Universidad Católica de Santa María

Facultad de Ciencias e Ingenierías Físicas y Formales

Escuela Profesional de Ingeniería de Sistemas

MÉTRICAS PARA EVALUAR LOS ACTIVOS DE INFORMACIÓN DEL ÁREA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN BASADOS EN LA ISO/IEC 27001 – ISO/IEC 27002 PARA UNA EMPRESA COOPERATIVA

Tesis presentada por el bachiller:
Córdova Quispe, Carlos Eduardo
Para optar el Título Profesional de:
Ingeniero de Sistemas
Asesor:
Ing. Calderon Ruíz Guillermo Enrique

Arequipa - Perú

2020

UCSM-ERP

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

INGENIERIA DE SISTEMAS

DICTAMEN APROBACIÓN DE BORRADOR DE TESIS

Arequipa, 02 de Julio del 2020

Dictamen: 000830-C-EPIS-2020

Visto el borrador de tesis del expediente 000830, presentado por:

2008200381 - CORDOVA QUISPE CARLOS EDUARDO

Titulado:

MÉTRICAS PARA EVALUAR LOS ACTIVOS DE INFORMACIÓN DEL ÁREA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN BASADOS EN LA ISO/IEC 27001 ? ISO/IEC 27002 PARA UNA EMPRESA COOPERATIVA

Nuestro dictamen es:

APROBADO

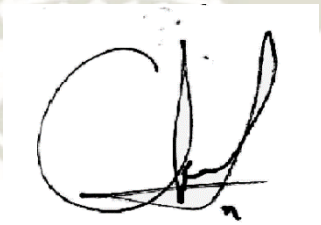
1748 - CALDERON RUIZ GUILLERMO ENRIQUE
DICTAMINADOR

1220 - ZUÑIGA CARNERO MANUEL MARIANO
DICTAMINADOR

PRESENTACIÓN

Director de la Escuela Profesional de Ingeniería de Sistemas
Sres. Miembros del Jurado.

De conformidad con las disposiciones del Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas, pongo a vuestra consideración el presente trabajo de aplicación titulado:
"MÉTRICAS PARA EVALUAR LOS ACTIVOS DE INFORMACIÓN DEL ÁREA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN BASADOS EN LA ISO/IEC 27001 – ISO/IEC 27002 PARA UNA EMPRESA COOPERATIVA", el mismo que de ser aprobado me permitirá optar el Título Profesional de Ingeniero de Sistemas.



Carlos Eduardo Córdova Quispe
Bachiller en Ing. de Sistemas

DEDICATORIA

Esta Tesis se la quiero dedicar en primer lugar a Dios por iluminarme y guiarme en el desarrollo de la misma y poder darme las fuerzas para culminarla y no rendirme en el camino.

En segundo lugar agradecer a mis padres Juana y Segundo quienes con todo su esfuerzo me brindaron la dicha de poder cursar una carrera profesional, los amo con todo mi corazon y estaré eternamente agradecido con ellos por sus enseñanzas y consejos, a mis hermanos Alex y Jimmy quienes son además mis mejores amigos, siempre se que contaré con ellos y les agradezco de corazon su apoyo y soporte.

AGRADECIMIENTOS

Agradezco a la UNIVERSIDAD CATÓLICA DE SANTA MARÍA por brindarme los conocimientos teóricos, prácticos y valores éticos y morales para convertirme en un profesional.

A mi asesor de tesis, Ing. Guillermo Calderon Ruiz, quien me brindó su conocimiento, experiencia y tiempo para la elaboración del presente proyecto.

Agradezco a los docentes de la ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS, que durante toda mi carrera profesional aportaron con mi desarrollo académico.

También agradezco a mis padres, amigos y personas que a lo largo del camino me apoyaron en mi constante mejora como persona y profesional.

EPÍGRAFE

"No es valiente aquel que no tiene miedo sino el que sabe conquistarlo"

Nelson Mandela

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Con el paso de los años las tecnologías de información han ido convirtiéndose en un elemento importante por no decir imprescindible en el desarrollo de las operaciones de todas las organizaciones, ya que es el área de tecnologías de información la cual se encarga de gestionar, administrar, mantener y mejorar en materia de tecnología los servicios, sistemas de información y servidores tanto centrales como de apoyo que soportan la operatividad y continuidad del negocio de estas organizaciones, así mismo dentro de todos aquellos sistemas y servidores que dependen del área de T.I. se alberga información de todo tipo, desde información básica hasta información crítica de la organización, dicha información es necesaria para la toma de decisiones de la organización ya que esta pueda mostrar el comportamiento del mercado, deudas de clientes, etc. Esta información puede estar almacenada tanto en bases de datos, servidores, discos duros, unidades extraíbles, cintas magnéticas, entre otros medios de almacenamiento y en su mayoría de veces no es resguardada de manera correcta, lo que puede ocasionar que la información sea propensa a modificaciones erróneas o mal intencionadas, perdida a nivel de confidencialidad o eliminación de la misma, es también necesario gestionar de manera apropiada y velar por la seguridad de los activos de información que sirven como medio para la prestación de los servicios del área de T.I. En la actualidad la mayoría de organizaciones cuenta con un área de tecnologías de la Información formada ya sea esta pequeña o estructurada con sus respectivas áreas, sea cual fuese el escenario el área de Tecnologías de Información tendrá bajo su gestión el mantenimiento y administración de la infraestructura tecnológica de la organización, en la cual se realizan todas las acciones necesarias para el mantenimiento de las comunicaciones, mantenimiento de las operaciones y correcto funcionamiento de los sistemas internos. Entonces si el área de Tecnologías de Información tienen bajo sus funciones y responsabilidades el mantenimiento de operaciones según lo descrito previamente, es necesario poder identificar aquellos dispositivos, equipos, sistemas, entre otros, que según la norma ISO27001 son los activos de información para poder darle un correcto seguimiento, tener conocimiento de los riesgos a los que estén expuestos estos activos y además poder tomar las decisiones oportunas en caso se presente

algún incidente que afecte críticamente a estos activos, por tal motivo la finalidad de este proyecto es elaborar métricas para la medición de estos activos de información del área de Infraestructura de Tecnologías de Información.

Palabras Clave

ISO/IEC 27001, ISO/IEC 27002, SGSI(Sistema de Gestión de Seguridad de la Información), métricas, Activos de Información, Infraestructura.

ABSTRACT

Over the years, Information Technologies have become an important, if not essential, element in the development of the operations of all organizations, since it is the Information Technology area which is responsible for managing, administering, Maintain and improve technology, services, information systems and central and support servers that support the operability and business continuity of these organizations, as well as all those systems and servers that depend on the IT area. Information of all kinds is housed, from basic information to critical information of the organization, such information is necessary for the decision-making of the organization since it can show the behavior of the market, customer debts, etc. This information can be stored both in Databases, Servers, Hard Disks, Removable Drives, magnetic tapes, among other storage media and in most cases it is not properly protected, which can cause the information to be prone to erroneous or malicious changes, loss of confidentiality or elimination of it, it is also necessary to manage appropriately and ensure the security of the information assets that serve as a means for the provision of IT services.

Currently most organizations have an Information Technology area formed either this small or structured with their respective areas, whatever the scenario the Information Technology area will have under their management the maintenance and administration of infrastructure technology of the organization, in which all the necessary actions are carried out for the maintenance of communications, maintenance of operations and proper functioning of internal systems.

So if the Information Technology area has operations and responsibilities under its functions and responsibilities as previously described, it is necessary to be able to identify those devices, equipment, systems, among others, that according to ISO27001 are the information assets to be able to give a correct follow-up, being aware of the risks to which these assets are exposed and also being able to make the appropriate decisions in the event of any incidents that critically affect these assets, for this reason the purpose of this project is to develop metrics for measurement of these information assets in the Information Technology Infrastructure area.

Keywords

ISO/IEC 27001, ISO/IEC 27002, ISMS(Information Security Management System), metrics, information assets, Infrastructure.

INTRODUCCIÓN

En la actualidad la creciente ola de incidentes informáticos así como los acontecimientos que se van dando como robos de información e intrusiones en plataformas digitales con la finalidad de extraer data, hace necesario que las organizaciones se planteen la implementación de Normas Internacionales de Seguridad y Gobierno de T.I. como COBIT 5 o la Norma Internacional ISO 27001:2014 entre otras, lo cual permitirá establecer marcos de trabajo e implementar controles para la prevención de posibles incidentes o ataques que puedan darse, así mismo el uso de buenas practicas garantizará a las organizaciones que los procesos utilizados están alineados a normas avaladas internacionalmente.

Descripción de los capítulos:

Capítulo I.- denominado planteamiento del problema, desarrolla el planteamiento del problema, el objetivo general, los objetivos específicos, las preguntas de aplicación, la línea y sub-línea de investigación, la justificación e importancia, los aportes, alcances y limitaciones, población y muestra o universo y métodos, técnicas e instrumentos empleados.

Capítulo II.- denominado fundamentos teóricos, desarrolla el estado del arte y las bases teóricas del trabajo.

Capítulo III.- denominado elaboración del modelo de métricas para el área de infraestructura de tecnologías de información.

Capítulo IV.- denominado resultados, desarrolla los hallazgos del presente trabajo.

Capitulo V.- denominado análisis y discusión, desarrolla un análisis de los resultados obtenidos

CAPÍTULO I:

1. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1. Planteamiento de la Investigación

En los últimos años la forma de ver la parte estratégica de las empresas ha venido cambiando, enfocándose ya no tanto en la parte operativa sino también centrando el foco de atención en un elemento al cual no se le venía dando la importancia adecuada, me refiero a la información. La información es un activo que como otros es de suma importancia para el negocio por ende lo es también para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado en el que se desenvuelven los negocios. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor abanico de amenazas y vulnerabilidades (Comite Tecnico de Normalizacion de Codificacion e Intercambio Electronico de Datos, 2007).

En la actualidad la información sea cual fuese el medio en el cual se presente es un activo muy importante para las organizaciones, ya que con esta se pueden obtener conocimientos del mercado, comportamiento de clientes, estadísticas de ventas, etc. Toda esta información que es generada, almacenada y gestionada por estas organizaciones, es resguardada de diferentes maneras pudiendo estar en bases de datos, discos, unidades extraibles, archivadores, servidores, etc. Es así que mantener esta información segura y disponible en todo momento es una labor de suma importancia que en general se sostiene bajo la implementación de un Sistema de Gestión de Seguridad de la Información, este sistema de gestión comprende la definición de políticas, normas y procedimientos los cuales sirven de apoyo para el correcto funcionamiento, gestión y mejora del mismo (Montoya Vega, 2013).

La norma internacional bajo la cual se implementa un SGSI es la norma internacional ISO/IEC 27001 que es el marco de gestión y desarrollo, parte de la gestión y mantenimiento del sistema de gestión requiere la identificación y valorización de todos los activos de información los cuales por su importancia y criticidad son los que pueden garantizar la continuidad del negocio de las organizaciones y evitar un impacto

irreversible de materializarse una amenaza que afecte a estos activos, almacenar información estratégica de la empresa, la cual al estar expuesta puede verse comprometida, menguar la competitividad de la empresa contra los competidores del mismo rubro. En fin, es importante para las organizaciones y para los encargados de la seguridad el saber que activos son los más importantes y por ende necesitan de más cuidado y seguimiento, todo esto teniendo en consideración que en los últimos años los ataques cibernéticos han venido en aumento. El Autor Jorge Mario Cadavid en su Articulo "Seguridad en Activos de Información Humanos", indico que "A partir del año 2010 América Latina ha sido el nuevo objetivo para los ciberdelincuentes ya que el crimen cibernético marco una subida de hasta 40% en 2012" (Cadavid-aguirre, 2013).

El objetivo de este proyecto es proveer a la cooperativa de una serie de métricas las cuales permitan evaluar y valorizar los activos de información críticos del área de Infraestructura para que de esta manera la gestión de incidentes y las respuestas hacia estos sea más eficiente, así mismo esto podrá facilitar la identificación de los riesgos a los cuales están expuestos estos activos y el impacto que pueda originar el que se vea afectada su confidencialidad, integridad o disponibilidad.

Como se mencionó previamente un SGSI tiene como marco de implementación la norma Internacional ISO/IEC 27001 la cual forma parte de la familia ISO 27000, dentro de esta familia existen normas complementarias que apoyan la implementación, gestión y mejora continua del sistema de gestión de seguridad de la información, para los fines del presente proyecto sé está considerando además de la ISO27001 también la norma ISO 27002 en la cual se consolida un listado de controles que podrían de ser considerados para su implementación y de esta manera garantizar la confidencialidad, integridad y disponibilidad de la información, esta norma se compone de 14 dominios de control, 35 objetivos de control y 114 controles, los cuales buscan abarcar todos aquellos activos de información y mitigar todas aquellas posibles amenazas con las que se puedan enfrentar la organización (Iso27000.es, 2013).

En Perú se cuenta con la norma NTP-ISO 27001:2014, la cual es el marco de gestión para la implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información, entendiéndose que la implementación del SGSI es una decisión

estratégica de las organizaciones para el resguardo y protección de su información (NTP-ISO/IEC 27001:2014, 2014).

Ahora bien, la implementación de los controles no es un tema sencillo ya que en muchas ocasiones desarrollar, implementar y mantener estos controles conlleva un costo tanto económico como de tiempo y se hace necesario evaluar aquellos activos que por la información que contengan o la criticidad de estos para la continuidad de la operativa de la empresa representan los activos más importantes o más críticos.

1.2. Objetivos de la Investigación

1.2.1. General

Definir métricas para evaluar los activos de información del área de infraestructura de T.I. basados en la ISO/IEC 27001 – ISO/IEC 27002 para una entidad financiera cuyas operaciones se limitan a las de una Cooperativa.

1.2.2. Específicos

- Identificar los activos de información del área de infraestructura de T.I.
- Clasificar los activos de información identificados para el entendimiento de su criticidad según ISO27001.
- Identificar los controles con base en la norma ISO 27002, para los activos de información del área de Infraestructura.
- Definir las métricas de evaluación de los activos de información del área de infraestructura de T.I. basados en la ISO/IEC 27001 e ISO/IEC 27002.

1.3. Preguntas de Investigación

- ¿En que medida serán útiles las métricas para la evaluación de los activos de información del área de infraestructura de tecnologías de información para la cooperativa?.

1.4. Línea y Sub-Línea de Investigación

1.4.1. Línea

Sistemas de Información y Bases de Datos.

1.4.2. Sub-Línea

Seguridad Informática.

1.5. Palabras Clave

ISO/IEC 27001, ISO/IEC 27002, SGSI(Sistema de Gestión de Seguridad de la Información), métricas, Activos de Información, Infraestructura.

ISMS(Information Security Management System), metrics, information assets, Infrastructure.

1.6. Solución Propuesta

1.6.1. Justificación e Importancia

En los últimos años un objetivo de las empresas en lo que respecta a la estrategia empresarial es el poder integrar la gestión de la calidad, el medio ambiente y la seguridad y salud en el trabajo. Cuando estos objetivos se han alcanzado, entran en escena otros aspectos a tratar y que se están convirtiendo en puntos clave para los modelos de negocio actuales (Portillo & Benavides, 2012).

Así mismo en la línea de los cambios y nuevos enfoques de la estrategia empresarial cada vez toma más importancia la gestión de riesgos como base para la toma de decisiones (Romeral & Torres Gallego, 2008).

Entre los diferentes aspectos a considerar está la información, es decir toda aquella data que desde algún punto de vista se considera necesario controlar, ya sea por obligación legislativa, por interés de terceros o bien por ser

esenciales para la actividad y toma de decisiones estratégicas de las organizaciones.

La información es un activo valioso que puede impulsar o destruir una organización, la defensa de este activo es una tarea esencial para asegurar la continuidad y la sostenibilidad del negocio, también es una exigencia legal (protección de la propiedad intelectual, protección de datos personales, servicios para la sociedad de la información), y además genera confianza a los clientes y/o usuarios.

Los activos son los recursos del sistema de gestión de seguridad de la Información de acuerdo a la ISO 27001, y son necesarios para que toda empresa funcione y consiga los objetivos que se ha propuesto la alta dirección. Cada activo tiene sus características, que difieren en el estado, en materia de seguridad, confidencialidad, integridad y disponibilidad, cada activo o grupo de activos conlleva diferentes tipos de indicadores para su valoración para de tal manera ofrezcan una orientación para calcular el impacto en caso se materialice alguna amenaza.

Esto es muy importante en ambientes de negocio cada vez más interconectados, pues, la información está ahora expuesta a un número mayor y a una variedad más amplia de amenazas y vulnerabilidades. Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada.

El desarrollo de este proyecto de investigación permitirá a la cooperativa, así como a otras empresas (públicas o privadas) del mismo giro de negocio y al personal responsable de velar por la seguridad de información, aplicar métricas para la evaluación de sus diferentes activos de información, considerando el incremento de la cantidad de incidentes de seguridad de la información, que afectan la operación y continuidad de negocio, con impacto a nivel económico, legal y de imagen para las empresas.

Las empresas pueden desarrollar e implantar un marco de trabajo para la gestión de la seguridad de sus activos de información, incluyendo información

financiera, propiedad intelectual y detalles de sus empleados, o información confiada a la organización por sus clientes o terceras partes.

Mejorar los aspectos relacionados con la seguridad de la información, proveer confianza a sus clientes o socios, son algunos de los motivos por los cuales las organizaciones deciden adoptar normas de seguridad y la implementación de un SGSI, la gestión de la Seguridad de la Información ofrece la libertad para crecer, innovar y ampliar la base de clientes sabiendo que toda la información cuenta con diferentes controles y basados en métricas para la evaluación de sus activos.

1.6.2. Descripción de la Solución

El resultado de la investigación fue el planteamiento de métricas para la evaluación de los activos de información del área de Infraestructura de Tecnologías de Información de una Cooperativa de Ahorros y Crédito, estas métricas fueron utilizadas para poder llevar un control de los activos en relación a los riesgos a los que estos se encuentran expuestos.

Las métricas planteadas están alineadas basándose en las normas Internacionales ISO27001 e ISO 27002 de Seguridad de la Información, lo cual garantiza que detrás de estas existe un soporte de buenas prácticas utilizadas a nivel internacional.

Para el planteamiento y posterior implementación de las métricas, se realizó la identificación de los activos de información pertenecientes la área de Infraestructura, para posterior a esto clasificar dichos activos identificados y valorizar los mismos, de tal manera poder tener idea de la criticidad y relevancia de cada activo en relación a los 3 pilares de Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad).

CAPÍTULO II:

2. FUNDAMENTOS TEÓRICOS

2.1. Estado de Arte

En su proyecto titulado “Métricas para evaluar la calidad de los Sistemas de Gestión de Información Contable - Financiera” para optar el grado de Master en Informatica Aplicada en la ciudad de Cuba (Pentón, 2016), propone un grupo de métricas para evaluar la calidad de un sistema de información con el objeto de apoyar la toma de decisiones basadas en métricas especificas para la evaluación de características y sub-características partiendo de los atributos del software para la selección de la herramienta idónea a utilizar.

El proyecto planteado por el autor, es de ayuda ya que tomando en consideración los aspectos evaluados por el mismo, se puede orientar la elaboración de métricas en relación al apartado de “Adquisición Desarrollo y Mantenimiento de los Sistemas de Información” de la norma ISO 27002, la cual dicta los aspectos a abarcar en la definición de controles para la seguridad de la información, entonces tomando en consideración los criterios planteados por el autor en el proyecto se puede orientar la elaboración de las métricas que se pretenden elaborar, además se debe de considerar que para el rubro de la empresa la cual se toma como caso de estudió las métricas de evaluación para el sistema contable son muy importantes.

Dentro del desarrollo del proyecto el autor se apoya de normas internacionales ISO, dentro de las cuales se puede destacas la Norma ISO/IEC 9126 de la cual rescata una tabla de características y sub-características que conforman el modelo base, para la medición de calidad de software, es así que el autor en su propuesta toma como base el marco referencial de la norma internacional antes mencionada y realiza modificaciones a la tabla, eliminando por ejemplo, usabilidad, eficiencia, mantenibilidad y portabilidad por considerarlas no relevantes para el dominio de un SGSI.

Al validar el modelo propuesto el autor tomo resultados de 37 expertos los cuales brindaron comentarios así como brindaron su aprobación o desaprobación al modelo propuesto, indicando que era necesario la evaluación de aspectos de seguridad en relación a la información contable que contendría el software y en general el Sistema de Gestión. Por otro lado el proyecto al enfocarse unicamente en el sistema de información contable limita las posibilidades de poder expandir el alcance de las métricas, pero el mismo sera importante para poder orientar la elaboración de las métricas que se plantearan en el proyecto.

Por otro lado, en el proyecto titulado "Métricas para el proceso de implementación del modelo de Gobierno de Seguridad de la Información Basado en COBIT 5.0", para optar el grado de Ingeniero de Sistemas en la ciudad de Mahala Ecuador (Correa, 2016), plantea la medición del desempeñó del gobierno de seguridad de la información, para lo mismo propone como referencia el marco de gobierno de COBIT 5.0, según indica el autor este marco es el más adecuado a tomarse en cuenta por medio de una tabla comparativa, se crean métricas basadas en los dominios indicados por el marco Cobit.

Este proyecto es útil, ya que para un Sistema de Gestión de Seguridad de la Información según la ISO 27001 es necesaria la existencia de un gobierno de T.I. establecido el cual se maneje en el marco de políticas, procesos y procedimientos, según COBIT 5.0 el mismo define dominios como "Evaluar, Orientar y Supervisar" y un segundo dominio como "Alinear, Planificar y Organizar", estos dominios se pueden orientar dentro de la Norma ISO 27001 al PDCA (Planificar, Hacer, Evaluar, Actuar).

El autor también considera dentro de la bibliografía estudiada la Norma ISO 27004 la cual es la Guía para la auditoria de un Sistema de Gestión de Seguridad de la Información y en la cual se considera la medición del nivel de seguridad basándose en 3 aspectos los cuales son: Estratégico, Táctico y Operativo, para más detalle se muestra la figura líneas abajo:

Figura 1. Modelo Estrategico de Métricas de Seguridad de la Información

Fuente: Métricas para el proceso de implementación del modelo de gobierno de seguridad de la información basado en COBIT 5.0 (Correa, 2016)

Es así entonces que se desprende que el autor hace un gran énfasis en orientar la solución propuesta tomando muy en consideración las normas ISO para la Seguridad de la Información y las cuales también son consideradas para la planteación del presente proyecto.

2.2. Bases Teóricas de la Investigación

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

El Sistema de Gestión de Seguridad de la Información es el concepto central sobre el que se construye ISO 27001 según (Iso27000.es, n.d.-b).

Así mismo un SGSI se debe de gestionar mediante la aplicación de procesos sistemáticos, documentados y que estos a su vez sean ser de conocimiento de toda la organización. Así mismo el propósito de un sistema de gestión de seguridad de la información es garantizar que los riesgos a los cuales están expuestos los diversos activos de información, sean conocidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente, y adaptada a los cambios que se puedan producir en los riesgos, el entorno y las tecnologías, es así que la necesidad de la implementación de este sistema de gestión nace en relación a las necesidades de:

- Identificar los riesgos y su costo.

- Analizar los riesgos y su costo.
- Darle un trato seguro a la información genarada y procesada por los sistemas de información.
- Darle un trato seguro a la información genarada y procesada por los sistemas de información.
- Identificar los activos de información críticos de la Organización.
- Implementar Controles los cuales permitan la minimización de los riesgos y el impacto hacia los activos.
- Garantizar la mejora continua de los procesos y la gestión del sistema de gestión de seguridad de la información.

En el contexto se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), por su origen (de la misma organización o generada por fuentes terceras) o de la fecha de elaboración.

Así mismo la seguridad de la información parte de 3 pilares considerados dentro de la Norma ISO 27000 son:

- **Confidencialidad:** La información mantendrá su confidencialidad y la misma solo podrá ser accedida por los usuarios autorizados.
- **Integridad:** La información deberá mantener la exactitud y completitud dentro de todos los niveles de procesamiento a los cuales sea sometida.
- **Disponibilidad:** La información y los sistemas de tratamiento podrán ser consultados y utilizados de manera irrestricta en cualquier momento y lugar.

2.2.2. Origen ISO 27000

Dentro de la publicación “ISO 27000” (Iso27000.es, n.d.-a). se hace referencia a los orígenes de la Norma, es así que se tiene, desde el año 1901, y como primera entidad normalizadora a nivel mundial se tuvo el BSI (British Standards Institution) la cual era equivalente a AENOR Española pero en su versión Británica, esta misma es responsable de la publicación de importantes normas como:

- Publicación BS5750 – ahora ISO 9001 en el año 1979.
- Publicación BS7750 – ahora ISO 14001 en el año 1992.
- Publicación BS 8800 – ahora OHSAS 18001 en el año 1996.

Entonces la norma BS 7799 aparece por primera vez en 1995 con objeto de proporcionar a cualquier empresa británica o no un conjunto de buenas practicas para la gestión de seguridad de la información, la primera parte de la norma (BS 7799-1) es una guía de buenas practicas para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de gestión de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002 se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión, en 2005 este esquema se publicó por ISO como ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta ultima norma se renombra como ISO27002:2005 el 1 de julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión, a continuación se muestra un imagen con la historia de la norma:

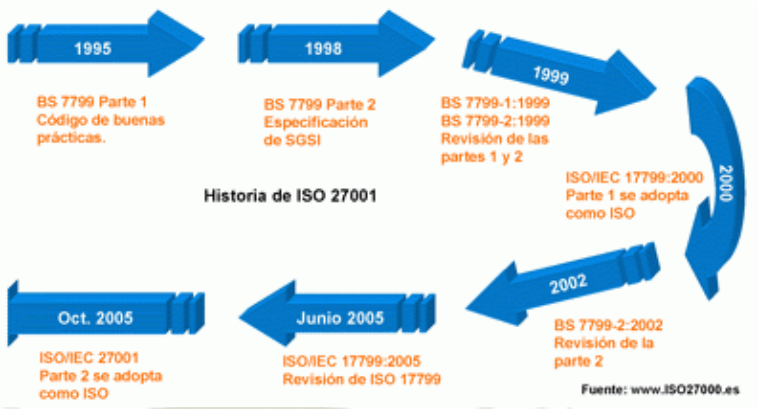


Figura 2. Historia de ISO27000

Fuente: "http://iso27000.es/iso27000.html" (Iso27000.es, n.d.-a)

Prosiguiendo con el desarrollo la serie 27000 se apoya en diferentes normas y guías las cuales complementan todo el desarrollo y mantenimiento del SGSI, dentro de estas guías de apoyo encontramos la norma ISO/IEC 27002 la cual es de interés para el presente proyecto.

2.2.3. ISO 27002

Según Lopez, Agustin (2005), la norma ISO 27002 es un estándar para la seguridad de la información publicada por la Organización Internacional de Normalización y de la Comisión Electrónica Internacional, con su versión más reciente en ISO/IEC 27002:2013.

Este documento contiene los controles a implementarse para la mitigación de riesgos, es un compendio de las mejores practicas según la colaboración de expertos en el tema de seguridad de la información, el mismo se compone de 14 dominios, 35 objetivos de control y 114 controles, según se detalla a continuación:

- **Políticas de Seguridad:** el presente dominio se refiere al desarrollo de un documento en el cual se detallen las directrices para la gestión de la seguridad de la información dentro de la organización, en la política se expresan las intenciones de la alta dirección para con la seguridad de la

información, el presente dominio se compone de 1 objetivo de control y 2 controles.

- **Aspectos Organizativos S.I.:** el objetivo es establecer la administración de la información como parte fundamental de los objetivos y actividades de la organización, designando los ámbitos de gestión, asignación de funcionales y responsabilidades, el mismo se compone de 2 objetivos de control y 7 controles.
- **Seguridad Ligada a los Recursos Humanos:** el objetivo del mismo es la concientización y toma de conocimiento de los colaboradores desde su ingreso para con la seguridad de la información, así mismo establece controles para la elección de personal idóneo y calificado además de poder tener conocimiento de la integridad de los colaboradores que ingresen, el mismo se compone de 3 objetivos de control y 6 controles.
- **Gestion de Activos:** el objetivo del presente dominio es la de identificar y tomar conocimiento de los activos de información que se poseen como parte importante de la administración de riesgos, y es en este dominio en el cual se hará más foco para el presente proyecto, el mismo se compone de 3 objetivos de control y 10 controles.
- **Control de Accesos:** el objetivo del dominio es controlar el acceso por medio de restricciones y excepciones a la información como base de todo sistema de seguridad informática, de tal manera de resguardar la información de accesos no autorizados, el dominio se compone de 4 objetivos de control y 14 controles.
- **Cifrado:** el dominio tiene por objetivo la utilización de sistemas y técnicas criptográficas para la protección de información sensible como contraseñas, entre otras, a fin de asegurar una adecuada protección de su confidencialidad e integridad, el mismo se compone de 1 objetivo de control y 2 controles.
- **Seguridad Física y Ambiental:** el objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la

organización, mediante el establecimiento de perímetros de seguridad y áreas protegidas, lo cual facilitará la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados, el mismo se compone de 2 objetivos de control y 15 controles.

- **Seguridad en la Operativa:** el objetivo del dominio es la de validar que se tiene en consideración los posibles impactos a la operativa, según los cambios que se vayan a realizar, así mismo se debe de tener documentación la misma que debe de controlarse, mantenerse y actualizarse, este dominio consta de 7 objetivos de control y 14 controles.
- **Seguridad en las Telecomunicaciones:** El objetivo del dominio es resguardar la seguridad de la información que transita por las redes, adicionalmente de garantizar la seguridad de la infraestructura de soporte, se debe de tener en cuenta la gestión de las redes, la cual abarca los límites organizacionales, el dominio se compone de 2 objetivos de control y 7 controles.
- **Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información:** el objetivo es la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas, se debe de contemplar la realización de documentación la cual incluya buenas practicas para el desarrollo seguro de aplicaciones y seguir un ciclo de desarrollo documentado bajos las normas adecuadas, se compone de 3 objetivos de control y 13 controles.
- **Relación con los Suministradores:** el objetivo es mantener un nivel adecuado de seguridad de la información y entrega de servicios prestados por terceros, los mismos que deben contemplar contratos cuyas clausulas estén orientadas a los objetivos de seguridad de la información de la organización, el mismo se compone de 2 objetivos de control y 5 controles.

- **Gestión de Incidentes:** el objetivo del dominio es la de darle el correcto tratamiento y gestión a las incidencias ocurridas hacia el sistema de gestión de seguridad de la información, de tal manera que se apliquen las acciones correctivas en el tiempo oportuno, este dominio lo componen 1 objetivo de control y 7 controles.
- **Aspectos de S.I. en la Continuidad del Negocio:** el objetivo es preservar la seguridad de la información en el desarrollo de los procedimientos y planes para la continuidad del negocio y de vuelta a la normalidad, se deben de considerar diferentes aspectos como la perdida de disponibilidad de información, perdida de integridad, o exposición de información y así mismo implementar planes de contingencia que contemplen estos escenarios, se compone de 2 objetivos de control y 4 controles.
- **Cumplimiento:** El objetivo del dominio es la de contemplar todas aquellas regulaciones legales que rijan según el estado o gobierno, para alinear de tal manera el sistema de gestión a la normativa en curso, el mismo se compone de 2 objetivos de control y 8 controles.

2.2.4. Métricas

Una métrica mide los resultados de un proceso o actividad a través de la determinación de si cierta variable cumple su objetivo especificado, los principios básicos incluyen métrica (ISO/IEC 20000).

Así mismo Corleti, Alejandro, de Alba, (n.d.), definen métrica como : “Una métrica de seguridad podría definirse como el conjunto de preceptos y reglas necesarios para poder medir de forma real el nivel de seguridad de una organización”

Por otro lado para la ISO/IEC 27004 las existen 2 tipos de medidas:

- **Medida Base:** Medida definida en términos de un atributo y el método para cuantificarlo.
- **Medida Derivada:** Medida que se define con la función de dos o más valores de medidas base.

– **Proceso de Medición:** Según la norma ISO/IEC 27004 se sigue una serie de pasos para el proceso de medición los cuales se pueden apreciar en la siguiente gráfica:

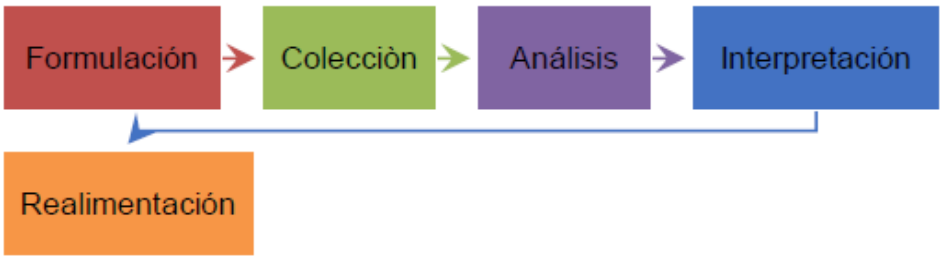


Figura 3. Proceso de Medición ISO/IEC27004

- Formulación: en esta parte el objetivo es el de elegir las métricas y medidas apropiadas para aplicar.
- Colección: se refiere a la parte de acumulación y obtención de todos los datos necesarios.
- Análisis: una vez se cuenten con la información recolectada en el paso anterior se procede con los cálculos de las métricas.
- Interpretación**:** culminado el paso anterior se realiza una evaluación con el fin de obtener una visión interna de la calidad de la representación.
- Realimentación: es la última etapa del proceso en la cual se realizan las mejoras identificadas según la interpretación de las métricas técnicas.

– **Creación de una Métrica:** Para la creación de una métrica se puede tomar en consideración lo indicado por Larrondo (2010), que en su proyecto titulado “Uso de la Norma ISO 27004 para la Auditoría Informática” nos indica que “a la hora de crear una métrica debemos de crear una tabla con toda la información correspondiente a dicha métrica, en el cual se indican todas las características que posee que van desde su nombre, propósito, costo que tiene para la empresa, localización, tipo, etc.”

- Titulo: Nombre significativo para describir la métrica.
- Propósito: Indicar para que esta diseñada la métrica, es decir que es lo que va a realizar.
- Costo: Consiste en la estimación de los costes reales de la recogida de la seguridad de dicha métrica.
- Tipo: Definimos que clase de métrica es.
- Localización: Aquí se sabrá donde se deben encontrar los datos a recoger, así como los datos previos utilizados con el fin de realizar dicha métrica.
- Frecuencia: Se refiere a la periodicidad para él recojo de datos, así como para la cantidad de veces para realizar la medición.

2.2.5. Activos de Información

Los activos de información son los recursos que utiliza el SGSI (Sistema de Gestión de Seguridad de la Información) para que las organizaciones funcionen y consigan los objetivos que se han propuesto la dirección según ISOTools Excellence en su Blog (https://www.pmg-ssi.com/).

Se puede entender por ende que los activos de información son todo aquel bien ya sea tangible, intangible, físico, digital ó humano el cual dada la naturaleza de su utilidad para la continuidad del negocio o resguardo de la información según los pilares de seguridad de la información resultan críticos para la organización.

Como parte de la implementación de un SGSI se requiere la identificación de los activos de información que se encuentren dentro del alcance de aplicación del sistema de gestión, esta etapa dentro de la implementación se le conoce como "Identificación de activos de la organización y definición de responsabilidades de protección apropiadas" según (NTP-ISO/IEC 27001:2014, 2014).

ISOTools Excellence en su articulo *"¿Cómo realizar un inventario de activos de información?"* (https://www.pmg-ssi.com/). Clasifica los activos de información en 3 grupos:

- Activos de información pura.
- Activos físicos.
- Activos Humanos.

Así mismo dentro de estos grupos se desglosa de forma general que activos pueden ser considerados dentro de cada categoría, para los fines del presente proyecto se desarrollaran los activos que forman parte del área Infraestructura de la organización, dentro de los activos de información pura se encuentran (Firewall, Servidor de base de datos, Servidor de correos, Servidor de telefonía VoIP, Directorio activo, Servidor de producción, Servidor de base de datos replicada y Servidor de impresión), para los activos físicos tendremos (Ambiente CDP (Centro de Datos Principal), Servidores Físicos, Centro de datos alterno, dispositivos de comunicaciones y Equipos terminales), a continuación se desglosan los activos:

- Ambiente de CDP (Centro de Datos Principal): Ambiente físico el cual alberga los servidores principales de la organización y en estos se albergan los principales servicios de la organización, se tienen estándares internacionales para el diseño confiable y seguro de un Centro de Datos, se tienen por ejemplo el estándar TIER implementado por Uptime Institute, así también se cuenta con la norma ANSI/TIA 942 entro otros.

	Tier I	Tier II	Tier III	Tier IV
Downtime anual	28.8 hrs	22.0 hrs	1.6 hrs	0.8 hrs
Disponibilidad	99.671%	99.741%	99.982%	99.995%

UPTIME INSTITUTE - White Paper
Tier Classification Defines Site Infraestructure Performance

Figura 4. Clasificación del Desempeño del Site

Fuente: Uptime Institute

- Firewall (Cortafuegos): Herramienta de Seguridad conocida como la a primera linea de defensa de la organización contra posible intentos de

acceso no autorizado a la red interna, es importante su gestión para evitar que la organización sea víctima de ataques externos.

Figura 5. Imagen de Firewall
Recuperado de https://www.globenetcorp.com

– Servidores Físicos (Hardware): Equipos Hardware que soportan entre otros el Sistema de Información Core, Gestor de Bases de datos, y en general los servicios prestados por el área de Tecnologías de Información en pro de la correcta operatividad de la organización, estos activos se encuentra albergados en el Ambiente CDP.

Figura 6. Servidores Físicos
Recuperado de https://www.valuehost.com.br

– Servidor de Base de Datos: En este activo se alberga el sistema gestor de base de datos que utilice la organización para el almacenamiento y gestión de la información (transacciones, pagos, información de clientes, etc.), por

esto el mismo es crítico para la continuidad de operaciones de la cooperativa.

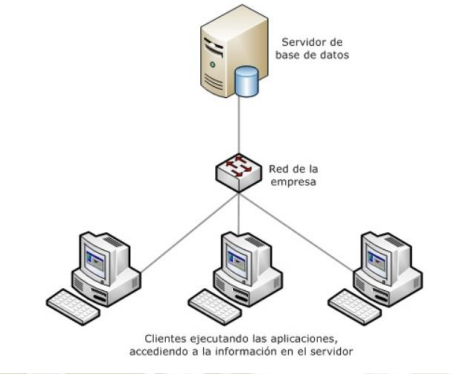


Figura 7. Serrvidor de Base de Datos

Recuperado de https://todoaccessvba.wordpress.com

– Servidor de Correos: Alberga el servicio de correo electrónico de la organización, es importante su gestión dado que es usual el tránsito de información crítica vía correo electrónico, como contratos, información sensible sobre clientes, autorizaciones, etc.

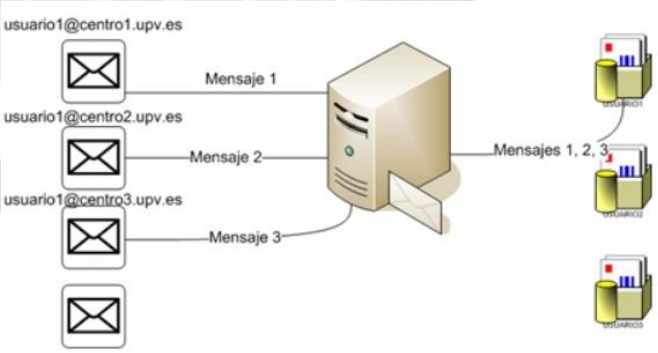


Figura 8. Proceso de Envió de Correos

Fuente: https://asic.blogs.upv.es

– Servidor de Telefonia VoIP: Alberga el servicio de telefonía de la organización, se debe de asegurar la disponibilidad de la comunicación tanto a nivel interno como externo de la organización, videoconferencias, llamadas con proveedores, etc.

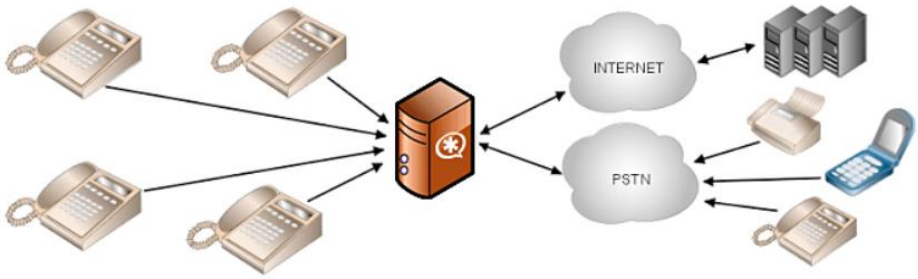


Figura 9. Modelo de Telefonía VoIP
Recuperado de http://www.salazarcarlos.com

– Directorio Activo: Este activo permite a los administradores de red gestionar los recursos de la red de la organización, la importancia del directorio activo radica en su capacidad de poder organizar y categorizar los usuarios de red, determinando políticas las cuales permitan fortalecer aspectos de seguridad, poder tener identificados a los distintos usuarios que se tienen creados en la organización.

Figura 10. Directorio Activo
Recuperado de https://www.solvetic.com

– Servidor de Producción: Junto con el servidor de Base de Datos es uno de los activos más importantes dentro de una organización si no el más importante, dado que este servidor es el que alberga el sistema core de la organización, todas las operaciones, transacciones, servicios, productos

que la organización oferte se gestionan mediante del Sistema de Información Core.

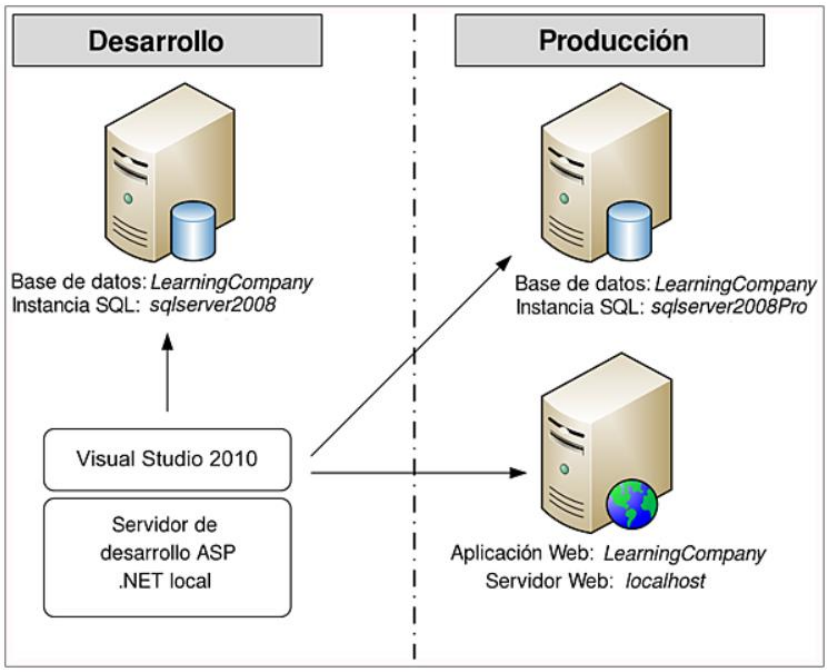


Figura 11. Servidor de Producción

Recuperado de https://www.ediciones-eni.com

- Centro de Datos Alterno: En este activo se albergan de manera preventiva los servicios básicos y las características mínimas requeridas con las cuales se puede garantizar la continuidad del negocio de la organización en caso se presente algún inconveniente que comprometa el centro de datos principal. Las buenas practicas en seguridad indican la necesidad e importancia de un centro de datos alterno, el cual debe de ser implementado en una localidad diferente a la del centro de datos principal.

- Dispositivos de Comunicaciones: En este punto se hace referencia a todos aquellos dispositivos que permitan la conexión y comunicación de terminales dentro de la organización.

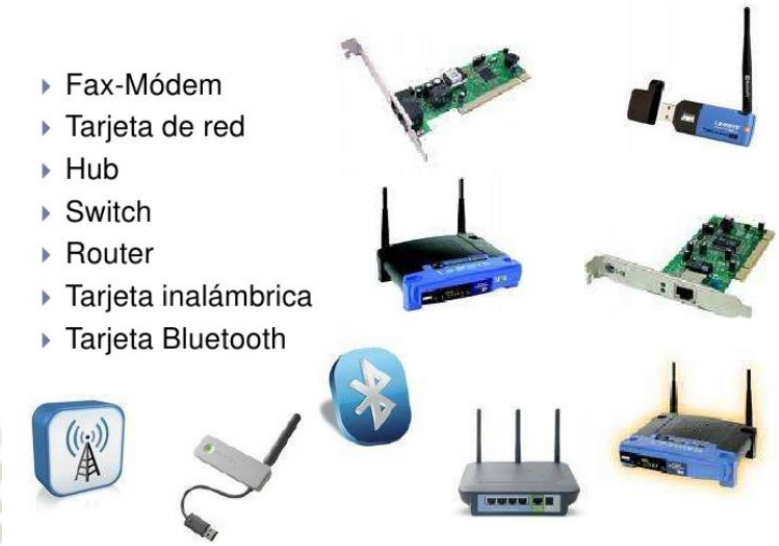


Figura 12. Dispositivos de Comunicaciones
Recuperado de https://es.slideshare.net

- Servidor de Base de Datos Replidaca: Para garantizar la continuidad del negocio, dentro de las buenas practicas de seguridad se requiere replicar la Base de Datos de producción en una Base de Datos alterna la cual almacenara información de las transacciones realizadas en caso suceda alguna incidencia con la Base de Datos principal.

- Servidor de impresión: Soporta el servicio de impresión de la Organización, se debe de garantizar la disponibilidad del servicio, ya que mediante este servicio se realizan las impresiones de contratos de servicio, contratos de personal, informes, etc.

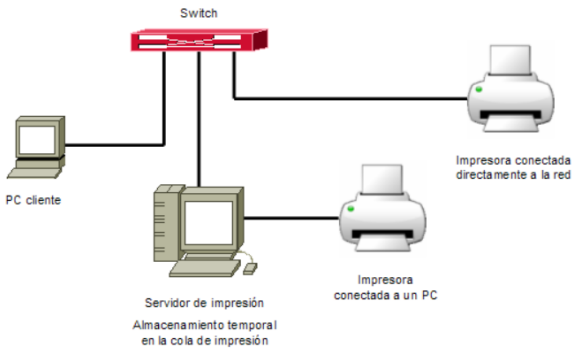


Figura 13. Servidor de Impresión

Recuperado de http://2008server.webcindario.com/linux/m5/servidor_de_impresin.html

- Equipos Terminales: Equipos para el desarrollo de las funciones de los colaboradores de la organización, se debe de velar por que estos funciones adecuadamente para que los colaboradores puedan desarrollar sin ningún inconveniente sus labores.

2.2.6. Continuidad del Negocio

Cuando nos referimos a continuidad del negocio nos referimos a una disciplina la cual entiende la capacidad de la organización para sobrevivir a las "cosas malas" que puedan tener un impacto negativo a la organización, esto va desde una infección por virus informático hasta incidentes naturales que puedan presentarse y que pongan en riesgos el correcto desarrollo de las operaciones de la organización.

Dentro de la continuidad del negocio se manejan diferentes conceptos dentro de los cuales para este proyecto son de interés 2:

- Tiempo Objetivo de Recuperación: Es el tiempo establecido por la empresa para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones, es menos al periodo máximo tolerable de interrupción (SBS, 2015).
- Periodo máximo tolerable de interrupción: Es el periodo de tiempo luego del cual la viabilidad de la empresa sería afectada seriamente, si un producto o servicio en particular no es reanudado (SBS, 2015).

CAPÍTULO III:

3. MARCO METODOLÓGICO

3.1. Alcances y Limitaciones

El presente trabajo tiene como alcance brindar a la empresa métricas mediante las cuales se puedan evaluar los activos de información del área de Infraestructura basándose en las normas internacionales ISO 27001 e ISO 27002, de esta manera se estandarizan los procesos y se garantiza que las métricas propuestas están basadas en normas internacional mundialmente aprobadas y adoptadas por otras organizaciones a nivel mundial. Junto con las métricas, una vez se identifiquen y valoricen los activos se podrá poner en marcha planes de acción para la implementación de controles que protejan la confidencialidad, disponibilidad e integridad de estos activos críticos.

No existe limitación para realizar la presente investigación, debido a que se cuenta con el conocimiento y asesoría necesaria para desarrollar las métricas de evaluación para activos de información del área de Infraestructura de T.I. basados en las normas internacionales ISO/IEC 27001 e ISO/IEC 27002 para la cooperativa la cual es caso de estudio en el presente proyecto, asimismo, se tiene acceso a una organización donde se puede operativizar la tesis, poniendo en práctica las métricas y tomar las lecturas que sean necesarias a efectos de obtener resultados que permitan determinar el grado de validación de dichas métricas.

3.2. Aporte

Las métricas propuestas para la evaluación de activos de información del área de infraestructura de la cooperativa, brindarán a la organización los indicadores para llevar a cabo una correcta evaluación de estos activos, tomar conciencia de cuales son los activos críticos, además de poder tomar acciones en caso se presenten incidentes que puedan ocasionar un impacto severo, basando el desarrollo de estas métricas en normas internacionales mundialmente aceptadas y adoptadas por muchas empresas,

lo que garantiza mayor nivel de cumplimiento y certeza al momento de evaluar, así mismo se homologarán procesos alineados a estándares internacionales.

3.3. Tipo y Nivel de Investigación

La presente investigación es de tipo aplicada, ya que la misma busca implementar las métricas planteadas en el área de Infraestructura de Tecnologías de la Información para una Cooperativa de Ahorros y Crédito, para la evaluación de los activos de información de esta área, basados en las normas internacionales ISO 27001 e ISO 27002 de Seguridad de la Información.

El nivel de investigación es descriptivo, ya que en el transcurso del desarrollo de la presente investigación se detallan los pasos que se siguieron para poder lograr plantear las métricas así como también el trabajo realizado previo al planteamiento propio de las métricas.

3.4. Población y Muestra O Universo

Para este caso el marco poblacional sujeto al estudio, tiene la característica de ser una empresa Financiera cuyas operaciones se limitan a las de una Cooperativa, en el Perú según reporta la SBS existen 437 cooperativas registradas de la cuales 50 se ubican en la ciudad de Arequipa.

La muestra puede ser probabilística o no probabilística, a efectos de validar la propuesta, se empleará una muestra no probabilística de tipo dirigida, la misma que estará conformada por una empresa financiera cuyas operaciones se limitan a las de una Cooperativa.

3.5. Métodos, Técnicas e Instrumentos Empleados

Para el presente proyecto se utilizará el método de la observación y muestreo selectivo de información clave, con la finalidad de poder tener un entendimiento del ambiente de la organización y desarrollo de las actividades por parte del área involucrada,

además de poder recoger la información relevante para el correcto desarrollo del presente proyecto.

Así mismo se utilizará la entrevista como técnica para establecer un diálogo con la gerencia y el área involucrada, así mismo se utilizará la técnica de análisis documental para poder obtener información que sea de interés para el desarrollo correcto del presente proyecto.

Para poder validar el grado de satisfacción con el proyecto se utilizará un cuestionario en el cual se formularán una cierta cantidad de preguntas dirigidas tanto a la gerencia como al área involucrada, esto nos brindará el nivel de satisfacción del área para con el proyecto planteado así como el análisis de resultados recogidos.

CAPÍTULO IV:

4. ELABORACIÓN DE MÉTRICAS PARA LOS ACTIVOS DEL ÁREA DE INFRAESTRUCTURA

4.1. Descripción De La Organización

Para el desarrollo del presente proyecto se ha tomado en consideración una entidad dedicada al rubro financiero cuyas operaciones se limitan a la de una cooperativa de ahorro y créditos a solicitud de la entidad se resguardará el nombre de la misma, la información obtenida de dicha cooperativa nos ayudara a poder establecer el contexto de la organización, así como de poder identificar los activos de información de la misma en su área de Infraestructura.

Es importante resaltar que la SBS (Superintendencia de Banca y Seguros) por sus siglas como ente regulador de todas las actividades financieras en el país, plantea mediante sus normativas los lineamientos para el correcto desempeño de las operaciones para las entidades crediticias, dentro de las diversas normativas que emite la SBS se pueden identificar las circulares G-140 para la Seguridad de la Información y G -180 para la Continuidad del Negocio, estas dos circulares se basan en los conceptos indicados en las normas internacionales ISO adecuándose a la realidad del Perú, es así que el desarrollo del presente proyecto que se basa en las normas ISO27001 e ISO27002 están alienadas a la documentación emitida por el regulador y que por ende son de conocimiento obligatorio de las organizaciones.

En su gran mayoría las entidades financieras cuentan con un área de Tecnologías de la Información en el cual se tiene al departamento de Infraestructura como la encargada de brindar el soporte necesario para el correcto funcionamiento de servidores tanto físicos como virtuales los cuales albergan los servicios de T.I. como el Sistema de Información principal, entre otros servicios esenciales para la operativa de la organización, así mismo esta área vela por el mantenimiento de las líneas de comunicación de la organización.

4.2. Desarrollo De Las Métricas Para Evaluación De Activos.

Para el desarrollo de las métricas se procederá a desarrollar las diferentes fases planificadas para poder identificar, diseñar e implementar dichas métricas para los activos de información del área de Infraestructura detalladamente.

Entonces para el desarrollo se seguirán los pasos según se detalla en la gráfica que se muestra lineas abajo:

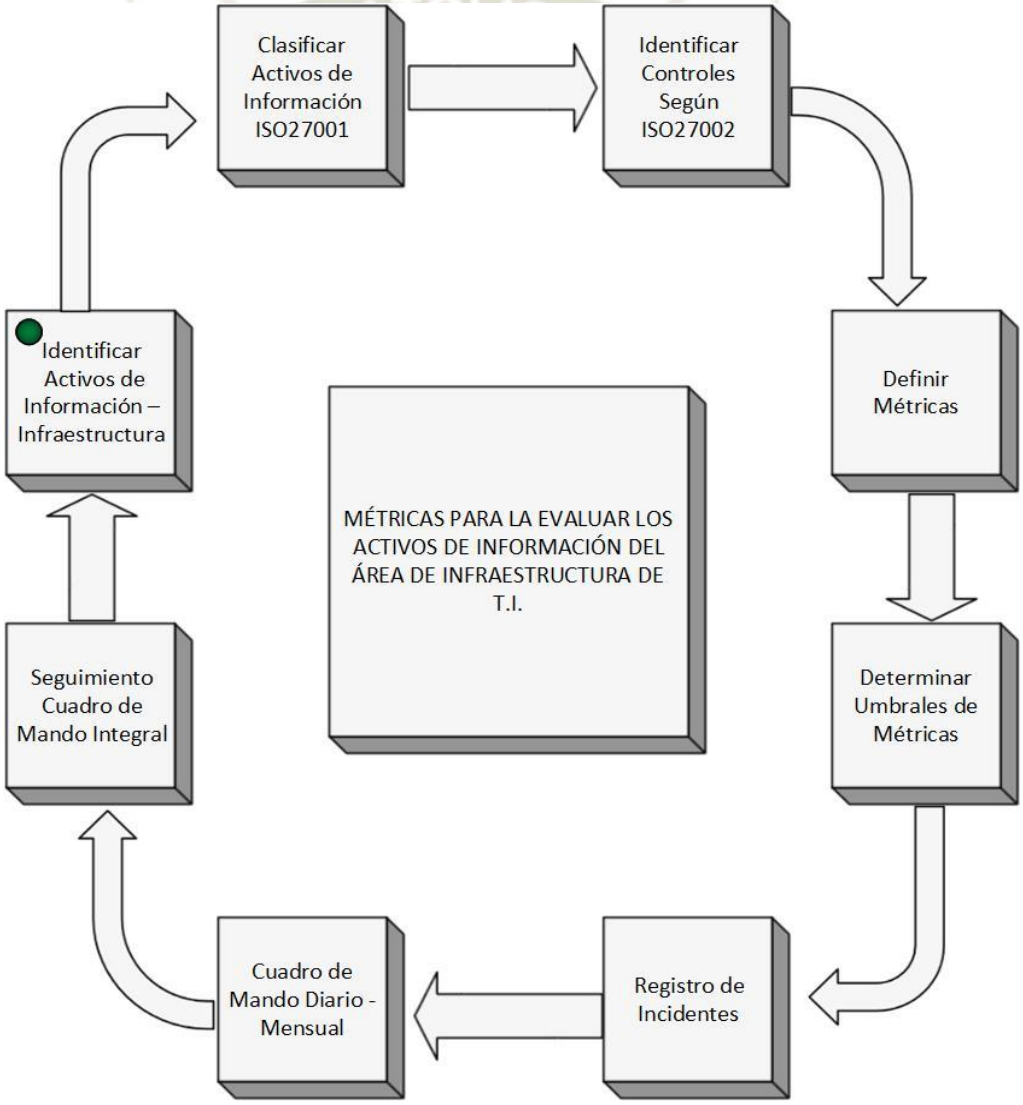


Figura 14. Modelo para la Elaboración de Métricas

Fuente: Elaboración Propia

Habiendo definido los pasos a seguir, se ha elaborado una plantilla la cual nos servirá para el desarrollo ordenado y correcto de las etapas antes descritas:

Tabla 1. Plantilla para identificación de activos de información

MÉTRICAS PARA ACTIVOS DE INFRAESTRUCTURA ISO 27001 - ISO 27002									
N°	ACTIVO DE INFORMACIÓN	DESCRIPCIÓN	TASACIÓN DE ACTIVOS POR PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN					CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PROMEDIO TASACIÓN	NIVEL DE TASACIÓN		
1									

Fuente: Elaboración propia

A continuación se procede a detallar cada campo:

- N° → En este campo se enumerarán la cantidad de activos de información que se vayan identificando.
- Activo de Información → En este campo se detallará el activo de información identificado.
- Descripción → En este campo se procederá a realizar una pequeña descripción del activo de información.
- Tasación de Activos de Información por principios de Seguridad de la Información → Esta sección comprendida por 5 campos contendrá los valores de calificación de los activos de información identificados, a continuación detallamos cada uno:
  - Confidencialidad → En este campo se debe de colocar una calificación del 1 al 5 según el nivel de confidencialidad del activo.
  - Integridad → En este campo se debe de colocar una calificación del 1 al 5 según el nivel la criticidad de conservar la integridad de la información del activo de información.
  - Disponibilidad → En este campo se debe de colocar una calificación del 1 al 5 según el nivel de importancia del activo en caso el mismo no se encuentre disponible en cuanto se requiera del mismo.
  - Promedio Tasación → En este campo se reflejará el promedio de la tasación según la formula que se detallará en adelante en el apartado clasificación de los activos de información.
  - Nivel de Tasación → En este campo se reflejará si el activo de información evaluado es “BAJO”, “MEDIO” o “ALTO”, según el promedio de tasación.
- Controles ISO 27002 Asociados → En este campo se colocarán los controles correspondientes al tipo de activo de información y a su clasificación, todos los controles seleccionados forman parte de la norma ISO27002.

- Métrica Asociada → En este campo se indicarán las métricas a considerar, esto teniendo en cuenta el control seleccionado, el tipo y clasificación de Activo de Información.

4.2.1. Identificación de Activos de Información Área de Infraestructura

En esta primera etapa se debe de llevar a cabo la identificación de los activos información del área de infraestructura, como se ha indicado en el capítulo anterior una de las etapas de la implementación de un sistema de gestión de seguridad de la información según la Norma ISO/IEC 27001 es la identificación de los activos de información, este es un proceso crítico para el éxito del sistema de gestión dado que a raíz de identificar los activos se podrán plantear los controles adecuados que son parte de la norma ISO27002.

De acuerdo a la experiencia adquirida por los años laborando en el área de seguridad de la información, tomando en consideración la data recogida en las visitas a la cooperativa y reuniones llevadas a cabo con la gerencia u jefatura de tecnologías de la información, se le planteó a la gerencia del área un listado de activos de información, los cuales son afines al área de Infraestructura o se encuentra bajo su gestión.

Según la criticidad que tiene cada activo para el área y continuidad de operaciones y servicios brindados por el área, así como aquellos activos que se requiere realizar un seguimiento, teniéndose los siguientes activos:

- Ambiente CDP (Centro de Datos Principal).
- Firewall.
- Servidores Físicos (Hardware).
- Servidor de Base de Datos.
- Servidor de Correos.
- Servidor de Telefonía VoIP.
- Directorio Activo.
- Servidor de Producción.
- Centro de Datos Alterno.

- Dispositivos de Comunicaciones.
- Servidor de Base de Datos Replicada.
- Servidor de impresión
- Equipos Terminales.

4.2.2. Clasificación de los activos según norma ISO/IEC 27001

La norma internacional ISO/IEC 27001 tiene como objetivo resguardar la información en cualquier medio o dispositivo en la que esta se almacene, bajo sus 3 pilares los cuales son:

- Confidencialidad.
- Integridad.
- Disponibilidad.

Tomando estos tres aspectos de la información, se determinó que los activos de información del área de infraestructura seleccionados, se clasifiquen según estos 3 aspectos dándole una ponderación a cada uno según corresponda para cada activo, esta clasificación se realizó en coordinación con la gerencia y jefatura de tecnologías de la información de la cooperativa.

Actualmente existen muchas metodologías para la gestión de riesgos y valorización de activos, la metodología MAGERIT V. 3.0 indica para poder determinar el valor de los activos lo siguiente:

“El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial” (Magerit, 2012).

Basándonos en lo que indica la metodología MAGERIT se entiende que el valor en esencia de un activo radica en la información contenida y servicios que estos prestan, entonces se puede concluir que lo indicado por la metodología está relacionada con los 3 pilares de la norma Internacional.

Se planteó una fórmula para categorizar los activos dándole una calificación cuantitativa a cada uno de estos basándonos en su confidencialidad, disponibilidad e integridad, así también se determinó una escala de calificación del 1 al 5, siendo 1 la calificación más baja y 5 la calificación más alta.

Entonces una vez colocadas las calificaciones se obtendrá un promedio de estas mediante la fórmula (C+D+I)/3, siendo C = Calificación de Confidencialidad, D = Calificación de Disponibilidad e I = Calificación de Integridad, resultado de las mismas se evaluará según el criterio detallado a continuación:

Resultado	Defición
4 - 5	ALTO
2 -3	MEDIO
1	BAJO

Figura 15. Escala de Clasificación

Fuente: Creación propia

Una vez realizada la clasificación se tuvo:

Tabla 2. Resultado de la Clasificación de activos de información del área de Infraestructura

N°	ACTIVO DE INFORMACIÓN	DESCRIPCIÓN	TASACIÓN DE ACTIVOS POR PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN				
			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PROMEDIO TASACIÓN	NIVEL DE TASACIÓN
1	Ambiente CDP	Ambiente físico en el cual se alojan los servidores físicos de la entidad	2	5	4	4	ALTO
2	Firewall	Cortafuegos de la Organización	4	3	5	4	ALTO
3	Servidores Físicos (Hardware)	Equipos en los cuales se instalaron servidores de la organización	3	4	5	4	ALTO
4	Servidor de Base de Datos	Servidor en el cual se ejecuta el SGBD	4	5	5	5	ALTO
5	Servidor de Correos	Servidor en el cual se ejecuta envíos y recepción de Correos Corporativos	3	3	4	3	MEDIO
6	Servidor de Telefonía VoIP	Servidor encargado de mantener el servicio de telefonía dentro de la organización	2	3	5	3	MEDIO

7	Directorio Activo	Herramienta mediante la cual se gestionan los usuarios de Red de la Organización	3	4	5	4	ALTO
8	Servidor de Producción	Servidor que aloja y en el que se ejecutan los aplicativos Core de la Organización	3	5	5	4	ALTO
9	Centro de Datos Alterno	Ambiente físico secundario en el cual se replica o se intenta replicar el Centro de Datos Principal en caso de Incidencias contra este ultimo	3	4	4	4	ALTO
10	Dispositivos de Comunicaciones	Equipos que brindan acceso a Internet y permitan la comunicación en red	2	4	4	3	MEDIO
11	Servidor de Base de Datos Replicada	Servidor en cual alberga la Base de Datos replicada en caso de incidencias contra la BD en producción	4	4	5	4	ALTO

12	Servidor de Impresión	Servidor que aloja el servicio de Impresión de la Organización	2	3	4	3	MEDIO
13	Equipos Terminales	Referido a los Terminales que ocupan los colaboradores de la Organización	1	3	3	2	MEDIO

Fuente: Elaboración Propia.

4.2.3. Identificación de Controles con Norma ISO/IEC 27002

Para esta etapa se tomó en consideración las características de los activos, así como también la utilidad, información contenida, criticidad para la operatividad de la organización y también los servicios del área de infraestructura que estos soportan, basándose en los dominios de la norma ISO 27002 y las características previamente descritas de los activos, se determinaron los controles para cada activo.

A continuación se procede a detallar activos asociados según controles asociados:

- **Ambiente CDP:**

  Para el Ambiente de Centro de Datos Principal, se han considerado 4 controles correspondientes a 2 objetivos de control las cuales son "áreas seguras" y "seguridad en los equipos", los mismos que corresponden al dominio de control Seguridad Física y Ambiental.

  La siguiente tabla muestra los controles según su objetivo de control y el Dominio al que pertenecen dentro de la Norma Internacional ISO27002:

Tabla 3. Controles para Ambiente CDP

ACTIVO - AMBIENTE CDP		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Seguridad física y ambiental	Áreas seguras	Controles físicos de entrada
		Protección contra amenazas externas y ambientales
	Seguridad de los equipos	Instalaciones de suministro
		Seguridad de cableado

Fuente: Elaboración Propia

- Controles físicos de entrada: Permitirá tener mapeado los ingresos realizados al centro de datos, los accesos se deben dar únicamente por el personal autorizado, el incumplimiento de

este control podría derivar en perdida de confidencialidad, integridad o disponibilidad tanto de los equipos alojados dentro del centro de datos como de los servicios que soportan los activos alojados dentro del ambiente.

- Protección contra las amenazas externas y ambientales: Se debe de considerar la posible ocurrencia de incidentes externos que afecten el centro de datos como incendio, inundación o algún incidente ambiental como un terremoto, el cual ocasione una paralización de los servicios y procesos que se ejecutan dentro de los activos alojados en el ambiente del centro de datos.
- Instalaciones de suministros: Se debe de garantizar la correcta instalación de los suministros eléctricos para prevenir fallas o paralización de actividades por cortes de fluido eléctrico, así mismo evitar daños que puedan darse hacia los activos por posibles cortes intempestivos, corto circuito, subidas de tensión.
- Seguridad en el cableado: Según la norma ISO 27002, se debe de proteger los cables tanto eléctricos como de red que transporten información, de posibles interferencias o daños.

– **Firewall:**

Se han seleccionado 3 controles correspondientes a los objetivos de control “requisitos del negocio para el control de accesos” y “gestión de la seguridad en las redes”, los mismos que corresponden a los objetivos de control, Control de Accesos y Seguridad en las Telecomunicaciones respectivamente, a continuación se muestra los dominios de control y objetivos de control asociados:

Tabla 4. Controles para Firewall

ACTIVO - FIREWALL		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Control de accesos	Requisitos de negocio para el control de accesos	Control de acceso a las redes y servicios asociados.
Seguridad en las telecomunicaciones	Gestión de seguridad en las redes	Controles de red

Fuente: Elaboración Propia

- Controles de acceso a las redes y servicios asociados: Se busca disminuir las incidencias por posibles equipos infectados por virus, se restringen los accesos en navegación de tal modo evitar que usuarios sin cultura de seguridad expongan sus equipos a posibles infecciones.
- Controles de red: Según la norma ISO27002 se deben de administrar y controlar las redes en pro de mantener seguros las aplicaciones y servicios prestados, monitoreando posibles intentos de ataques, accesos a páginas potencialmente peligrosas, etc.

– **Servidores Físicos (Hardware):**

Son los equipos que albergan los servicios de T.I. dentro de estos el Sistema Core de la Organización además de procesos críticos del negocio. Por ende se seleccionaron controles según las características de los activos así mismo tenemos, 5 controles correspondientes a 2 objetivos de control como son seguridad de los equipos y Clasificación de la información, estos forman parte de los dominios seguridad física y ambiental y gestión de activos respectivamente.

A continuación los dominios y objetivos de control de los cuales dependen los controles involucrados:

Tabla 5. Controles para Servidores Físicos

ACTIVO - SERVIDORES FÍSICOS (HARDWARE)		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Gestión de activos	Clasificación de la información	Manipulación de activos
Seguridad física y ambiental	Seguridad de los equipos	Instalaciones de suministros
		Seguridad del cableado
		Mantenimiento de los equipos
Seguridad en la operativa	Responsabilidades y procedimientos de operación	Gestión de capacidades

Fuente: Elaboración propia.

- Manipulación de Activos: La organización deberá de contar con personal debidamente capacitado para la manipulación y manejo de los servidores como instalación de los mismos, previniendo posibles fallas por mala manipulación de estos.
- Instalaciones de suministros: Se debe de garantizar la correcta instalación y correcto funcionamiento de los suministros de poder, de esta manera evitar caída del servicio por falta de suministro eléctrico o en su defecto daños por cortos.
- Seguridad en el Cableado: Se debe de proteger el cableado de red para evitar interferencias en las comunicaciones, perdida de comunicación o de integridad de la información que circula mediante estos.
- Mantenimiento de equipos: Es necesario garantizar el funcionamiento óptimo de los equipos, por ende se deben de realizar mantenimientos periódicos a estos, de tal manera se puedan prevenir incidentes por fallas de estos activos.

- Gestión de capacidades: Se busca prevenir incidentes por fallas relacionadas con sobrepasar la capacidad de los recursos requeridos para la correcta ejecución de los servicios o sistemas que se ejecutan en el servidor.

– **Servidor de Base de Datos:**

Es uno de los activos más críticos junto con el servidor de producción del área de infraestructura, en este activo se aloja la base de datos del sistema core de la organización, en cuanto a información, se trata del activo más crítico dado que de darse alguna incidencia en contra del mismo podría suponer perdida de información y se puede atentar contra los 3 pilares de seguridad de la información (confidencialidad, integridad y disponibilidad).

Considerando los riesgos a los cuales está afecto el servidor de base de datos, se han seleccionado 4 controles de la norma ISO27002 los cuales forman parte de los dominios control de accesos, Cifrado y seguridad en la operativa.

Tabla 6. Controles para Servidor de Base de Datos

ACTIVO - SERVIDOR DE BASE DE DATOS		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Control de accesos	Gestión de acceso de usuario	Revisión de los derechos de acceso de los usuarios
Cifrado	Controles criptográficos	Gestión de claves
Seguridad en la operativa	responsabilidades y procedimientos de operación	Gestión de capacidades
	Copias de seguridad	Copias de seguridad de la información

Fuente: Elaboración Propia.

- Revisión de los derechos de acceso de los usuarios: El acceso al Sistema Gestor de la Base de Datos, solo puede estar otorgado a personal debidamente autorizado y capacitado para el manejo de la información contenida.así mismo se debe administrar los privilegios brindados a los distintos usuarios que por sus labores deberán de ingresar a la base de datos de la organización.
- Gestión de claves: Se debe de utilizar técnicas criptográficas para la protección de la data contenida, así mismo la organización definirá un ciclo de vida de las contraseñas, se debe de controlar el cifrado de contraseñas para accesos a servicios y/o aplicativos de la organización.
- Gestión de Capacidades: Se debe de contemplar modificaciones a futuro que impacten en la Base de Datos, de tal manera que se planifique correctamente los recursos necesarios, así mismo evitar que la data ingresada no sea soportada por la base de datos.
- Copias de seguridad de la Información: Se debe de planificar la generación periódica de copias de seguridad de la Base de Datos, para de esta manera prevenir perdida de información, así mismo se debe de probar las copias restaurando las mismas y considerar tiempos de demora de restauración, para poder continuar con la correcta operativa.

– **Servidor de Correos:**

El servicio de mensajería electrónica debe de funcionar correctamente para no detener el flujo de información entre la organización y clientes o proveedores entre otros. Para el mismo se han considerado 2 controles pertenecientes a 2 dominios, “seguridad en la operativa” y “seguridad en las telecomunicaciones”:

Tabla 7. Controles para Servidor de Correos

ACTIVO - SERVIDOR DE CORREOS		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Seguridad en la operativa	responsabilidades y procedimientos de operación	Gestión de capacidades
Seguridad en las telecomunicaciones	Intercambio de información con partes externas	Mensajería electrónica

Fuente: Elaboración Propia.

- Gestión de capacidades: Se debe de controlar que la capacidad de almacenamiento del servidor sea la necesaria para garantizar el correcto funcionamiento del mismo y de esta manera evitar caídas en el servicio.
- Mensajería Electrónica: Se deben de configurar aspectos de seguridad para bloquear o identificar posibles correos maliciosos, estos deberán de ser identificados y gestionados para evitar una infección en la red, así mismo se debe de concientizar a los usuarios para que estos informen de correos sospechosos.

– **Servidor de Telfonía VoIP:**

Se debe de mantener disponible el servicio de telefonía para garantizar la comunicación tanto entre usuarios internos como también con usuarios externos, para el activo se han seleccionado 2 controles según la norma ISO27002 correspondientes a los dominios como es Seguridad en las Telecomunicaciones y seguridad en los equipos:

Tabla 8. Controles para Servidor de Telefonia VoIP

ACTIVO – SERVIDOR DE TELEFONIÍA VoIP		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Seguridad en las telecomunicaciones	Gestión de seguridad en las redes	Mecanismos de seguridad asociados a servicios en red
Seguridad física y ambiental	Seguridad de los equipos	Mantenimiento de los equipos

Fuente: Elaboración Propia.

- Mecanismos de seguridad asociados a servicios en red: Según la norma ISO27002 se debe de proteger todos los servicios que estén asociados a la red sean estos externos o internos, así mismo se debe determinar los niveles de servicio para garantizar el levantamiento del servicio.
- Mantenimiento de equipos: Se debe de garantizar la continuidad del servicio de telefonía mediante el correcto mantenimiento de los equipos que soporten dicho servicio.

– **Directorio Activo:**

Se deben de gestionar correctamente todos los privilegios a escala de red para evitar abuso de privilegios o violación de información sensible de la organización, así mismo se debe de administrar el alta y cese de nuevos usuarios de la organización para que puedan empezar con sus funciones, pare esto se han considerado 4 controles los mismos que forman parte de los dominios, control de accesos y seguridad en la operativa.

Tabla 9. Controles para Directorio Activo

ACTIVO – DIRECTORIO ACTIVO		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Control de accesos	Requisitos del negocio para el control de accesos	Control de acceso a las redes y servicios asociados
	Gestión de acceso de usuario	Gestión de altas/bajas en el registro de usuarios
		Retirada o adaptación de los derechos de acceso
Seguridad en la operativa	Gestión de vulnerabilidad técnica	Restricción en la instalación de software

Fuente: Elaboración Propia.

- Control de acceso a las redes y servicios asociados: el control busca administrar y controlar de manera correcta los servicios y permisos que se le otorgaran a los usuarios de acuerdo a las labores a realizar, el usuario solo podrá contar con todos privilegios necesarios para su correcto desempeño laboral.
- Gestión de altas/bajas en el registro de usuarios: la norma ISO27002 pide realizar una gestión sobre la creación y baja de usuarios, esto con la finalidad de poder llevar un control y evitar el uso de cuentas cesadas por terceros, así mismo se debe de promover el alta de usuarios en tiempos cortos o establecidos por la organización los cuales no afecten el pronto desarrollo de las funciones del usuario ingresante.
- Retirada o adaptación de los derechos de acceso: se debe de controlar los derechos de acceso otorgados en diversos casos ya sea por promociones internas, altas nuevas o acceso para terceros a los sistemas de información de la organización, ya que el no llevar el control podría exponer información la cual no debería poder ser accedida por cualquier usuario.

- Restricción en la instalación del software: el objetivo del control es que los usuarios de los equipos eviten instalar software que podría resultar potencialmente riesgoso para la red institucional, solo debería de poder instalar software el equipo de Tecnologías de Información mediante una debida autorización.

– **Servidor de Producción:**

El servidor de producción soporta el sistema de información core del negocio y todas las operaciones que se realicen para el usuario interno y externo de la organización se presenta como uno de los activos más críticos del área de infraestructura y de la organización en sí, tomando en cuanta esto se han seleccionado 5 controles correspondientes a 2 dominios, seguridad en la operativa y seguridad en las telecomunicaciones:

Tabla 10. Controles para Servidor de Producción

ACTIVO - SERVIDOR DE PRODUCCIÓN		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Seguridad en la operativa	Responsabilidades y procedimientos de operación	Gestión de cambios
	Registro de actividad y supervisión	Sincronización de relojes
		Registros de actividad del administrador y operador del sistema
	Protección contra código malicioso	Controles contra código malicioso
Seguridad en las telecomunicaciones	Gestión de seguridad en las redes	Segregación de redes

Fuente: Elaboración Propia.

- Gestión de Cambios: la norma nos indica que se debe de controlar los cambios que se realicen en ambientes de procesamiento de datos con la finalidad de evitar ocasionar incidencias que puedan decaer en paralización de la operativa, así mismo controlar cambios que puedan afectar la seguridad de la información, ya sea por pases a producción por desarrollos o por cambios en el propio servidor.
- Sincronización de relojes: se debe de procurar que los relojes de los activos involucrados en el procesamiento de información estén sincronizados, de esta manera se podrá garantizar integridad en la información y así mismo se hará posible realizar trazabilidad de información.
- Controles contra el código malicioso: se debe de garantizar que el servidor esta debidamente resguardado en contra de virus, malware o cualquier tipo de infección que ponga en riesgo su correcto funcionamiento.
- Registros de actividad del administrador y operador del sistema: se tiene que llevar un registro "log" de las actividades realizadas por usuarios privilegiados, en este caso el administrador y operador del sistema en busca de posibles malas manipulaciones o accesos no autorizados a información sensible.
- Segregación de redes: es necesario realizar la separación o segmentación de redes teniendo en consideración segmentos de usuarios internos, segmentos de producción, segmentos de desarrollo, etc. De tal manera garantizar que la red en la cual se brindan los servicios de producción no puedan ser accedidos o estén expuestos a terceros no autorizados.

– **Centro de Datos Alterno:**

Se han seleccionado 3 controles los cuales pertenecen a 2 dominios de control los cuales son seguridad física y ambiental y aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Tabla 11. Controles para Centro de Datos Alterno

ACTIVO - SERVIDOR DE PRODUCCIÓN		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Seguridad física y ambiental	Seguridad de los equipos	Emplazamiento y protección de equipos
		Mantenimiento de los equipos
Aspectos de S.I. en la continuidad del negocio	Redundancias	Disponibilidad de instalaciones para el procesamiento de la información

Fuente: Elaboración Propia.

- Emplazamiento y protección de equipos: Garantizar la correcta operatividad de los equipos albergados en el centro de datos alterno cuando se requiera de estos, así también protegerlos de incidentes ambientales y accesos no autorizados.
- Mantenimiento de Equipos: Garantizar la operatividad de los equipos y desempeño correcto de los mismos, mediante el su correcto mantenimiento y monitoreo.
- Disponibilidad de instalaciones para el procesamiento de la información: Se debe de garantizar que el centro alterno estará disponible en cuanto se requiera de este, por ende se deben de realizar pruebas traslado de operaciones al centro alterno y determinar si estas son satisfactorias o no.

– **Dispositivos de Comunicaciones:**

Se deben de mantener operativas las conexiones a la red tanto interna como externa, por ende se deben de mantener operativos los dispositivos de comunicación, tales como, routers, antenas de comunicaciones, switches, etc.

Tabla 12. Controles para Dispositivos de Comunicaciones

ACTIVO - SERVIDOR DE PRODUCCIÓN		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Seguridad física y ambiental	Seguridad de los equipos	Mantenimiento de los equipos

Fuente: Elaboración Propia

- Mantenimiento de Equipos: Se debe de evitar caída de las comunicaciones por falta del correcto mantenimiento de los dispositivos que soporten este servicio.

– **Servidor de Base de Datos Replicada:**

Este activo se encuentra en servidor albergado en el centro de datos alterno y en el mismo se replican y almacenan las operaciones realizadas en la base de datos de producción.

Tabla 13. Controles para Servidor de Base de Datos Replicada

ACTIVO - SERVIDOR DE PRODUCCIÓN		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Control de accesos	Gestión de acceso de usuario	Revisión de los derechos de acceso de los usuarios

Fuente: Elaboración Propia.

- Revisión de los derechos de acceso de los usuarios: Se debe de monitorear e identificar posibles accesos o intentos de acceso, por personal no autorizado para evitar manos manejos de información sensible o intento de intrusión para poder obtener información.

– **Servidor de Impresión:**

Se hace necesario garantizar que el servicio de impresión se mantenga operativo, para de tal manera no interrumpir por ejemplo la generación de contratos o documentación crítica para la operativa del negocio, para tal efecto se han seleccionado 3 controles los cuales pertenecen a 2 dominios de control como son "Gestión de Activos" y "Seguridad en la Operativa", es así que se tiene:

Tabla 14. Controles para Servidor de Impresión

ACTIVO - SERVIDOR DE IMPRESIÓN		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Gestión de activos	Responsabilidad sobre los activos	Uso aceptable de los activos
Seguridad en la operativa	Responsabilidades y procedimientos de operación	Gestión de capacidades
	Gestión de la vulnerabilidad técnica	Gestión de las vulnerabilidades técnicas

Fuente: Elaboración Propia

- Uso aceptable de activos: Se debe de controlar que el activo sea utilizado de manera correcta, para los fines previstos y de carácter laboral más no para otros fines, el presente control no se aplica únicamente al servidor sino también a todo equipo relacionado con el servicio.

- Gestión de capacidades: Se debe de monitorear que los recursos del activo sean las mínimas requeridas para el correcto desarrollo de la operativa.
- Gestión de vulnerabilidades técnicas: Se deben controlar las fallas técnicas que se presenten para el activo, así mismo se debería tener conocimiento de los posibles fallos técnicos a los cuales puede estar expuesto el mismo.

– **Equipos Terminales:**

Por último se cuenta con los equipos terminales o PC's otorgadas a los colaboradores para el correcto desempeño de sus funciones, así mismo se debe de controlar y monitorear el correcto desempeño del activo, para tal fin se han seleccionado 4 controles los mismos que pertenecen a los dominios de control "Gestión de Activos" y "Seguridad en la Operativa":

Tabla 15. Controles para equipos terminales

ACTIVO – EQUIPOS TERMINALES		
DOMINIO DE CONTROL	**OBJETIVO DE CONTROL**	**CONTROL**
Gestión de activos	Responsabilidad sobre los activos	Uso aceptable de los activos
Seguridad en la operativa	Responsabilidades y procedimientos de operación	Gestión de capacidades
	Gestión de la vulnerabilidad técnica	Gestión de las vulnerabilidades técnicas

Fuente: Elaboración Propia.

- Uso aceptable de activos: Se debe de controlar que los activos se utilicen para temas laborales solamente, así como también realizar revisiones las cuales permitan identificar si los equipos no tiene instalados software no permitido por la organización.

- Gestión de capacidades: Se debe de controlar que los equipos cuenten con los recursos necesarios para el correcto desempeño de las labores de los colaboradores.
- Gestión de vulnerabilidades técnicas: Se deben controlar las fallas técnicas que se presenten para el activo, así mismo se debería tener conocimiento de los posibles fallos técnicos a los cuales puede estar expuesto el activo.

En la siguiente tabla se muestra cuantos dominios de control, objetivos de control y controles se han seleccionado de la norma ISO27002, de los 14 “Dominios de Control”, 35 “Objetivos de Control” y 114 “Controles” que comprende la norma, se consideró para el presente proyecto, 7 “Dominios de Control” lo que equivale al 50% del total, 15 “Objetivos de Control” equivalente al 43% del total y 25 “Controles” equivalente al 22% del total indicado en la Norma.

Tabla 16. Consolidado de controles seleccionados de la norma ISO27002

DOMINIO DE CONTROL	OBJETIVO DE CONTROL	CONTROL	DOMINIO DE CONTROL	OBJETIVO DE CONTROL	CONTROL
Gestión de Activos	Clasificación de la información	Manipulación de activos	Seguridad en la operativa	Responsabilidad y procedimientos de operación	Gestión de capacidades
	Responsabilidad sobre los activos	Uso aceptable de los activos			Gestión de cambios
Control de Accesos	Requisitos de negocio para el control de accesos	Control de acceso de las redes y servicios asociados		Copias de seguridad	Copias de seguridad de la información
	Gestión de acceso de usuario	Revisión de los derechos de acceso de los usuarios		Gestión de vulnerabilidad técnica	Restricción en la instalación de software
		Gestión de altas/bajas en el registro de usuarios			Gestión de las vulnerabilidades técnicas
		Retirada o adaptación de los derechos de acceso			Sincronización de relojes

Cifrado	Controles criptográficos	Gestión de claves		Registro de actividad y supervisión	Registro de actividades del administrador y operador del sistema
Seguridad física y ambiental	Áreas seguras	Controles físicos de entrada		Protección contra código malicioso	Controles contra código malicioso
		Protección contra amenazas externas y ambientales	Seguridad en las telecomunicaciones	Gestión de seguridad en las redes	Mecanismos de seguridad asociados a servicios en red
	Seguridad de los equipos	Instalaciones de suministro			Segregación de redes
		Seguridad en el cableado		Intercambio de información con partes externas	Mensajería electrónica
		Mantenimiento de los equipos	Aspectos de seguridad de la información en la continuidad del negocio	Redundancias	Disponibilidad de instalaciones para el procesamiento de la información
		Emplazamiento y protección de equipos			

Fuente: Elaboración Propia

4.2.4. Determinación de Métricas

En la presente etapa se procederá a determinar las métricas acordes a los activos de información identificados y también en relación con los controles de la norma ISO27002 previamente seleccionados, entonces a continuación procederemos a detallar las métricas desarrolladas:

- **Ambiente CDP:**

Tabla 17. Métricas para activo Ambiente CDP

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Ambiente CDP	Controles físicos de entrada	# de accesos a ambientes físicos por personal no autorizado
	Protección contra las amenazas externas y ambientales.	# de incidencias presentadas por eventos externos o naturales
	Instalaciones de suministro	# de fallas del suministro eléctrico
	Seguridad del cableado	# incidencias por fallos de equipos

Fuente: Elaboración Propia.

Para el activo Centro de Datos se han determinado 4 métricas acorde a los cuatro controles seleccionados, a continuación se detalla cada uno de ellos:

- Número de accesos a ambientes físicos por personal no autorizado: Se debe poder identificar accesos no autorizados, para de tal manera evitar que personal no autorizado o no preparado ocasione incidencias por malas manipulaciones o fallas por acciones premeditadas.
- Número de incidencias presentadas por eventos externos o naturales: Registrar incidentes que procedan ya sea por hechos

naturales o por causas externas ayudará a tomar precauciones ante eventos iguales.

- Número de fallas del suministro eléctrico: Se debe de registrar y monitorear las fallas que se puedan ocasionar debido a problemas en las instalaciones eléctricas del ambiente de datos.
- Incidencias por fallos de equipos: Se debe de monitorear las fallas o incidencias que se presenten por una mala organización del cableado dentro del centro de datos.

– **Firewall:**

Tabla 18. Métricas para activo Firewall

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Firewall	Control de acceso a las redes y servicios asociados	# de accesos no permitidos en red por usuarios.
	Controles de red	# de intentos de intrusión a la red

Fuente: Elaboración Propia.

Para el activo se han considerado 2 métricas:

- Número de Accesos no permitidos en red por usuarios: Se debe de garantizar que cada uno de los usuarios de la organización cuenta con los accesos en red según las necesidades que demanden sus funciones, brindando permisos de navegación necesarios y así evitar que el usuario visite páginas no permitidas o sature la red.
- Número de intentos de intrusión a la red: Se debe de monitorear y registrar los intentos de posibles ataques externos, tomando en consideración que actualmente la ciberdelincuencia está en aumento.

– **Servidores Fisícos (Hardware):**

Tabla 19. Métricas para activo Servidores Físicos

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Servidores Físicos (Hardware)	Mantenimiento de los equipos	# de fallas de equipos por falta de mantenimiento.
	Manipulación de activos	# de incidencias por mala manipulación de servidores
	Gestión de capacidades	# de fallas por déficit en funcionamiento
	Instalaciones de suministro	# de fallas del suministro eléctrico
	Seguridad del cableado	# incidencias por fallos de equipos

Fuente: Elaboración Propia.

Para el activo se han considerado 5 métricas:

- Número de fallas de equipos por falta de mantenimiento: Se debe de llevar un monitoreo de los equipos que por falta de mantenimiento presenten fallas, esto ayudará a gestionar de mejor manera el calendario de mantenimientos definido.
- Número de incidentes por mala manipulación de servidores: En esta métrica se desea llevar un control de cuantas incidencias se pueden presentar por cualquier mala manipulación de servidores, ya sea por personal de limpieza mal capacitado, personal nuevo que no cuenta con la experiencia necesaria para la manipulación de los servidores, etc.
- Número de incidentes por déficit en funcionamiento: Registrar las incidencias que se presenten por sobrepasar los recursos disponibles del activo, ayudará a planificar de mejor manera la adquisición o repotenciación de los activos, para

que de esta manera soporten el crecimiento de la organización y no se paralicen los servicios.

- Número de fallas del suministro eléctrico: Se debe de llevar un control de posibles incidencias por fallas eléctricas de los equipos de energía tanto principales como de contingencia que apoyen a los servidores.
- Número de incidencias por fallos de equipos: Se debe de registrar los incidentes relacionados con fallas del servidor en red como falta de orden en el cableado, duplicidad de IP's, etc.

– **Servidor de Base de Datos:**

Tabla 20. Métricas para activo Servidor de Base de Datos

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Servidor de Base de Datos	Revisión de los derechos de acceso de los usuarios	# accesos no autorizados a la BD
	Gestión de claves	# incidencias por claves no cifradas en la BD
	Copias de seguridad de la información	# incidencias por fallas al realizar o reestablecer backups
	Gestión de capacidades	# Incidencias por déficit de rendimiento de activo

Fuente: Elaboración Propia.

Para el activo se han definido 4 métricas:

- Número de accesos no autorizados a la Base de Datos: Se debe de poder identificar accesos no autorizados al activo, de tal manera que se pueda identificar posibles manipulaciones o intentos de manipulación a la misma.

- Número de incidencias por claves no cifradas en la Base de Datos: Se debe de realizar revisiones de manera periódica las cuales demuestren que se realiza la encriptación de claves del sistema, las tablas que mantengan contraseñas en la Base de Datos deben de tener un algoritmo de cifrado, así mismo se debe de solicitar los cambios periódicos de las contraseñas.
- Número de incidencias por fallas al realizar o reestablecer backups: Se debe de llevar un registro de todas aquellas incidencias que se produzcan al realizar un Backup de la Base de Datos y así mismo incidencias que se presenten al reestablecer las mismas, de tal manera poder tener mapeado estos incidentes y poder tomar acciones correctivas.
- Número de Incidencias por déficit de rendimiento de activo: Se debe de monitorear el desempeño de la Base de Datos y registrar cualquier incidencia producida a raíz de falta de recursos para procesar alguna solicitud a la misma.

– **Servidor de Correos:**

Tabla 21. Métricas para activo Servidor de Correos

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Servidor de correos	Gestión de capacidades	# incidencias por caída de correos
	Mensajería electrónica	# incidencias por correos maliciosos

Fuente: Elaboración Propia.

Para el activo se han determinado 2 métricas:

- Número de incidencias por caída de correos: Se debe de llevar un registro de la cantidad de incidencias que se puedan presentar por caída del servicio de correo electrónico, ya sea

porque el servicio se interrumpe o por una caída total del mismo.

- Número de incidencias por correos maliciosos: Se debe de monitorear los intentos de infección de los sistemas mediante correos maliciosos o intentos de ataques mediante phishing.

– **Servidor de Telefonía VoIP:**

Tabla 22. Métricas para activo Servidor de Telefonía VoIP

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Servidor de Telefonía VoIP	Mecanismos de seguridad asociados a servicios en red	# incidencias de red no permitida
		# solicitudes de información
	Mantenimiento de los equipos	# perdidas de comunicación o conexión

Fuente: Elaboración Propia.

Para el activo se ha determinado 3 métrica:

- Número de incidencias de red no permitida: la métrica está relacionada a las incidencias por intentos de comunicación con anexos o destinatarios no permitidos.
- Número de Solicitudes de Información: la métrica está relacionada con las incidencias que se presenten por no actualizar el directorio telefónico de la organización y esto conlleve a perdida de comunicación con estos nuevos anexos.
- Número de perdidas de comunicación o conexión: Se debe de garantizar en la medida de lo posible la fluidez en la

comunicación tanto de clientes internos como de estos con usuarios externos mediante las líneas telefónicas.

– **Directorio Activo:**

Tabla 23. Métricas para activo Directorio Activo

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Directorio Activo	Control de acceso a las redes y servicios asociados	# fallas por privilegios mal asignados a usuarios
	Gestión de Altas/Bajas en el registro de usuarios	# incidencias por demora en alta/baja de usuarios
	Retirada o adaptación de los derechos de acceso	# incidencias por identificación de usuarios no desactivados / derechos de acceso erróneos
	Restricción en la instalación de software	# de equipos con software no autorizado

Fuente: Elaboración Propia.

Para el activo se han determinado 4 métricas:

- Número de fallas por privilegios mal asignados a usuarios: Se deben identificar y registrar los incidentes por privilegios mal otorgados a usuario o grupo de usuarios, que puedan ocasionar el acceso no autorizado a información o temas que no corresponda al usuario.
- Número de incidencias por demora en alta/baja de usuarios: Se deben de registrar las incidencias por demora en cese o alta de usuarios, para de esta manera gestionar de manera correcta el proceso y evitar retrasos a usuarios nuevos y/o abusos por uso de cuentas cesadas por terceros.

- Número de incidencias por identificación de usuarios no desactivados / derechos de acceso erroneos: Se debe de monitorear cada cierto periodo de tiempo que las cuentas de usuarios cesados hayan sido inhabilitadas correctamente, así mismo se debe de administrar los derechos de accesos de los usuarios sobre el sistema core de la organización.
- Número de equipos con software no autorizado: Se debe registrar las incidencias por identificación de equipos con software no permitido por la organización instalado.

– **Servidor de Producción:**

Tabla 24. Métricas para activo Servidor de Producción

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Servidor de Producción	Gestión de Cambios	# Incidencias por error en cambios de pases a producción
	Sincronización de Relojes	# de fallas en sincronización de relojes
	Controles contra el código malicioso	# incidentes de infecciones por software malicioso
	Registros de actividad del administrados y operador del sistema	# intentos fallidos de ingresos al Servidor
	Segregación de redes	# equipos no autorizados en red de producción

Fuente: Elaboración Propia.

Se han determinado 5 métricas para el activo:

- Número de Incidencias por error en cambios de pases a producción: Se debe de registrar los errores o incidencias que se presenten producto de cambios en el sistema, es decir

nuevos desarrollos, nuevos módulos que entren en producción, etc.

- Número de fallas en sincronización de relojes: Se debe de garantizar que los relojes de los terminales estén sincronizados a fin de poder mantener la información integra para las transacciones u operaciones realizadas.
- Número de incidentes de infecciones por software malicioso: Se debe registrar incidentes relacionados con fallas del servidor que puedan estar relacionadas con posible software malicioso albergado en el mismo.
- Número de intentos fallidos de ingreso al servidor: Se debe de poder identificar y registrar todo aquel intento de acceso al servidor por parte de usuarios no autorizados, ya sea por ataques de fuerza bruta, entre otros.
- Número de equipos no autorizados en red de producción: Se debe de monitorear la segregación de las redes, a fin de poder identificar terminales que no deberían de estar en red de producción por ejemplo los terminales de los equipos de desarrollo no deberían de estar en la misma red que la de producción.

– **Centro de Datos Alterno:**

Tabla 25. Métricas para activo Centro de Datos Alterno

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Centro de Datos Alterno	Emplazamiento y protección de equipos	# equipos en mal estado
	Mantenimiento de los equipos	# de pruebas erróneas por funcionamiento de equipos

	Disponibilidad de instalaciones para el procesamiento de la información	# de pruebas erróneas al activar centro de datos alterno

Fuente: Elaboración Propia.

Para el activo se han determinado 3 métricas:

- Número de equipos en mal estado: Se debe de identificar y registrar los incidentes que involucren equipos en mal estado, para de tal manera garantizar el óptimo rendimiento del centro alterno, de ser necesario trasladar operaciones al mismo.
- Número de pruebas erroneas de funcionamiento de equipos: Se debe registrar todo incidente relacionado con deficiencias en el ámbito de los sistemas y software de los equipos en el centro alterno, de las pruebas realizadas al trasladar operaciones.
- Número de prubeas erróneas al activar centro de datos alterno: Se debe de registrar los incidentes que se presenten al intentar poner en funcionamiento el centro de datos alterno como parte de las pruebas por continuidad del negocio.

– **Dispositivos de Comunicaciones:**

Tabla 26. Métricas para activo Dispositivos de Comunicaciones

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Dispositivos de Comunicaciones	Mantenimiento de los Equipos	# de incidencias por perdida de comunicación

Fuente: Elaboración Propia.

Se ha determinado 1 métrica para el activo:

- Número de incidencias por perdida de comunicación: Se debe de llevar un registro de todos aquellos incidentes que se puedan dar a raíz de perdidas de comunicación o fallas en los dispositivos de comunicación.

– **Servidor de Base de Datos Replicada:**

Tabla 27. Métricas para activo Servidor de Base de Datos Replicada

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Servidor de Base de Datos Replicada	Revisión de los derechos de acceso de los usuarios	# de accesos no autorizados a la BD alterna

Fuente: Elaboración Propia

Se ha determinado 1 métrica para el activo:

- Número de accesos no autorizados a la Base de Datos Alterna: Se deben de registrar todo intento de acceso no autorizado a la base de datos replicada, esto mediante la revisión de logs de acceso de la Base de Datos.

– **Servidor de Impresión:**

Tabla 28. Métricas para activo Servidor de Impresión

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Servidor de Base de Datos Replicada	Uso aceptable de los activos	# incidencias por error de formato de hojas
		# de fallas en el equipo
	Gestión de capacidades	# de pérdidas de comunicación con el servidor

	Gestión de vulnerabilidades técnicas	# de fallas en la cola de impresión

Fuente: Elaboración Propia

Se han determinado 4 métricas para el activo:

- Número de incidencias por error de formato de hojas: Se deben de monitorear los errores que se presenten en caso no se puedan realizar impresiones por algún error de formato de archivo o de hoja al imprimir.
- Número de fallas de equipos: Se deben de monitorear los equipos que forman parte de los servicios de impresión y registrar las fallas de estos.
- Número de perdidas de comunicación con el servidor: Se debe de monitorear los eventos de perdida de comunicación con el servidor de impresión lo cual detenga este servicio.
- Número de fallas en al cola de impresión: Identificar los errores que bloqueen la cola de impresión por enviar archivos los cuales produzcan dicho bloqueo de tal manera configurar el que se puedan imprimir estos documentos.

- **Equipos Terminales:**

Tabla 29. Métricas para activo Equipos Terminales.

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
Equipos terminales	Gestión de vulnerabilidades técnicas	# incidencias por errores de hardware
		# incidencias por errores de software
		# de fallas en acceso a carpetas
	Uso aceptable de los activos	# bloqueos de cuentas de usuario
	Gestión de capacidades	# perdidas de comunicación

Fuente: Elaboración Propia.

Se han determinado 4 métricas para el activo:

- Número de incidencias por errores de hardware: Se debe de registrar las incidencias que se presenten por errores a nivel de hardware que presenten los PC's de los usuarios, ya sea porque se modificó algún aspecto de la máquina.
- Número de incidencias por errores de software: Se debe de registrar incidencias a raíz del software instalado en los equipos que causen problemas de funcionamiento del equipo.
- Número de fallas en acceso a carpetas: Se debe de registrar los errores que presente los colaboradores en acceder a carpetas que almacenen documentos de trabajo en común con varios usuarios.

- Número de bloqueos de cuentas de usuario: Se debe de registrar la cantidad de cuentas bloqueadas por temas de olvido de contraseñas.
- Número de perdidas de comunicación: Se debe de registrar los incidentes relacionados con perdidas de comunicación de los terminales ya sea por falta de conexión a internet, perdida de conexión en red interna, etc.

4.2.5. Establecimiento de Umbrales

En esta etapa una vez completas las anteriores de manera correcta, se procede con el establecimiento de los umbrales para la medición de los activos del área, esta determinación de umbrales está sujeta a la tolerancia por parte tanto de la organización como del área hacia los incidentes que se puedan presentar y así también dependiente de que tan crítico resulta para la operativa el activo de información, es por esto que estos umbrales son determinados por el especialista del área en conjunto con la gerencia e interesados del área de infraestructura y de la organización.

Es necesario resaltar que no es necesario ni obligatorio tomar en consideración todas las métricas desarrolladas en el presente proyecto, pero se recomienda la utilización de todas estas métricas para que de esta manera sea óptima la gestión de los incidentes y el monitoreo de los activos según sus métricas.

Se han determinado 2 criterios para la medición de las métricas, “tiempo de Inactividad del activo” y “Número de Incidencias presentadas”, así mismo para la correcta gestión de los incidentes se requiere que se actúe de manera preventiva ante los incidentes y no de manera reactiva, por ende se han determinado 2 umbrales, los mismos que determinarán los límites entre lo que esta dentro de lo aceptable y lo que no se puede permitir, estos son “Máximo Permitido” y “Mínimo no Permitido”, estos umbrales son definidos por el área de Infraestructura de la Organización.

- **Tiempo de Inactividad:** Este criterio de medición se le ha asignado a aquellos activos que por el control elegido y la métrica asociada, sea importante representar su medida en tiempo por el impacto que representaría tener paralizado el servicio que soporte el activo. Según la Circular G-180 – 2015 "Indicadores clave de riesgo para la gestión de la continuidad del negocio" define interrupción del negocio como: "evento que genera la interrupción total o de parte importante de una o más líneas de negocio o sus procesos de soporte por treinta (30) minutos continuos o más" (SBS, 2015).
- Número de Incidencias: Este criterio de medición se le asigna a los activos que se requiera registrar las incidencias o errores que los afecten, no necesariamente la ocurrencia de un evento hacia un activo paralizará el servicio del mismo, por ende se hace necesario monitorear la cantidad de ocurrencias que se presenten.

En la siguiente tabla se puede apreciar los umbrales definidos por todos los interesados de la Cooperativa, de acuerdo a los activos de información y según la clasificación de estos:

Tabla 30. Plantilla para determinar umbrales por incidentes

ASOCIADA	UNIDAD DE MEDIDA	UMBRAL PERMITIDO	MAXIMO PERMITIDO	MINIMO NO PERMITIDO
# de accesos a ambientes físicos por personal no autorizado	# INCIDENTES	5	2	3
# de incidencias presentadas por eventos externos o naturales	TIEMPO INACTIVO	30 Min	15	25
# de fallas del suministro eléctrico	TIEMPO INACTIVO	30 Min	15	25
# incidencias por fallos de equipos	TIEMPO INACTIVO	30 Min	15	25
# de accesos no permitidos en red por usuarios	# INCIDENTES	3	1	2
# de intentos de intrusión a la red	# INCIDENTES	3	1	2
# de fallas de equipos por falta de mantenimiento	# INCIDENTES	3	1	2
# de incidencias por mala manipulación de servidores	TIEMPO INACTIVO	30 Min	17	25
# de fallas por déficit en funcionamiento	TIEMPO INACTIVO	30 Min	17	25
# de fallas del suministro eléctrico	TIEMPO INACTIVO	30 Min	17	25
# incidencias por fallos de equipos	TIEMPO INACTIVO	30 Min	17	25
# accesos no autorizados a la BD	# INCIDENTES	3	1	2

ASOCIADA	UNIDAD DE MEDIDA	UMBRAL PERMITIDO	MAXIMO PERMITIDO	MINIMO NO PERMITIDO
# incidencias por claves no cifradas en la BD	# INCIDENTES	3	1	2
# incidencias por fallas al realizar o reestablecer backups	# INCIDENTES	3	1	2
# Incidencias por déficit de rendimiento de activo	TIEMPO INACTIVO	30 Min	18	25
# Incidencias por caída de correos	TIEMPO INACTIVO	30 Min	18	25
# Incidencias por correos maliciosos	# INCIDENTES	3	1	2
# incidencias de red no permitida	# INCIDENTES	3	1	2
# solicitudes de información	# INCIDENTES	3	1	2
# perdidas de comunicación o conexión	TIEMPO INACTIVO	30 Min	18	25
# fallas por privilegios mal asignados a usuarios	# INCIDENTES	3	1	2
# incidencias por demora en alta/baja de usuarios	# INCIDENTES	3	1	2
# incidencias por identificación de usuarios no desactivados / derechos de acceso erróneos	# INCIDENTES	3	1	2

ASOCIADA	UNIDAD DE MEDIDA	UMBRAL PERMITIDO	MAXIMO PERMITIDO	MINIMO NO PERMITIDO
# de equipos con software no autorizado	# INCIDENTES	3	1	2
# Incidencias por error en cambios de pases a producción	TIEMPO INACTIVO	30 Min	19	25
# de fallas en sincronización de relojes	# INCIDENTES	3	1	2
# incidentes de infecciones por software malicioso	TIEMPO INACTIVO	30 Min	19	25
# intentos fallidos de ingresos al Servidor	# INCIDENTES	3	1	2
# equipos no autorizados en red de producción	# INCIDENTES	3	1	2
# equipos en mal estado	# INCIDENTES	3	1	2
# de pruebas erroneas por funcionamiento de equipos	# INCIDENTES	3	1	2
# de pruebas erroneas al activar centro de datos alterno	TIEMPO INACTIVO	30 Min	20	25
# de incidencias por perdida de comunicación	TIEMPO INACTIVO	30 Min	21	25

Fuente: Elaboración Propia.

4.2.6. Registro de Incidentes

En la presente etapa se deberá de registrar todos aquellos incidentes que se presenten en la operativa diaria y que vean involucrados a los activos de información identificados previamente del área de Infraestructura, para poder mantener la data organizada y parametrizar los datos se ha determinado una plantilla de registro de incidentes la cual se detalla a continuación:

Tabla 31. Plantilla para registro de Incidentes Diario

REGISTRO DE INCIDENTES INFRAESTRUCTURA						
Nro.	Fecha	ACTIVO INVOLUCRADO	MÉTRICA RELACIONADA	DESCRIPCIÓN BREVE DEL INCIDENTE	UNIDAD DE MEDIDA	NRO. DE INCIDENTES O TIEMPO QUE DURO INCIDENTE

Fuente: Elaboración Propia.

A continiación se procede a detallar cada campo de la plantilla previamente descrita:

- Nro. → El campo "Nro." nos indicará la cantidad de registros que se van ingresando en la plantilla, con fines de control.
- Fecha → En este campo se deberá de ingresar la fecha (día, mes y año) en el que se presentó el incidente registrado.
- Activo Involucrado → En el presente campo se deberá de seleccionar de una lista desplegable el activo afectado.
- Métrica relacionada → En el presente campo se deberá seleccionar de una lista desplegable según el incidente, la métrica relacionada.
- Descripción breve del incidente → En el presente campo se deberá de ingresar una pequeña descripción del incidente ocurrido, a fin de especificar del detalle del incidente y el mismo sea entendible para otro especialista que consulte la base.
- Unidad de Medida → En este campo se indicará de manera automática si el incidente debe de ser registrado por tiempo de paralización o por número de incidentes presentados, por ejemplo si hubiese una paralización del Servidor, la misma deberá de registrarse en minutos, ya que el formato en este campo especificará "Tiempo Inactivo", por otro lado en caso de presentarse incidentes como accesos no autorizados al Centro de Datos, el formato automáticamente mostrara en el campo "# de Incidentes", lo que haría referencia a que se debe de ingresar la cantidad de incidentes presentados.
- Número de Incidentes o Tiempo que duro Incidente → En este campo se ingresará o bien el tiempo de paralización o bien la cantidad de incidentes presentados, con relación a lo indicado en el campo anterior "Unidad de Medida".

4.2.7. Cuadro de Mando Integral - Diario y Mensual

Con la finalidad de poder expresar gráficamente y hacer más amigable el entendimiento del registro de incidentes, se ha desarrollado un cuadro de mando integral con ayuda de la herramienta Power BI, en el cual se desarrollaron gráficas a modo de velocímetro con 3 zonas representadas por colores (Verde → Zona correcta, Amarillo → Zona de precaución, Rojo → Zona crítica).

Las gráficas desarrolladas servirán para que la gestión por parte del área de Infraestructura en relación con los incidentes que afecten los activos, sea más eficaz y de tal manera poder tomar decisiones oportunas o elaborar los planes de acción para mitigar y contrarrestar los incidentes que se presenten.

Se cuenta con 4 pestañas dentro de la herramienta en la cual se grafican los incidentes por "diarios", "mensuales", además de por tipo de medición "Tiempo de Inactividad" y "Número de Incidentes", de esta manera se podrá gestionar diariamente los incidentes que se presenten e identificar en el periodo más corto de tiempo que incidente sobrepasa el umbral permitido, también se muestra gráficamente el consolidado mensual de incidentes, a continuación se muestra los gráficos del dashboard:

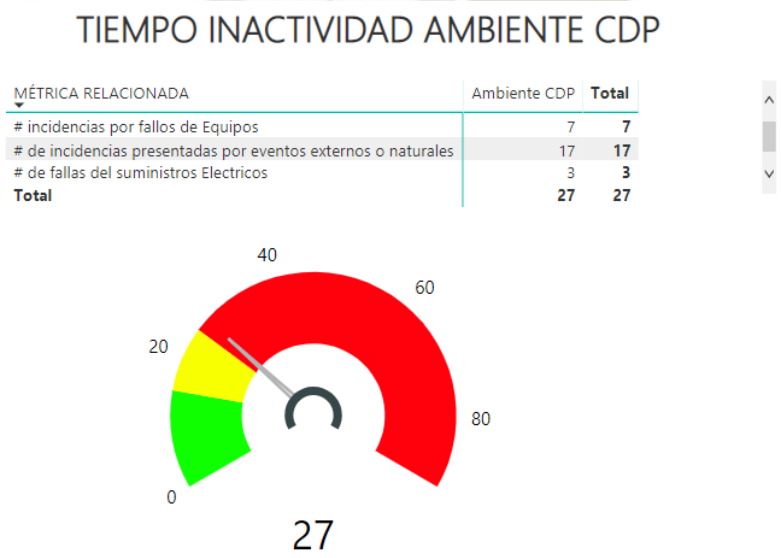


Figura 16. Grafica Velocímetro Tiempo Inactivo Ambiente CDP

Fuente: Elaboración Propia

TIEMPO INACTIVIDAD SERVIDORES FÍSICOS

MÉTRICA RELACIONADA	Servidores Físicos (Hardware)	Total
# de fallas por deficit en funcionamiento	10	**10**
# incidencias por fallos de Equipos	2	**2**
Total	**12**	**12**

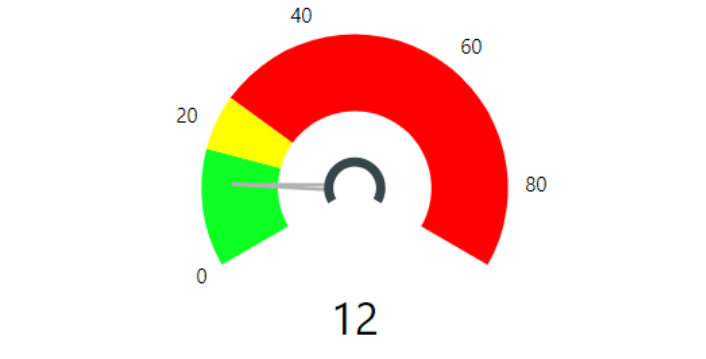


Figura 17. Grafica Velocimetro Tiempo Inactivo Servidores Físicos

Fuente: Elaboración Propia

TIEMPO INACTIVIDAD SERVIDOR BASE DE DATOS

MÉTRICA RELACIONADA	Servidor de Base de Datos	Total
# Incidencias por deficit de rendimiento de activo	6	**6**
Total	**6**	**6**

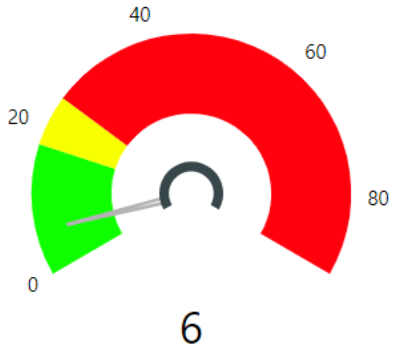


Figura 18. Gráfica Velocímetro tiempo inactividad Servidor Base de Datos

Fuente: Elaboración Propia

Figura 19. Gráfica Velocímetro tiempo inactivicad Servidor de Correos

Fuente: Elaboración Propia

Figura 20. Gráfica Velocímetro incidentes Ambiente CDP

Fuente: Elaboración Propia

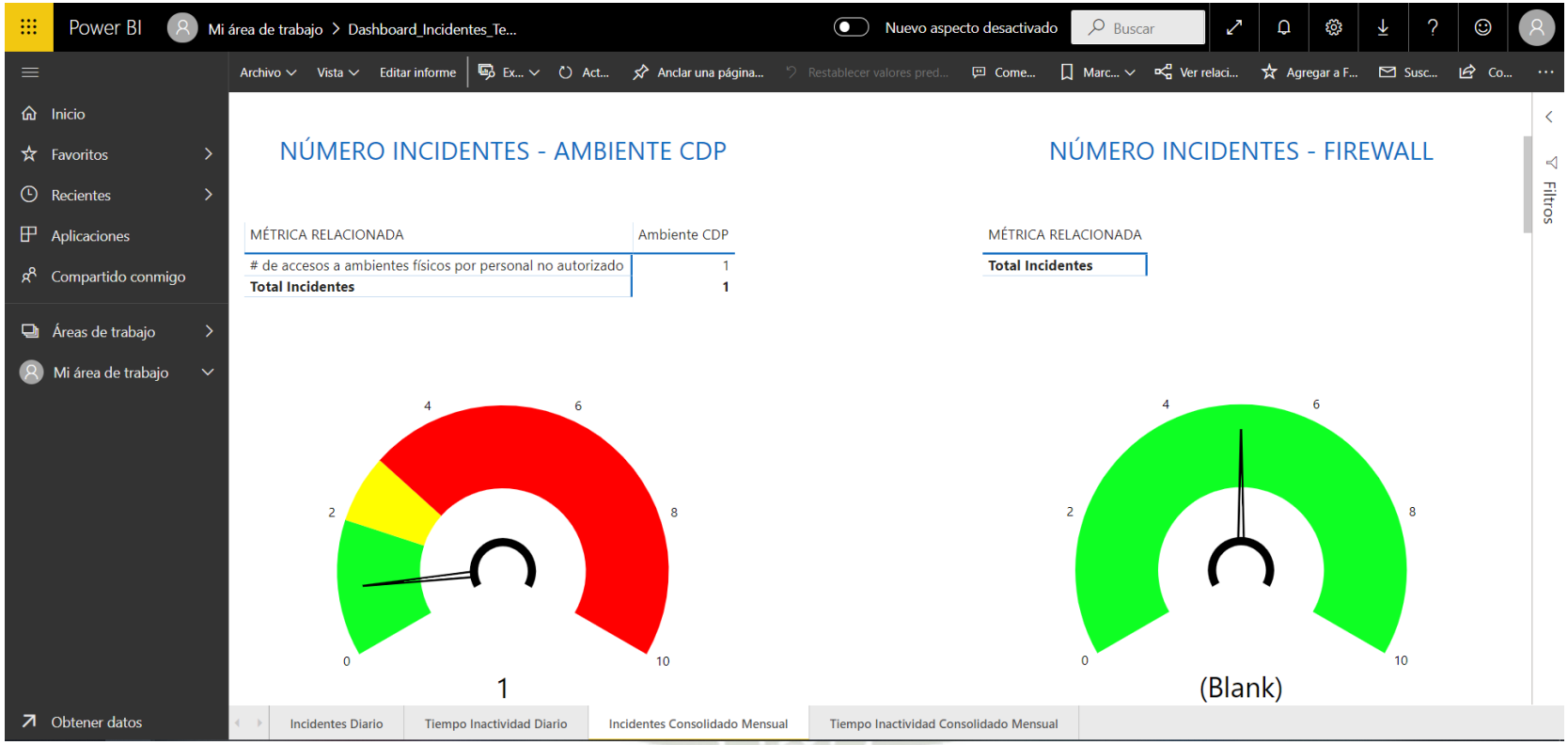


Figura 21. Gráfica de Dashboard en la herramienta Power BI

Fuente: Elaboración Propia.

CAPÍTULO V:

5. RESULTADOS

5.1. Evaluación Del Funcionamiento De Las Métricas Propuestas Para Los Activos De Información Del Área De Infraestructura De T.I.

El área de tecnologías de información de la cooperativa utilizaba para la gestión de incidentes y requerimientos, una plantilla desarrollada internamente en una hoja de cálculo Excel, en esta plantilla se ingresaban los incidentes identificados y solicitudes que se realizaban hacia el área, dentro del archivo se pudo evidenciar diversas hojas como:

- **Incidencias Desarrollo:** En esta hoja según se pudo validar se registran los incidentes correspondientes al área de Desarrollo de Sistemas.
- **Incidencias Diarias:** En esta hoja se registraban los incidentes que se presentaban o que eran reportados a la gerencia de T.I. de la organización, analizando el registro se pudo validar que se categorizaron los incidentes para poder segmentar las incidencias pero en muchos casos se validaron incidencias iguales en diferentes categorías.
- **Cierre diario:** En esta hoja se registraban los tiempos de cierre diario de los colaborares en relación con las incidencias resultas.
- **Categorias:** En esta hoja se detallaban las categorizaciones realizadas internamente según el tipo de activo involucrado (Sistemas, Equipos, Software, etc).
- **Calculo:** En la misma se llevaba un control del total de incidentes resueltos por los analistas del área de Soporte, así como también los tiempos invertidos.
- **Indicador 1:** En esta hoja se monitoreaba la cantidad de incidentes resueltos por analista en el día.
- **Indicador 2:** En esta hoja se monitoreaba el tiempo promedio de resoluión de problemas.

- **Indicador 3:** En esta hoja se monitoreaba los incidentes resueltos en el mes, de acuerdo a tiempo empleado por cada analista, categorizándolo en 3 colores (rojo, ámbar y verde), para determinar efectividad.
- Al verificar la plantilla se observa que la misma no cuenta con un orden ni una parametrización que sirva para poder categorizar los incidentes y asignarlos a algún activo en particular, así también no se registra correctamente los incidentes, se valida incidentes que no se han cerrado o solucionado por lo que se entiende que los mismos siguen existiendo o no se les da solución oportunamente, todo esto debido a que no se cuenta con medidas establecidas las cuales estén orientados a la tolerancia del área hacia los incidentes que se presenten.

  Analizando los indicadores planteados por el área, se puede determinar que los mismos están orientados a medir la eficiencia de los colaboradores en relación con el tiempo empleado para la solución de problemas, más no están orientados a poder identificar la cantidad o impacto en caso se susciten incidentes que afecten a los activos de información sean estos críticos o no y tampoco están orientados a gestionar planes de acción para mitigar estos incidentes.

  En coordinación con el gerente de tecnologías de información y jefatura de sistemas de la cooperativa se acordó la utilización de las métricas propuestas en el presente proyecto, el mismo entro en funcionamiento a inicios del mes de setiembre del año 2019 hasta el mes de noviembre del mismo año exactamente quincena de mes, fecha de corte de la data recogida de la cooperativa, esto para determinar el aporte de la herramienta hacia el área de Infraestructura.

  Además a petición de la gerencia de tecnología de sistemas, se encargó al analista de infraestructura migrar todos aquellos incidentes registrados en la plantilla inicial del área, que por sus características se puedan considerar en la nueva plantilla propuesta de registro de incidente, es importante resaltar que a solicitud de la cooperativa no se podrán mostrar a detalle los incidentes del

área por un tema de confidencialidad, entonces luego del levantamiento de data y funcionamiento de las métricas se tiene:

- Producto de la migración de las incidencias de la plantilla inicial del área hacia la plantilla de las métricas propuesta, se valida el registro de 06 eventos correspondientes a los meses de julio y agosto del año 2019 (01 correspondientes al mes de julio y los restantes 05 al mes de agosto).
- A partir del mes de setiembre cuando inicio la utilización de la plantilla propuesta hasta la fecha de corte (quincena de noviembre), se identifica el registro de 63 eventos o incidentes:

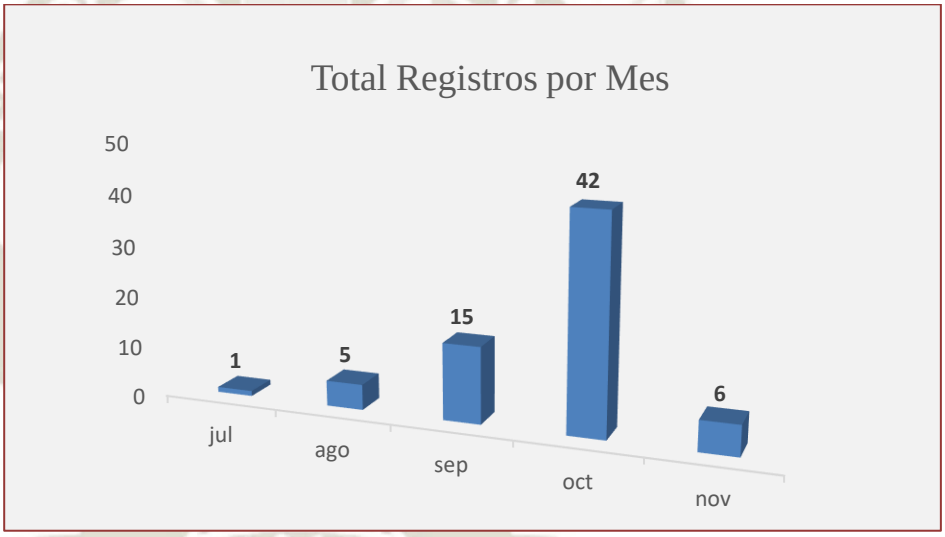


Figura 22. Cantidad de incidentes registrados por mes

Fuente: Elaboración Propia

- Como se aprecia antes de la utilización de la herramienta el registro de incidentes relacionados a activos de Infraestructura era mínimo, presentando para el mes de julio solo un incidente registrado y para agosto apenas 5 incidentes, a partir de la utilización de la herramienta se evidencia el aumento significativo de los incidentes registrados.

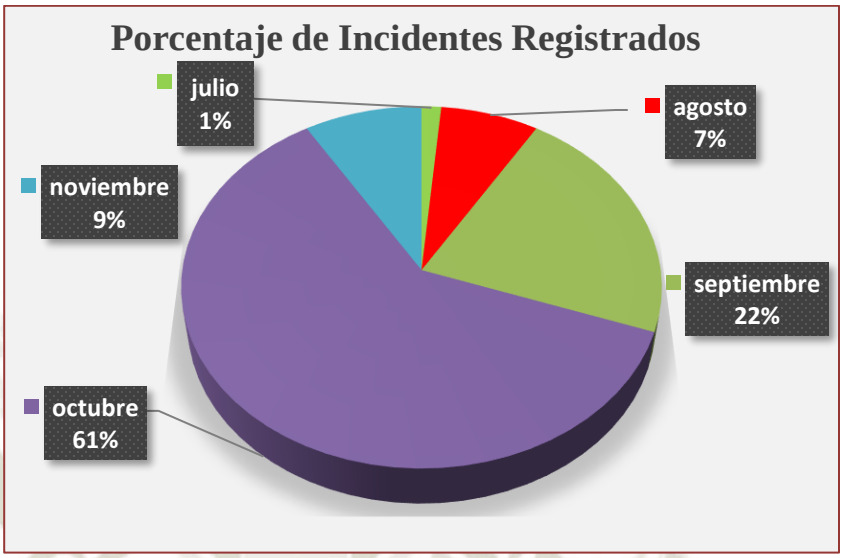


Figura 23. Porcentaje de Registro de incidentes por mes

Fuente: Elaboración Propia

– En la gráfica se puede apreciar que del 100% de incidentes registrados a la fecha de corte, tan solo el 1% corresponde al mes de julio y el 7% al mes de agosto, el restante 92% se reparten en los meses de setiembre (22%), octubre (61%) y noviembre (9%), tomando en consideración que la fecha de corte es quincena del mes de noviembre, por lo que se pudo esperar que el porcentaje de registro de incidentes de dicho mes sea mayor.

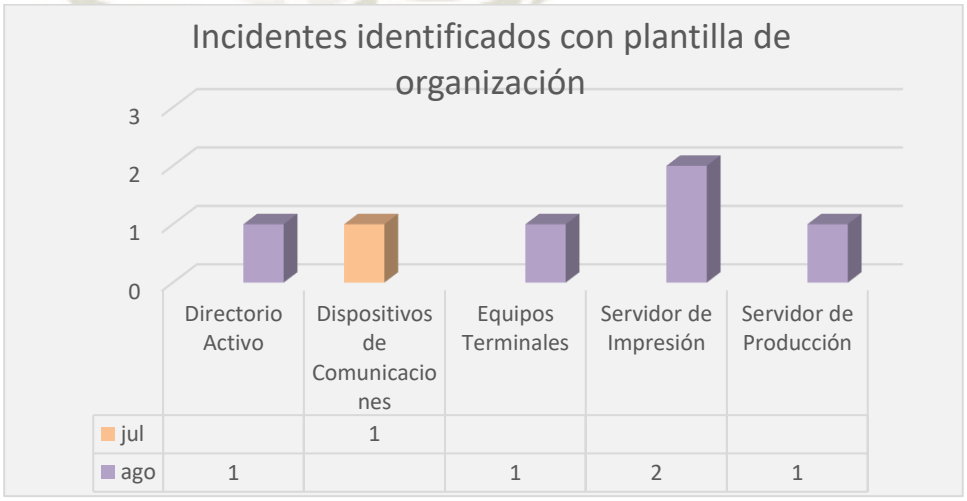


Figura 24. Activos asociados a incidentes con plantilla de Organización

Fuente: Elaboración Propia.

– En los meses que se utilizó la plantilla de la organización se logró identificar 6 incidentes asociados a 5 activos de infraestructura, sin embargo con la plantilla propuesta se pudo evidenciar un aumento de los activos asociados a los incidentes en 3 totalizando 8 activos.

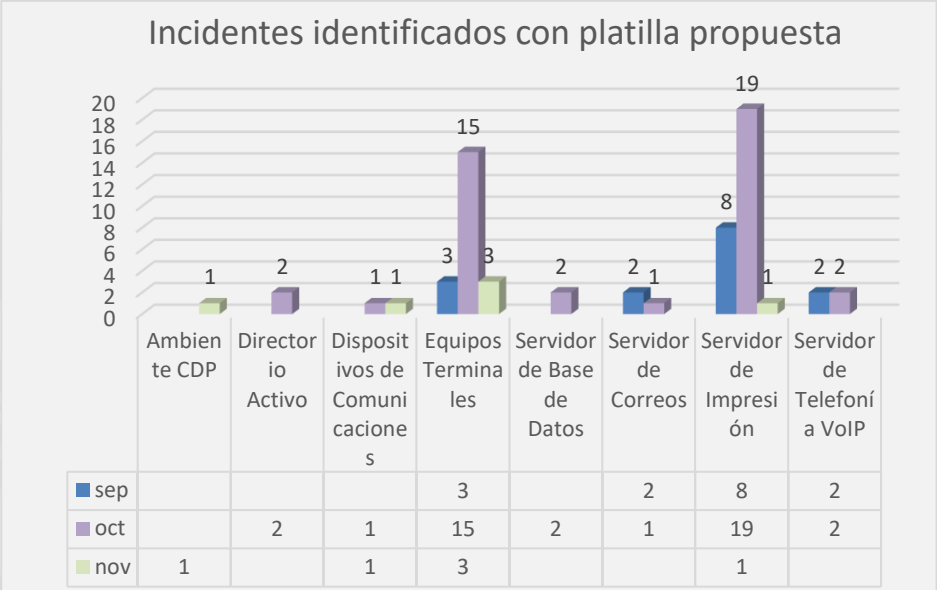


Figura 25. Activos asociados a incidentes con plantilla propuesta.

Fuente: Elaboración Propia.

Por último se pudo validar que con la utilización de la plantilla anterior a la propuesta, se identificaron 6 métricas asociadas a activos de información del área de infraestructura, con la utilización de la plantilla propuesta se incrementó a 13 las métricas asociadas a activos de información, un aumento del 116% aproximadamente.

Para poder validar la propuesta de métricas para activos de información del área de infraestructura de tecnologías de la información de la cooperativa, se empleó una encuesta de satisfacción dirigida a los trabajadores del área de T.I. de la cooperativa.

Se optó por una escala de satisfacción para las respuestas la misma que podrá indicar como perciben los colaboradores la gestión de incidentes antes de la utilización de las métricas y su percepción luego de la utilización de las métricas propuestas y los lineamientos desarrollados en el presente proyecto, para esto se han detallado 5 niveles de calificación los cuales se detallan a continuación en la siguiente tabla:

Tabla 32. Escala de Satisfacción

Escala	**Grado de satisfacción**
1	Muy Mala
2	Mala
3	Regular
4	Bueno
5	Muy Bueno

Fuente: Elaboración propia

El área de Tecnologías de Información de la Cooperativa lo comprenden 10 trabajadores, los mismos que fueron tomados en cuenta para la encuesta propuesta, los mismos se distribuyen en los siguientes cargos:

- 01 Gerente de Tecnologías de Información.
- 01 Jefe del área de Tecnologías de Información.
- 02 Analistas de Infraestructura de T.I.
- 03 Analistas de Soporte de T.I.
- 03 Analistas de Desarrollo de T.I.

El modelo de la encuesta aplicada a la organización para medir la gestión de incidentes en el área de Tecnologías de la Información se muestra en la siguiente figura:

Tabla 33. Encuesta de satisfacción para el área de Infraestructura.

ENCUESTA PARA MEDIR GESTIÓN DE INCIDENTES DEL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN						
Observaciones: A cada pregunta se responderá según el grado de satisfacción que se tiene, teniendo en consideración que **1 = Muy mala 2= Mala 3=Regular 4= Bueno y 5= Muy bueno.**						
Nro.	**Pregunta**	**Nivel de Satisfacción**				
		1	**2**	**3**	**4**	**5**
1	¿Cómo considera la gestión de incidentes antes de la utilización de las métricas propuestas?					
2	¿Cómo considera la categorización de incidentes antes de la utilización de las métricas propuestas?					
3	¿Cómo considera la respuesta a los incidentes por parte del área antes de la utilización de las métricas propuestas?					
4	¿Cómo considera que era la identificación de incidentes por parte del área antes de la utilización de las métricas propuestas?					
5	¿Cómo considera la gestión de incidentes con la utilización de las métricas propuestas?					
6	¿Cómo considera la categorización de incidentes con de la utilización de las métricas propuestas?					
7	¿Cómo considera la respuesta a los incidentes por parte del área con la utilización de las métricas propuestas?					
8	¿Cómo considera es la identificación de incidentes por parte del área con de la utilización de las métricas propuestas?					

Fuente: Elaboración Propia.

5.2. Resultados De La Encuesta De Satisfacción Para El Estado Actual De La Organización Ante La Gestión De Incidentes

1. ¿Cómo considera la gestión de incidentes antes de la utilización de las métricas propuestas?

Tabla 34. Respuestas a Pregunta N°1

Ponderación	Escala	Nro. De Resuestas
1	Muy mala	0
2	Mala	5
3	Regular	5
4	Buena	0
5	Muy buena	0

Fuente: Elaboración propia

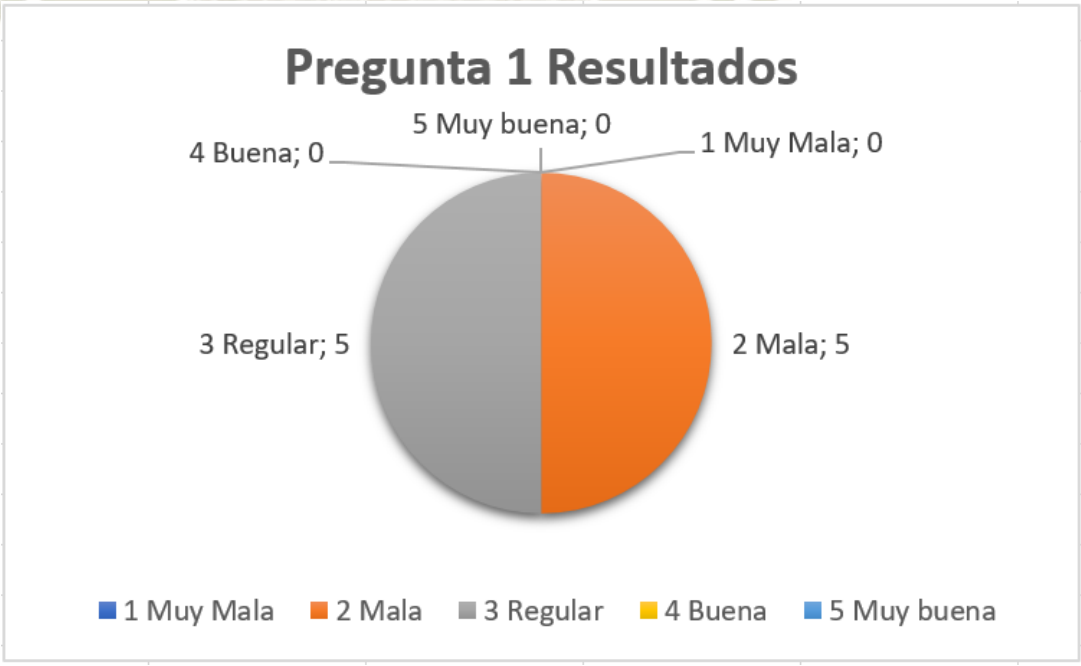


Figura 26. Gráfico Circular de la Pregunta N°1

Fuente: Elaboración propia

Interpretación

El sentir de los encuestados con relación a la forma en como se venía dando la gestión de incidentes en el área se distribuye en 50% (regular) y 50% (mala), esto evidencia que los colaboradores en su totalidad sentían que no se llevaba correctamente una gestión de incidentes dentro del área apenas la mitad considera que la gestión que se realizaba era regular, lo cual no generá confianza en la labor diaria de los colaboradores.

2. ¿Cómo considera la categorización de incidentes antes de la utilización de las métricas propuestas?

Tabla 35. Respuestas a Pregunta N°2

Ponderación	Escala	Nro. De Respuestas
1	Muy mala	3
2	Mala	4
3	Regular	3
4	Buena	0
5	Muy buena	0

Fuente: Elaboración propia

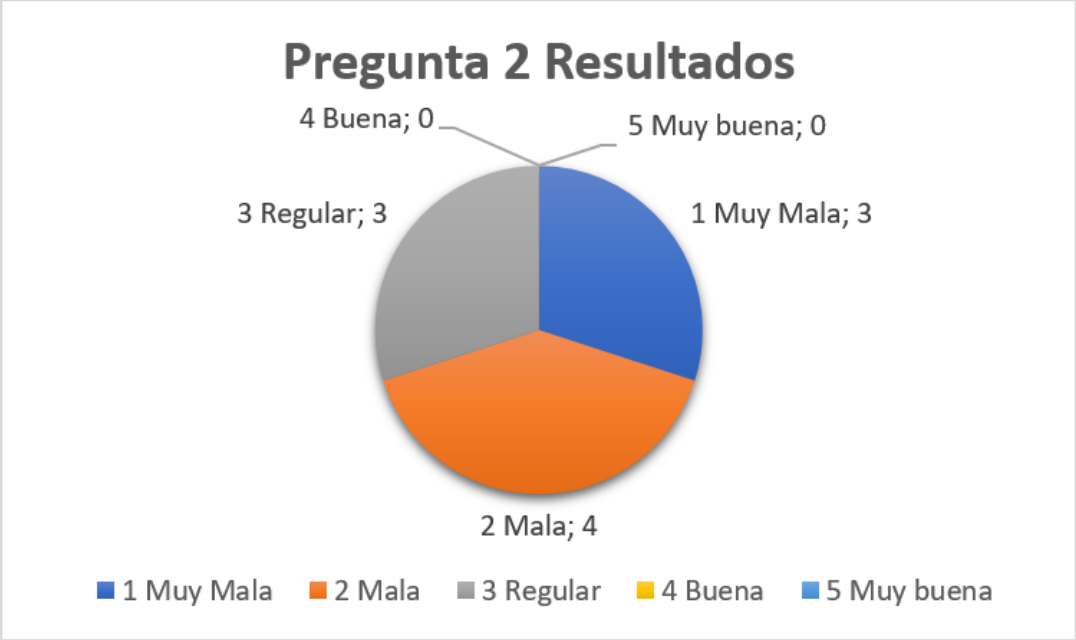


Figura 27. Gráfico Circular de la Pregunta N°2

Fuente: Elaboración propia

Interpretación

Para la forma en como se categorizó los incidentes en el área previo a la utilización de las métricas propuestas, el sentir de los encuestados va en relación con la primera interrogante, así pues se tiene que 30% piensa que la categorización era regular, 40 % considera que la categorización era mala y 30% considera la categorización como muy mala, por ende se concluye que no se contaba con una categorización adecuada para la correcta gestión de incidentes.

3. ¿Cómo considera la respuesta a los incidentes por parte del área antes de la utilización de las métricas propuestas?

Tabla 36. Respuestas a Pregunta N°3

Ponderación	Escala	Nro. De Respuestas
1	Muy mala	0
2	Mala	5
3	Regular	4
4	Buena	1
5	Muy buena	0

Fuente: Elaboración propia

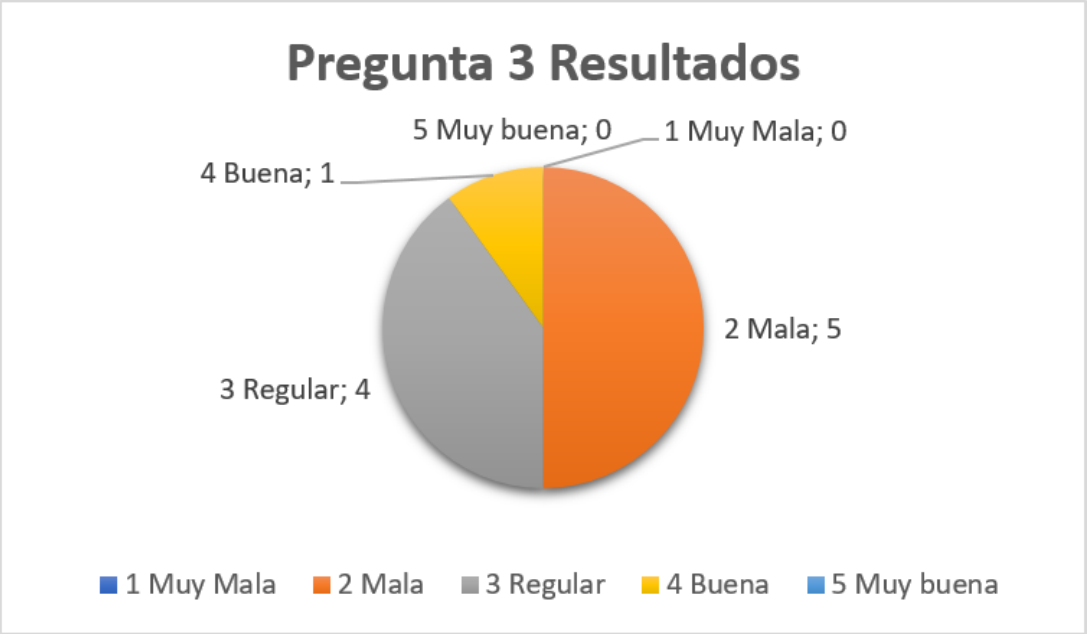


Figura 28. Gráfico Circular de la Pregunta N°3

Fuente: Elaboración propia

Interpretación

A la interrogante planteada la respuesta más seleccionada fue la opción 2 – "Mala" seguida de la opción 3 – "Regular" y apenas 1 persona del total de encuestados escogió la opción 1 – "Buena", para la respuesta del área ante los

incidentes, esto se sustenta por el análisis de la plantilla previa utilizada por el área, en la cual se validaron incidentes que no tenían estado cerrado y que tenían un periodo largo sin ser solucionados o atendidos.

4. ¿Cómo considera que era la identificación de incidentes por parte del área antes de la utilización de las métricas propuestas?

Tabla 37. Respuestas a Pregunta N°4

Ponderación	Escala	Nro. De Respuestas
1	Muy mala	2
2	Mala	5
3	Regular	3
4	Buena	0
5	Muy buena	0

Fuente: Elaboración propia

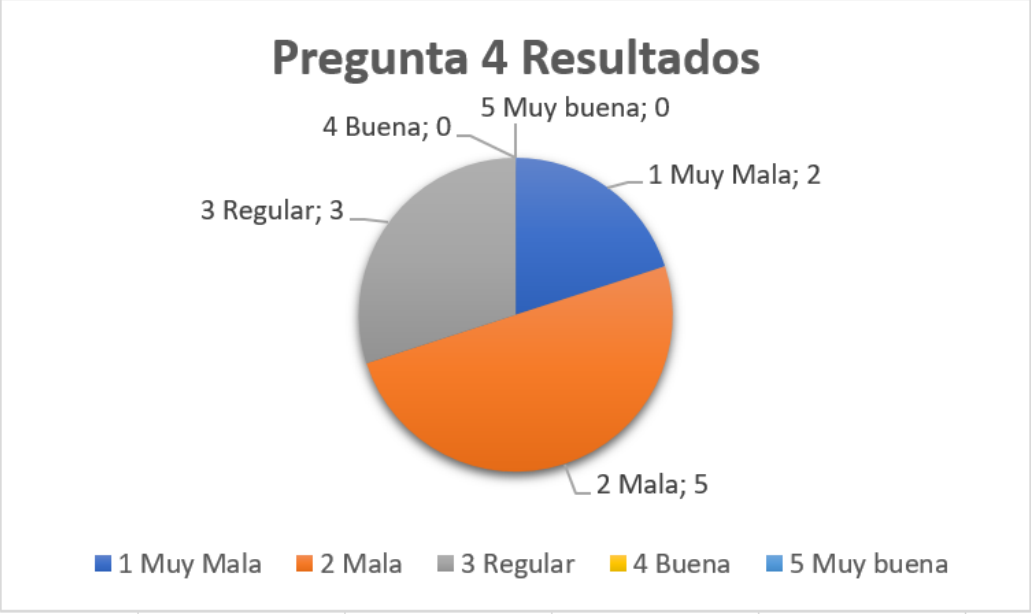


Figura 29. Gráfico Circular de la Pregunta N°4

Fuente: Elaboración propia

Interpretación

Del total de encuestados el 50% respondió que la identificación de los incidentes por parte del área de Infraestructura era “Mala”, el 20% considera que es “Muy mala” y el 30% considera que la identificación del incidentes es “Regular”, esto debido a que la plantilla utilizada previamente por el área, no estaba enfocada al registro de incidentes solamente, además de esto en la misma se recopilaban también solicitudes que se le hacían al área como configuraciones de correo, instalación de drivers, etc. propias de un helpdesk o mesa de ayuda, por ende la identificación propia de incidentes no se realizaba de manera correcta.

5. ¿Cómo considera la gestión de incidentes con la utilización de las métricas propuestas?

Tabla 38. Respuestas a Pregunta N°5

Ponderación	Escala	Nro. De Respuestas
1	Muy mala	0
2	Mala	0
3	Regular	1
4	Buena	7
5	Muy buena	2

Fuente: Elaboración propia

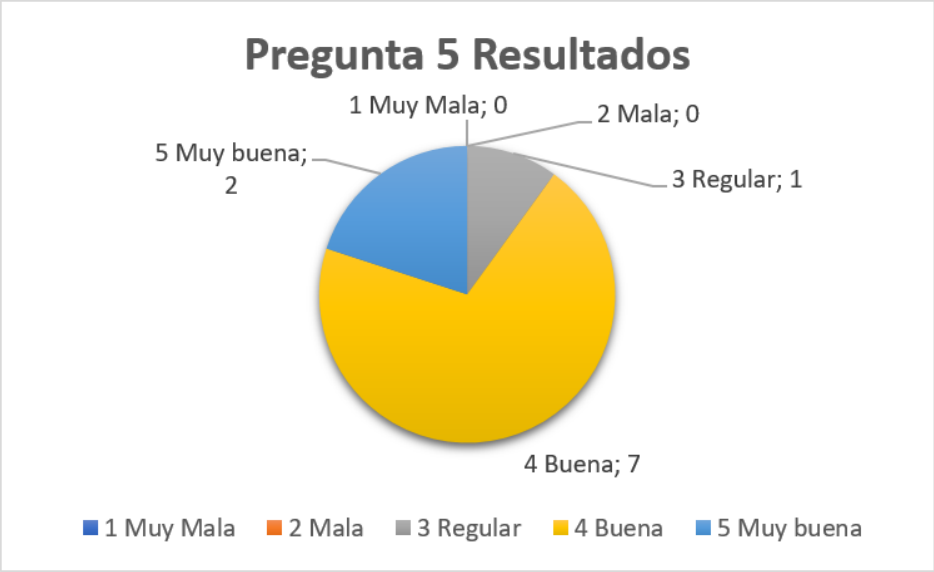


Figura 30. Gráfico Circular de la Pregunta N°5

Fuente: Elaboración propia

Interpretación

A partir de la presente interrogante se consulta a los encuestados el sentir de los mismos una vez utilizadas las métricas propuestas. En comparación con la interrogante nro. 1 al consultar como se considera la gestión de incidentes con las métricas se obtiene de manera marcada la aprobación de las mimas, teniendo que el 70% considera "Buena", el 20% considera "Muy buena" la gestión de incidentes y apenas el 10% considera "Regular" la gestión.

6. ¿Cómo considera la categorización de incidentes con de la utilización de la herramienta?

Tabla 39. Respuestas a Pregunta N°6

Ponderación	Escala	Nro. De Respuestas
1	Muy mala	0
2	Mala	0
3	Regular	7
4	Buena	3
5	Muy Buena	0

Fuente: Elaboración propia

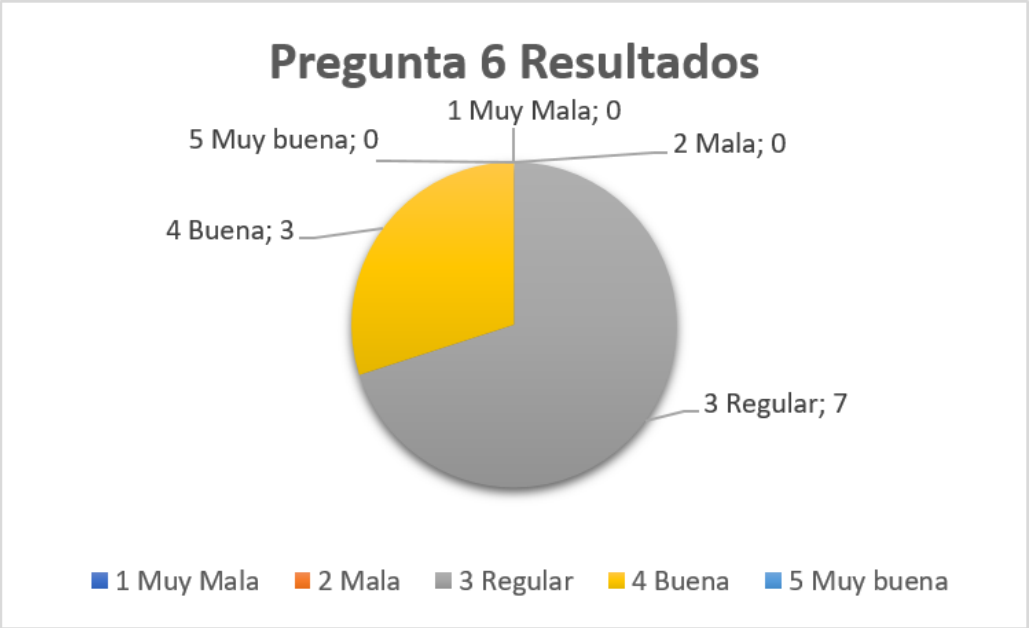


Figura 31. Gráfico Circular de la Pregunta N°6

Fuente: Elaboración propia

Interpretación

Así mismo para la categorización de los incidentes el 70% de los encuestados indica que considera “Regular” y el 30% considera “Buena” la categorización de

los incidentes, en relación con los resultados obtenidos antes de la utilización de las métricas en los que los encuestados indicaron en su mayoría que la categorización de incidentes era “Mala”. Es necesario destacar que se entiende que la mayoría indique que la categorización sea “Regular”, dado que en los entrevistados no están familiarizados en su totalidad con las Normas Internacionales ISO27001 e ISO27002, pero en líneas generales la sensación de los encuestados mejora.

7. ¿Cómo considera la respuesta a los incidentes por parte del área con la utilización de las métricas propuestas?

Tabla 40. Respuestas a Pregunta N°7

Ponderación	Escala	Nro. De Respuestas
1	Muy mala	0
2	Mala	0
3	Regular	0
4	Buena	6
5	Muy buena	4

Fuente: Elaboración propia

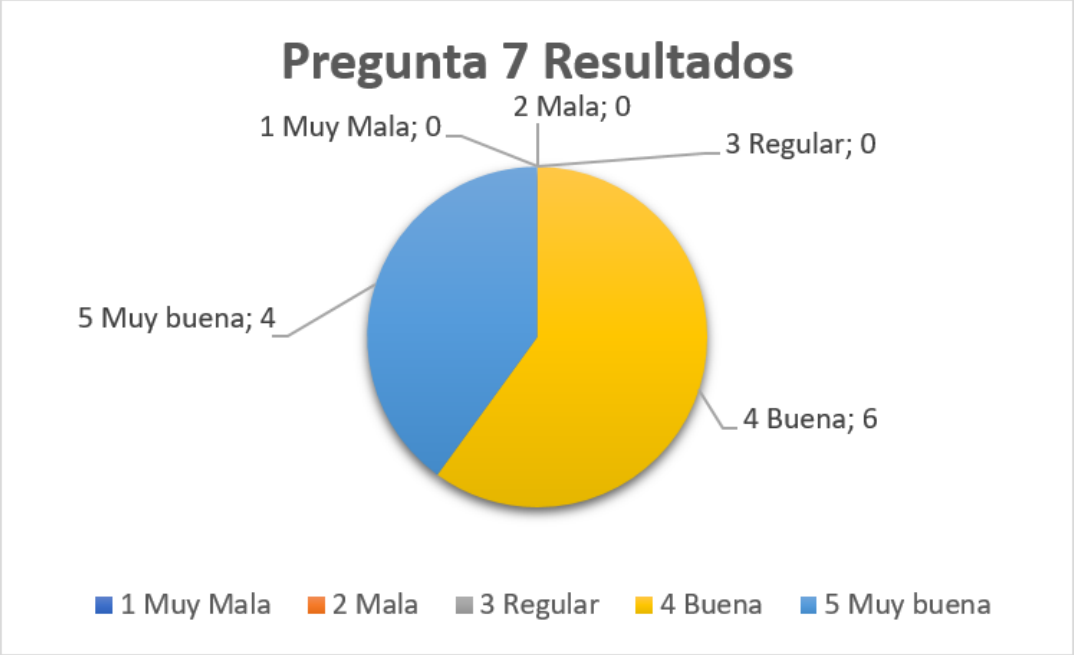


Figura 32. Gráfico Circular de la Pregunta N°7

Fuente: Elaboración propia

Interpretación

En la respuesta a incidentes se nota una gran aceptación por parte de los encuestados teniendo un 60% de estos que indica que la respuesta a incidentes es "Buena" y un 40% considera que la respuesta a incidentes del área es "Muy buena" luego de la utilización de las métricas propuestas, esto básicamente se debe a que al plantear límites de tolerancia o umbrales para los incidentes que se presenten por activos, las acciones a tomar serán más oportunas a medida de evitar que se susciten incidentes reiterativos o que los mismos lleguen a los límites de tolerancia.

8. ¿Cómo considera es la identificación de incidentes por parte del área con de la utilización de las métricas propuestas?

Tabla 41. Respuestas a Pregunta N°8

Ponderación	Escala	Nro. De Respuestas
1	Muy mala	0
2	Mala	0
3	Regular	1
4	Buena	8
5	Muy Buena	1

Fuente: Elaboración propia

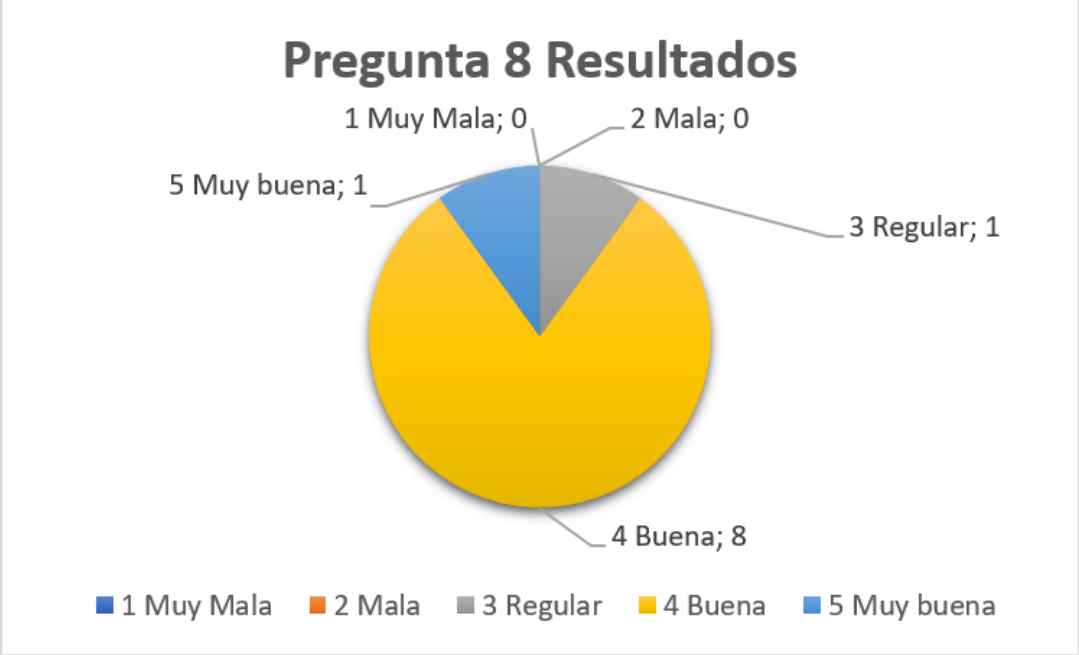


Figura 33. Gráfico Circular de la Pregunta N°8

Fuente: Elaboración propia

Interpretación

Al igual que la interrogante anterior, en la presente interrogante para la identificación de incidentes se nota una aceptación notoria por parte de los

encuestados, un 80% de estos considera la identificación de incidentes "Buena" luego de la utilización de las métricas, el 10% la considera "Muy buena" y únicamente el 10% de los encuestados la considera "Regular" la identificación de incidentes con las métricas propuestas, esta aceptación se puede entender básicamente por que al tener categorizados los incidentes por activo y teniendo las métricas determinadas la asociación de incidentes hacia activo se hace más fácil para el encargado de esta tarea.

En general realizando un comparativo del nivel de satisfacción de los encuestados en relación con la gestión de incidentes por parte del área de Infraestructura antes y después de la utilización de las métricas propuestas se tiene:

Tabla 42. Resumen de respuestas de encuesta antes de la utilización de las métricas

Ponderación	Escala	Nro. De Respuestas
1	Muy mala	5
2	Mala	19
3	Regular	15
4	Buena	1
5	Muy buena	0

Fuente: Elaboración propia

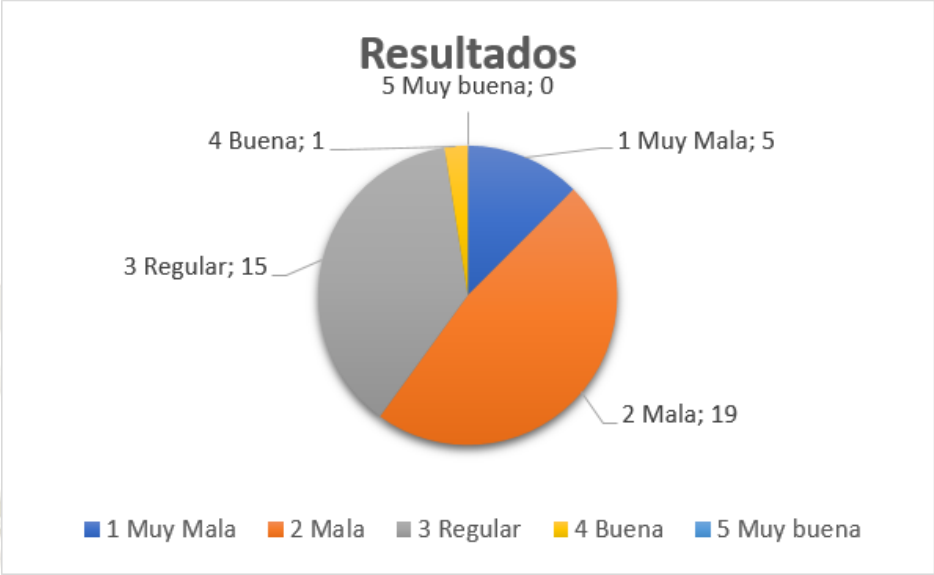


Figura 34. Gráfico circular resumen de encuesta antes de la utilización de las métricas

Fuente: Elaboración propia.

Tabla 43. Resumen de respuestas de encuesta despues de la utilización de las métricas

Ponderación	Escala	Nro. De Respuestas
1	Muy mala	0
2	Mala	0
3	Regular	9
4	Buena	24
5	Muy buena	7

Fuente: Elaboración propia

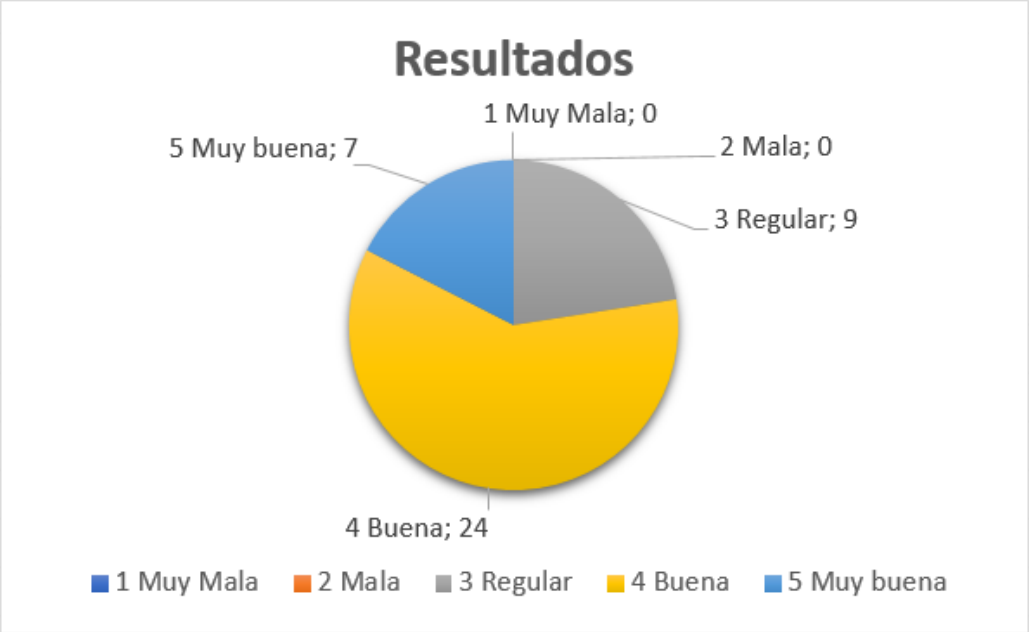


Figura 35. Gráfico circular resumen de encuesta despues de la utilización de las métricas

Fuente: Elaboración propia

CONCLUSIONES

Primera.- Se logró el desarrollo de las métricas para la evaluación de los activos de información del área de tecnologías de información para la cooperativa sujeto de estudio, estas métricas están basadas en las normas internacionales ISO27001 e ISO27002.

Segunda.- Se realizó exitosamente la identificación de activos de información del área de infraestructura de la cooperativa en conjunto con las partes interesadas, logrando abarcar todos los activos que más incidencia tienen en la operativa y se requieren monitorear.

Tercera.- Se clasificaron los activos de información basándonos en la norma ISO27001, con lo cual se pudo entender mejor la criticidad de cada uno de estos en la operativa de la cooperativa y en los servicios brindados por el área de Infraestructura de T.I.

Cuarta.- Se realizaron las métricas para los activos de información del área de infraestructura, con lo cual se logró una mejor gestión de incidentes por parte del área y así también un monitoreo de estos activos para la toma oportuna de decisiones en caso se presente incidentes que afecten considerablemente estos activos.

Quinta.- Se han elaborado cuadros de mando integral en el cuales se realizará el seguimiento de incidentes de acuerdo a los umbrales determinados por la organización, en los mismos se puede realizar el seguimiento diario así como verificar el consolidado mensual de incidentes para la toma de decisiones.

RECOMENDACIONES

Primera.- Se recomienda abarcar los restantes dominios de control de la Norma ISO27002, dado que por la naturaleza de los activos identificados en el presente proyecto, estos no pueden asociarse a los restantes dominios de control. Considerando los restantes dominios de la norma ISO27002 se puede abarcar todos los activos de información críticos no solo del área de Infraestructura, sino también de todas las áreas que comprendan el departamento de Tecnologías de Información de la cooperativa.

Segunda.- Se recomienda la implementación de una aplicación para la automatización del registro de incidentes, en la cual se puedan almacenar los incidentes en una base de datos para poder obtener información más relevante como por ejemplo incidentes recurrentes, historial de incidentes, etc, lo cual permita una mejor gestión de incidentes y toma de decisiones.

Tercera.- A raíz del presente proyecto dada la identificación de activos y basándose en las normas ISO27001 – ISO27002, se recomienda la implementación de un Sistema de Gestión de Seguridad de la Información el cual gestione de manera centralizada todos los temas en seguridad y riesgos tanto del área como de la cooperativa, con una estructura basada en políticas, procedimientos, etc, y de esta manera la cooperativa cuente con un modelo de gestión reconocido internacionalmente.

REFERENCIAS BIBLIOGRÁFICAS

Baldecchi, R. (2014). Implementación efectiva de un SGSI ISO 27001. *2014*, 30. Retrieved from http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014 - Exposici%25C3%25B3n 2 CIGRAS ISO 27001 - rbq.pdf

Bilbao, E. / I. (2011). Modelo Unificado de Análisis de Riesgos de Seguridad Física y Lógica. *2011*, 30. Retrieved from http://www.cuevavaliente.com/sites/default/files/ponencia_inteco_2011.pdf

Cadavid-aguirre, J. M. (2013). Seguridad en activos de información humanos, 17–19.

Comite Tecnico de Normalizacion de Codificacion e Intercambio Electronico de Datos. (2007). NTP-ISO / IEC 17799 EDI . Tecnología de la información . Código de buenas. *El Peruano*, *2a. Edició*(Lima 41), 179. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=39612

Correa, G. (2016). *Métricas para el proceso de implementación del modelo de gobierno de seguridad de la información basado en COBIT 5.0*.

Iso27000.es. (n.d.-a). Iso 27000.

Iso27000.es. (n.d.-b). Sistema de Gestión de la Seguridad de la Información.

Iso27000.es. (2013). ControlesISO27002-2013, 27002. Retrieved from http://iso27000.es/download/ControlesISO27002-2013.pdf

ISO27004. (2012). PERUANA NTP-ISO / I NTP-I SO / IEC EC 27004 TECNOLOGÍA DE LA INFORMACIÓN . Técnicas de Medición.

Magerit. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Montoya Vega, C. M. (2013). La norma ISO27001: Aspectos claves de su diseño e implementación. *ISOTools*, 1–6.

NTP-ISO/IEC 27001:2014. (2014). NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la

información. Requisitos. *Normas Técnicas Peruanas*, 45. Retrieved from http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf

Orozco Vinces, Y. (Universidad C. V. (2015). Diseño de una métrica para evaluar el grado de cumplimiento del plan de continuidad de negocio en Tecnologías de la Información en la Empresa Altamar Foods Perú S.AC., 1–23.

Pentón, Á. E. S. "Jose A. E. A. (2016). *Métricas para evaluar la calidad de los Sistema de Gestión de Información Contable - Financiera*.

Portillo, P. B. del, & Benavides, L. O. (2012). Importancia de los sistemas integrados de gestión, *4*. Retrieved from http://repository.unimilitar.edu.co/bitstream/10654/6787/1/GarzonHernandezJaime2015.pdf

Romeral, L. M., & Torres Gallego, Á. (2008). Gestión De Los Riesgos Tecnológicos. *Procesos y Métricas*, *5*, 9. Retrieved from http://www.aemes.org/documentos/revistaprocesosmetricas/2008/numero13/RPM_v5_01.03.pdf

SBS. (2015). CIRCULAR N° G-180-2015, (30).

Ahmad, A., Maynard, S., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35(6), 717–723.

Beingolea, H. (2015). Diseño de un modelo de gobierno de TI utilizando el marco de trabajo de COBIT 5 con enfoque en seguridad de la información. Caso de estudio: una empresa privada administradora de fondos de pensiones. Pontificia Universidad Católica del Perú.

*Resolución Gerencial Ejecutiva N°376-2012-GRA-PEMS-GG/OAI.(*2012). Autoridad Autónoma de Majes.

Safa, N.S., y Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451.

Salazar, J. (2016). *Evaluación del nivel de madurez de los procesos de TI aplicando COBIT en el Gobierno Regional de Piura*. Universidad Nacional Pedro Ruiz Gallo.

Sánchez, J., Fernández Vicente, E., & Moratilla, A. (2013). ITIL, COBIT and EFQM: Can They Work Together? *International Journal of Combinatorial Optimization Problems & Informatics*, *4*(1), 54–64.

Santana, M. (2011). *¿Qué tan importante resulta la TI en las empresas? Esan.edu.pe*. Revisado de: https://www.esan.edu.pe/conexion/actualidad/2011/10/14/que-tan-importante-resulta-la-ti-en-las-empresas/

Secretaría de Gestión Pública de la Presidencia del Consejo de Ministros. (2013). Lineamientos Para La Implementación De La Gestión Por Procesos En Las Entidades De La Administración Pública En El Marco Del D.S. N° 004-2013-Pcm – Política Nacional De Modernización De La Gestión Pública Al 2021. *Presidencia Del Consejo de Ministros*, 1–8.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, *57*, 14–30.

Vieira, M., & Souza, J. (2016). Information technology service management processes maturity in the Brazilian Federal direct administration. Journal of Information Systems and Technology Management, 12(3), 663–686.

Yan, F., & Zavala, C. (2013). *Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT*. Universidad Privada Antenor Orrego.

ISOTools Excellence (2017). *¿Cómo realizar un inventario de activos de información?*. Revisado de: https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

ANEXOS

Anexo A – Plan de Tesis

Universidad Católica de Santa María

Facultad de Ciencias e Ingenierías Físicas y Formales

Escuela Profesional de Ingeniería de Sistemas

"MÉTRICAS PARA EVALUAR LOS ACTIVOS DE INFORMACIÓN DEL AREA DE INFRAESTRUCTURA DE TI BASADOS EN LA ISO/IEC 27001 - ISO/IEC 27002 PARA UNA EMPRESA RECAUDADORA - CALL CENTER"

LÍNEA: SISTEMAS DE INFORMACIÓN Y BASE DE DATOS

SUBLÍNEA: SEGURIDAD DE LA INFORMACIÓN

Proyecto de Tesis presentado para optar el:

Título profesional de Ingeniero de Sistemas

Córdova Quispe Carlos Eduardo

Arequipa, 2018

1. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 Planteamiento del problema

En los últimos años la forma de ver la parte estratégica de las empresas ha venido cambiando, enfocándose ya no tanto en la parte operativa sino también centrando el foco de atención en un elemento, al cual no se le venía dando la importancia adecuada, me refiero a la información.(Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos, 2007)

En la actualidad la información sea cual fuese el medio en el cual se presente es un activo muy importante para las empresas, ya que con esta se pueden obtener conocimientos del mercado, comportamiento de los clientes, estadísticas de ventas, etc. Toda esta información que es generada, almacenada y gestionada por las empresas, es resguardada de diferentes maneras, pudiendo estar en bases de datos, discos, unidades extraíbles, archivadores, servidores, etc. Así mismo el mantener esta información resguardada y disponible en todo momento es una labor de suma importancia que en general se sostiene bajo la implementación de un Sistema de Gestión de Seguridad de la información, dentro de este se definen políticas, normas y procedimientos los cuales sirven de apoyo para el correcto funcionamiento del Sistema de gestión.(Montoya Vega, 2013)

Basado en la norma internacional ISO/IEC 27001 la cual es el marco de gestión y desarrollo de un SGSI, parte de la gestión y mantenimiento del Sistema de Gestión requiere la identificación y valorización de todos los activos de información los cuales, por su importancia y criticidad son los que en ocasiones pueden garantizar la continuidad de negocio de la organización, contener información estratégica de la empresa, la cual al estar expuesta a amenazas puede verse comprometida, menguar la competitividad de la empresa contra los competidores del mismo rubro. En fin, es importante para la organización y para los encargados de la seguridad el saber que activos son los más importantes y por ende necesitan de más cuidado y seguimiento, teniendo en consideración que en los últimos años los ataques cibernéticos han venido en aumento.

Es así que según el Autor Jorge Mario Cadavid en su Artículo "Seguridad en Activos de Información Humanos", indicó que *"A partir del año 2010 América Latina ha sido en nuevo objetivo para los ciberdelincuentes ya que el crimen cibernético marco una subida de hasta 40% en 2012"* (Cadavid-aguirre, 2013).

El objetivo de este proyecto es proveer a la empresa de una serie de métricas las cuales permitirán evaluar y valorizar los activos de información críticos para de esta manera poder identificar los riesgos a los cuales están expuestos los activos y el impacto que pueda originar el que se vea afectada su confidencialidad, integridad o disponibilidad.

La Norma Internacional ISO27001:2013 forma parte del paquete de ISO27000, la cual cuenta con normas complementarias, dentro de estas normas se tiene la ISO 27002:2013 que es la norma que indica los posibles controles a ser implementados para garantizar la confidencialidad, integridad y disponibilidad de la información, esta norma se compone de 14 dominios, 35 objetivos de control y 114 controles, los cuales buscan abarcar todos aquellos activos de información con los que pueda contar una organización.(Iso27000.es, 2013)

En Perú se cuenta con la Norma NTP-ISO27001:2014, la cual es el marco de gestión para la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información, entendiéndose que la implementación del SGSI es una decisión estratégica de las organizaciones para el resguardo y protección de la su información.(NTP-ISO/IEC 27001:2014, 2014)

Ahora bien, la implementación de los controles no es un tema sencillo ya que en muchas ocasiones desarrollar, implementar y mantener estos controles conlleva un costo tanto económico como de tiempo y se hace necesario evaluar aquellos activos que por la información que contengan o la criticidad de estos para la continuidad de la operativa de la empresa representan los activos más importantes o más críticos.

Una vez identificados estos activos se hace necesaria la evolución de los riesgos a los cuales están afectos los activos de información críticos de la empresa.

1.2 Objetivos de la Investigación

1.2.1 General

Definir métricas para evaluar los activos de información del área de infraestructura de TI basados en la ISO/IEC 27001 - ISO/IEC 27002 para una empresa Cooperativa.

1.2.2 Específicos

- Identificar los activos de información del área de infraestructura de TI.
- Elaborar las métricas de evaluación de los activos de información del área de infraestructura de TI basados en la ISO/IEC 27001 e ISO/IEC 27002.
- Aplicar las métricas para valorizar los activos de información del área de infraestructura de TI que permitan clasificar los activos a los cuales debe brindarse mayor protección.

1.3 Preguntas de Investigación

- ¿En qué medida serán útiles las métricas para la evaluación de los activos de información del área de infraestructura de TI?

1.4 Línea y Sub-Línea de investigación a la que corresponde el problema

- Línea: Sistemas de Información y Bases de Datos.
- Sub-Línea: Seguridad de la Información.

1.5 Palabras Clave

SGSI (Sistema de Gestión de Seguridad de la Información), métricas, amenaza, vulnerabilidad, riesgo, confidencialidad, integridad, disponibilidad, activo de información, criterios, evaluación de riesgos.

1.6 Solución Propuesta

1.6.1. Justificación e Importancia

En los últimos años un objetivo de las empresas en lo que respecta a la estrategia empresarial es la de poder integrar la gestión de la calidad, el

medio ambiente y la seguridad y salud en el trabajo. Cuando estos objetivos se han alcanzado, entran en escena otros aspectos a tratar y que se están convirtiendo en puntos clave para los modelos de negocio actuales.

Cada vez toma más importancia la gestión de riesgos como base para la toma de decisiones. Entre los diferentes aspectos a considerar está la información; es decir, todos aquellos datos que desde algún punto de vista se considera necesario controlar, ya sea por obligación legislativa, por interés de terceros o bien por ser esenciales para la actividad y estrategia de la organización.

La información es un activo valioso que puede impulsar o destruir una organización. La defensa de este activo es una tarea esencial para asegurar la continuidad y la sostenibilidad del negocio, así como también es una exigencia legal (protección de la propiedad intelectual, protección de datos personales, servicios para la sociedad de la información), y además genera confianza a los clientes y/o usuarios.

Los activos son los recursos del sistema de gestión de seguridad de la Información de acuerdo a la ISO 27001, y son necesarios para que toda empresa funcione y consiga los objetivos que se ha propuesto la alta dirección. Cada activo tiene sus características, que difieren en el estado, en materia de seguridad, confidencialidad, integridad y disponibilidad.

Cada activo o grupo de activos conlleva diferentes tipos de indicadores de valoración que ofrecen una orientación para calcular el impacto que materializa la amenaza que puede provocar.

Esto es muy importante en ambientes de negocio cada vez más interconectados, pues, la información está ahora expuesta a un número mayor y a una variedad más amplia de amenazas y vulnerabilidades. Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada.

El desarrollo de este proyecto de investigación permitirá a las empresas (públicas o privadas) y personal responsable que vela por la seguridad de información, aplicar métricas para la evaluación de sus diferentes activos de información; considerando el incremento de la cantidad de incidentes de seguridad de la información a nivel de las organizaciones, que afectan la operación y continuidad de negocio de las mismas, con impacto a nivel económico, legal y de imagen.

Las empresas pueden desarrollar e implantar un marco de trabajo para la gestión de la seguridad de sus activos de información, incluyendo información financiera, propiedad intelectual y detalles de sus empleados, o información confiada a la organización por sus clientes o terceras partes.

Mejorar los aspectos relacionados con la seguridad de la información, proveer confianza a sus clientes o socios, son algunos de los motivos por los cuales las organizaciones deciden adoptar normas de seguridad y la implementación de un SGSI. La gestión de la Seguridad de la Información ofrece la libertad para crecer, innovar y ampliar la base de clientes sabiendo que toda la información cuenta con diferentes controles y basados en métricas para la evaluación de sus activos.

1.6.2. Descripción de la Solución

La presente investigación consistirá en la identificación y análisis de los diferentes activos de información de la organización, para de esta manera poder plantear las métricas para la evaluación de los activos de información bajo la norma internacional ISO 27001 e ISO 27002 y de esta manera poder identificar en un principio a que riesgos se encuentran expuestos, así como también lograr la evaluación y valorización de los activos según su criticidad.

Se desarrollarán las métricas bajo los marcos de las normas Internacionales ISO 27001 e ISO 27002, así como también considerando el giro de negocio de la empresa que se toma como caso de estudio.

2. FUNDAMENTOS TEÓRICOS

2.1 Estado del arte

En su proyecto titulado “Métricas para evaluar la calidad de los Sistemas de Gestión de Información Contable- Financiera” para optar el grado de Master en Informatica Aplicada en la ciudad de Cuba (Pentón, 2016), propone un grupo de métricas para evaluar la calidad de un sistema de información con el objeto de apoyar la toma de decisiones basadas en métricas especificas para la evaluación de catacteristicas y sub-caracteristicas partiendo de los atributos del software para la selección de la herramienta idonea a utilizar.

El proyecto planteado por el autor, es de ayuda ya que tomando en cosideración los aspectos evaluados por el mismo, se puede orientar la elaboración de métricas en realción al apartado de “Adquisición Desarrollo y Mantenimiento de los Sistemas de Información” de la norma ISO 27002, la cual dícta los aspectos a abarcar en la definición de controles para la seguridad de la información, entonces tomando en consideración los criterios planteados por el autor en el proyecto se puede orientar la elaboración de las métricas que se pretenden elaborar, además se debe de considerar que para el rubro de la empresa la cual se toma como caso de estudió las métricas de evaluación para el sistema contable son muy importantes.

Dentro del desarrollo del proyecto el autor se apoya de normas internacionales ISO, dentro de las cuales se puede destacas la Norma ISO/IEC 9126 de la cual rescata una tabla de caracteristicas y sub-caracteristicas que conforman el modelo base, para la medición de calidad de software, es así que el autor en su propuesta toma como base el marco referencial de la norma internacional antes mencionada y realiza modificaciones a la tabla, eliminando por ejemplo, usabilidad, eficiencia, mantenibilidad y portabilidad por considerarlas no relevantes para el dominio de un SGIC.

Al validar el modelo propuesto el autor tomo resultados de 37 expertos los cuales brindaron comentarios así como brindaron su aprobación o desaprobración al modelo propuesto, indicando que era necesario la evaluación de aspectos de seguridad en relación a la información contable que contendria el software y en general el Sistema

de Gestión. Por otro lado el proyecto al enfocarse unicamente en el sistema de información contable limita las posibilidades de poder expandir el alcance de las métricas, pero el mismo sera importante para poder orientar los elaboración de las métricas que se plantearan en el proyecto.

Por otro lado, en el proyecto titulado "Metricas para el proceso de implementación del modelo de Gobierno de Seguriad de la Información Basado en COBIT 5.0", para optar el grado de Ingeniero de Sistemas en la ciudad de Mahala Ecuador (Correa, 2016), plantea la medición del desempreño del gobierno de de segurida de la información, para lo mismo propone como referencia el marco de gobierno de COBIT 5.0, según indica el autor este marco es el más adecuado a tomarse en cuenta por medio de una tabla comparativa, se crean métricas basadas en los dominios indicados por el marco Cobit.

Este proyecto es util, ya que para un Sistema de Gestión de Seguridad de la Información según la ISO 27001 es necesaria la existencia de un gobierno de T.I. establecido el cual se maneje en el marco de políticas, procesos y procedimientos, según COBIT 5.0 el mismo define dominios como "Evaluar, Orientar y Supervisar" y un segundo dominio como "Alinear, Planificar y Organizar", estos dominios se pueden orientar dentro de la Norma ISO 27001 al PDCA (Planificar, Hacer, Evaluar, Actuar).

El autor también considera dentro de la bibliografía estudiada la Norma ISO 27004 la cual es la Guía para la auditoria de un Sistema de Gestión de Seguridad de la Informaición y en la cual se considera la medición del nivel de seguridad en base a 3 aspectos los cuales son: Estrategíco, Táctivo y Operativo, para mas detalle se muestra la figura líneas abajo:

Figura 1. Modelo Estratégico de Métricas de Seguridad de la Información (Correa, 2016)

Es así entonces que se desprende que el autor hace un gran efasis en orientar la solución propuesta tomando muy en consideración las normas ISO para la Seguridad de la Información y las cuales también son consideradas para la planteación del presente proyecto.

Continuando con el marco teorico dentro de la ISO 27002 tenemos la sección orientada a la Continuidad del Negocio, este aspecto es importante ya que dentro del mismo se definen todas las estrategias para garantizar la continuidad de las operaciones de la Organización ante cualquier indicendia que pueda presentarse, (Orozco Vinces, 2015), en su proyecto titutlado "Diseño de una métrica para evaluar el grado de cumplimiento del plan de continuidad de negocio en tecnologías de información en la empresa Altamar Foods Perú S.A.C.", para optar el grado de Ingeniero de Sistemas en la Ciudad de Piura- Perú, propone la elaboración de una métrica la cual brinde el nivel de cumplimiento del plan de Continuida del Negocio implementado por la empresa involucrada.

Así mismo la autora utiliza como referencia la Norma ISO 27004 la mismo que según cita *"permitira a la organización dar respuesta a las interrogantes de cúan efectivo y eficiente es el SGSI y que niveles de implementación y madurez han sido alcanzados, Estas mediciones permitiran comparar los logros obtenidos en seguridad de la información sobre periododos de tiempo en áreas de negocio similares a la organización y como parte de mejora continua"*(ISO27004, 2012).

El proyecto realizado por la autora es de utilidad ya que dentro de las métricas a proponer en el presente proyecto, para el apartado de "Continuidad del Negocio"

indicado en la ISO 27002, se puede analizar los cuadros propuestos por la autora para su evaluación y posible adecuación al nuestro caso de estudio, así también se considerará las mediciones realizadas para los activos de información tanto a nivel hardware y nivel humano considerados. por otro lado las desventajas evidenciadas en el proyecto de la autora es la orientación cerrada a una empresa, sin generalizar la métrica para su adecucación en otras organizaciones.

Como parte de la definición de las métricas para la evalución de activos de infomación es importante no dejar de lado el Sistema de Gestión de Seguridad de la Información el cual dentro de su ciclo de vida incluye la medición de activos de información, es por eso que (Baldecchi, 2014), en el Congreso CIGRAS (Congreso Internacional sobre Gobierno, Riesgos, Auditoria y Seguridad de la Información), por sus siglas, en la ponencia “Implementación efectiva de un SGSI ISO 27001”, nos brinda las pautas y pasos para lograr la una efectiva implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma Internacional ISO 27001, así como tambien brindar conceptos que puedan definir y hacer comprender como la información es un activo importante para una organización y la mismas necesita ser resguardada para poder garactizar su confidencialidad, integridad y disponibilidad.

Dentro de la presentación el autor indica que como punto de partida la implementación de un cierto número de controles puede servir, *“Un cierto número de controles puede ser considerado un buen punto de partida para implementar la seguridad de la información. Estos están basados en requisitos legales esenciales o que se consideren práctica habitual de la seguridad de la información.”*(Baldecchi, 2014), así mismo dentro de las etapas a considerar para la implementación se hace alución a Auditorías interna y Mejoras, es aquí en donde se ponen en funcionamiento las métricas para evaluar Activos de Información ya que dentro del proceso de revisión se validan si la criticidad de un activo es la correcta o en el tiempo el mismo ya no es tan crítico como en un principio, esto esta enlasado a la gestión de riesgos que se debe de realizar dentro del proceso de mantenimiento del SGSI.

Entonces se tiene claro que para implementar correctamente un Sistema de Gestión de Seguridad de la Información, es necesarió partir de una cantidad de controles, pero estos controles no solamente se orientan a activos fisicos o digitales, tambíen es importante considerar como un activo de información importante al colaborador de la organización.

Es por eso que (Cadavid-aguirre, 2013), en su articulo titulado “Seguridad en Activos de Información Humanos”, hace incapie en la importancia del ser humano como activo de información, considerando además que el factor humano es considerado el eslabon mas debil de la cadena en lo que a seguridad de la inforamción se refiere, ya que el mismo es propenso a caer en ataques de phishing, ingeniería social o simplemente a exponer la red interna de la organización al abrir correos infectados con malware.

Tomando en consideración esto es que el articulo brinda aspectos a tener en cuenta para evitar que ourran incidentes que esten directamente involucrados con el factor humano, como capacitaciones, charlas de sensibilización, la creación de cultura de seguridad, etc.

Ya teniendo mas en claro el alcance de todo lo relacionado a Seguridad de la Información, y lo relacionado a las métricas para activos de información, es importante no olvidar que la necesidad de evaluar activos de información nace en relación a la exposición de estos a los Riesgos que se encuentran presentes.

Es asi que el Instituto Nacional de Tecnologías de la Comunicación INTECO en su ponencia titulada “Modelo Unificado de Análisis de Riesgos de Seguridad Física y Lógica” (Bilbao, 2011), plantea una metodología la cual permite unificar dos metodologías de análisis de riesgos tradicionalmente independientes como sin las normas ISO 31000 e ISO 27001, simplificando de esta manera el analisis de riesgos logícos y riesgos físicos, la información brindada en la ponencia es de utilidad ya que con las misma se entienden las necesidades de evaluación de activos tanto a nivel físico como lógico, y así mismo plantea niveles CMMI para las necesidades de Salvaguardas o controles según la situación actual de la gestión de seguridad de la organización.

3. MARCO METODOLÓGICO

3.1 Alcances y Limitaciones

Alcance:

El presente trabajo, tiene como alcance brindar a la empresa métricas mediante las cuales se puede evaluar los activos de información de esta, basándose en las normas internacionales ISO 27001 e ISO 27002, de esta manera se estandarizan los procesos de la empresa y así mismo se garantiza a la empresa que las métricas están basadas en normas internacional mundialmente aprobadas y adoptadas para otras empresas, es así que la empresa una vez se identifiquen y valoricen sus activos podrá poner en marcha planes de acción para el resguardo de aquellos activos que por su nivel de criticidad necesiten salvaguardas que garanticen su confidencialidad, integridad y disponibilidad ya que de verse afectada alguna de estas características el impacto hacia la empresa podría ser grave.

Limitaciones:

No existe limitación para realizar la presente investigación, debido a que se cuenta con el conocimiento y asesoria necesaria para desarrollar las metricas de evealuavión para activos de información del área de Infraestructura de TI basados en las normas internacionales ISO/IEC 27001 e ISO/IEC 27002 para la empresa recaudadora - call center la cual es caso de estudió en el presente proyecto, Asimismo, se tiene acceso a una empresa donde se puede operativizar la tesis, poniendo en practica las metricas y tomar las lecturas que sean necesarias a efectos de obtener resultados que permitan determinar el grado de validacion de dichas metricas.

3.2 Aporte:

Las metricas propuestas para la evaluación de activos brindara a la organización los indicadores para llevar a cabo una correcta evaluación de los de los activos de información del área de Infraestructura de tecnologías de la información de la empresa, basando el desarrollo de dichas metricas en normas

internacionales mundialmente aceptadas y adoptadas por muchas empresas, lo que brindará mayor nivel de cumplimiento y certeza al momento de evaluar, así mismo se homologaran procesos alineados a estandares internacionales.

3.3 Tipo y Nivel de la Investigación

El tipo de investigación, es aplicativa ya que el modelo planteado en el presetne proyecto pretende utilizarse para apoyar en la gestión de riesgos en una empresa recaudarora – call center.

El nivel de la investigación, es relacional porque con el modelo para la evaluación de de activos de información basados en controles ISO27002:2013 para una empresa recaudadora – call center se puede mejorar la evaluación de riesgos tecnologícos ademas de mejorar la gestión de riesgos.

3.4 Población y Muestra o Universo

Para este caso el marco poblacional sujeto al estudio, tiene la característica de ser una empresa recaudadora – call center. Por consiguiente, la población o universo está representada por la cantidad de organizaciónes de este tipo que existen en la ciudad de Arequipa.

La muestra puede ser probabilista o no probabilística. A efectos de validar la propuesta, se empleara una muestra no probabilística de tipo dirigida, la misma que estará conformada por una empresa recaudadora – call center.

3.5 Métodos, Técnicas e Instrumentos de Recolección de Datos

Para la presente investigación se utilizará la técnica de la entrevista para poder establecer contacto con los interesados de la organización, así mismo se recabará toda la información necesaria en relación a los activos de información de la organización esto mediante reuniones programadas con los encargados de la organización. Por último, se utilizará la técnica del análisis documental para poder obtener información sobre los riesgos a los cuales se ven expuestos todos aquellos activos de información de la organización, así como de otras variables de interés para la presente investigación.

3.6 Plan de análisis estadístico de los datos

Para la presente investigación en lo que se refiere al análisis de datos, se utilizará un análisis cuantitativo descriptivo, para determinar el nivel de cumplimiento de las métricas para la evaluación de los activos de información del área de Infraestructura de tecnologías de la información.

4. PLAN DE TRABAJO

La presente tabla nos muestra las actividades, tiempo y responsables que están organizadas para la ejecución de este trabajo de investigación. Todas las actividades tendrán como responsable al Investigador de la presente Tesis.

Etapa	Actividad	Duración
1	1.1 Investigación del problema	8 días
	1.2 Aprobación del Plan de Tesis	3 días
	1.3 Estructuración preliminar	7 días
	1.4 Obtención de Información	4 días
2	2.1 Reunión con Representantes de la Organización	1 día
	2.2 Identificar y analizar los Activos de Información	4 días
	2.4 Documentar información obtenida	2 días
	2.5 Análisis de Riesgos asociados a los activos.	4 días
3	3.1 Planteamiento de las Métricas de evaluación de activos de información del área de Infraestructura.	6 días
	3.2 Análisis de cumplimiento basado en los controles ISO27002	5 días
	3.3 Ajuste de las métricas de evaluación de activos de información del área de Infraestructura.	8 días
4	4.1 Aplicación de métricas	19 días
5	5.1 Aplicación cuestionario	5 días

Etapa	Actividad	Duración
	5.2 Tabulación	**5 días**
	5.3 Análisis	**5 días**
6	**6.1 Estructuración de resultados**	**15 días**
	6.2 Redacción del Informe final	**7 días**
7	**7.1 Culminación del Informe Final**	**10 días**

5. REFERENCIAS BIBLIOGRÁFICAS

Baldecchi, R. (2014). Implementación efectiva de un SGSI ISO 27001. *2014*, 30. Retrieved from http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014 - Exposici%25C3%25B3n 2 CIGRAS ISO 27001 - rbq.pdf

Bilbao, E. / I. (2011). Modelo Unificado de Análisis de Riesgos de Seguridad Física y Lógica. *2011*, 30. Retrieved from http://www.cuevavaliente.com/sites/default/files/ponencia_inteco_2011.pdf

Cadavid-aguirre, J. M. (2013). Seguridad en activos de información humanos, 17–19.

Comite Tecnico de Normalizacion de Codificacion e Intercambio Electronico de Datos. (2007). NTP-ISO / IEC 17799 EDI . Tecnología de la información . Código de buenas. *El Peruano*, *2a. Edició*(Lima 41), 179. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=39612

Correa, G. (2016). *Métricas para el proceso de implementación del modelo de gobierno de seguridad de la información basado en COBIT 5.0*.

Iso27000.es. (n.d.-a). Iso 27000.

Iso27000.es. (n.d.-b). Sistema de Gestión de la Seguridad de la Información.

Iso27000.es. (2013). ControlesISO27002-2013, 27002. Retrieved from http://iso27000.es/download/ControlesISO27002-2013.pdf

ISO27004. (2012). PERUANA NTP-ISO / I NTP-I SO / IEC EC 27004 TECNOLOGÍA DE LA INFORMACIÓN . Técnicas de Medición.

Magerit. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Montoya Vega, C. M. (2013). La norma ISO27001: Aspectos claves de su diseño e implementación. *ISOTools*, 1–6.

NTP-ISO/IEC 27001:2014. (2014). NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. *Normas Técnicas Peruanas*, 45. Retrieved from

http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf

Orozco Vinces, Y. (Universidad C. V. (2015). Diseño de una métrica para evaluar el grado de cumplimiento del plan de continuidad de negocio en Tecnologías de la Información en la Empresa Altamar Foods Perú S.AC., 1–23.

Pentón, Á. E. S. "Jose A. E. A. (2016). *Métricas para evaluar la calidad de los Sistema de Gestión de Información Contable - Financiera*.

Portillo, P. B. del, & Benavides, L. O. (2012). Importancia de los sistemas integrados de gestión, *4*. Retrieved from http://repository.unimilitar.edu.co/bitstream/10654/6787/1/GarzonHernandezJaime2015.pdf

Romeral, L. M., & Torres Gallego, Á. (2008). Gestión De Los Riesgos Tecnológicos. *Procesos y Métricas*, *5*, 9. Retrieved from http://www.aemes.org/documentos/revistaprocesosmetricas/2008/numero13/RPM_v5_01.03.pdf

SBS. (2015). CIRCULAR N° G-180-2015, (30).

6. POSIBLE TEMARIO DEL INFORME FINAL

La presente investigación, se desarrollará teniendo en cuenta los siguientes puntos:

1. Cubierta
2. Cubierta Interna
3. Copia del Dictamen Aprobatorio del Borrador de Tesis
4. Presentación
5. Agradecimientos
6. Dedicatoria
7. Epígrafe
8. Índice o Tablas de Contenidos
9. Índice de Tablas
10. Índice de Figuras
11. Resumen y Abstract
12. Introducción
13. Planteamiento de la Investigación
14. Fundamentos Teóricos
15. Marco Metodológico
16. Resultados
17. Discusión
18. Conclusiones
19. Trabajos Futuros
20. Referencias Bibliográficas
21. Apéndice(s)

Anexo B – Plantilla para Identificación de Activos

MÉTRICAS PARA ACTIVOS DE INFRAESTRUCTURA ISO 27001 - ISO 27002								
N°	ACTIVO DE INFORMACIÓN	DESCRIPCIÓN	TASACIÓN DE ACTIVOS POR PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN					CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA
			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PROMEDIO TASACIÓN	NIVEL DE TASACIÓN		

N° → Campo para enumerar registros.

Activo de Información → Identifica al activo del área.

Descripción → Se describe brevemente el activo.

Confidencialidad → Campo para calificar por Confidencialidad el activo.

Integridad → Campo para calificar por Integridad el activo.

Disponibilidad → Campo para calificar por Disponibilidad el activo.

Promedio Tasación → Campo indica la tasación promedio según criterios previos.

Nivel Tasación → Campo indica según promedio nivel de Tasación de cada Activo (ALTO-MEDIO-BAJO).

Controles ISO27002 Asociados → Se indica los controles en base a la norma ISO27002 según activo.

Métrica Asociada → Se inidica la métrica asociada.

Anexo C – Plantilla para la determinación de Umbrales

ACTIVO DE INFORMACIÓN	CONTROLES ISO 27002 ASOCIADOS	MÉTRICA ASOCIADA	UNIDAD DE MEDIDA	UMBRAL PERMITIDO	MAXIMO PERMITIDO	MINIMO NO PERMITIDO

Activo de Información → Identifica al activo del área.

Controles ISO27002 Asociados → Se indica los controles en base a la norma ISO27002 según activo.

Métrica Asociada → Indica la métrica asociada.

Unidad de Medida → Indica como se medira la métrica (Tiempo Inactividad – Nro. Incidentes).

Maximo Permitido → Determina el valor maximo tolerable para la métrica.

Minimo no Permitido → Determina el valor minimo antes de que el incidente sea crítico.

Anexo D – Plantilla para Registro Diario de Incidentes

REGISTRO DE INCIDENTES INFRAESTRUCTURA						
Nro.	Fecha	ACTIVO INVOLUCRADO	MÉTRICA RELACIONADA	DESCRIPCIÓN BREVE DEL INCIDENTE	UNIDAD DE MEDIDA	NRO. DE INCIDENTES O TIEMPO QUE DURO INCIDENTE

Nro. → Campo para enumerar registros.

Fecha. → Fecha en la que se registra el incidente.

Activo Involucrado → Identifica el activo incolucrado del área.

Métrica Relacionada → Hace referencia a la métrica que compete para el incidente.

Descripción breve del incidente → Campo para detallar el incidente.

Unidad de Medida → Campo indica como se medirá el incidente (Tiempo Inactividad)

Nro. De Incidentes o Tiempo que duro incidente. → Se debe colocar en números el tiempo de paralización del activo o cantidad de incidentes presentados.