :

		A1	A2	A3	A4	A5
I.1	¿Puede generar inexactitudes en los estados financieros u otros reportes gerenciales que afecten a la empresa? (Decisiones de Negocios)					
I.2	¿Podrían ocasionar multas o incumplimiento de obligaciones legales, regulatorias o contractuales? (Responsabilidad Legal o Regulatorio)					
I.3	¿Es difícil detectar errores a corregir?, ¿puede desencadenar un siguiente error? (Impacto en el negocio / hackers)					
I.4	¿Puede ocasionar demoras en las operaciones o afectar negativamente a relaciones comerciales, de negocio o servicios? (Costo / Imagen / Efecto Colateral)					

Disponibilidad - La información debe ser fácilmente accesible en forma organizada para las personas autorizadas y cuando sea requerida. **No llenar -->**

Si la información demora o no está disponible al ser solicitada :

		A1	A2	A3	A4	A5
D.1	¿Podría generar multas o responsabilidades legales a la empresa? (Responsabilidad Legal o Regulatorio)					
D.2	¿Podría afectar el correcto funcionamiento de otros sistemas, procesos o servicios? [operaciones tardías] (Relaciones Comerciales / Imagen)					
D.3	¿Podría afectar a alguna función o decisión de negocio crítica u ocasionar algún tipo de estafa? (Decisiones de Negocios / Fraude)					

	Activo de Información	**Custodios** (cargos, con permiso para crear, modificar o mantener la información)	**Usuarios** (cargos, áreas o personas que utilizan la información)
A1			
A2			
A3			
A4			
A5			

Cuadro Resumen

	Tipo	Clasificación	Criticidad
A1			
A2			
A3			
A4			
A5			

Lugar, 11 de Marzo de 2020

Especialista en Seguridad de la Información
Jaime F. Polar Fuentes
DNI N° 00790381

Propietario de los activos de información decritos

5.4. ACTA DE ACEPTACIÓN DE PROPIEDAD DE ACTIVOS DE INFORMACIÓN

Terminada la valoración y clasificación de los activos de información, las copias impresas de las encuestas a ser entregadas al propietario de los activos, serán acompañadas del formato 2 que corresponde al Acta de Aceptación de Propiedad de Activos de Información, cuyos datos deberán ser debidamente llenados e impreso con copia para el archivo, para la firma respectiva del propietario de los activos de información, cumpliendo de esta forma con las evidencias que las normas requieren.

LOGO	Sistema de Gestión de la Seguridad de la Información	Formato 2
	ACTA DE ACEPTACIÓN DE PROPIEDAD DE ACTIVOS DE INFORMACIÓN	Versión: 01
		DE USO INTERNO
		Página 1/1

Yo, _____ identificado con DNI N° _____, en cumplimiento de las funciones a mi asignadas en virtud de la relación laboral vigente con [Nombre de la Organización], **Acepto la Propiedad**[1] de los Activos de Información indentificados, clasificados y valorados, según el Formato 1 de Clasificación y Valoración de Activos de Información, desarrollado y firmado por mi persona.

Como propietario de los activos de información me comprometo a:

1. Mantener actualizada la clasificación y la valoración del activo bajos los criterios de confidencialidad, integridad y disponibilidad de la información, así como los controles para su adecuada protección, en términos de su valor, requerimientos legales, sensibilidad y grado crítico acorde a mis funciones y fines de negocio.
2. Comunicar al área de seguridad de la identificación el hallazgo de nuevos activos.
3. Proteger la información confidencial y de alta criticidad, contra modificación, pérdida, divulgación o destrucción accidental o no autorizada, así como cumplir las políticas de seguridad de la información de la organización.
4. Asignar opcionalmente custodios para los activos de información, para que supervise, administre, proteja o mantenga el activo, pero la responsabilidad permanece conmigo en calidad de propietario.
5. En casos de transferencias de cargo o cambios en los procesos, he de transferir los documentos existentes relacionados con los activos de información y la propiedad sobre los dichos activos.

Lugar, ___ de _____ de 2020

_____
Nombre completo
Cargo

[1] El termino propiedad (y derivados) identifica a una persona que cuenta con la responsabilidad gerencial aprobada para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término propietario no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

5.5. MATRIZ DE INVENTARIO DE ACTIVOS DE INFORMACIÓN

La información obtenida en las encuestas de clasificación y valoración de activos de información [Formato 1], debe ser ingresada en la matriz de inventario de activos de información [Formato 3]. Ambos formatos están desarrollados en hojas de cálculo, pero pueden ser automatizados en un sistema de información que facilite su tratamiento y cumpla con lo especificado en esta guía.

En la matriz de inventario de activos de información se registra todos los datos vistos hasta ahora y registrados en las encuestas, el traspaso de esta data tiene el objeto de facilitar su gestión, simplificar la toma de decisiones y fundamentalmente para la selección de controles de seguridad de la información, para una adecuada gestión del riesgo.

En la matriz se registra el proceso al cual pertenece cada activo de información, así como el nombre de cada activo de información y su respectiva descripción, luego, utilizando una lista desplegable se selecciona la clasificación y el tipo del activo de información dada por el propietario, las celdas de la columna clasificación, se colorearán automáticamente como se muestra en la imagen siguiente**:**

	ACTIVO DE INFORMACIÓN					Activo de Soporte	
				Seleccione			
Proceso	Código	Nombre	Descripción	Clasificación	Tipo	Ubicación Física	Ubicación Electrónica
				Confidencial			
				De Uso Interno			
				Pública			
					Físico		---
					Digital	---	
					Mixto		
					Persona		---

Luego, de acuerdo al tipo de activo seleccionado, se registrará la ubicación física y/o electrónica, según corresponda; esta ubicación permitirá

definir el activo de soporte que contiene a la información y sobre el cual se implantarán los controles adecuados para mitigar los riesgos asociados.

Según las normas, cada activo deberá contar con un código único de identificación, el departamento de seguridad de la información deberá definir la estructura de dicho código, el mismo que deberá contemplarse en esta matriz.

Para el registro de la valoración solamente se deberá utilizar los tres primeros casilleros (tres columnas) correspondientes a la confidencialidad, integridad y disponibilidad, según el valor promedio que se registra para cada pilar de la información en las encuestas. Dicho valor se encuentra en la primera línea pintada de color oscuro de cada bloque de preguntas.

VALORACIÓN				
Confidencialidad	Integridad	Disponibilidad	No llenar	
			Valor	Criticidad
1	1	1	**1**	Bajo
1	1	2	**2**	Medio
1	2	3	**3**	Alto
2	3	4	**4**	Muy Alto
2	4	4	**4,4**	Extremadamente Alto

El valor de tasación final y correspondiente criticidad de cada activo de información será calculado de forma automática, según lo descrito en el punto 5.3.2. Valoración de los activos de información.

El registro de cada activo en la matriz de inventario de activos de información, concluye con los datos del propietario, custodios, usuarios y opcionalmente con datos de observaciones anotadas como fecha del registro y descripción de la observación realizada.

LOGO	Sistema de Gestión de la Seguridad de la Información	Formato 3
	MATRIZ DE INVENTARIO DE ACTIVOS DE INFORMACIÓN	Versión: 01
		DE USO INTERNO
		Página 1/1

	ACTIVO DE INFORMACIÓN					Activo de Soporte		VALORACIÓN								Observaciones	
				Seleccione				Confidencialidad	Integridad	Disponibilidad	No llenar						
Proceso	Código	Nombre	Descripción	Clasificación	Tipo	Ubicación Física	Ubicación Electrónica				Valor	Criticidad	Propietario	Custodios	Usuarios	Fecha	Descripción de la observación realizada.
				Confidencial				1	1	1	1	Bajo					
				De Uso Interno				1	1	2	2	Medio					
				Pública				1	2	3	3	Alto					
					Físico		---	2	3	4	4	Muy Alto					
					Digital	---		2	4	4	4,4	Extremadamente Alto					
					Mixto												
					Persona		---										

CAPÍTULO VI

DISCUSIÓN

El objetivo general de esta investigación es el diseño de un modelo para la valoración de los activos de información, basado en los requerimientos de las normas internacionales ISO de la familia 27000, que considere, la identificación y caracterización de los activos de información críticos, la clasificación de estos activos, según su tratamiento y alcance dentro de la organización, así como la valoración de los activos de acuerdo con los tres principales criterios normados en seguridad de la información: confidencialidad, integridad y disponibilidad.

Como resultado se presenta la “Guía para la valoración de activos de información”, siendo de mucha importancia la validación de este instrumento, producto de la investigación y del cual se sostendrá la gestión de riesgos de información.

La guía para la valoración de activos de información con sus respectivos archivos como la encuesta de clasificación y valoración de activos de información, el acta de aceptación de propiedad, y la matriz de inventarios de activos de información, ha sido utilizada en una versión menos elaborada y con gran éxito en una reconocida entidad financiera, pero los resultados no pueden ser mostrados por criterios de confidencialidad, sin embargo, se requiere a modo de análisis y discusión la validación de esta guía, con la cual se van a recabar los datos para luego presentar la información consolidada en una matriz de activos de información.

La utilidad, alcance y aplicabilidad de esta guía, dependerá de la obtención de resultados coherentes y acordes con los objetivos planteados, y para ello es necesario su validez a través de un método de validación útil y aceptado como el juicio de expertos.

6.1. JUICIO DE EXPERTOS

El juicio de expertos es un método que verifica la fiabilidad de una investigación, y de acuerdo con Escobar y Cuervo (2008, p.29), se define como "una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones".

Escobar y Cuervo (2008, p.35) establecen, además, cuatro categorías para dar validez de contenido a los ítems, a través de una plantilla que abarca: suficiencia, claridad, coherencia y relevancia, y para cada categoría se establecen indicadores que representan la opinión del juez.

Para la valoración de juicio de expertos, adoptamos lo establecido por las citadas Jazmine Escobar y Ángela Cuervo, y adaptando los indicadores para las cuatro categorías indicadas, se establecieron los siguientes, a ser aplicadas en esta investigación:

6.1.1. Suficiencia

Evalúa si los ítems pertenecen a una misma dimensión y bastan para obtener la medición de ésta. En esta categoría se calificará si la guía para la valoración de activos de información, alcanza a medir el valor de los activos para la organización.

Indicadores**:**

- Los ítems son suficientes.
- Debe incrementarse algunos criterios de valoración.
- Se miden algunos aspectos, pero no corresponden a la total dimensión.
- Los ítems no miden la valoración real de los activos de información.

6.1.2. Claridad

Evalúa si el ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. Aplicado a la guía se evalúa si ésta se comprende fácilmente, su aplicación es clara y con semántica y sintáctica adecuadas.

Indicadores**:**

- La guía es clara, tiene semántica y sintaxis adecuadas.
- Se requiere de algunas modificaciones a la guía.
- Se requiere de bastantes modificaciones.
- La guía no es clara ni aplicable.

6.1.3. Coherencia

Si existe relación lógica con la dimensión o indicador que se está midiendo, en este caso, en la caracterización y valoración de los activos de información.

Indicadores**:**

- La guía es acorde a las normas en seguridad de la información.
- Existe una relación moderada entre el instrumento y la valoración de activos.
- La guía mide algunos aspectos, pero no valora los activos adecuadamente.
- No hay relación alguna entre el uso de la guía y la valoración de activos.

6.1.4. Relevancia

Si el ítem es esencial o importante, y si debe ser incluido. Aquí se evaluará si la guía es esencial o importante, es decir, si se recomienda su aplicación.

Indicadores**:**

- El uso de la guía es relevante y se recomienda su aplicación.
- El uso de la guía es relativamente importante.
- Existen otros métodos de valorar los activos de información.
- La guía no cumple con el objetivo.

6.2. SELECCIÓN DE EXPERTOS

Julio Cabero y María del Carmen Llorente, afirman que la selección del número de expertos depende de aspectos como la facilidad, para acceder a ellos o la posibilidad de conocer expertos suficientes sobre la temática objeto de la investigación (Cabero & Llorente, 2013, p.16), y por su parte, Jazmine Escobar y Ángela Cuervo, señalan que el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento (Escobar & Cuervo, 2008, p.29).

De lo expuesto, deducimos que no hay un parámetro definido en el número de expertos necesarios, sin embargo, para efectos de fiabilidad se establece para esta investigación un mínimo de cinco (5) expertos, quienes deberán contar con experiencia en la aplicación y análisis de las normas ISO en materia de seguridad de la información, además, de certificaciones en la materia.

Se logró, finalmente, la participación de 6 jueces de renombre, a quienes se les presenta con las letras de la A, a la F, en el cuadro siguiente se muestra su experticia a través de su experiencia profesional y certificaciones**:**

Juez	Experiencia	Certificaciones
A	15 años en Bancos, Financieras. CISO (*chief information security officer***:** oficial principal de seguridad de la información) en Bancos y EsSalud.	Ingeniero Informático y MBA ambos en la PUCP Certificaciones: *Cybersecurity, Technology, Application and Policy* del MIT
B	17 años en Seguridad de la información, *Network Security*, Oficial de Seguridad de Información. Especialista en Arquitectura de Seguridad de Información.	Ingeniero de sistemas con cursos especializados de Seguridad de Información y Seguridad Informática/ Ciberseguridad, con certificación en Implementación de Seguridad bajo la norma ISO27001/2
C	Auditor jefe en NQA (Empresa certificadora).	Ingeniero de sistemas,

	Auditor líder en ISO 27001, Docente de Postgrado en temas de ISO 27001, Jefe de Proyectos IBM del Perú	Auditor Líder en ISO 27001, Auditor NQA, Auditor Líder en ISO 20000 (calidad de servicios TI), *Risk Manager* ISO 31000
D	10 años de experiencia en empresas financieras. Analista Senior en Seguridad de la Información.	Ingeniero de sistemas e informática, Especialista en proyectos de sistemas de información. Certificado en ISO 27001 y en Ley de protección de datos personales 29733, entre otros relacionados como PCI-DSS (industria de tarjetas de crédito y débito)
E	14 años en Seguridad de la Información como analista, jefe y gerente de riesgos en entidades financieras.	Ingeniero de sistemas, *Certified Information Systems Auditor* (CISA) respaldada por ISACA
F	30 años de experiencia en seguridad de la información a nivel nacional e internacional. Docente de Postgrado y en aplicación de COSO, COBIT y procesos de Certificación *Sarbanes-Oxley*. - Miembro del CGEIT *Test Enhancement Subcommitee* - Expositor en Latín CACS y CEIC Las Vegas. - Miembro del Comité de Expertos sobre *Cloud Computing* – CSA - Miembro del Consejo Directivo de ISACA, Capítulo Lima - Miembro del *Government and Regulatory Advocacy Regional Subcommittee 2* - Líder de la Comunidad de Entrega de Valor de TI – Val IT - Experto Revisor de la publicación ISACA-Journal - Miembro del Consejo de Gobernabilidad de Tecnologías de Información - ISACA	Lic. en Computación UNMSM, MBA en UPC. Certificación: CISM, Certificación: CGEIT, Certificación: CRISC, Certificación: CISA, Certificación: ISO 27002, Certificación: *Cobit 5 Foundations*, Certificación: *APMG trainer* Certificación: CRMA

6.3. CONSIDERACIONES PARA LA PLANTILLA DE JUICIO DE EXPERTO

Las participaciones de los jueces pueden ser dirigidas a la mejora de algún ítem, pero también hacia aspectos generales (Galicia, Balderrama & Edel, 2017) y tomando esta apreciación de Liliana Galicia, Jorge Balderrama y Rubén Edel, se consideró crear una plantilla para el respectivo Juicio de Experto, que incluya además de los datos de identificación del experto, el objetivo de la investigación, objetivo del juicio de experto, cuadro de calificación por categoría e indicadores, y una parte final para los comentarios, apreciaciones o sugerencias por parte del experto sobre la guía a validar.

Es aquí donde el rol del experto se convierte en una labor fundamental que permita observar y eliminar aspectos de poca relevancia, así como, considerar e incorporar aquellos que se requieran para lograr una herramienta útil, de mayor alcance y aplicabilidad.

La plantilla elaborada para el Juicio de Experto se presenta en el Anexo III de este trabajo.

6.3.1. Descripción del proceso de validación

Las categorías e indicadores se presentan en una tabla de fácil observación, donde se incluye una escala numérica y nominal para la respectiva calificación; se les solicitó a los expertos que valoraran la guía con una calificación de 1 a 4, según su criterio y objetivos siguientes**:**

a) Objetivo de la investigación: Diseñar un modelo para la valoración de los activos de información, basado en los requerimientos de las normas internacionales ISO de la familia 27000.

b) Objetivo del juicio de expertos. Evaluar el instrumento para determinar si con su uso se logra caracterizar, clasificar y valorar los activos de información, de acuerdo con los criterios normados en seguridad de la información.

c) Tabla de calificación

Categoría	Escala de calificación	Indicador	Calificación
SUFICIENCIA La guía alcanza a medir el valor de los activos para la organización.	4. Alto	Los ítems son suficientes.	
	3. Moderado	Debe incrementarse algunos criterios de valoración.	
	2. Bajo	Se miden algunos aspectos, pero no corresponden a la total dimensión.	
	1. No cumple	Los ítems no miden la valoración real de los activos de información.	
CLARIDAD Se comprende fácilmente, su aplicación es clara y con semántica y sintáctica adecuadas.	4. Alto	La guía es clara, tiene semántica y sintaxis adecuadas.	
	3. Moderado	Se requiere de algunas modificaciones a la guía.	
	2. Bajo	Se requiere de bastantes modificaciones.	
	1. No cumple	La guía no es clara ni aplicable.	
COHERENCIA Existe relación lógica en la caracterización y valoración de los activos de información.	4. Alto	La guía es acorde a las normas en seguridad de la información.	
	3. Moderado	Existe una relación moderada entre el instrumento y la valoración de activos.	
	2. Bajo	La guía mide algunos aspectos, pero no valora los activos adecuadamente.	
	1. No cumple	No hay relación alguna entre el uso de la guía y la valoración de activos.	
RELEVANCIA La guía es esencial o importante, es decir, se recomienda su aplicación.	4. Alto	El uso de la guía es relevante y se recomienda su aplicación.	
	3. Moderado	El uso de la guía es relativamente importante.	
	2. Bajo	Existen otros métodos de valorar los activos de información.	
	1. No cumple	La guía no cumple con el objetivo.	

El valor de calificación asignado por cada experto, será consolidado en una tabla para el cálculo del promedio correspondiente a cada categoría y, aplicando un redondeo simple, se establecerá la calificación final por cada ítem,

reflejando de esta forma la validación final de la guía y sus herramientas complementarias.

6.3.2. Preguntas complementarias de validación

Finalmente, se consideró un espacio para las apreciaciones de los jueces, que, en base a su experiencia en seguridad de la información, pueden dar alcances u opiniones que permitan mejorar los instrumentos validados. De esta forma, se establece al final un cuestionario de dos preguntas abiertas**:**

- ¿Hay alguna dimensión que no fue evaluada, cuál?
- ¿Tiene algún comentario sobre la guía para la valoración de activos de información?

6.3.3. Resultados de la validación de expertos

Tras la evaluación de los jueces, se obtiene los siguientes resultados:

Categoría	A	B	C	D	E	F	Promedio	Calificación Final
Suficiencia	4	4	4	4	3	4	3.83	**4**
Claridad	4	4	4	4	4	4	4	**4**
Coherencia	4	4	3	4	3	4	3.67	**4**
Relevancia	4	4	3	4	3	4	3.67	**4**

En todos los criterios se observa la más alta calificación, denotando que el instrumento, la guía para la valoración de activos de información y sus herramientas básicas complementarias, es decir, los tres formatos que complementan la guía, cumplen satisfactoriamente con los objetivos propuestos.

De igual forma, se presenta a continuación las apreciaciones de cada experto con respecto a las dos preguntas formuladas al final de la plantilla utilizada para la validación como experto.

Pregunta: **¿Hay alguna dimensión que no fue evaluada, cuál?**	
Juez	**Respuesta**
A	Ninguna, están todas.
B	Considero que todas las dimensiones fueron evaluadas.
C	De acuerdo al alcance de este trabajo (CIA= principios de seguridad) En referencia a la disponibilidad, ahondaría en preguntas que permitan identificar las repercusiones económicas que podría afectar una falta de dicha disponibilidad.
D	Ninguna, es conforme.
E	Sí, además de la Confidencialidad, Integridad y Disponibilidad, las cuales son las dimensiones clásicas para valorar un activo, se deben tener en consideración las siguientes: 1. **Dependencia.** No todos los activos de información son independientes, muchos de ellos dependen de otros activos, por lo tanto, el activo que soporta a los otros tiene mayor valor. Ejemplo: el servidor de servicios es un activo con mayor valor y peso que el activo de *Active Directory*, ya que el primero contiene al segundo. Este criterio es muy importante ya que ayuda a priorizar los planes de continuidad para los activos que son soportados. 2. **Autenticidad.** Este criterio está relacionado a que perjuicio existiría si no se sabe quién ha hecho o utilizado cierto activo de información. En esa línea, se otorga mayor peso, a los activos que, al ser vulnerados o utilizados fraudulentamente, podrían generar pérdidas económicas o reputacionales. 3. **Trazabilidad.** Este criterio hace la pregunta ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?, este criterio es aplicado especialmente en los activos de información relacionados a base de datos y sistemas y complementa el criterio de confidencialidad.
F	Ninguna.

Nota del investigador**:** Los principios básicos de la seguridad de la información, confidencialidad, integridad y disponibilidad, son también conocidos como CIA por sus siglas del inglés *Confidentiality, Integrity, Availability*.

Pregunta: **¿Tiene algún comentario sobre la guía para la valoración de activos de información?**	
Juez	**Respuesta**
A	Creo que es un instrumento valioso, intuitivo, que de manera simple permite realizar una correcta valoración de los activos. Por otro lado, en el proceso metodológico de la encuesta, mediante las preguntas escogidas por cada dimensión de la seguridad, permite además concientizar y/o recordarles a los custodios su responsabilidad sobre la información.
B	La Seguridad de Información, tiene como punto de partida del SGSI, la correcta recolección y valoración de activos, ello permite hacer inversiones en seguridad de manera objetiva para minimizar los riesgos asociados a éstos. Ésta guía que fue aplicada con éxito en Caja Arequipa cuando estuve como Jefe de Seguridad de Información, constituyó el punto de partida de la gestión de seguridad de la entidad, bajo los estándares internacionales y de acuerdo a las buenas prácticas en Seguridad de Información. Observo que las mejoras que en esta versión se hicieron, la convierten en una potente herramienta basada en metodologías/estándares internacionales y alineadas a las normas locales.
C	Particularmente, me parece una buena guía.
D	Respecto al Formato 2 de Aceptación de Propiedad de los Activos de Información, es recomendable que se incluya, la responsabilidad del Propietario y Custodio del activo de información en la gestión de los riesgos asociados a los activos de información primarios y tecnológicos (identificación, evaluación y tratamiento en plan de acción), comunicando al Dpto. Seguridad de Información de forma oportuna los avances de su gestión.
E	Me parece muy interesante, sugiero agregar los 3 componentes mencionados, los dos últimos permiten ayudar a contar con planes de contingencia y estar prevenidos ante situaciones de robo de información.
F	Es adecuada, sin embargo, aunque no es relevante, la tipología de activos solo contempla algunas de las opciones propuesta en ISO 27005. Adicionalmente, sugiero evaluar la adaptación a otros grupos

	de tipo de activos; por ejemplo, algunas instancias como ISACA recomiendan tipificarlos como: “datos”, “infraestructura”, “procesos” y “personas”.

Recordemos que las apreciaciones de los jueces, expertos en seguridad de la información, son posteriores a la presentación de resultados, es decir, ellos han evaluado la guía para la valoración de activos de información, presentada como resultado de esta investigación, la cual ha recogido durante su desarrollo, el *feedback* de diversas personas que laboran en la implantación de Sistemas de Seguridad de Información (SSI), en sus organizaciones, así como también, la experiencia del investigador en seguridad de la información, levantamiento de activos de información y en gestión del riesgo, además, de los estudios complementarios realizados para el auditor interno en seguridad de la información y para la certificación como implementador líder en ISO 27001.

Un modelo es un arquetipo, y sirve como pauta para ser imitada, reproducida o copiada, por tanto, se puede y se recomienda utilizar la guía para la valoración de activos de información, con sus archivos complementarios desarrollados en hojas de cálculo, para el proceso de identificación, caracterización, clasificación y valoración de los activos de información en las organizaciones, cualquiera sea su tipo, tamaño o naturaleza, pues su desarrollo y presentación considera como base a las normas internacionales ISO de la familia 27000.

CONCLUSIONES

1. La seguridad de información tiene como punto de partida el SGSI, la correcta recolección y valoración de activos permite hacer inversiones en seguridad de manera objetiva para minimizar los riesgos asociados a éstos, constituyéndose así en el punto de partida de la gestión de seguridad, bajo los estándares internacionales y de acuerdo a las buenas prácticas en seguridad de información.

2. El objetivo propuesto en la presente investigación ha sido cumplido de manera satisfactoria según se aprecia en la validación realizada por los expertos en seguridad de la información, quienes revisaron y aprobaron su aplicación en ítems por dimensión, bajo las categorías de claridad, coherencia, relevancia y suficiencia; con la más alta calificación, definiéndolo como adecuado, acorde a las normas en seguridad de la información y de uso recomendado.

3. La investigación logra resolver el problema de identificar, caracterizar, clasificar y valorar, la información; cumpliendo con las normas ISO de la familia 27000, y, de acuerdo a la opinión de los expertos, la investigación ofrece un instrumento valioso e intuitivo, que de manera simple permite realizar una correcta valoración de los activos de información, mientras que, en el proceso metodológico de la encuesta, mediante las preguntas escogidas por cada dimensión de la seguridad, se permite la concientización, recordando a los custodios y propietarios, su responsabilidad sobre la información.

4. Como modelo, el resultado de esta investigación, puede ser reproducido y adaptado a la realidad de cada organización cualquiera sea su tipo, tamaño o naturaleza, siendo el área de seguridad de la información de la organización y los responsables capacitados quienes establecerán su aplicación.

5. El modelo para la valoración de los activos de información basado en las normas ISO 27000, permitirá a las organizaciones, establecer una relación costo beneficio en la implementación de controles de seguridad de la información y en la determinación de cómo ayuda a los procesos de la organización la implementación de un sistema de gestión de seguridad de la información, facilitando la identificación de los activos de información y procesos, de mayor criticidad para una adecuada gestión del riesgo.

RECOMENDACONES

1. Los expertos en seguridad de la información recomiendan que, en las preguntas referentes a la disponibilidad de la información, se considere las repercusiones económicas que podría afectar una falta de dicha disponibilidad, y que, además, de la confidencialidad, integridad y disponibilidad, las cuales son las dimensiones básicas para valorar un activo, se puede también considerar, la dependencia, autenticidad y trazabilidad, si bien estos criterios son importantes en los planes de continuidad y en la gestión de los riesgos de información, su consideración pueden ayudar a mitigar pérdidas económicas o reputacionales.

2. En el formato 2 corresponde al acta de aceptación de propiedad de los activos de información, los expertos recomiendan que se incluya, la responsabilidad de los custodios del activo de información, junto a las del propietario, además de considerar los activos de soporte tecnológicos, comunicando al departamento de seguridad de información y de forma oportuna los avances de cada gestión.

3. Dependiendo de las metodologías de gestión de riesgos que se utilicen en la organización, los expertos sugieren evaluar la adaptación a otros grupos de tipo de activos; por ejemplo, algunas instancias como ISACA recomiendan tipificarlos como: “datos”, “infraestructura”, “procesos” y “personas”.

4. De acuerdo con la madurez de la organización, la guía para la valoración de activos de información, puede aplicarse inicialmente para la valoración del riesgo inherente, sin la consideración de ningún control y así tener un inventario con el valor real de cada activo; luego, se podrá volver a aplicar la guía a los procesos críticos o activos de mayor valor, considerando los controles ya existentes para estimar el riesgo residual.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez Villanueva, C. (2010). *Hacia un Nuevo Modelo de Valoración de Intangibles* (Tesis inédita de doctorado). Univeritat Jaume I. Castellón. España.

Cabero Almenara, J. & Llorente Cejudo, M. (2013). *La aplicación del juicio de experto como técnica de evaluación de las tecnologías de la información (TIC)*. Eduweb. Revista de Tecnología de Información y Comunicación en Educación, vol. 7, núm. 2, pp.11-22. Recuperado de http://servicio.bc.uc.edu.ve/educacion/eduweb/v7n2/art01.pdf

Centro de Desarrollo Industrial. 2018. *Empresas acreditadas en ISO 270001-2005 en el Perú*. Empresas Certificadas, CDI. Recuperado de: http://www.cdi.org.pe/asistencia_ empacreditadas_ISO27001.htm

Escobar Pérez, J. & Cuervo Martínez, Á. (2008). *Validez de contenido y juicio de expertos: una aproximación a su utilización*. Avances en Medición, vol. 6, núm. 1, pp. 27-36. Recuperado de http://www.humanas.unal.edu.co/psicometria/files/7113/8574/5708/Articulo3_Juicio_de_expertos_27-36.pdf

Galicia Alarcón, L., Balderrama Trápaga, J. & Edel Navarro, R. (2017). *Validez de contenido por juicio de expertos: propuesta de una herramienta virtual*. Apertura, 9 (2), pp. 42-53. http://dx.doi.org/10.18381/Ap.v9n2.993

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodología de la Investigación*. 6ta Edición. McGraw-Hill. México.

INDECOPI. (2014). PERUANA NTP-ISO / IEC 27001 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de información. Requisitos. R.0129-2014/CNB-INDECOPI. Publicado el 01 de diciembre de 2014. Recuperado de http://repositorio.indecopi.gob.pe

ISO/IEC 27000. (2014). ISO Seguridad de la información 27000-2014. Técnicas de seguridad – Resumen y Vocabulario. *International Organization for Standardization*, *2014.* Número de Referencia: ISO/IEC 27000:2014(E). Recuperado de www.iso.org

ISO/IEC 27001. (2005). ISO Seguridad de la información 27001-2005. Técnicas de seguridad. *International Organization for Standardization*, *2005*, Sistemas de gestión de seguridad de la información – Requerimientos, 1ra Edición. Recuperado de www.iso.org

ISO/IEC 27001. (2013). ISO Seguridad de la información 27001-2013. Técnicas de seguridad. *International Organization for Standardization*, *2013*, Sistemas de gestión de seguridad de la información – Requerimientos, 2da Edición. Recuperado de www.iso.org

ISO/IEC 27002. (2013). ISO Seguridad de la información 27002-2013. Técnicas de seguridad. *International Organization for Standardization*, *2013*, Código de buenas prácticas para la implementación de controles de gestión de la seguridad de la información. Recuperado de www.iso.org

ISO/IEC 27005. (2011). ISO Seguridad de la información 27005-2011. Técnicas de seguridad. *International Organization for Standardization*, *2011*, Gestión del Riesgo de la Seguridadde la Información. Recuperado de www.iso.org

Martínez Ruiz, H. (2012). *Metodología de la Investigación*. Cengage Learning Latinoamérica. México.

Presidencia del Concejo de Ministros. (2004). RESOLUCIÓN MINISTERIAL N° 224-2004-PCM del 23 de julio de 2004. Aprueban uso obligatorio de la Norma Técnica "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" en las Entidades integrantes del Sistema Nacional de Informática. Publicada en *Diario Oficial El Peruano*, 26 de julio de 2004. Lima. Perú.

Presidencia del Concejo de Ministros. (2005). RESOLUCIÓN MINISTERIAL N° 395-2005-PCM del 08 de noviembre de 2005. Modifican plazos para implementar la Norma Técnica Peruana cuyo uso obligatorio se aprobó mediante la R.M. N° 224-2004-PCM. Publicada en *Diario Oficial El Peruano*, 12 de noviembre de 2005. Lima. Perú.

Presidencia del Concejo de Ministros. (2007). RESOLUCIÓN MINISTERIAL N° 246-2007-PCM del 22 de agosto de 2007. Aprueban uso obligatorio de la Norma Técnica "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. Publicada en *Diario Oficial El Peruano*, 25 de agosto de 2007. Lima. Perú.

Presidencia del Concejo de Ministros. (2011). RESOLUCIÓN MINISTERIAL N° 197-2011-PCM del 14 de julio de 2011. Establecen fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica "NTP ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la gestión de la seguridad de la información". Publicada en *Diario Oficial El Peruano*, 21 de julio de 2011. Lima. Perú.

Presidencia del Concejo de Ministros. (2012). RESOLUCIÓN MINISTERIAL N° 129-2012-PCM del 23 de mayo de 2012. Aprueban 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 la seguridad de la Información. Requisitos" en todas las entidades del Sistema Nacional de Informática. Publicada en *Diario Oficial El Peruano*, 25 de mayo de 2012. Lima. Perú.

Presidencia del Concejo de Ministros. (2016). RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM del 8 de enero de 2016. 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. Publicada en *Diario Oficial El Peruano*, 14 de enero de 2016. Lima. Perú.

Presidencia del Concejo de Ministros. (2017). RESOLUCIÓN MINISTERIAL Nº 166-2017-PCM del 20 de junio de 2017. Modifican el artículo 5 de la R.M. N°004-2016-PCM, referente al Comité de Gestión de Seguridad de la Información; sobre las funciones del Comité. Publicada en *Diario Oficial El Peruano*, 21 de junio de 2017. Lima. Perú.

Presidencia del Concejo de Ministros. (2019). RESOLUCIÓN MINISTERIAL Nº 087-2019-PCM del 19 de marzo de 2019. Aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital. Publicada en *Diario Oficial El Peruano*, 22 de marzo de 2019. Lima. Perú.

Quecedo Lecanda, R. & Castaño Garrido, C. (2003). Introducción a la metodología de la investigación cualitativa. Revista de Psicodidáctica No.14-2003, pp.5-40. Universidad del País Vasco. España.

Ramírez Atehortúa, F. & Zwerg-Villegas, A. (2012). Metodología de la investigación: más que una receta. AD-minister No.20. enero-junio 2012, pp.91-111, ISSN 1692-0279. Colombia.

SBS Circular N° G-140-2009. (2009). *Gestión de la seguridad de la información*, *113*(2), 207–221, SBS. Superintendencia de Banca y Seguros y AFP. Publicada en *Diario Oficial El Peruano*, 06 de abril de 2009. Lima. Perú.

Secretaría de Gobierno Digital. (2019). Sistema Nacional de Informática. Recuperado de: www.gobiernodigital.gob.pe/sistema/sistema.asp

Solarte, F., Enríquez, E, & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *ESPOL-RTE*. Vol.28, N.5, 492-507

Superintendencia Nacional de Migraciones. (19 de abril de 2018). *Ministro del Interior recibe Certificación ISO de Seguridad de Información otorgado a*

MIGRACIONES. Oficina de Imagen y Comunicación Estratégica, Recuperado de: https://www.migraciones.gob.pe/ index.php/iso-seguridad-informacion/

UNJBG. 2017. *Reglamento para elaboración y sustentación de tesis de maestría y doctorado*. Aprobado con R.CU. N°13861-17-UNJBG. Escuela de Postgrado-Universidad Nacional Jorge Basadre Grohmann - Tacna

ANEXOS

ANEXO I

ACTIVOS DE INFORMACIÓN SEGÚN LA NORMA ISO 27005

Un activo es todo lo que tiene valor para la organización y, por lo tanto, requiere protección. Para la identificación de activos de información, debe tenerse en cuenta que un sistema de información consiste en más que hardware y software.

La identificación de activos, debe realizarse con un nivel de detalle adecuado que proporcione información suficiente para la evaluación del riesgo. El nivel de detalle utilizado en la identificación del activo, influirá en la cantidad y cualidad de información recopilada para la evaluación del riesgo.

Tomando como referencia el ***Anexo B: Identificación y valoración de activos y evaluación de impacto, del ISO/IEC 27005:2005***, se identifican los activos bajo los siguientes dos tipos:

A) Activos Primarios

a.1) Procesos y actividades empresariales.

a.2) Información.

B) Activos de soporte (basados en los elementos primarios)

b.1) Hardware.

b.2) Software.

b.3) Redes.

b.4) Personas.

b.5) Lugares.

b.6) Organización.

A) Identificación de Activos Primarios

Referida a los procesos centrales y a la información relacionada al negocio.

a.1) Activos de procesos y actividades empresariales

Hace referencia a los procesos o subprocesos, como:

Procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización.

Procesos que contienen procesos secretos o procesos que involucran patentes.

Procesos que si se modifican pueden afectar en gran medida el cumplimiento de la misión de la organización.

Procesos que son necesarios para que la organización cumpla con los requerimientos contractuales, legales o regulatorios.

a.2) Activos de Información

Comprende principalmente a la información sensible, como:

Información vital para el ejercicio de la misión del negocio u organización.

Información personal privada, sujeta a la ley de protección de datos.

Información estratégica necesaria para alcanzar los objetivos del negocio.

Información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión requieren mucho tiempo y/o implican un alto costo de adquisición.

B) Activos de Soporte

Los activos de soporte son de varios tipos y por sus vulnerabilidades son aprovechables por las amenazas que apuntan a deteriorar a los activos primarios.

El objetivo es identificarlos y describirlos para ser considerados en un análisis de gestión de riesgos. Su adecuada identificación permitirá valorar el activo de información asociado.

b.1) Activos de Hardware

Se refiere a todos los elementos físicos que soportan los procesos o subprocesos, ejemplos:

Equipos de procesamiento de datos

Equipos portables (laptops, PDAs, Smartphones)

Equipos fijos (servidores, PCs)

Equipos periféricos (impresoras, unidades de discos extraíbles, etc.)

Dispositivos (CDs, DVDs, discos duros externos, memorias flash, cintas magnéticas, etc.)

Otros no electrónicos, se refiere a los medios de comunicación estáticos que contienen datos, documentación física en papel (informes, reportes, contratos, fotos, impresiones, fax, etc.), diapositivas, transparencias, archivadores, etc.

b.2) Activos de Software

Se refiere a todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos.

Sistemas Operativos

Software de mantenimiento o administración del SO

Paquetes de software o software estándar

Aplicaciones

b.3) Activos de Redes

Consiste en todos los dispositivos de telecomunicaciones.

De medios y soporte (ADSL, Ethernet, GigabitEthernet, WiFi 802.11), Bluetooth, etc.)

Dispositivos de interconexión (bridge, router, hub, switch, etc.)

Interfaces de comunicación (GPRS, adaptador Ethernet, etc.).

b.4) Activos de Personas

Comprende a todos los grupos de personas que participan en el proceso de información.

Tomador de decisiones (dueños o propietarios de los activos primarios, alta dirección)

Usuarios, son el personal que maneja elementos sensibles en el contexto de su actividad, pueden tener derechos especiales de acceso al sistema de información para llevar a cabo sus tareas cotidianas. Ejemplos: gestión de recursos humanos, gestión financiera, gestor de riesgos.

Personal de Infraestructura y operaciones TI, personal encargado de operar y mantener el sistema de información. Tienen derechos especiales de acceso al sistema de información para llevar a cabo sus tareas cotidianas. Ejemplos: administrador de sistemas, administrador de datos, respaldo, Help Desk, operador de implementación de aplicaciones, agentes de seguridad.

Desarrolladores, personas a cargo de desarrollar las aplicaciones de la organización. Tienen acceso a parte del sistema de información con derechos de alto nivel, pero no toman ninguna acción sobre los datos de producción.

b.5) Activos de Lugares

Llamados también activos de sitio, comprende todos los lugares que contienen el ámbito o parte del alcance y los medios necesarios para que las operaciones del negocio.

Ambiente externo

Locales, establecimientos y edificios

Por zonas de acceso reservado, oficinas, zonas seguras, ambientes

Servicios esenciales, de comunicación y complementarios (operadores de servicios telefónicos, redes telefónicas internas, cableado, UPS, suministro de agua, depósitos de basura, equipos de refrigeración y purificación del aire, entre otros)

b.6) Organización o Activos de Estructura Organizacional

Describe el marco organizativo, todas las estructuras de personal asignadas a una tarea y procedimientos.

Autoridades (junta de accionistas, directorio, gerencia mancomunada)

Estructura organizativa (gerencias, jefaturas, dependencias)

De proyecto (organización establecida para un proyecto o servicio específico como para nuevas aplicaciones, comité de inventario)

Terceros, organizaciones que proporcionan servicios o recursos vinculados por contrato (subcontratistas, proveedores, fabricantes, outsourcing, consultoría)

ANEXO II

SISTEMA NACIONAL DE INFORMÁTICA

De acuerdo con la Resolución Ministerial N°197-2011-PCM del 14 de julio de 2011, y de acuerdo con la Resolución Ministerial Nº 129-2012-PCM del 23 de mayo de 2012, se presenta en este anexo, la relación de las entidades que forman parte del Sistema Nacional de Informática.

Entiéndase también que, algunas entidades actualmente han cambiado como por ejemplo ANR por SUNEDU, y que los Ministerios agrupan a todos los organismos públicos adscritos, como también programas, proyectos especiales, unidades ejecutoras, centros de formación, redes asistenciales, sociedades (de beneficencia, por ejemplo), hospitales, organismos, cortes superiores para el caso del Poder Judicial, universidades nacionales, gobiernos locales, gobiernos regionales, etc. Las resoluciones hacen mención a todas las entidades de la Administración Pública.

Son Miembros del Sistema Nacional de Informática

- El Consejo Consultivo Nacional de Informática (CCONI).
- El Comité de Coordinación Interinstitucional de Informática (CCOII).
- Las Oficinas Sectoriales de Informática y demás Oficinas de Informática de los Ministerios, de los Organismos Centrales, Instituciones Públicas Descentralizadas y Empresas del Estado.
- Los órganos de Informática de los Gobiernos Regionales.
- Los órganos de Informática de las Municipalidades.
- Los órganos de Informática de los Poderes Públicos y de los Organismos Autónomos.

Son Entidades del Sistema Nacional de Informática

PODER LEGISLATIVO

1. Congreso de la República

PODER JUDICIAL

1. Poder Judicial (PJ)

ORGANISMOS AUTÓNOMOS

1. Asamblea Nacional de Rectores (ANR)

2. Banco Central de Reserva del Perú (BCRP)

3. Consejo Nacional de la Magistratura (CNM)

4. Defensoría del Pueblo (DP)

5. Jurado Nacional de Elecciones (JNE)

6. Contraloría General de la República (CGR)

7. Ministerio Público - Fiscalía de la Nación (MPFN)

8. Oficina Nacional de Procesos Electorales (ONPE)

9. Registro Nacional de Identificación y Estado Civil (RENIEC)

10. Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS)

11. Tribunal Constitucional (TC)

PODER EJECUTIVO

Sector: Comercio Exterior y Turismo

1. Comisión de Promoción del Perú para la Exportación y el Turismo (PROMPERU)

2. Ministerio de Comercio Exterior y Turismo (MINCETUR)

Sector: Defensa

3. Instituto Geográfico Nacional (IGN)

4. Ministerio de Defensa (MINDEF)

Sector: Economía y Finanzas

5. Agencia de Promoción de la Inversión Privada (PROINVERSION)

6. Comisión Nacional Supervisora de Empresas y Valores (CONASEV)

7. Ministerio de Economía y Finanzas (MEF)

8. Ofi cina de Normalización Previsional (ONP)

9. Organismo Supervisor de las Contrataciones del Estado (OSCE)

10. Superintendencia Nacional de Administración Tributaria (SUNAT)

Sector: Educación

11. Ministerio de Educación (MED)

Sector: Energía y Minas

12. Instituto Geológico Minero y Metalúrgico (INGEMMET)

13. Instituto Peruano de Energía Nuclear (IPEN)

14. Ministerio de Energía y Minas (MEM)

Sector: Interior

15. Ministerio del Interior (MININTER)

16. Policía Nacional del Perú (PNP)

Sector: Justicia

17. Ministerio de Justicia (MINJUS)

18. Superintendencia Nacional de los Registros Públicos (SUNARP)

Sector: Mujer y Desarrollo Social

19. Ministerio de la Mujer y Desarrollo Social (MIMDES)

Sector: Presidencia del Consejo de Ministros

20. Centro Nacional de Planeamiento Estratégico (CEPLAN)

21. Comisión Nacional para el Desarrollo y Vida sin Drogas (DEVIDA)

22. Despacho Presidencial (DP)

23. Dirección Nacional de Inteligencia (DINI)

24. Instituto Nacional de Defensa Civil (INDECI)

25. Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)

26. Organismo Supervisor de Inversión Privada en Telecomunicaciones. (OSIPTEL)

27. Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN)

28. Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público (OSITRAN)

29. Presidencia del Consejo de Ministros (PCM)

30. Superintendencia Nacional de Servicios y Saneamiento (SUNASS)

Sector: Producción

31. Ministerio de la Producción (PRODUCE)

Sector: Relaciones Exteriores

32. Agencia Peruana de Cooperación Internacional (APCI)

33. Ministerio de Relaciones Exteriores (RREE)

Sector: Salud

34. Instituto Nacional de Oftalmología (INO)

35. Instituto Nacional de Salud (INS)

36. Instituto Nacional de Salud del Niño (INSN)

37. Ministerio de Salud (MINSA)

38. Superintendencia Nacional de Aseguramiento en Salud (SUNASA)

Sector: Trabajo y Promoción del Empleo

39. Ministerio de Trabajo y Promoción del Empleo (MTPE)

40. Seguro Social de Salud (ESSALUD)

Sector: Transportes y Comunicaciones

41. Corporación Peruana de Aeropuertos y Aviación Comercial (CORPAC S.A.)

42. Empresa Nacional de Puertos S.A. (ENAPU S.A.)

43. Ministerio de Transportes y Comunicaciones (MTC)

44. Servicios Postales del Perú S.A. (SERPOST S.A.)

Sector: Vivienda, Construcción y Saneamiento

45. Banco de Materiales SAC (BANMAT SAC)

46. Fondo MIVIVIENDA S. A. (FMV S.A.)

47. Ministerio de Vivienda, Construcción y Saneamiento (VIVIENDA)

48. Servicio de Agua Potable y Alcantarillado de Lima (SEDAPAL)

49. Superintendencia Nacional de Bienes Estatales (SBN)

50. Organismo de Formalización de la Propiedad Informal (COFOPRI)

ANEXO III

PLANTILLA PARA JUICIO DE EXPERTO

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento GUÍA PARA LA VALORACIÓN DE ACTIVOS DE INFORMACIÓN que hace parte de la investigación MODELO PARA VALORACIÓN DE ACTIVOS DE INFORMACIÓN BASADO EN LAS NORMAS ISO 27000. La evaluación de este instrumento es de gran relevancia para lograr que los resultados obtenidos a partir de éste, sean utilizados eficientemente en la aplicación de controles para la seguridad de la información. Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS DEL JUEZ**:**

_____

EXPERIENCIA EN SEGURIDAD DE LA INFORMACIÓN**:**

_____

_____

FORMACION ACADÉMICA, CERTIFICACIONES**:**

_____

_____

CARGO ACTUAL**:**

_____

INSTITUCIÓN**:**

_____

Objetivo de la investigación:

Diseñar un modelo para la valoración de los activos de información, basado en los requerimientos de las normas internacionales ISO de la familia 27000.

Objetivo del juicio de expertos:

Evaluar el instrumento para determinar si con su uso se logra caracterizar, clasificar y valorar los activos de información de acuerdo con los criterios normados en seguridad de la información.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Escala de calificación	Indicador	Calificación
SUFICIENCIA La guía alcanza a medir el valor de los activos para la organización.	4. Alto	Los ítems son suficientes.	
	3. Moderado	Debe incrementarse algunos criterios de valoración.	
	2. Bajo	Se miden algunos aspectos, pero no corresponden a la total dimensión.	
	1. No cumple	Los ítems no miden la valoración real de los activos de información.	
CLARIDAD Se comprende fácilmente, su aplicación es clara y con semántica y sintáctica adecuadas.	4. Alto	La guía es clara, tiene semántica y sintaxis adecuadas.	
	3. Moderado	Se requiere de algunas modificaciones a la guía.	
	2. Bajo	Se requiere de bastantes modificaciones.	
	1. No cumple	La guía no es clara ni aplicable.	
COHERENCIA Existe relación lógica en la caracterización y valoración de los activos de información.	4. Alto	La guía es acorde a las normas en seguridad de la información.	
	3. Moderado	Existe una relación moderada entre el instrumento y la valoración de activos.	
	2. Bajo	La guía mide algunos aspectos, pero no valora los activos adecuadamente.	
	1. No cumple	No hay relación alguna entre el uso de la guía y la valoración de activos.	

RELEVANCIA La guía es esencial o importante, es decir, se recomienda su aplicación.	4. Alto	El uso de la guía es relevante y se recomienda su aplicación.	
	3. Moderado	El uso de la guía es relativamente importante.	
	2. Bajo	Existen otros métodos de valorar los activos de información.	
	1. No cumple	La guía no cumple con el objetivo.	

¿Hay alguna dimensión que no fue evaluada, cuál?

_____

_____

¿Tiene algún comentario sobre la guía para la valoración de activos de información?

_____

_____

Fecha y Firma